EURÓPAI
BIZOTTSÁG

AZ UNIÓ KÜLÜGYI ÉS
BIZTONSÁGPOLITIKAI
FŐKÉPVISELŐJE

Brüsszel, 2017.9.13.
JOIN(2017) 450 final

KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése

1. BEVEZETÉS

A kiberbiztonság jólétünk és biztonságunk szempontjából egyaránt kiemelten fontos. Mivel mindennapi életünk és gazdaságunk egyre inkább függ a digitális technológiáktól, egyre nagyobb veszélyeknek vagyunk kitéve. A kiberbiztonsági események sokfélesége az elkövetők, illetve az általuk elérni kívánt célok szempontjából egyaránt fokozódik. A rossz szándékú kibertevékenységek nem csupán gazdaságunkat, valamint a digitális egységes piac lendületét fenyegetik, hanem demokráciánk működését, szabadságjogainkat és értékeinket is. Biztonságunk jövője azon múlik, hogy kapacitásainkat hogyan tudjuk úgy kiigazítani, hogy megvédjük az Uniót a kiberfenyegetésekkel szemben: a civil infrastruktúra és a katonai kapacitás egyaránt digitális biztonsági rendszerekre támaszkodik. Ezt az Európai Tanács 2017. júniusi ülése[1], valamint az Európai Unió globális kül- és biztonságpolitikai stratégiája[2] is elismerte.

A kockázatok exponenciálisan növekednek. Egyes tanulmányok szerint a kiberbűnözés gazdasági hatása 2013 és 2017 között ötszörösére nőtt, 2019-ig pedig ez az érték újból megnégyszereződhet[3]. A zsarolóvírus-támadások[4] terén különösen nagy növekedés tapasztalható, és a közelmúltbeli támadások[5] a kiberbűnözői tevékenység drasztikus emelkedését jelzik. A zsarolóvírus mellett azonban más fenyegetések is léteznek.

A kiberfenyegetés nem állami és állami szereplőktől egyaránt érkezhet: gyakran bűnözőkről van szó, akiket a nyereség motivál, de a támadások politikai és stratégiai indíttatásúak is lehetnek. A bűnözés általi fenyegetést fokozza a kiberbűnözés és a „hagyományos” bűnözés közötti határvonal elmosódása, hiszen a bűnözők az internetet tevékenységük kiterjesztésére, illetve arra is használják, hogy új módszereket és eszközöket találjanak a bűncselekmények elkövetéséhez[6]. Az esetek túlnyomó többségében azonban a bűnözők nyomon követésének esélye minimális, a vádemelés esélyei pedig még ennél is kisebbek.

Ugyanakkor az állami szereplők egyre gyakrabban nem a hagyományos eszközökkel, például katonai erővel szereznek érvényt geopolitikai céljaiknak, hanem diszkrétebb kibereszközökkel, például a belső demokratikus folyamatokba történő beavatkozással. A kibertér hadszíntérként történő használata – akár önállóan, akár hibrid megközelítés részeként – ma már széles körben ismert. A dezinformációs kampányok, álhírek és kritikus infrastruktúrák elleni kiberműveletek egyre inkább terjednek, és válaszreakciót igényelnek. Ezért az európai védelem jövőjéről szóló vitaanyagban[7] a Bizottság hangsúlyozta a kibervédelmi együttműködés fontosságát.

Ha nem sikerül jelentős mértékben javítanunk a kiberbiztonságon, a kockázat a digitális átalakulással párhuzamosan egyre nagyobb lesz. 2020-ra a dolgok internetét alkotó több tízmilliárd eszköz fog csatlakozni az internethez, de tervezésük során a kiberbiztonságot

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Lásd például a McAfee & Centre for Strategic and International Studies 2014-es tanulmányát, amelynek címek „Net losses: Estimating the Global Cost of Cybercrime” (Nettó veszteség: a kiberbűnözés globális költségének becslése).

4 A zsarolóvírus olyan rossz szándékú számítógépes program, amely megakadályozza vagy korlátozza a felhasználó saját rendszeréhez való hozzáférését úgy, hogy bizonyos váltságdíj megfizetéséig zárolja a rendszer képernyőjét vagy a felhasználó fájljait.

5 2017 májusában a WannaCry nevű zsarolóvírus-támadás több mint 150 országban 400 000-nél is több számítógépet érintett. Egy hónappal később a „Petya” söpört végig Ukrajnán és világszerte több cégen.

6 EUROPOL, A súlyos és szervezett bűnözésre vonatkozó fenyegetésértékelés, 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf.

egyelőre nem kezelik prioritásként[8]. Ha nem sikerül megvédeni azokat az eszközöket, amelyek a villamosenergia-hálózatainkat, autóinkat és közlekedési hálózatainkat, a gyárainkat, pénzügyeinket, kórházainkat és otthonainkat fogják irányítani, az pusztító következményekkel járhat, és óriási károkat okozhat az új technológiákba vetett fogyasztói bizalom terén. A polgári célpontok ellen elkövetett, politikailag motivált támadások és a katonai kibervédelem hiányosságai jelentette kockázatok tovább súlyosbítják a veszélyt.

Az ebben a közös közleményben felvázolt megközelítés segíteni fogja az EU-t abban, hogy felkészültebb legyen az ilyen fenyegetettségekkel szemben. A megközelítés nagyobb ellenállóképesség és stratégiai függetlenség kialakítását teszi lehetővé, fokozza a technológia és az ismeretek terén mutatkozó kapacitásokat, és hozzásegít az erős egységes piac kiépítéséhez. Ehhez pedig arra van szükség, hogy megfelelő struktúrák álljanak rendelkezésre az erős kiberbiztonság kiépítéséhez, valamint arra, hogy szükség esetén az összes fontosabb szereplő teljes körű bevonásával reagálni lehessen. A megközelítés a felelősök felkutatásával, nyomon követésével és felelősségre vonásával kapcsolatos munka fokozása révén jobban el tudná hárítani a kibertámadásokat. Az Unió kiberbiztonsággal kapcsolatos vezető szerepének platformjaként fejlesztené a nemzetközi együttműködést, ezáltal a jelenség globális dimenzióját is elismerné. Ezek a lépések a digitális egységes piac, a globális stratégia, az európai biztonsági stratégia[9], a hibrid fenyegetésekkel szembeni fellépés közös kerete[10], valamint az Európai Védelmi Alap felállításáról szóló közlemény[11] [12] által megfogalmazott megközelítésekre alapoznak.

Az Unió az említett témák közül már többel is foglalkozik: elérkezett az idő, hogy a különböző munkafolyamatokat összefogjuk. 2013-ban az EU kidolgozott egy kiberbiztonsági stratégiát, amelynek része volt több, a kibertámadásokkal szembeni ellenálló képesség javítását célzó fontosabb munkafolyamat is[13]. A stratégia fő céljai és elvei – azaz a megbízható, biztonságos és nyitott kiber-ökoszisztéma elősegítése – továbbra is érvényesek. De a folyamatosan változó és súlyosbodó fenyegetettségi helyzet nagyobb aktivitást kíván ahhoz, hogy a jövőben ellen lehessen állni a támadásoknak, és el lehessen hárítani azokat[14].

Az Unió szakpolitikái hatályának és a rendelkezésére álló eszközöknek, struktúráknak és kapacitásoknak köszönhetően kellően felkészült arra, hogy a kiberbiztonsági kérdésekre megoldást találjon. Míg továbbra is a tagállamok felelősek saját nemzetbiztonságukért, a fenyegetettség mértéke és határokon átnyúló jellege miatt egyértelmű szükség van az uniós fellépésre, ugyanakkor ösztönzést és támogatást kell nyújtani a tagállamoknak, hogy több és jobb nemzeti kiberbiztonsági kapacitást fejlesszenek és tartsanak fenn, az uniós szintű kapacitások egyidejű építése mellett. Ez a megközelítés az összes szereplő – az EU, a tagállamok, az ágazat képviselői és az egyes személyek – összefogását szolgálja, hogy ezáltal biztosítsa a kiberbiztonság számára az ahhoz szükséges elsőbbséget, hogy ellenálló

---

8 IDC és TXT Solutions (2014), SMART 2013/0037, számítási felhő és a dolgok internetének kombinációja, a Bizottság számára készített tanulmány.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 A megközelítést az Európai Bizottságon belül működő tudományos tanácsadási mechanizmus – tudományos tanácsadók magas szintű csoportja által nyújtott független tudományos tanácsadás is alátámasztotta (lásd az alábbi hivatkozásokat).

13 JOIN(2013) 1 final. Az említett stratégia értékelését az SWD (2017) 295 tartalmazza.

14 Eltérő utalás hiányában az ebben a közleményben megfogalmazott javaslatok költségvetési szempontból semlegesek. A költségvetési vonzattal járó kezdeményezések szabályszerűen az éves költségvetési eljárást fogják követni, és nem érinthetik a következő, 2020 utáni többéves pénzügyi keretet.

képességet építsen és megfelelőbb uniós válaszlépéseket adjon a kibertámadásokra. A megközelítés konkrét lépéseket fogalmaz annak elősegítéséhez, hogy az EU és tagállamai elleni kiberincidensek bármely formáját feltárják és kivizsgálják, valamint hogy megfelelő válaszreakció szülessen, amely a bűnözők büntető eljárás alá vonását is magában foglalja. Ez pedig lehetővé teszi az EU külső tevékenysége számára, hogy a globális színtéren is hathatósan támogassa a kiberbiztonságot. Ennek eredményeként az EU a reaktív megközelítésről áttérhet a proaktív megközelítésre, hogy megóvja az európai jólétet, társadalmat és értékeket, alapvető jogokat és szabadságjogokat, az aktuális és a jövőbeli fenyegetettségekre egyaránt reagálva.

2.AZ UNIÓ KIBERTÁMADÁSOKKAL SZEMBENI ELLENÁLLÓ KÉPESSÉGÉNEK KIÉPÍTÉSE

A kibertámadásokkal szembeni ellenálló képesség erősítése közös és mindenre kiterjedő megközelítést tesz szükségessé. Mindez szilárdabb és eredményesebb struktúrákat igényel, amelyek elősegítik a kiberbiztonságot és reagálnak a tagállamokban, illetve az EU saját intézményeiben, ügynökségeiben és szervezeteiben elkövetett kibertámadásokra. Átfogóbb, szakpolitikákon átívelő megközelítésre van szükség a kibertámadásokkal szembeni ellenálló képesség és stratégiai függetlenség kiépítéséhez, erős egységes piaccal, az uniós technológiai kapacitás terén nagyobb fejlesztésekkel és sokkal több képzett szakemberrel. Ennek középpontjában annak szélesebb körű felismerése áll, hogy a kiberbiztonság közös társadalmi kihívásunk, ezért a kormány, a gazdaság és a társadalom több rétegét is be kell vonni a folyamatba.

