Az Európai Unió
Tanácsa

**Brüsszel, 2020. december 16.**
**(OR. en)**

**14133/20**

**Intézményközi referenciaszám:**
**2020/0305(NLE)**

| | |
|---|---|
| **CYBER 280** | **RECH 529** |
| **JAI 1118** | **COMPET 642** |
| **JAIEX 121** | **IND 273** |
| **EJUSTICE 107** | **COTER 115** |
| **COSI 254** | **ENFOPOL 350** |
| **DATAPROTECT 154** | **COPS 485** |
| **COPEN 387** | **MI 578** |
| **TELECOM 269** | **IXIM 139** |
| **PROCIV 99** | **POLMIL 201** |
| **CSC 367** | **HYBRID 48** |
| **CIS 65** | **CSCI 96** |
| **RELEX 1019** | **POLGEN 234** |

**FEDŐLAP**

| | |
|---|---|
| Küldi: | az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató |
| Az átvétel dátuma: | 2020. december 16. |
| Címzett: | Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára |
| Biz. dok. sz.: | JOIN(2020) 18 final |
| Tárgy: | KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Az EU kiberbiztonsági stratégiája a digitális évtizedre |

Mellékelten továbbítjuk a delegációknak a JOIN(2020) 18 final számú dokumentumot.

Melléklet: JOIN(2020) 18 final

EURÓPAI
BIZOTTSÁG

AZ UNIÓ KÜLÜGYI ÉS
BIZTONSÁGPOLITIKAI
FŐKÉPVISELŐJE

Brüsszel, 2020.12.16.
JOIN(2020) 18 final

# KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

## Az EU kiberbiztonsági stratégiája a digitális évtizedre

# KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

## Az EU kiberbiztonsági stratégiája a digitális évtizedre

## I. BEVEZETÉS: KIBERBIZTONSÁGOS DIGITÁLIS ÁTALAKULÁS ÖSSZETETT FENYEGETÉSI KÖRNYEZETBEN

A kiberbiztonság az európaiak biztonságának szerves része. Legyen szó csatlakoztatott eszközökről, villamosenergia-hálózatokról, bankokról, repülőgépekről, közigazgatási szervekről vagy kórházakról, az emberek megérdemlik, hogy azzal tudattal használják vagy keressék fel ezeket, hogy védve vannak a kiberfenyegetésekkel szemben. Az EU gazdasága, demokráciája és társadalma minden eddiginél jobban függ a biztonságos és megbízható digitális eszközöktől és az összekapcsoltságtól. A kiberbiztonság ezért alapvető szerepet játszik a reziliens, környezetbarát és digitális Európa megteremtésében.

**A közlekedés, az energiaügy, az egészségügy, a telekommunikáció, a pénzügy, a biztonság, az űrpolitika, a védelem és a demokratikus folyamatok nagymértékben függenek az egyre inkább összekapcsolt hálózati és informatikai rendszerektől.** Az ágazatközi egymásrautaltság rendkívül nagy, mert a hálózati és informatikai rendszerek működése viszont a megbízható villamosenergia-ellátástól függ. A csatlakoztatott eszközök száma már meghaladja a bolygónk lakosságát, és az előrejelzések szerint 2025-re eléri a 25 milliárdot[1], s ezek egynegyede Európában lesz majd. A Covid19-világjárvány hatására felgyorsult a munkavégzés digitalizációja, és ennek során az uniós munkavállalók 40 %-a váltott távmunkára, ami valószínűleg tartós hatással lesz a mindennapi életre[2]. Ezáltal fokozódik a kibertámadásokkal szembeni sebezhetőség[3]. A fogyasztóknak gyakran olyan csatlakoztatott eszközöket szállítanak, amelyek gyenge pontjai ismertek, ami tovább növeli a rosszindulatú kibertevékenységek támadási felületét[4]. Az uniós ipari környezetet egyre inkább a digitalizálás és összekapcsoltság jellemzi, ami azt is jelenti, hogy a kibertámadások minden eddiginél nagyobb hatást gyakorolhatnak az iparra és az ökoszisztémákra.