2.1.Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség erősítése

Az **Európai Uniós Hálózat- és Információbiztonsági Ügynökség** (ENISA) kiemelt szerepet tölt be az EU kibertámadásokkal szembeni ellenálló képességének és válaszreakciójának erősítése terén, de jelenlegi megbízatása korlátozza ebben. A Bizottság ezért egy ambiciózus reformprogramot terjeszt elő, amely **állandó megbízatást ad az ügynökségnek**[15]. Ez biztosítja, hogy az ENISA képes legyen támogatni a tagállamokat, uniós intézményeket és vállalkozásokat olyan kiemelt területeken, mint például a hálózati és információs rendszerek biztonságáról szóló irányelv[16] (a kiberbiztonsági irányelv) és a javasolt kiberbiztonsági tanúsítási keretrendszer.

A megreformált ENISA markáns tanácsadói szereppel bír majd a szakpolitikák kidolgozása és végrehajtása terén, beleértve az ágazati kezdeményezések és kiberbiztonsági irányelv közötti koherencia biztosítását, valamint a kritikus fontosságú ágazatokban az információmegosztó és -elemző központok létrehozásának elősegítését. Az ENISA magasabbra teszi a mércét, és fokozza az európai felkészültséget azáltal, hogy éves összeurópai kiberbiztonsági gyakorlatokat szervez, amelyekben ötvözi a különböző szintek válaszreakcióit. Támogatja továbbá az információs és kommunikációs technológiák (IKT) kiberbiztonsági tanúsítványával kapcsolatos uniós szakpolitikák kidolgozását, és fontos szerepet játszik az uniós szintű operatív együttműködés és válságkezelés erősítésében. Az ügynökség továbbá a kiberbiztonsági közösség információ- és tudáscserét szolgáló kapcsolattartó pontjaként fog működni.

---

[15] COM(2017) 477.

[16] 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.

A kibontakozó fenyegetések és incidensek gyors és közös értelmezése előfeltételként szolgál annak eldöntéséhez, hogy szükség van-e az EU által támogatott közös kockázatcsökkentő intézkedésekre vagy válaszreakcióra. Az említett információcseréhez az összes érintett szereplő – uniós szervek és ügynökségek, valamint tagállamok – technikai, operatív és stratégiai szintű bevonása szükséges. Az ENISA a tagállami és uniós érintett szervezetekkel, különösen a számítógép-biztonsági eseményekre reagáló csoportok hálózatával[17], a CERT-EU-val, az Europollal, valamint az Európai Unió Helyzetelemző Központjával (INTCEN) együttműködve az uniós szintű helyzetismerethez is hozzájárul. Mindez pedig a fenyegetettségi helyzet rendszeres nyomon követésének és a hatékony operatív együttműködésnek az összefüggésében becsatornázható a fenyegetettségi elemzésbe és politikai döntéshozatalba, valamint a nagyszabású, határokon átnyúló incidensekre adott válaszreakciókba.

2.2.Az egységes kiberbiztonsági piac felé

A kiberbiztonsági piac növekedését az EU-ban – a termékek, szolgáltatások és eljárások tekintetében – számos tényező visszafogja. Ezek közül a legfontosabb az egész Unióban elismert kiberbiztonsági tanúsítási rendszerek hiánya, amely lehetővé tenné a termékekbe magasabb fokú ellenálló képesség beépítését, és az uniós szintű piaci bizalom megalapozását. A Bizottság ezért egy **uniós kiberbiztonsági tanúsítási keretrendszer** létrehozására irányuló javaslatot terjeszt be[18]. A keretrendszer állapítaná meg az uniós szintű kiberbiztonsági tanúsítási rendszerek létrehozásának eljárását, amely olyan termékekre, szolgáltatásokra és/vagy rendszerekre vonatkozik, amelyek a megbízhatósági szintet az érintett felhasználási módhoz igazítják (legyen szó kritikus infrastruktúráról vagy fogyasztási cikkekről)[19]. Ez egyértelmű előnyöket jelent a vállalkozásoknak, mivel nem kell majd a határokon átnyúló kereskedés esetén több tanúsítási eljárást is lefolytatniuk, így csökkennek az adminisztratív és pénzügyi terheik. A szóban forgó keretrendszerben létrehozott programok használata segít továbbá a fogyasztói bizalom kiépítésében azzal, hogy a megfelelési tanúsítvány tájékoztatja és biztosítja a vásárlókat és felhasználókat az általuk megvett és használt termékek és szolgáltatások biztonsági jellemzőiről. Ennek köszönhetően a szigorú kiberbiztonsági előírások versenyelőnyt is biztosíthatnak. Ennek eredményeként megnövekedne az ellenálló képesség, mivel az IKT termékeket és szolgáltatásokat előre meghatározott kiberbiztonsági szabványok alapján hivatalosan is ellenőriznék, amelyeket az IKT-szabványokkal kapcsolatban jelenleg is folyó munkával szoros összefüggésben lehetne kidolgozni[20].

Az említett keretrendszer programjai önkéntes jellegűek, és az eladókra vagy szolgáltatókra nézve nem járnak azonnali szabályozói kötelezettségekkel. Ezek a programok nem ütköznek az alkalmazandó jogi követelményekbe, például az adatvédelemről szóló uniós jogszabályokba.

Amint a keretrendszer létrejön, a Bizottság felkéri az érdekelt feleket, hogy három kiemelt területre összpontosítsanak:

[17] A kiberbiztonsági irányelv 9. cikkének rendelkezései szerint.

[18] COM(2017) 477.

[19] A megbízhatósági szint jelzi a biztonsági ellenőrzés szigorúságának fokát, és általában megfelel az adott alkalmazási területhez vagy funkcióhoz társítható kockázati szintnek (azaz a nagy kockázatú alkalmazási területeken vagy funkciókban használt IKT termékek és szolgáltatások esetében magasabb megbízhatósági szint szükséges).

[20] COM(2016) 176.

- Biztonság a kritikus vagy magas kockázatú alkalmazások területén[21]: egyre nagyobb mértékben digitalizálódnak és összekapcsolódnak az olyan rendszerek, amelyektől mindennapi tevékenységeink során függünk, a gépkocsiktól a gyárakban található gépekig, a legnagyobb rendszerektől, mint például a repülőgépek vagy erőművek, egészen a legkisebb rendszerekig, amilyenek például az orvostechnikai eszközök. Ezért az ilyen termékekben és rendszerekben található legfontosabb IKT-elemeknél szigorú biztonsági értékelésre van szükség.

- A magán- és az állami szektor által a támadások elleni védelem, valamint a jogszabályi kötelezettségek alkalmazása céljából a széles körben használt digitális termékek, hálózatok, rendszerek és szolgáltatások esetében használt kiberbiztonság[22], például email-titkosítás, tűzfalak és virtuális magánhálózatok; kiemelten fontos, hogy az ilyen eszközök egyre terjedő használata ne vezessen új veszélyforrásokhoz vagy új támadási felületekhez.

- A „beépített biztonság” módszereinek használata a dolgok internetét alkotó olcsó, digitális, összekapcsolt tömegfogyasztási cikkek esetében: a keretrendszerben kialakított programokat lehetne felhasználni annak jelzésére, hogy a termékeket a legmodernebb biztonsági fejlesztési módszerek alapján alakították ki, megfelelő biztonsági ellenőrzésen estek át, és hogy az eladók vállalták, hogy az újonnan felfedezett gyengeségek vagy fenyegetések esetén frissítik szoftverüket.

Ezeknek a prioritásoknak kiemelten figyelembe kell venniük a változó kiberbiztonsági fenyegetettségi helyzetet, valamint a létfontosságú szolgáltatások – mint például a közlekedés, energia, egészségügyi ellátás, banki tevékenység, pénzügyi piaci infrastruktúrák, ivóvízellátás vagy digitális infrastruktúra – jelentőségét[23].

Noha semmilyen IKT-termék, rendszer vagy szolgáltatás esetében nem garantálható a „100 %-os” biztonságosság, több jól ismert és jól dokumentált hiba létezik az IKT-termékek kialakításában, amelyek támadásra felhasználhatóak. Az összekapcsolt eszközök, informatikai szoftverek és berendezések gyártói által alkalmazott „beépített biztonság” megközelítés biztosítaná, hogy a kiberbiztonsággal már az új termékek piaci bevezetése előtt foglalkozzanak. Ez része lehetne a „gondossági kötelezettség” elvnek, amelyet az iparággal együtt kell továbbfejleszteni, és csökkenti tudná a termékek/szoftverek sebezhetőségét a tervezéstől a tesztelésen át az ellenőrzésig terjedő módszerek skálájának alkalmazásával, beleértve adott esetben a hivatalos ellenőrzést, a hosszú távú karbantartást és a biztonságos fejlesztési életciklus-folyamatok alkalmazását, valamint a frissítések és hibajavítások kidolgozását a korábban fel nem tárt sebezhetőségek kezelése, valamint a gyors frissítés és javítás érdekében[24]. Ez egyben növelné a fogyasztók digitális termékek iránti bizalmát is.

Ezen túlmenően el kell ismerni a harmadik fél biztonsági kutatók fontos szerepét a meglevő termékekben és szolgáltatásokban fellelhető sebezhetőségek feltárásában, és valamennyi

[21] Kivételt képez ez alól, ha a kötelező vagy önkéntes tanúsítást egyéb uniós jogi aktusok szabályozzák.

[22] Például az (EU) 2016/1148 irányelv, az (EU) 2016/679 rendelet, az (EU) 2015/2366 irányelv és egyéb jogszabály-javaslatok – mint az Európai Elektronikus Hírközlési Kódex – előírják, hogy a szervezeteknek a releváns kiberbiztonsági kockázatok kezelése érdekében megfelelő biztonsági intézkedéseket kell bevezetniük.

[23] A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelv hatálya alá tartozó ágazatok.

[24] Kiberbiztonság az egységes európai digitális piacon. Tudományos tanácsadók magas szintű munkacsoportja, 2017. március

tagállamban ki kell alakítani az összehangolt sebezhetőség-feltárást lehetővé tevő feltételeket[25], a bevált gyakorlatokra[26] és a vonatkozó szabványokra építve[27].

Ugyanakkor **egyes ágazatok** egyedi problémákkal szembesülnek, és ezeknél szorgalmazni kell saját megközelítésük kidolgozását. Ilyen módon az általános kiberbiztonsági stratégiákat ágazat-specifikus kiberbiztonsági stratégiák egészítenék ki olyan területeken, mint a pénzügyi szolgáltatások[28], az energetika, a szállítás és az egészségügy[29].

A Bizottság már rámutatott azokra a problémákra, amelyeket az új digitális technológiák a **felelősséggel** kapcsolatban vetnek fel[30], és jelenleg is folyik a munka a hatások elemzése tárgyában; a következő lépések 2018 júniusáig fognak befejeződni. A kiberbiztonság problémákat vet fel a kár vállalkozásoknak vagy ellátási láncoknak tulajdonítása terén, és ha ezek a kérdések rendezetlenül maradnak, az hátráltatni fogja a kiberbiztonsági termékek és szolgáltatások erős egységes piacának kialakulását.

Végül az egységes uniós piac kialakulása attól is függ, hogy miként épül be a kiberbiztonság a kereskedelmi és beruházási szakpolitikába. A kritikus technológiákkal (például a kiberbiztonsággal) kapcsolatos külföldi felvásárlások kulcsfontosságú szempontot alkotnak az **Európai Unióban végrehajtott közvetlen külföldi befektetések szűrésének**[31] keretében, amelynek célja a harmadik országokból érkező befektetések biztonsági és közrendi alapú szűrésének lehetővé tétele. Ugyanezen okból a kiberbiztonsági előírások máris kereskedelmi korlátokat képeznek az uniós termékek és szolgáltatások számára számos harmadik ország gazdaságának fontos ágazataiban. Az uniós kiberbiztonsági tanúsítási keret tovább fogja erősíteni Európa nemzetközi helyzetét, de további erőfeszítésekkel kell kiegészíteni nagybiztonságú globális szabványok és kölcsönös elismerési megállapodások kidolgozása érdekében.

2.3.A hálózati és információs rendszerek biztonságáról szóló irányelv teljes körű végrehajtása

Mivel a kiberbiztonság elleni küzdelem legfontosabb eszközei jelenleg nemzeti hatáskörben vannak, az EU felismerte, hogy szükség van a szabványok magasabb szintre emelésére. A nagy kiterjedésű kiberbiztonsági incidensek ritkán érintenek csak egyetlen tagállamot, az olyan alapvető ágazatok egyre globalizáltabb, digitálisan függő és egymással összekapcsolt jellege miatt, mint a bankrendszer, az energetika vagy a szállítás.

A hálózati és információs rendszerek biztonságáról szóló irányelv (kiberbiztonsági irányelv) az első, az egész EU-ra kiterjedő kiberbiztonsági jogszabály[32] Célja az ellenálló képesség

---

[25] Az összehangolt sebezhetőség-feltárás az együttműködés olyan formája, amely megkönnyíti és lehetővé teszi a biztonsági kutatók számára a sebezhetőségek informatikai rendszer tulajdonosának vagy eladójának történő bejelentését, lehetőséget adva a szervezetnek arra, hogy megfelelően és időben diagnosztizálja és korrigálja a sebezhetőséget, mielőtt a részletes sebezhetőségi információkat harmadik felek vagy a nyilvánosság elé tárnák.

[26] Például: Sebezhetőség-feltárási bevált gyakorlatok útmutatója. A kihívásoktól a javaslatokig. ENISA, 2016.

[27] ISO/IEC 29147:2014 Informatika -- Biztonságtechnika -- Sebezhetőség-feltárás.

[28] A Bizottság pénzügyi technológiára vonatkozó, közelgő munkája ki fog terjedni a pénzügyi ágazat kiberbiztonságára is.

[29] Például az energetikai ágazatban a régi és a legmodernebb információtechnológia egyesítése, különösen a villamosenergia-hálózat valós idejű követelményeivel.

[30] COM(2017) 228.

[31] COM(2017) 478.

[32] 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.

kialakítása a nemzeti kiberbiztonsági kapacitások javításával; a tagállamok közötti jobb együttműködés előmozdítása; és az, hogy kötelezettségvállalásokat írjon elő a fontos gazdasági ágazatokban a hatékony kockázatkezelési gyakorlatok alkalmazása érdekében és azért, hogy a súlyos incidenseket bejelentsék a nemzeti hatóságoknak. Ezek a kötelezettségek az alapvető internetszolgáltatásokat nyújtók három típusára is vonatkoznak: felhőalapú számítástechnika, keresőmotorok és online piacterek. Célja az erőteljesebb és módszeresebb megközelítés és az információáramlás javítása.

A kibertámadásokkal szembeni uniós ellenálló képességhez elengedhetetlen, hogy az irányelvet valamennyi tagállam 2018 májusáig teljes körűen végrehajtsa. A folyamatot a tagállamok kollektív munkája támogatja, ami 2017 őszére iránymutatást fog eredményezni az összehangoltabb végrehajtás támogatására, különösen az alapvető szolgáltatások üzemeltetői tekintetében. A Bizottság közleményt fog kiadni[33] az említett kiberbiztonsági csomag részeként, hogy azzal támogassa a tagállamok erőfeszítéseit, az irányelv végrehajtására vonatkozó bevált gyakorlatokat a tagállamoknak átadva és útmutatással szolgálva arról, hogy az irányelvnek miként kellene a gyakorlatban működnie.

Az információáramlás az egyik olyan terület, ahol az irányelvet kiegészítésre fog szorulni. Például az irányelv csak a kulcsfontosságú stratégiai ágazatokra terjed ki – de logikus, hogy a kibertámadások által sújtott minden érdekelt fél részéről hasonló megközelítésre lenne szükség a sebezhetőségek és a kibertámadók bejutási pontjainak módszeres értékeléséhez. Emellett a közszféra és a magánszféra közötti együttműködés is számtalan akadályba ütközik. A kormányok és a hatóságok vonakodnak megosztani a kiberbiztonsággal összefüggő információkat, mert tartanak a nemzetbiztonság vagy a versenyképesség veszélyeztetésétől. A magánvállalkozások pedig vonakodnak megosztani a kibersebezhetőségeikre és az abból eredő veszteségeikre vonatkozó információkat, mert tartanak a kényes üzleti információk sérülésétől, amivel kockáztatják a hírnevüket vagy az adatvédelmi szabályok megszegését[34]. Erősíteni kell a bizalmat a közszféra és magánszféra közötti partnerségek iránt, hogy meg lehessen alapozni a több ágazat közötti szélesebb körű együttműködést és információcserét. Az információcsere és -elemző központok szerepe különösen fontos abban, hogy kiépítsék a szükséges bizalmat a közszféra és a magánszféra közötti információcsere iránt. Történtek bizonyos első lépések egyes kritikus ágazatok tekintetében, mint például a repülés terén az Európai Repülési Kiberbiztonsági Központ,[35] illetve az energetikában az információcserei és -elemző központok létrehozásával.[36] A Bizottság teljes mértékben hozzájárul ehhez a megközelítéshez az ENISA által nyújtott támogatás révén, jóllehet fel kell gyorsítani a folyamatot, különösen a kiberbiztonsági irányelvben azonosított alapvető szolgáltatásokat végző ágazatok tekintetében.

2.4.Ellenálló képesség gyors vészhelyzeti reagálás útján

[33] COM(2017) 476.

[34] Kiberbiztonság az egységes európai digitális piacon. Tudományos tanácsadók magas szintű munkacsoportja, 2017. március. Konkrét problémát jelentenek az üzleti titkok, mivel a 2016. júliusi „Európa kibertámadásokkal szembeni ellenálló képességének erősítése” című közlemény említést tett az üzleti titkok számítógépes rendszereken keresztül való ellopásának bejelentésétől való vonakodásról, továbbá a titoktartást biztosító megbízható bejelentési csatornákról.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Ezek olyan non-profit, a tagok által irányított szervezetek, amelyeket magánjogi és közjogi szereplők hoztak létre a kiberfenyegetésekkel, -kockázatokkal, azok megelőzésével, enyhítésével és az azokra való reagálással összefüggő információk megosztására. Lásd: európai energetikai információcsere és -elemző központok (http://www.ee-isac.eu).

Kibertámadás esetén a gyors és hatékony reagálás enyhítheti a hatásokat. Egyben azt is képes igazolni, hogy a hatóságok nem tehetetlenek a kibertámadásokkal szemben, és hozzájárulhat a bizalomépítéshez is. Az uniós intézmények saját válaszát illetően a kiberszempontokat először is be kell illeszteni a meglevő uniós válságkezelési mechanizmusokba: a Tanács elnöksége által összehangolt[37], integrált uniós politikai válságreagálás, és az EU általános riasztási rendszerei[38]. Egy különösen súlyos kiberincidensre vagy támadásra adandó válasznak elegendő alapul kell szolgálnia ahhoz, hogy egy tagállam az EU szolidaritási klauzulájára hivatkozzon[39].

A gyors és hatékony reagálás függ még az összes kulcsfontosságú nemzeti és uniós szintű szereplő közötti zökkenőmentes információcserétől is, amely viszont megköveteli mindezek szerepkörének és felelősségének pontosítását. A Bizottság egy „Tervezetről" egyeztetett intézményekkel és a tagállamokkal azzal a céllal, hogy hathatós folyamatot biztosítson a nagyszabású kiberincidensekre uniós és tagállami szinten adandó operatív reagáláshoz. A csomag részét képező ajánlásban bemutatott **Tervezet**[40] ismerteti, hogy a kiberbiztonságot miként illesztik be a meglévő uniós szintű válságkezelési mechanizmusokba, és meghatározza a tagállamok egymás közötti, valamint a tagállamok és az illetékes uniós intézmények, szervezeti egységek, ügynökségek és testületek[41] együttműködésének céljait és módszereit a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való reagálás terén. Az ajánlás felkéri a tagállamokat és az uniós intézményeket arra is, hogy hozzanak létre egy uniós kiberbiztonsági válságreagálási keretet a Tervezet működőképességének megteremtéséhez. A Tervezetet rendszeresen tesztelni fogják kiber- és egyéb válságkezelési gyakorlatokkal,[42] és szükség szerint frissítésre kerül.

Mivel a kiberbiztonsági incidensek jelentős hatással lehetnek a gazdaság működésére és az emberek mindennapi életére, az egyik lehetőség az lenne, hogy megvizsgálják egy **Kiberbiztonsági Vészhelyzet-elhárítási Alap** létrehozását, a más uniós szakpolitikai területeken meglevő ilyen válságmechanizmusok példája nyomán. Ez lehetővé tenné a tagállamok számára, hogy uniós szinten kérjenek segítséget egy jelentős incidens alatt vagy után, feltéve, hogy az adott tagállam prudens kiberbiztonsági rendszert alakított ki az incidenst megelőzően, ideértve a kiberbiztonsági irányelv teljes körű végrehajtását és a nemzeti szintű, fejlett kockázatkezelési és felügyeleti kereteket. Az uniós szintű válságkezelési mechanizmusokat kiegészítő említett Alap gyors reagálásra lenne képes a szolidaritás érdekében, és olyan konkrét vészhelyzeti válaszlépéseket tudna finanszírozni, mint például a sérült berendezések cseréje vagy mérséklő, illetve válaszeszközök bevetése, az uniós polgári védelmi mechanizmusokban szerzett nemzeti tapasztalatokra építve.

2.5. Kiberbiztonsági kompetenciahálózat és az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont

A kiberbiztonság technológiai eszközei stratégiai eszközök, emellett a jövő alapvető növekedési technológiáit is jelentik. Az EU stratégiai érdeke annak biztosítása, hogy az EU

---

37 Ez a legmagasabb politikai szinten teszi lehetővé a jelentős, ágazatokon átívelő válságokra való reagálás összehangolását.

38 Lehetővé teszik a belső információcserét és összehangolást a kialakuló, több ágazatot érintő válságok vagy az uniós szintű fellépést igénylő, előre látható vagy közvetlen fenyegetések esetén.

39 Az Európai Unió működéséről szóló szerződés 222. cikke alapján.

40 C(2017) 6100.

41 Beleértve a következőket: Europol, ENISA, az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) és az EU Helyzetelemző Központja (INTCEN).

42 Többek között az ENISA által végrehajtottak: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

megőrizze és fejlessze a szükséges kapacitásokat a digitális gazdasága, társadalma és demokráciája biztonsága érdekében, hogy óvja a létfontosságú hardvereket és szoftvereket, és biztosítsa a kulcsfontosságú kiberbiztonsági szolgáltatásokat.