---

[1] A GSMA telekommunikációs szakmai szövetség becslése szerint (https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). Az International Data Corporation előrejelzése szerint a csatlakoztatott eszközök, szenzorok és kamerák száma el fogja érni a 42,6 milliárdot (https://www.idc.com/getdoc.jsp?containerId=prUS45213219).

[2] Egy 2020 júniusi felmérés szerint az üzleti vezetők 47 %-a tervezi lehetővé tenni a munkavállalók számára, hogy teljes munkaidőben távmunkát végezzenek azután is, hogy lehetőség lesz visszatérni a munkahelyekre; 82 %-uk pedig azt tervezi, hogy legalább részben engedélyezi a távmunkát (https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time).

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Az eddigi egyik legkárosabb rosszindulatú szoftver (malware), a Mirai több mint 600 000 készülékből álló botneteket hozott létre, amelyek számos nagyobb honlap működését akadályozták Európában és az Egyesült Államokban.

**A fenyegetést súlyosbítja a globális és nyílt internettel, valamint az ellátási lánc egészében a technológiák ellenőrzésével kapcsolatos geopolitikai feszültség**[5]. Ezt a feszült helyzetet tükrözi, hogy egyre több nemzetállam állít digitális határokat. Az internet korlátozása, illetve az interneten való korlátozások veszélyeztetik a globális és nyílt kiberteret, valamint a jogállamiságot, az alapvető jogokat, a szabadságot és a demokráciát – vagyis az EU alapvető értékeit. Egyre nagyobb mértékben kerül sor a kibertér politikai és ideológiai célú használatára, és a fokozott nemzetközi polarizáció akadályozza a hatékony multilateralizmust. A hibrid fenyegetések a dezinformációs kampányokat az infrastruktúra, a gazdasági folyamatok és a demokratikus intézmények elleni kibertámadásokkal ötvözik, ami fizikai támadásokkal, a személyes adatokhoz való jogellenes hozzáféréssel, ipari vagy állami titkok lopásával, bizalmatlanság szításával és a társadalmi kohézió gyengítésével járhat. Ezek a tevékenységek veszélyeztetik a nemzetközi biztonságot és stabilitást, valamint a kibertér által a gazdasági, társadalmi és politikai fejlődés terén biztosított előnyöket.

**A kritikus infrastruktúra elleni rosszindulatú támadás jelentős globális kockázatot jelent**[6]. Az internet decentralizált felépítése nélkülözi a központi struktúrát, és irányítására az érdekelt felek sokasága jellemző. Sikerült fenntartania a forgalom exponenciális növekedését, miközben a zavarására irányuló rosszindulatú támadások állandó célpontja[7]. Egyre fontosabb szerepet kapnak ugyanakkor a globális és nyílt internet alapvető funkciói, mint például a doménnévrendszer (DNS), továbbá a kommunikáció, tárhelyszolgáltatás, alkalmazások és adatok tekintetében az alapvető internetes szolgáltatások. Ezek a szolgáltatások egyre inkább néhány magánvállalkozás kezében koncentrálódnak[8]. Az európai gazdaság és társadalom ezáltal kiszolgáltatottá válik a geopolitikai vagy műszaki zavaroknak, amelyek az internet lényegét vagy az említett vállalkozásokat fenyegetik. A világjárvány hatására bekövetkező fokozott internethasználat és változó internethasználati minták még inkább megmutatták az ettől a digitális infrastruktúrától függő ellátási láncok sebezhetőségét.

**A biztonsággal kapcsolatos aggodalmak jelentős mértékben akadályozzák az online szolgáltatások igénybevételét**[9]**.** Az uniós felhasználók mintegy kétötöde tapasztalt biztonsági problémákat, háromötödük pedig nem tudja megvédeni magát a kiberbűnözés ellen[10]. Az elmúlt három évben egyharmaduk kapott csalásra irányuló, a személyes adataik

---

[5] Ideértve az elektronikus alkatrészeket, az adatelemzést, a felhőt, a gyorsabb és intelligensebb, legalább 5G hálózatokat, a titkosítást, a mesterséges intelligenciát (MI), valamint az olyan új számítástechnikai és elfogadott adatkezelési paradigmákat, mint a blokklánc, a peremhálózat és a kvantum-számítástechnika.