A 2016-ban létrehozott közszféra és magánszféra közötti, kiberbiztonsági partnerség[43] egy fontos induló lépés volt, amely 2020-ig 1,8 milliárd euró befektetést generál. Azonban a világ más részein folyamatban levő befektetések nagyságrendje[44] arra enged következtetni, hogy az EU-nak többet kell tennie a befektetések terén és azért, hogy leküzdje az Unió-szerte elhelyezkedő kapacitások széttöredezettségét.

Az EU tud hozzáadott értéket nyújtani, tekintettel a kiberbiztonsági technológia kifinomultságára, a szükséges nagyléptékű befektetésre és arra, hogy az egész EU-ban működőképes megoldásokra van szükség. A tagállamok és a közszféra-magánszféra partnerség munkájára alapozva egy további lépés lenne az EU kiberbiztonsági képességének megerősítése **kiberbiztonsági kompetenciaközpontok hálózata**[45] révén, amelynek középpontjában az **Európai Kiberbiztonsági Kutatási és Kompetenciaközpont** állna. Ez a hálózat és annak Központja serkentené a kiberbiztonság területén a technológia fejlesztését és bevetését, és uniós és nemzeti szinten kiegészítené a terület kapacitásépítési erőfeszítéseit. A Bizottság hatásvizsgálatot fog indítani a rendelkezésre álló lehetőségek tanulmányozására, beleértve a közös vállalkozás indításának lehetőségét, annak érdekében, hogy ez a struktúra 2018-ban létrejöjjön.

A Bizottság – első lépésként és az előre gondolkodás támogatására – a Horizont 2020 keretében beindítandó kísérleti szakaszt fog javasolni, amely segít a nemzeti központok hálózatba szervezésében, hogy új lendületet adjanak a kiberbiztonsági kompetenciának és technológiai fejlődésnek. A Bizottság e célból 50 millió euró rövid távú finanszírozás biztosítására tervez javaslatot tenni. A tevékenység kiegészül a közszféra és magánszféra közötti, kiberbiztonsági partnerség folyamatos bevezetésével.

A kutatási erőfeszítések összevonása és formálása lenne a hálózat lényege és a Központ kezdeti fő feladata. Az ipari kapacitások támogatása érdekében a Központ multinacionális projektek kezelésére képes kapacitásfejlesztési projektvezetőként működhetne. Ez globális szinten adna többletnyomatékot az uniós ipar innovációjának és versenyképességének a következő generációs digitális technológiák fejlesztése terén, beleértve a mesterséges intelligenciát, a kvantum számítástechnikát, a blokkláncot és a biztonságos digitális személyazonosságot, valamint ahhoz, hogy biztosítsák a hozzáférést a tömeges adatokhoz az Unióban székhellyel rendelkező cégek számára, amelyek mind kulcsfontosságúak a kiberbiztonság szempontjából a jövőben. A Központ hasznosítaná a nagyteljesítményű számítástechnikai infrastruktúra növelése érdekében folyó uniós munkát: ez elengedhetetlen a nagy mennyiségű adatok elemzéséhez, az adatok gyors titkosításához és visszafejtéséhez, a személyazonosság ellenőrzéséhez, kibertámadások szimulálásához és képi anyagok elemzéséhez[46].

A kompetenciaközpontok hálózatának tesztelés és szimuláció révén lehetősége lenne az ipar támogatására a 2.2. fejezetben ismertetett kiberbiztonsági tanúsítás alátámasztására. A

[43] C(2016) 4400 final.

[44] Az USA csak 2017-ben 19 milliárd dollárt fektet a kiberbiztonságba, ami 35 %-os emelkedés 2016-hoz képest. Fehér Ház, a sajtótitkár irodája: „Tájékoztató: Kiberbiztonsági nemzeti intézkedési terv”, 2016. február 9.

[45] A hálózat a tagállamokban jelenleg meglevő és a jövőben létrejövő kiberbiztonsági központokból állna, és a hálózat tagjai jellemzően a nyilvános kutatási szervezetek és laboratóriumok lennének.

[46] COM(2012) 45 final és COM(2016) 178 final.

Központ uniós kiberbiztonsági tevékenység teljes skálájában való részvétele biztosítaná, hogy a célkitűzéseit igényeknek megfelelően folyamatosan frissítse. A Központ célja az lenne, hogy a magas szintű kiberbiztonsági szabványokat ne csak a technológiai és kiberbiztonsági rendszerekben alkalmazzák, hanem a szakemberek magas színvonalú készségfejlesztésében is, a digitális készségek alkalmazását célzó nemzeti erőfeszítésekre vonatkozó megoldások és minták átadásával. Ebben a tekintetben uniós szinten növelné a kiberbiztonsági kapacitásokat is, emellett építene a szinergiákra, különösen az ENISA-val, a CERT-EU-val, az Europollal, a lehetséges jövőbeli Kiberbiztonsági Vészhelyzet-elhárítási Alapppal és a nemzeti CSIRT-ekkel.

A kompetenciaközpontok útján végzett munka egyik fontos fókuszpontjának kell lennie annak, hogy Európában hiányzik a polgárok, vállalkozások és kormányzatok által az egységes digitális piacon használt termékek és szolgáltatások **titkosításának** felmérését szolgáló kapacitás. Az erős titkosítás az alapja a biztonságos digitális azonosítási rendszereknek, amelyek kulcsszerepet töltenek be a hathatós kiberbiztonságban[47]; emellett biztonságban tartja az emberek szellemi tulajdonát és lehetővé teszi az olyan alapvető jogok védelmét, mint a szólásszabadság, továbbá a személyes adatok védelmét, valamint biztosítja a biztonságos internetes kereskedelmet[48].

Mivel az európai polgári és védelmi kiberbiztonsági piacok előtt közös kihívások tornyosulnak[49] és a kettős felhasználású technológia megköveteli a szoros együttműködést a kritikus területeken, a hálózat és a Központ második szakasza továbbfejleszthető a kibervédelmi dimenzióval – teljes mértékben tiszteletben tartva a Szerződés közös biztonság- és védelempolitikára vonatkozó rendelkezéseit. A technológiai súlypont mellett a védelmi dimenzió hozzájárulhat a tagállamok között együttműködéshez a kibervédelem területén, beleértve az információcserét, a helyzetismeretet, a tapasztalatszerzést és az összehangolt reagálást, és támogathatja a tagállamok közös képességeinek fejlesztését. Olyan platformként is működhetne, amely lehetővé teszi a tagállamok számára az uniós kibervédelem prioritásainak azonosítását, a közös megoldások vizsgálatát, a közös stratégiák kidolgozásához való hozzájárulást, a közös uniós szintű kibervédelmi képzések, gyakorlatok és tesztelések kialakítását, és támogatja a kiberbiztonsági osztályozási rendszerekkel és szabványokkal kapcsolatos munkát, amelyben a Központnak támogató és tanácsadó szerepe lenne. A fenti tevékenységek végzéséhez a Központnak szorosan együtt kell működnie az Európai Védelmi Ügynökséggel, amit ki is kell egészítenie a kibervédelem területén, továbbá együtt kell működnie az ENISA-val a kibertámadásokkal szembeni ellenálló képesség területén. Ez a védelmi dimenzió figyelembe venné az európai védelem jövőjéről szóló vitaanyaggal elindított folyamatot.

A kibervédelem területén indokolt magas szintű ellenálló képesség megköveteli a kutatási és technológiai erőfeszítések pontos célkiválasztását. A vállalkozások által kidolgozott kibervédelmi projektek vagy technológiák számíthatnak az Európai Védelmi Alap finanszírozására, amikor a kutatás-fejlesztési szakaszra kerül sor[50]. Ebben az összefüggésben különösen relevánsak lehetnek az olyan konkrét területek, mint például a kvantumtechnológiákon alapuló titkosítási rendszerek, a kiber-helyzetismeret, a biometrikus

[47] A Bizottság már a Horizont 2020 keretében el fog indítani egy új Horizont Díj versenyt, amely 4 millió eurót ítél oda az akadálymentes online hitelesítési módszerekre vonatkozó legjobb innovatív megoldásoknak.

[48] Kiberbiztonság az egységes európai digitális piacon. Tudományos tanácsadók magas szintű munkacsoportja, 2017. március.

[49] „Study on synergies between the civilian and the defence cybersecurity markets” (Tanulmány a polgári és a védelmi kiberbiztonsági piacok közötti szinergiákról, Optimity; SMART 2014-0059).

[50] Az európai védelmiipar-fejlesztési program már most is prioritást ad a kibervédelmi projekteknek, és a 2018-ban megjelenő pályázati felhívásnak is a kibervédelem lesz az egyik témája.

beléptető rendszerek, a tartós fenyegetések fejlett észlelése vagy az adatbányászat. A főképviselő, az Európai Védelmi Ügynökség és a Bizottság támogatni fogja a tagállamokat azon területek azonosításában, amelyeken a közös kiberbiztonsági projekteket figyelembe lehet venni az Európai Védelmi Alap általi finanszírozásban.

2.6.Erős uniós kiberkészségbázis kiépítése

A kiberbiztonságnak van egy erős oktatási dimenziója is. A hatékony kiberbiztonság erősen támaszkodik az érintett személyek készségeire. Azonban az előrejelzések szerint a kiberbiztonsági szakemberhiány a privát szektorban 2022-re 350 000 fő lesz[51]. A kiberbiztonsági oktatást minden szinten fejleszteni kell, kezdve a kibermunkaerő rendszeres képzésétől az IKT-szakemberek kiegészítő kiberbiztonsági képzésén át az új konkrét kiberbiztonsági tananyagokig. Erős tudományos kompetenciaközpontokat kell létrehozni a felgyorsult oktatási és képzési igények kielégítésére, felhasználva az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont és az ENISA iránymutatását. A cél az, hogy természetessé váljon olyan IKT-termékek és szolgáltatások tervezése, amelyek a kezdetektől fogva beépítik a biztonsági elveket. A kiberbiztonsági oktatás nem korlátozódhat az informatikai szakemberekre, hanem más területek (például: mérnöki tevékenység, üzletvezetés vagy jog) tantervébe, valamint az ágazatspecifikus oktatási anyagokba is be kell építeni. Végezetül a tanárokat és az általános és középiskolai tanulókat a digitális kompetenciák iskolai elsajátítása során tudatosítani kell a kiberbűnözésről és a kiberbiztonságról.

Az EU-nak a tagállamokkal együtt hozzá kell járulnia ehhez a munkához a digitális készségekkel és munkahelyekkel foglalkozó koalíció[52] munkájából kiindulva, és például azzal, hogy kiberbiztonsági gyakorlati képzéseket vezetnek be a KKV-k számára.

2.7.A kiberhigiénia és -tudatosság elősegítése

Mivel az incidensek mintegy 95 %-át állítólag „valamilyen – szándékos vagy nem szándékos emberi hiba” teszi lehetővé,[53] erőteljes az emberi tényező szerepe is. Ezért a kiberbiztonság mindenki felelőssége. Ez azt jelenti, hogy a személyes, vállalati és közigazgatási magatartásnak is meg kell változnia azt biztosítandó, hogy mindenki megértse a fenyegetést és rendelkezzen eszközökkel és készségekkel a támadások gyors felismerésére és az azokkal szembeni aktív védekezésre. Az embereknek kiberhigiéniai szokásokat kell kialakítaniuk, a vállalkozásoknak és a szervezeteknek pedig megfelelő kockázat-alapú kiberbiztonsági programokat kell alkalmazniuk, amelyeket rendszeresen frissíteni kell a változó kockázati környezet követéséhez.

A kiberbiztonsági irányelv nemcsak azt írja elő kötelezettségként a tagállamok számára, hogy az uniós szintű kibertámadásokkal kapcsolatos információs kicseréljék egymással, hanem azt is, hogy fejlett nemzeti kiberbiztonsági stratégiákat, valamint a hálózatok és informatikai rendszerek biztonságára vonatkozó kereteket rendszeresítsenek. A közigazgatásnak uniós és nemzeti szinten is továbbra is vezető szerepet kell betöltenie ezen erőfeszítések továbbvitelében.

A tagállamoknak először is maximalizálniuk kell a kiberbiztonsági eszközök elérhetőségét a vállalkozások és magánszemélyek számára. Többet kell tenni különösen a kiberbűnözés végfelhasználókra gyakorolt hatásának megelőzése és enyhítése érdekében. Erre van már

[51] Global Information Security Workforce Study 2017. A globális hiány 1,8 millió fő.
[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.
[53] IBM: „The Cybersecurity Intelligence Index” (Kiberbiztonsági felderítési index) 2014, hivatkozás: Securitymagazine.com, 2014. június 19.

példa az Europol munkájában a „NoMoreRansom” kampány révén[54], amelyet a bűnüldöző szervekkel és a kiberbiztonsági cégekkel szoros együttműködésben hoztak létre azzal a céllal, hogy segítsék a felhasználókat a zsarolóvírus-fertőzések megelőzésében, illetve ha már támadás áldozatává váltak, az adatok visszafejtésében. Az ilyen programokat ki kellene terjeszteni a rossz szándékú számítógépes programok (malware) bizonyos fajtáira és más területekre, és az EU-nak ki kellene alakítania egy **egységes portált, ahol az összes ilyen eszközt összegyűjti egyablakos rendszerben**, tanácsot adva a felhasználóknak a malware-ek megelőzéséhez és észleléséhez, és linkeket biztosítva a bejelentési mechanizmusokhoz.

Másodszor: a tagállamoknak fel kellene gyorsítania azt, hogy **több kiberbiztonsági eszközt használjanak az e-kormányzás fejlesztésében,** és teljes mértékben ki kellene használniuk a kompetenciahálózat nyújtotta előnyöket. Támogatni kell az azonosítás biztonságos módszereinek alkalmazását az uniós belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosítási és bizalmi szolgáltatások keretére támaszkodva, amely 2016 óta létezik és kiszámítható szabályozási környezetet nyújt, lehetővé téve a biztonságos és folyamatos elektronikus együttműködést a vállalkozások, magánszemélyek és hatóságok között[55]. Emellett a közintézményeknek – különösen azoknak, amelyek alapvető szolgáltatásokat kínálnak – biztosítaniuk kell, hogy a személyzetük képzést kapjon a kiberbiztonsággal kapcsolatos területeken.

Harmadszor: a tagállamoknak prioritássá kell tenniük a kibertudatosságot a többek között az iskoláknak, az egyetemeknek, az üzleti közösségnek és a kutatási szerveknek szóló **tájékoztatási kampányokban**. Az ENISA által összehangolt, minden év októberében tartott kiberbiztonsági hónapot kibővítik, hogy uniós és nemzeti szintű közös kommunikációs erőfeszítésként szélesebb közönséget érjenek el. Hasonlóképpen fontos a demokratikus folyamatok és az európai értékek aláaknázására irányuló **online félretájékoztató kampányokkal** és a közösségi médiában megjelenő **álhírek**kel kapcsolatos figyelemfelkeltés. Miközben az elsődleges felelősség továbbra is nemzeti szinten marad – az európai parlamenti választások tekintetében is –, a szakértelem összevonása és a tapasztalatok megosztása európai szinten bizonyítottan hozzáadott értéket képvisel a fellépések összpontosítása terén.[56].

Ezenfelül az **ipar** is fontos szerepet tölt be általánosságban, különös tekintettel azonban a digitális szolgáltatások nyújtóira és előállítóira. Olyan eszközökkel kell támogatnia a felhasználókat (egyéneket, vállalkozásokat és közigazgatási szerveket), amelyek lehetővé teszik számukra, hogy felelősséget vállaljanak saját online fellépéseikért, egyértelművé téve, hogy a kiberhigiénia megőrzése a fogyasztók felé tett ajánlat elválaszthatatlan részét képezi[57]. A sebezhetőségek felderítése és felszámolása érdekében az iparágnak törekednie kell olyan belső folyamatok bevezetésére, amelyek a gyenge pontok kivizsgálásával, osztályozásával és megoldásával foglalkoznak, tekintet nélkül arra, hogy egy esetleges sebezhetőség külső forrásból vagy az érintett vállalaton belüli forrásból származott.

---

54 https://www.nomoreransom.org/.

55 A belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló, 2014. július 23-án elfogadott 910/2014/EU rendelet (eIDAS rendelet). Az Európai Bizottság emellett építőkockákat és eszközöket biztosít az eID és az elektronikus aláírás kölcsönös átjárhatóságához (pl. megbízható szolgáltatók listái) az Európai Hálózatfinanszírozási Eszközön keresztül.

56 Erre példa a keleti stratégiai kommunikációval foglalkozó munkacsoport, amelyet a tagállamok és a főképviselő 2015-ben hozott létre Oroszország folyamatban lévő félretájékoztató kampányainak kezelése érdekében. Ez a munkacsoport olyan kommunikációs termékek és kampányok kidolgozásával foglalkozik, amelyek középpontjában a keleti partnerség régiójára vonatkozó uniós politikák megismertetése áll.

57 Egyes gyártók már használják ezt a fogalmat, mivel a termékekkel kapcsolatos európai szabályozások (mint például a gépekről szóló 2006/42/EK irányelv) „beépített biztonságra” vonatkozó elveket határoznak meg.

Fő intézkedések

- A hálózati és információs rendszerek biztonságáról szóló irányelv teljes körű végrehajtása;
- Az ENISA-ra vonatkozó új megbízás és egy európai tanúsítási keretrendszer meghatározásáról szóló rendelet gyors elfogadása az Európai Parlament és a Tanács által[58];
- A „gondossági kötelezettség” elvének meghatározására irányuló közös bizottsági/iparági kezdeményezés a termékek/szoftverek sebezhetőségének csökkentése és a „beépített biztonság” előmozdítása érdekében;
- A határokon átnyúló, súlyos problémákra való reagálásra vonatkozó tervezet gyors végrehajtása;
- Hatásvizsgálat végzése, melynek során vizsgálják annak a lehetőségét, hogy 2018-ban bizottsági javaslatot fogalmazzanak meg, amely arra irányul, hogy egy azonnali kísérleti szakaszra támaszkodva létrehozzák a kiberbiztonsági kompetenciaközpontok hálózatát, valamint az Európai Kiberbiztonsági Kutatási és Kompetenciaközpontot;
- A tagállamok támogatása azoknak a területeknek az azonosítása során, amelyeken közös kiberbiztonsági projektek tekintetében megfontolható az Európai Védelmi Alap támogatásának igénybevétele;
- Az egész Unióra kiterjedő egyablakos ügyintézés a kibertámadások áldozatainak megsegítése, az aktuális veszélyekre vonatkozó tájékoztatás nyújtása, valamint a gyakorlati tanácsok és a kiberbiztonsági eszközök összekapcsolása érdekében;
- A tagállamok fellépése a kiberbiztonság képzési programokba, valamint e-kormányzati és figyelemfelkeltő kampányokba való beépítése érdekében;
- Iparági fellépés a személyzet számára a kiberbiztonsággal kapcsolatban szervezett képzések kiszélesítése, valamint a termékek, szolgáltatások és folyamatok „beépített biztonság” szempontú megközelítése érdekében.

3.HATHATÓS UNIÓS KIBERTÁMADÁS-ELHÁRÍTÁS LÉTREHOZÁSA

A hatékony támadáselhárítás olyan intézkedési keret bevezetését jelenti, amely meggyőző és visszatartó erejű a leendő kiberbűnözők és -támadók számára. Amíg a – nem állami és állami – kibertámadások elkövetőinek a kudarcon kívül nincs mitől félniük, addig vajmi kevés késztetést fognak érezni arra, hogy felhagyjanak a próbálkozással. Az eredményes támadáselhárítás szempontjából központi jelentőséggel bír az eredményesebb bűnüldözői fellépés, amelynek középpontjában a kiberbűnözők felderítése, nyomon követhetősége és büntető eljárás alá vonása áll. Ezen túlmenően pedig szükség van arra, hogy az EU támogassa tagállamait a kettős felhasználású kiberbiztonsági kapacitások kifejlesztésében. Csak azzal indítjuk meg a kibertámadások áradatának visszafordítását, ha növeljük a lelepleződés, valamint a támadások elkövetéséért járó büntetés kiszabásának esélyét.A kibertámadásokat haladéktalanul ki kell vizsgálni, az elkövetőket bíróság elé kell állítani, illetve intézkedéseket kell tenni a megfelelő politikai vagy diplomáciai válaszlépések érdekében. Jelentős nemzetközi és védelmi vonatkozású válság esetében a főképviselő a Tanács elé terjesztheti a megfelelő reagálás lehetőségeit.

Az információs rendszerek elleni támadásokról szóló irányelv[59] 2013-as elfogadásával már történt egy lépés a kibertámadásokra adandó büntetőjogi reakció javítása terén. Ez az irányelv

[58] COM(2017) 477.

minimumszabályokat állapított meg a bűncselekményi tényállások és a büntetési tételek tekintetében az információs rendszerek elleni támadások terén, és műveleti intézkedéseket írt elő a hatóságok közötti együttműködés javítása érdekében. Az irányelv az összes tagállamban hasonló szintű, jelentős előrehaladást eredményezett a kibertámadások bűncselekménnyé nyilvánítása terén, elősegítve ezáltal az ilyen típusú bűncselekmények ügyében nyomozó bűnüldöző hatóságok közötti, határokon átnyúló együttműködést. Az irányelvben rejlő teljes potenciál mindazonáltal akkor lenne kihasználható, ha a tagállamok annak minden rendelkezését teljes mértékben végrehajtanák.[60]. A Bizottság továbbra is támogatja a tagállamokat az irányelv végrehajtásában, és jelenleg úgy látja, hogy nincs szükség arra, hogy módosításokat javasoljon.