[6] A Világgazdasági Fórum globális kockázatokról szóló, 2020. évi jelentése.

[7] A Gazdasági Együttműködési és Fejlesztési Szervezet szerint a világjárvány hatására 60 %-kal nőtt az internetforgalom (https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/). Az Európai Elektronikus Hírközlési Szabályozók Testülete és a Bizottság rendszeresen jelentéseket tesz közzé az internetkapacitás állapotáról a koronavírus miatti korlátozások időtartama alatt. Az ENISA jelentése szerint 2018 harmadik negyedévéhez képest 2019 harmadik negyedévében 241 %-kal nőtt az elosztott szolgáltatásmegtagadási támadások száma. Az elosztott szolgáltatásmegtagadási támadások intenzitása fokozódik, és a legnagyobb ilyen támadás során 2020 februárjában a csúcsforgalom elérte a másodpercenkénti 2,3 terabitet. 2020 augusztusában a CenturyLink leállása, vagyis az említett amerikai internetes szolgáltató útválasztási (routing) problémája hatására 3,5 %-kal csökkent a globális internetes forgalom (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service).

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy (Globális jelentés az internetről: Az internetes gazdaság konszolidációja) (https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/).

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[10] A digitális gazdaság és társadalom fejlettségét mérő mutató, 2020 (https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG).

iránt érdeklődő e-maileket vagy telefonhívásokat, de 83 %-uk soha nem tett bejelentést kiberbűnözésről. Minden nyolcadik vállalkozást ért már kibertámadás[11]. A rosszindulatú szoftverekkel megfertőzött üzleti és személyes asztali számítógépek több mint fele még ugyanabban az évben újra megfertőződik[12]. Évente több száz millió feljegyzés veszik el adatvédelmi incidensek miatt, és egy ilyen esemény vállalkozásonkénti átlagos költsége 2018-ban meghaladta a 3,5 millió EUR nagyságú összeget[13]. A kibertámadások hatása gyakran nem elszigetelt, és az egész gazdaságra és társadalomra kiterjedő, emberek millióit érintő láncreakciókat válthatnak ki[14].

**A nyomozásnak szinte valamennyi bűncselekménytípus esetében van digitális eleme.** 2019-ben az incidensek éves száma a jelentések szerint megháromszorozódott. A becslések szerint a kibertámadások leggyakoribb módjának számító rosszindulatú szoftvereknek 700 millió új mintája létezik[15]. A kiberbűnözés a becslések szerint 2020-ban 5,5 billió EUR éves költséggel jár a globális gazdaság számára, és ez a 2015. évi költségek kétszerese[16]. Ez a gazdasági javak legnagyobb mértékű átadása, amely a globális kábítószer-kereskedelem során gazdát cserélő javak nagyságát is meghaladja. Egyetlen nagyobb esemény, a 2017-ben támadó WannaCry zsarolóvírus esetében a globális gazdaság költsége a becslések szerint meghaladta a 6,5 milliárd EUR-t[17].

**A digitális szolgáltatások és a pénzügyi ágazat a kibertámadások leggyakoribb célpontjai közé tartoznak a közszféra és a gyártás mellett, de a vállalkozások és egyének kiberfelkészültsége és kibertudatossága továbbra is alacsony[18], a munkaerő körében pedig a kiberbiztonsági készségek jelentős hiánya figyelhető meg**[19]. 2019-ben csaknem 450 olyan kiberbiztonsági eseményre került sor, amelyek európai kritikus infrastruktúrákat érintettek, így például a pénzügy és az energiaellátás területén[20]. A világjárvány során

[11] Eurostat sajtóközlemény, ICT security measures taken by vast majority of enterprises in the EU (Az uniós vállalkozások nagy többsége által hozott ikt-biztonsági intézkedések), 2020/6 – 2020. január 13. Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation (A kritikus infrastruktúrák elleni kibertámadások megszokottá válása olyan ágazatokban, mint az energiaügy, egészségügy és közlekedés); A Világgazdasági Fórum globális kockázatokról szóló, 2020. évi jelentése.