3.1.A rossz szándékú szereplők azonosítása

Annak érdekében, hogy növeljük annak az esélyét, hogy az elkövetők bíróság elé kerüljenek, sürgősen javítani kell a kibertámadásokért felelős tettesek azonosításához szükséges kapacitásunkat. A bűnüldöző hatóságok számára a kiberbűnözéssel kapcsolatos vizsgálatok során nagy kihívást jelent a jobbára digitális nyomok formájában fellelhető információk felderítése. Ezért bővíteni kell technológiai képességünket az eredményes nyomozás érdekében, többek között úgy, hogy kiberszakértőkkel erősítjük meg az Europol kiberbűnözés elleni egységét.Az Europol kulcsfontosságú szereplővé vált a tagállamok több országot érintő nyomozásai terén. Szakértői központtá kell válnia a tagállamok bűnüldözési hatóságai számára az online nyomozások és a kiberkriminalisztika terén.

Az az elterjedt gyakorlat, hogy több felhasználó – néha több ezer – tartozik ugyanahhoz az IP-címhez, műszaki szempontból nagyon megnehezíti a rossz szándékú online magatartás felderítését. Emiatt esetenként – például olyan súlyos bűncselekményekkel kapcsolatban, mint gyermekek szexuális zaklatása – nagy számú felhasználót kell lenyomozni egyetlen rossz szándékú szereplő azonosítása érdekében. Az EU ezért szorgalmazza az új protokoll (IPv6) alkalmazását, mivel az IP-címenként egyetlen felhasználó hozzárendelését teszi lehetővé, ami egyértelműen hasznos a bűnüldözés és a kiberbiztonsági nyomozások szempontjából. Az új protokoll alkalmazását ösztönző első lépésként a Bizottság beépíti valamennyi politikájába az IPv6 protokollra történő áttérés követelményét, így a közbeszerzések, projektek és kutatások finanszírozására vonatkozó követelmények, valamint a szükséges oktatási anyagok támogatása tekintetében. Ezenfelül a tagállamoknak fontolóra kell venniük, hogy önkéntes megállapodásokat kössenek az internet-hozzáférést biztosító szolgáltatókkal az IPv6 protokoll alkalmazásának fellendítése érdekében.

Belgium globális vezető szerepet tölt be[61] az IPv6 protokoll bevezetése terén, többek között a köz- és a magánszféra közötti együttműködésnek köszönhetően: az érdekelt felek fontolóra vették, hogy egy önkéntes önszabályozó intézkedés részeként maximum 16 felhasználóra korlátozzák ugyanazon IP-cím használatát, ami ösztönözte az IPv6 protokollra való áttérést[62].

---

59 Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról.

60 COM(2017)474.

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

Általánosságban még inkább ösztönözni kell az online elszámoltathatóságot. Ez magában foglalja a domain-nevekkel nem kívánt üzenetek továbbítása és adathalászati támadások céljából elkövetett visszaélések megakadályozása érdekében tett intézkedések ösztönzését. Ennek érdekében a Bizottság azon dolgozik, hogy javítsa a domain-név és IP„WHOIS" adatbázis[63] működését és az abban szereplő információk rendelkezésre állását és pontosságát, a Bejegyzett Nevek és Számok Internetszervezete által tett erőfeszítésekkel összhangban[64].

3.2.A bűnüldözési reagálás fokozása

A kiberbűnözés hatékony **kivizsgálása** és **üldözése** komoly elrettentő erővel hat a kibertámadások terén. Szükség van ugyanakkor a jelenlegi eljárási keretnek az internetes korhoz történő igazítására[65]. Eljárásaink nem tudnak lépést tartani a kibertámadások gyorsaságával, és sajátos igény jelentkezik a határokon átnyúló gyors együttműködésre. Ennek érdekében – amint az bejelentésre került az európai biztonsági stratégia keretében – 2018 elején a Bizottság javaslatokat nyújt be **az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférés elősegítése** érdekében. Ezzel párhuzamosan a Bizottság gyakorlati intézkedéseket hajt végre annak érdekében, hogy javítsa az elektronikus bizonyítékokhoz való, nemzetközi hozzáférést bűnügyi nyomozások során, ennek keretében pedig finanszírozást nyújt a határokon átnyúló együttműködésre vonatkozó képzésekhez, az Unión belüli információcserére szolgáló elektronikus platform fejlesztéséhez, valamint a tagállamok között alkalmazott igazságügyi együttműködési formák szabványosításához.

A hathatós bűnüldözés egyik további akadálya, hogy a tagállamok más és más kriminalisztikai eljárásokkal rendelkeznek az elektronikus bizonyítékok kiberbűnözéssel kapcsolatos vizsgálatok során történő gyűjtése terén. Ez a probléma enyhíthető lenne közös kriminalisztikai szabványok kidolgozásával. Ezenfelül a nyomon követhetőség és az elkövető kiléte megállapításának támogatása érdekében meg kell erősíteni a kriminalisztikai kapacitásokat. Az Europol kriminalisztikai kapacitásainak továbbfejlesztése érdekében teendő lépések egyike, hogy az Europol Számítástechnikai Bűnözés Elleni Európai Központjában meglévő költségvetési és emberi erőforrásokat hozzá kell igazítani a határokon átnyúló, kiberbűnözéssel kapcsolatos vizsgálatok működési támogatás iránti növekvő igényéhez. További lépés lehet a fent ismertetett technológiai fókusz megjelenítése a titkosítás terén, megvizsgálva, hogy az azzal történő visszaélés miként eredményez jelentős kihívásokat a súlyos bűncselekmények, így a terrorizmus és a kiberbűnözés elleni küzdelemben. A Bizottság a **titkosítás bűnügyi nyomozásokban betöltött szerepével**[66] kapcsolatos jelenlegi mérlegelési folyamat eredményeit 2017 októberéig terjeszti elő[67].

Tekintettel az internet határokat nem ismerő jellegére, az Európa Tanács által Budapesten elfogadott, a **Számítástechnikai bűnözésről szóló egyezményben**[68] meghatározott

---

[63] Adott internetes forrás regisztrált felhasználóit vagy kedvezményezettjeit tároló adatbázisokban végrehajtott keresések során széles körben használt kérdés-válasz protokoll.

[64] A Bejegyzett Nevek és Számok Internetszervezete (ICANN) egy nonprofit szervezet, amelynek feladata az internet névjelzéseihez kapcsolódó adatbázisok fenntartásának és eljárásainak összehangolása.

[65] Hogy csak egyetlen példát említsünk, az Avalanche botnet (virtuális) központi irányító és vezérlő szervere ötpercenként költöztette át a fizikai szervereket és domaineket.

[66] A Tanács elnöksége, „A Bel- és Igazságügyi Tanács 2016 december 8-9-i tanácskozásának eredménye", 15391/16. sz.

[67] Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról, 2017. június 29., (COM(2017) 354 final).

[68] Az Egyezmény az első olyan nemzetközi egyezmény az interneten és egyéb számítógépes hálózatokon elkövetett bűncselekményekről, amely elsősorban a szerzői jogsértésekkel, a számítógépes csalással, a gyermekpornográfiával, valamint a hálózati biztonság megsértésével foglalkozik.

nemzetközi együttműködési keret felkínálja azt a lehetőséget, hogy különböző országok változatos csoportján belül optimális jogi normát alkalmazzanak a kiberbűnözéssel foglalkozó eltérő nemzeti jogszabályok tekintetében. Jelenleg foglalkoznak annak a lehetőségével, hogy egy jegyzőkönyvet csatolnak az Egyezményhez[69], ami további hasznos lehetőséget nyújthat az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférés problémájának nemzetközi összefüggésben történő kezelésére. A kiberbűnözéssel összefüggő kérdésekre vonatkozó új nemzetközi jogi eszközök megalkotása helyett az EU arra szólítja fel az országokat, hogy alkossanak megfelelő nemzeti jogszabályokat és törekedjenek együttműködésre a meglévő nemzetközi kereten belül.

Az anonimizálási eszközök általános elérhetősége megkönnyíti a bűnözők számára a rejtőzködést. A **„sötét web (darknet)”**[70] új lehetőségeket teremtett a bűnözők számára gyermekek szexuális zaklatására vonatkozó anyagokhoz, kábítószerekhez vagy fegyverekhez való hozzáféréshez, és sokszor elenyésző a lebukás kockázata.[71]. Továbbá most az a kiberbűnözés során használt eszközök, így a rossz szándékú számítógépes programok és a feltörésre szolgáló eszközök legfontosabb forrása is. A Bizottság az érdekelt felekkel együtt megvizsgálja a nemzeti megközelítési módokat annak érdekében, hogy új megoldásokat határozzon meg. Az Europolnak elő kell segítenie és támogatnia kell a sötét webbel kapcsolatos vizsgálatokat, értékelnie kell a fenyegetéseket és segítenie kell a joghatóság meghatározását, valamint előnyben kell részesítenie a nagy kockázatú eseteket; az EU pedig vezető szerepet tölthet be a nemzetközi fellépés összehangolásában[72].

A kiberbűnözési tevékenységek egyik bővülő területe a hitelkártya adatok vagy egyéb elektronikus fizetési eszközök csalárd módon történő felhasználása. Az online kiskereskedőktől vagy más törvényes üzleti vállalkozásoktól kibertámadások útján megszerzett fizetéshitelesítési adatokkal aztán interneten kereskednek, és azokat a bűnözők felhasználhatják csalások elkövetésére[73]. A Bizottság javaslatot terjeszt elő a támadáselhárítás előmozdítására **a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló irányelven** keresztül[74]. Ennek célja az e területen meglévő szabályok aktualizálása, valamint az, hogy erősítse a bűnüldözés azon képességét, hogy fellépjen ezen bűnözési forma ellen.

Javítani kell továbbá a tagállamok bűnüldöző hatóságainak a képességét a kiberbűnözések kivizsgálására, valamint a kiberbűnözés és a vizsgálati lehetőségek ügyészek és a bírói kar általi megértését. Az Eurojust és az Europol támogatja e célkitűzés elérését, valamint a fokozott együttműködést, szorosan együttműködve az Europol Számítástechnikai Bűnözés Elleni Központján belül működő különleges tanácsadó csoportokkal és a kiberbűnözés elleni

---

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 2017-ben 55 kormány erősítette meg a Európa Tanács számítástechnikai bűnözésről szóló egyezményét, illetve csatlakozott ahhoz.

69 A számítástechnikai bűnözésről szóló budapesti egyezmény 2. kiegészítő jegyzőkönyvtervezetének elkészítésére vonatkozó megbízás, T-CY (2017)3.

70 A sötét web olyan egymást átfedő hálózatok tartalmából áll, amelyek az internetet használják, de a hozzájuk való hozzáféréshez különleges szoftver, konfiguráció vagy engedély kell. A sötét web a mély web, vagyis a világháló keresőmotorok által nem indexált részének egy kis részét képezi.

71 Figyelemre méltó kivétel a legnagyobb bűnözői sötét web piacok közül kettő, az AlphaBay és a Hansa közelmúltbeli eltávolítása: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Az Europol már fontos szerepet tölt be ezen a területen. Közelmúltbeli példaként lásd: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

73 A csalásból származó jövedelem a szervezett bűnözés fontos bevételi forrása, ezáltal pedig támogat más bűncselekményeket is, így a terrorizmust, a kábítószer-kereskedelmet, valamint az emberkereskedelmet.

74 COM(2017) 489.

egységek vezetői, valamint a kiberbűnözésre szakosodott ügyészek hálózataival. A Bizottság 10,5 millió EUR összeggel támogatja a kiberbűnözés elleni küzdelmet, elsősorban **Belső Biztonsági Alap – Rendőrségi Program** keretében. A képzés fontos alkotóelem, és a Számítástechnikai Bűnözés Elleni Európai Képzési és Oktatási Csoport számos hasznos anyagot fejlesztett ki. Ezeket az Európai Unió Bűnüldözési Képzési Ügynöksége (CEPOL) támogatásával széles körben elérhetővé kell tenni a bűnüldözési szakemberek számára.

3.3.Az állami és a magánszféra együttműködése a kiberbűnözés ellen

A hagyományos bűnüldözési mechanizmusok eredményességét a jórészt magántulajdonú infrastruktúrából és többféle országban működő számos szereplőből felépülő digitális világ jellemzői kihívások elé állítják. Ennek következtében a magánszektorral való együttműködés – az iparágra és a civil társadalomra kiterjedően – alapvető jelentőségű a hatóságok számára a bűnözés elleni eredményes küzdelemhez. Ezzel összefüggésben a pénzügyi ágazat ugyancsak kulcsszerepet kap, és az együttműködést fokozni kell. Például erősíteni kell a pénzügyi információs egységek[75] kiberbűnözéssel kapcsolatos szerepét.

Egyes tagállamok már tettek fontos lépéseket. Hollandiában a pénzügyi intézmények és a bűnüldöző hatóságok együtt dolgoznak az internetes csalás és a kiberbűnözés kezelésén az elektronikus bűnözéssel foglalkozó munkacsoport keretében. A kiberbűnözés elleni német kompetenciaközpont a tagjai számára operatív információcsere-csomópontot biztosít a német szövetségi rendőrséggel szoros együttműködésben, és a kiberbűnözés elleni védelem biztosítását célzó intézkedéseket dolgoz ki. 16 tagállam[76] hozott létre a kiberbűnözés elleni kiválósági központokat a bűnüldöző hatóságok, tudományos körök és magánpartnerek együttműködésének megkönnyítésére, a bevált gyakorlatok kidolgozása és cseréje, képzés és kapacitásépítés céljából.
A Bizottság célzott projektek révén támogatja a köz- és magánszféra közötti partnerségek és együttműködési mechanizmusok létrehozását, ilyen az Online csalással foglalkozó kiberközpontok és szakértők hálózata,[77] amely imformációmegosztási modellt és normákat vezet be az elektronikus bűnözés kockázata és az online csalás elemzése és mérséklése érdekében.

A kiberbűnözéssel összefüggésben a magánvállalkozásoknak módot kell arra kapniuk, hogy – a személyes adatokra kiterjedően, az adatvédelmi szabályok teljes körű betartása mellett – megosszák a konkrét esetekre vonatkozó információkat a bűnüldöző hatóságokkal. A 2018 májusában hatályba lépő uniós adatvédelmi reform egységes szabályrendszert ír elő, amely meghatározza a bűnüldöző hatóságok és a magánszervezetek működési feltételeit. Az Európai Bizottság az Európai Adatvédelmi Testülettel és az érintett érdekeltekkel együtt fog dolgozni e terület bevált gyakorlatainak azonosításán, és adott esetben útmutatást fog nyújtani.

[75] A pénzügyi információs egységek nemzeti szervként fogadják és elemzik a gyanús ügyletekre vonatkozó jelentéseket, és a pénzmosás, az előcselekménynek tekintett kapcsolódó bűncselekmények és a terrorizmus finanszírozása szempontjából jelentőséggel bíró egyéb információkat; valamint terjesztik az elemzés eredményeit.

[76] Ausztria, Belgium, Bulgária, Ciprus, Cseh Köztársaság, Észtország, Franciaország, Németország, Görögország, Írország, Litvánia, Lengyelország, Románia, Szlovénia, Spanyolország és az Egyesült Királyság.

[77] Az EU-OF2CEN kezdeményezés célja az internetes csalással kapcsolatos információk módszeres, egész EU-ra kiterjedő megosztásának lehetővé tétele a bankok és a bűnüldöző szolgálatok között annak érdekében, hogy meg lehessen előzni a csalóknak és a futároknak (money mules) történő kifizetéseket, valamint az érintett elkövetőket azonosítani lehessen, valamint büntető eljárás alá lehessen vonni. A kezdeményezés uniós társfinanszírozásban részesül (Belső Biztonsági Alap-Rendőrségi Program).

3.4.A politikai válaszlépések erősítése

A nemrégiben elfogadott, a **rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete**[78] („kiberdiplomáciai eszköztár”) fekteti le a közös kül- és biztonságpolitika keretébe tartozó intézkedéseket, ideértve azokat a korlátozó intézkedéseket, amelyek az EU politikai, biztonsági és gazdasági érdekeit sértő tevékenységekre adott reagálás erősítésére felhasználhatóak. A keretrendszer fontos lépést képez az uniós és tagállami szintű jelző- és reagálási kapacitások fejlesztésében. Fokozni fogja a rossz szándékú kibertevékenységek elkövetői felderítésének képességét, a potenciális agresszorok magatartásának befolyásolása céljából, egyidejűleg figyelembe véve az arányos reagálás biztosításának szükségességét. Az állami vagy nem állami szereplőknek tulajdonítás a minden forrást igénybe vevő hírszerzésre alapított, szuverén politikai döntés marad. A keret végrehajtását célzó munka jelenleg folyik a tagállamokkal, és a Tervezettel szorosan összehangolva zajlik, a nagyszabású kiberincidensekre való reagálás céljából[79]. Az INTCEN-nek kell egyesítenie, elemeznie és megosztania a keretbe tartozó intézkedések használatához szükséges helyzetismeretet,[80] a tagállamokkal és az uniós intézményekkel szorosan együttműködésben végzett munkával.

3.5.Kiberbiztonsági támadáselhárítás kiépítése a tagállami védelmi kapacitások révén

A tagállamok már fejlesztenek kibervédelmi kapacitásokat. Ezen túlmenően, figyelemmel a kibervédelem és a kiberbiztonság határának elmosódására és a kibereszközök és -technológiák fettős felhasználású jellegére, illetőleg a tagállami megközelítések nagyfokú változatosságára, az EU megfelelő helyzetben van ahhoz, hogy elősegítse a katonai és polgári erőfeszítések szinergiáját[81].

A fejlettebb kiberbiztonsági kapacitásokkal rendelkező és azok egyesítésére hajlandó tagállamok a főképviselő, a Bizottság és az Európai Védelmi Ügynökség támogatásával mérlegelhetnék a kiberbiztonság felvételét az „állandó strukturált együttműködés” (PESCO) keretébe. Ezt alátámaszthatná a fentiekben ismertetett munka, az Unió ipari kapacitásai és stratégiai autonómiája ösztönzése céljából. Az EU a kapacitásfejlesztés elősegítése, a képzési és oktatási, valamint a kettős felhasználású termékek szabványosítására vonatkozó erőfeszítések révén is előmozdíthatná a kölcsönös átjárhatóságot.

A gyakran kibertámadásokat is magukban foglaló hibrid fenyegetésekre való reagáláshoz teljes mértékben hasznosítani kell a közös keretet, nevezetesen a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport és a közelmúltban Helsinkiben létrehozott Hibrid Fenyegetések Elleni Küzdelem Európai Központja révén, amelynek küldetése a stratégiai párbeszéd szorgalmazása, kutatás és elemzés végzése.

Az EU megújult hangsúlyt fog fektetni a 2014-es uniós kibervédelmi politikai keretre[82] a kiberbiztonság és -védelem közös biztonság- és védelempolitikába (KBVP) való további integrálása eszközeként. Maguknak a KBVP-missziónak és -műveleteknek a kibertámadásokkal szembeni ellenálló képessége alapvető fontosságú: olyan szabványosított eljárások és műszaki kapacitások kerülnek kifejlesztésre, amelyek egyaránt támogathatják a kiküldött polgári és katonai missziókat, illetve azok tervezési és végrehajtási szolgálatát és az

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.
[79] C(2017) 6100.
[80] JOIN(2016) 018 final.
[81] Az EU a kiberteret ugyanolyan műveleti területként fogja fel, mint a szárazföldet, a légteret és a tengert. A kibervédelmi erőfeszítéseknek részét képezik a világűrbe telepített eszközök és a kapcsolódó földi infrastruktúra is.
[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

EKSZ információtechnológiai szolgáltatóit. A tagállami együttműködés fejlesztése és a területen kifejtett uniós erőfeszítések jobb irányítása érdekében az Európai Védelmi Ügynökség és az EKSZ a Bizottság szervezeti egységeivel együttműködésben fogja előmozdítani a stratégiai szintű szerepvállalást a tagállamok kibervédelemmel foglalkozó döntéshozói között. Az Unió támogatni fogja az európai kiberbiztonsági megoldások fejlesztését is, az európai védelmi ipari és technológiai bázis javát szolgáló erőfeszítései részeként. Ebbe beletartozik a regionális kiberbiztonsági és -védelmi kiválósági klaszterek támogatása is.

A Bizottság szervezeti egységei az EKSZ-szel, a tagállamokkal és más érintett uniós szervekkel szorosan együttműködve 2018-ra működésbe állítanak egy **kibervédelmi képzési és oktatási platformot,** a kibervédelem terén jelenleg fennálló készséghiány megoldására. Ez ki fogja egészíteni az Európai Védelmi Ügynökség ezen a területen folytatott munkáját, segítve ezzel a kiberbiztonság és kibervédelem jelenlegi készségszűkének felszámolását.

Fő intézkedések

- A Bizottság kezdeményezése az elektronikus bizonyítás határokon túlnyúló elérhetősége érdekében (2018 eleje);
- A nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló európai parlamenti és tanácsi irányelvre irányuló javaslat gyors elfogadása;
- Az IPv6 követelményeinek bevezetése az uniós közbeszerzésben, kutatás- és projektfinanszírozásban; önkéntes megállapodások a tagállamok és internetszolgáltatók között az Ipv6 elterjedésének gyorsítása érdekében;
- Az Europol keretében a kiberkriminalisztikára és a sötét web figyelésére irányuló megújult/nagyobb figyelem;
- A rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének végrehajtása
- Megemelt pénzügyi támogatás a büntető igazságszolgáltatás kibertérben történő fejlesztését célzó nemzeti és nemzetközi projekteknek.
- Kiberbiztonsággal kapcsolatos oktatási platform a kiberbiztonság és kibervédelem jelenlegi készségszűkének 2018-ban történő felszámolására.

4.A KIBERBIZTONSÁGI NEMZETKÖZI EGYÜTTMŰKÖDÉS ERŐSÍTÉSE

Az Unió alapvető értékei és az alapvető jogok – mint a szólásszabadság, és a magánélet és a személyes adatok védelméhez való jog –, valamint a nyílt, szabad és biztonságos kibertér előmozdítása által vezérelten az Unió nemzetközi kiberbiztonsági stratégiájának kialakítása a globális kiberstabilitás előmozdításának folyamatosan változó kihívásának kezelését, illetőleg Európa kibertérbeli stratégiai autonómiájához való hozzájárulást szolgálja.