[12] Forrás: Comparitech.

[13] 2020. évi jelentés az adatvédelmi incidensek éves költségéről, Ponemon Institute, továbbá 524 közelmúltbeli, 17 földrajzi területen és 17 iparágban történt, az adatok megsértésével járó esemény mennyiségi elemzése alapján (https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf).

[14] A Közös Kutatóközpont (JRC) jelentése, Cybersecurity, our digital anchor (Kiberbiztonság – a digitális világunk alapja) (https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor).

[15] Forrás: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor (Kiberbiztonság – a digitális világunk alapja).

[17] Forrás: Cyence.

[18] A vállalatok, különösen a kkv-k, továbbra is kevéssé vannak tudatában, hogy az üzleti titkok kibertechnológiai módszerekkel ellophatók; PwC, Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018 (Tanulmány az ipari kémkedés és az üzleti titkok kibertechnológiával elkövetett lopásának mértékéről és hatásáról: Jelentés az üzleti titkok kibertechnológiával elkövetett lopásának kezelésére és megelőzésére irányuló intézkedésekről, 2018).

[19] Lásd az ENISA Threat Landscape 2020 (Fenyegetési környezet, 2020) jelentését. Lásd még az adatvédelmi incidensek ügyében folytatott vizsgálatokról szóló, a Verizon által készített 2020. évi jelentést (https://enterprise.verizon.com/resources/reports/dbir/).

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

különösen súlyosan érintettek az egészségügyi szervezetek és szakemberek. Ahogy a technológia és a fizikai világ egyre jobban összefonódik, a kibertámadások kockára teszik a legkiszolgáltatottabb népességcsoportok életét és jólétét[21]. A vállalkozások több mint kétharmada, különösen a kkv-k „újoncnak" számítanak a kiberbiztonság területén, és az európai vállalkozások felkészültsége alacsonyabbnak tekinthető, mint az ázsiai és amerikai vállalatoké[22]. A becslések szerint Európában 291 000 betöltetlen kiberbiztonsági álláshely van. A kiberbiztonsági szakértők felvétele és képzése lassú folyamat, amely nagyobb kiberbiztonsági kockázatokkal jár a szervezetek számára[23].

**Az EU nem rendelkezik kollektív helyzetismerettel a kiberfenyegetésekkel kapcsolatban.** Ennek az az oka, hogy a nemzeti hatóságok nem gyűjtenek és osztanak meg következetesen adatokat – például a magánszektorban elérhető adatokat –, amelyek segíthetnének felmérni az uniós kiberbiztonsági helyzetet. A tagállamok csak az események töredékét jelentik be, az információmegosztás se nem következetes, se nem átfogó[24], és a kibertámadások az európai társadalom elleni összehangolt rosszindulatú támadásoknak feltehetően csak egy részét képezik. A tagállamok között jelenleg korlátozott a kölcsönös operatív segítségnyújtás, illetve nem létezik a tagállamok és az uniós intézmények, ügynökségek és szervek közötti operatív mechanizmus a nagyszabású, határokon átnyúló kibereseményekvagy -válságok esetére[25].

**A kiberbiztonság javítása ezért elengedhetetlen egyrészt ahhoz, hogy az emberek bízzanak az innovációban, az összeköttetésben és az automatizálásban, illetve használják és előnyükre fordítsák őket, másrészt az alapvető jogok és szabadságok – beleértve a magánélethez való jogot, a személyes adatok védelmének jogát, valamint a véleménynyilvánítás szabadságát és az információszabadságot – védelméhez.** A kiberbiztonság nélkülözhetetlen a hálózati összeköttetéshez, illetve a globális és nyílt internethez, amelynek támogatnia kell a gazdaság és társadalom átalakulását a 2020-as években. Hozzájárul a jobb, több és rugalmasabb munkahelyhez, a hatékonyabb és fenntarthatóbb közlekedéshez és gazdálkodáshoz, valamint az egészségügyi szolgáltatásokhoz való egyszerűbb és méltányosabb hozzáféréshez. A kiberbiztonság az európai zöld megállapodás[26] értelmében a tisztább energiára való átállás szempontjából is elengedhetetlen a határokon átnyúló hálózatok és intelligens fogyasztásmérők révén, illetve az adattárolás szükségtelen megkettőzésének elkerülésével. Végezetül, a nemzetközi biztonság és stabilitás, valamint globálisan a gazdaságok, demokráciák és társadalmak fejlődéséhez is nélkülözhetetlen. A kormányoknak, vállalkozásoknak és egyéneknek ezért felelősen, a biztonságot szem előtt tartva kell használniuk a digitális eszközöket. A kiberbiztonsági tudatosságnak és higiéniának támogatnia kell a mindennapi tevékenységek digitális átalakítását.

[21] Zsarolóvírus segítségével vettek célba kórházakat és egészségügyi nyilvántartásokat például Romániában (2020. június), Düsseldorfban (2020. szeptember) és Vastaamóban (2020. október).

[22] PwC, The Global State of Information Security 2018 (Az információbiztonság globális helyzete, 2018); ESI Thoughtlab, The Cybersecurity Imperative, 2019.

[23] Európai Uniós Kiberbiztonsági Ügynökség, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees (A kiberbiztonsági készségek fejlesztése az EU-ban: a kiberbiztonsági diplomák tanúsítása) és az ENISA felsőoktatási adatbázisa, 2019. december.

[24] A tagállamoknak éves összefoglaló jelentést kell benyújtaniuk az együttműködési csoportnak a hálózati és információs rendszerek biztonságáról szóló irányelv (az (EU) 2016/1148 irányelv) 10. cikkének (3) bekezdése értelmében vett bejelentésekről.

[25] A CSIRT-ek hálózatának tagjai között kölcsönös segítségnyújtásra vonatkozó eljárási standardok vannak érvényben.

[26] Az európai zöld megállapodás (COM(2019) 640 final).

A digitális évtizedre vonatkozó új uniós kiberbiztonsági stratégia központi szerepet játszik az „Európa digitális jövőjének megtervezése” című közleményben[27], a Bizottság európai helyreállítási tervében[28], a biztonsági unióra vonatkozó, a 2020–2025 közötti időszakra szóló stratégiában[29], az uniós kül- és biztonságpolitikára vonatkozó globális stratégiában[30], valamint az Európai Tanács 2019–2024 közötti időszakra szóló stratégiai menetrendjében[31]. Meghatározza, hogyan fogja megvédeni az EU a lakóit, a vállalkozásokat és az intézményeket a kibertámadásoktól, hogyan fogja előmozdítani a nemzetközi együttműködést, illetve hogyan fog vezető szerepet játszani a globális és nyílt internet biztosításában.

## II. GLOBÁLIS GONDOLKODÁS, EURÓPAI CSELEKVÉS

Ez a stratégia úgy kívánja biztosítani a globális és nyílt internetet, hogy erős biztosítékok álljanak rendelkezésre az európaiak biztonságát, illetve alapvető jogait és szabadságait veszélyeztető kockázatok kezelésére. A korábbi stratégiák keretében elért eredmények alapján konkrét javaslatokat tartalmaz **három fő (szabályozási, beruházási és szakpolitikai) eszköz alkalmazására az uniós fellépés alábbi három területén: 1. reziliencia, technológiai szuverenitás és vezető szerep, 2. operatív kapacitásépítés a megelőzés, elrettentés és reagálás érdekében, és 3. a globális és nyílt kibertér előmozdítása**. Az EU elkötelezte magát e stratégia támogatása mellett, és **a következő hét évben soha nem látott mértékű uniós digitális átállási beruházásokat tervez** – lehetőség szerint megnégyszerezve az előző beruházások mértékét – az új technológiai és ipari szakpolitikák, illetve a helyreállítási menetrend részeként[32].