4.1.Kiberbiztonság a külkapcsolatokban

Bizonyítékok utalnak arra, hogy az emberek világszerte a kibertámadásokat tekintik a nemzetbiztonságra leselkedő egyik legnagyobb veszélynek[83]. A fenyegetés globális jellegét tekintve, alapvető fontosságú harmadik országokkal szilárd szövetségek és partnerségek kiépítése és fenntartása a nemzetközi stabilitás és biztonság terén egyre inkább központi helyre kerülő kibertámadások megelőzéséhez és azok elhárításához. Az Unió prioritást fog adni kétoldalú, regionális, többszereplős és multilaterális szerepvállalásaiban a kibertérbeli konfliktusmegelőzést és stabilitást szolgáló stratégiai keret kiépítésének.

[83] A Pew Research Centre 2017. évi globális attitűdfelmérése.

Az Unió határozottan képviseli azt az álláspontot, hogy a nemzetközi jog – és különösen az ENSZ Alapokmánya – a kibertérben is érvényesül. A kötelező nemzetközi jogi normák kiegészítéseként az Unió elfogadja a felelős állami magatartás ENSZ kormányzati szakértői csoportja által megfogalmazott önkéntes, nem kötelező erejű normáit, szabályait és elveit[84]; szorgalmazza egyben a regionális bizalomépítő intézkedések kidolgozását és végrehajtását, az Európai Biztonsági és Együttműködési Szervezetben és más régiókban egyaránt.

Kétoldalú szinten a kiberpárbeszédek[85] továbbfejlesztésre kerülnek és kiegészítik azokat a harmadik országokkal a kibertérbeli átvilágítás és állami felelősség elveinek megerősítését célzó együttműködést elősegítő erőfeszítések. Az Unió nemzetközi szerepvállalásaiban is prioritást fog adni a kibertér biztonsági problémáinak, biztosítva ugyanakkor, hogy a kiberbiztonság ne váljon a piacvédelem álcájává és az alapvető jogok és szabadságok korlátjává, a szólásszabadságot és az információkhoz való hozzáférés szabadságát. A kiberbiztonság átfogó megközelítése az emberi jogok tiszteletben tartását igényli, és az Unió továbbra is tartani fogja magát alapvető értékeihez világszerte, az Unió online szabadságra vonatkozó emberi jogi iránymutatásából kiindulva[86]. Az Unió ebben a vonatkozásban hangsúlyozza az internet irányításában valamennyi résztvevő részvételének fontosságát.

A Bizottság is beterjesztett egy javaslatot[87] az Unió exportszabályozásának modernizálására, ideértve az emberi jogok megsértésére alkalmas vagy az Unió saját biztonsága ellen visszaélésre alkalmat adó kritikus kibermegfigyelési technológiák behozatali ellenőrzésének bevezetését, valamint fel fogja gyorsítani a harmadik országokkal folytatott párbeszédet ezen a területen a globális konvergencia és felelős magatartás népszerűsítése érdekében.

4.2.Kiberbiztonsági kapacitásépítés

A globális kiberstabilitás alapja valamennyi ország helyi és nemzeti képessége a kiberincidensek megelőzésére és az azokra való reagálásra, valamint a kiberbűncselekmények kinyomozására és büntető eljárás alá vonására. A harmadik országbeli nemzeti ellenálló képesség kiépítését célzó erőfeszítések támogatása globálisan fogja emelni a kiberbiztonsági szintet, ami az Unióra is kedvező következményekkel jár. A gyorsan fejlődő kiberfenyegetések elleni fellépés képzési, szakpolitika- és jogszabály-fejlesztési erőfeszítések szükségességére utal, illetve a világ összes országában hatékonyan működő számítógépes vészhelyzeteket elhárító csoportokat és kiberbűnözési egységeket igényel.

Az Unió 2013 óta tölt be vezető szerepet a nemzetközi kiberkapacitás-építésben és ezen erőfeszítéseket módszeresen összeköti fejlesztési együttműködési tevékenységével. Az Unió továbbra is a jogokon alapuló kapacitásépítési modellt fogja előmozdítani, a digitálisan a fejlődésért (Digital4Development) megközelítésnek megfelelően[88]. A kapacitásépítés prioritásait az Unió szomszédsága és fejlődő harmadik országok fogják jelenteni, amelyek az internetkapcsolat gyors terjedését és a fenyegetések gyors kialakulását tapasztalják. Az Unió erőfeszítései az uniós fejlesztési programot a fenntartható fejlődésre vonatkozó 2030-as menetrendre és az átfogó intézményi kapacitásépítési intézkedésekre figyelemmel egészítik ki.

---

84 A/68/98 és A/70/174.

85 Az Unió 2017 szeptemberében kiberpárbeszédet folytatott az USA-val, Kínával, Japánnal, a Koreai Köztársasággal és Indiával.

86 Az Unió emberi jogi iránymutatása az online és offline véleménynyilvánítás szabadságáról.

87 SWD(2016) 616.

88 SWD(2017) 157.

Az Unió kollektív szakértelmének a kapacitásépítés támogatása céljából történő mobilizálási képessége fejlesztése érdekében létre kell hozni egy célzott uniós kiberkapacitás-építő hálózatot, amely egybefogja az EKSZ-t, a tagállami kiberhatóságokat, az uniós ügynökségeket, a bizottsági szervezeti egységeket, tudományos köröket és a civil társadalmat. A harmadik országok támogatásában a politikai útmutatás és az uniós erőkifejtés prioritásai meghatározásának javítását elősegítendő uniós kiberkapacitás-építési iránymutatás kerül kidolgozásra.

A különböző régiókban az átfedéseket megelőzendő és a célzottabb kapacitásépítés lehetővé tételére az Unió más támogatókkal is együtt fog működni ezen a területen.

4.3.EU–NATO együttműködés

A már elért jelentős előrelépésre építve az Unió el fogja mélyíteni az EU és a NATO között a kiberbiztonság, a hibrid fenyegetések és a védelem terén folyó együttműködést, a 2016. július 8-i közös nyilatkozatban előre vetítettek szerint[89]. A prioritások körébe tartozik az átjárhatóság támogatása következetes kibervédelmi követelmények és szabványok révén, a képzési és gyakorlati együttműködés erősítése, a képzési követelmények harmonizálása.

Az Unió és a NATO támogatni fogja továbbá a kibervédelmi kutatási és innovációs együttműködést, ami a kiberbiztonsági testületeik közötti, kiberbiztonsági információcserére vonatkozó, aktuális technikai megállapodásokra fog épülni[90]. A hibrid fenyegetésekkel szembeni fellépés terén tett közelmúltbeli közös erőfeszítések, különösen a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport és a NATO hibrid fenyegetéseket elemző csoportja közötti együttműködés tovább élénkítendő az ellenálló képesség és a kiberválságokra való reagálás erősítése érdekében. Az Unió és a NATO közötti további együttműködés támogatása kibervédelmi gyakorlatok révén fog történni, az EKSZ és más uniós szervek, valamint az illetékes NATO-partnereik részvételével, ideértve a NATO tallini Kibervédelmi Kiválósági Együttműködési Központját. A NATO és az Unió első alkalommal fog végrehajtani párhuzamos és összehangolt gyakorlatokat egy hibrid forgatókönyvre reagálva, 2017-ben NATO-irányítással, 2018-ban pedig az Unió vezetésével. Az EU-NATO együttműködésre vonatkozó, az illetékes Tanácsnak 2017-ben benyújtásra kerülő jelentés alkalmat fog kínálni az együttműködés további bővítésére, nevezetesen az összes érintett részt vevő intézmény és szervezet – az ENISA-t is ideértve – közötti közös, biztonságos és megbízható kommunikációs eszközök biztosítása révén.

Fő intézkedések

- A kibertérbeli konfliktusmegelőzést és stabilitást szolgáló stratégiai keret fejlesztése;
- Új kapacitásépítési hálózat kiépítése harmadik országok azon képességét javítandó, hogy kezelni tudják a kiberfenyegetéseket, valamint uniós kiberbiztonsági kapacitásépítési iránymutatás az uniós erőfeszítések prioritásmeghatározását javítandó;
- Az Unió és a NATO közötti együttműködés kibővítése, ideértve a párhuzamos és összehangolt gyakorlatokban való részvételt és a kiberbiztonsági szabványok nagyobb kölcsönös átjárhatóságát.

5.KÖVETKEZTETÉS

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

[90] A CERT-EU és a NATO hálózatbiztonsági incidenskezelő kapacitása (NCIRC).

Az Unió kiberfelkészültsége egyaránt központi jelentőségű az egységes digitális piac, valamint biztonsági és védelmi uniónk szempontjából. Az európai kiberbiztonság fokozása és a polgári és katonai célpontokra egyaránt irányuló fenyegetések megoldása elengedhetetlen.

Az észt elnökség által 2017. szeptember 29-re szervezett közelgő digitális csúcs alkalmat ad azon közös elszántság demonstrálására, hogy a kiberbiztonság az Unióban – mint digitális társadalomban – központi szerepet kapjon. E közös vállalás részeként a Bizottság felhívja a tagállamokat arra, hogy vállaljanak kötelezettséget arra, miként szándékoznak eljárni azokon a területeken, amelyeken elsődleges felelősséget viselnek. Ebbe bele kell tartoznia a kiberbiztonság alábbiak révén történő erősítésének:

- A kiberbiztonsági irányelv 2018. május 9-ig történő teljes és eredményes végrehajtásának, illetve a kiberbiztonságért felelős hatóságok feladatai eredményes ellátásához szükséges erőforrásoknak a biztosítása;
- Azonos szabályok alkalmazása a közigazgatásra, tekintve annak a társadalom és a gazdaság egészében betöltött szerepét;
- Kiberbiztonsági vonatkozású képzés nyújtása a közigazgatásban;
- A kiberbiztonság előtérbe állítása információs kampányokban, és a kiberbiztonság beépítése az egyetemi és szakképzési tantervekbe;
- Az „állandó strukturált együttműködés” (PESCO) kezdeményezéseinek és az Európai Védelmi Alapnak a felhasználása a kibervédelmi projektek támogatására.

E közös közlemény meghatározta a kihívás nagyságrendjét és azon intézkedések palettáját, amelyeket az Unió megtehet. Olyan Európára van szükségünk, amely ellenálló, és hathatósan képes lakosait megvédeni a lehetséges kiberbiztonsági incidensekre való felkészüléssel, struktúráiba és magatartásába erőteljes védelem beépítésével, a kibertámadásokból való gyors talpra állással és a felelősök elrettentésével. Ez a közlemény olyan célzott intézkedésekre tesz javaslatot, amelyek összehangolt módon tovább erősítik az Unió kiberbiztonsági struktúráit és kapacitásait, a tagállamok és az érintett uniós szervek teljes körű együttműködésével, azok hatáskörét és feladatkörét tiszteletben tartva. Végrehajtása egyértelműen igazolni fogja, hogy az Unió és a tagállamok közösen munkálkodnak azon, hogy olyan kiberbiztonsági színvonalat biztosítsanak, amely megfelel az Európa előtt tornyosuló, egyre gyarapodó kihívásoknak.