**A kiberbiztonságot ösztönzők, kötelezettségek és teljesítménymérő referenciaértékek használatával integrálni kell ezekbe a digitális beruházásokba, különös tekintettel olyan kulcsfontosságú technológiákra, mint a mesterséges intelligencia (MI), a titkosítás és a kvantum-számítástechnika.** Ez ösztönzőleg hathat az európai kiberbiztonsági ipar fejlődésére, és biztosíthatja a korábbi rendszerek fokozatos kivezetésének megkönnyítéséhez szükséges bizonyosságot. Az Európai Védelmi Alap (EDF) az európai védelmi technológiai és ipari bázis részeként támogatni fogja az európai kibervédelmi megoldásokat. A kiberbiztonság szerepet kap a partnereinket támogató külső finanszírozási eszközökben, mindenekelőtt a Szomszédsági, Fejlesztési és Nemzetközi Együttműködési Eszközben. A technológiákkal való visszaélések megakadályozása, a kritikus infrastruktúra védelme és az ellátási láncok integritásának biztosítása is lehetővé teszi, hogy az EU betartsa a felelős állami magatartásra vonatkozó ENSZ előírásokat, szabályokat és elveket[33].

---

[27] Európa digitális jövőjének megtervezése (COM(2020) 67 final).
[28] Európa nagy pillanata: helyreállítás és felkészülés – a jövő generációért (COM(2020) 98 final).
[29] A biztonsági unióra vonatkozó uniós stratégia (2020–2025) (COM(2020) 605 final).
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#
[32] A digitális technológia ellátási láncának egészébe történő, a digitális átálláshoz hozzájáruló vagy az abból fakadó kihívásokat kezelő beruházások a Helyreállítási és Rezilienciaépítési Eszköz keretében biztosított, vissza nem térítendő támogatásokból és hitelekből álló 672,5 milliárd EUR legalább 20 %-át (134,5 milliárd EUR) adják. A 2021–2027 közötti időszakra vonatkozó többéves pénzügyi keret tekintetében a Digitális Európa program keretében a kiberbiztonság, illetve a Horizont Európa keretében a kiberbiztonsági kutatás uniós finanszírozása, különös figyelmet fordítva a kkv-k támogatására, elérheti az összesen 2 milliárd EUR nagyságú összeget a tagállami és ipari beruházásokon felül.
[33] https://undocs.org/A/70/174

# 1. REZILIENCIA, TECHNOLÓGIAI SZUVERENITÁS ÉS VEZETŐ SZEREP

Az uniós kritikus infrastruktúra és az alapvető szolgáltatások egyre inkább egymásra vannak utalva és digitalizáltak. Az EU-ban valamennyi internetre csatlakoztatott eszköznek, legyen szó automatizált autókról, ipari ellenőrzési rendszerekről vagy háztartási készülékről, illetve az ezeket elérhetővé tevő ellátási láncoknak beépített jellemzőik révén biztonságosnak és a kibertámadásokkal szemben reziliensnek kell lenniük, és úgy kell megtervezni őket, hogy sebezhetőségek felfedezése esetén gyorsan javíthatók legyenek. Ez nélkülözhetetlen ahhoz, hogy az uniós köz- és magánszféra választhasson a legbiztonságosabb infrastruktúrák és szolgáltatások közül. A következő évtized lehetőséget kínál az EU-nak arra, hogy vezető szerepet játsszon a biztonságos technológiák kidolgozásában az ellátási lánc egészében. A reziliencia, valamint a fokozott kiberbiztonsági ipari és technológia kapacitás biztosítása során mozgósítani kell valamennyi szükséges szabályozási, beruházási és szakpolitikai eszközt. Az ipari folyamatok, műveletek és eszközök esetében a kiberbiztonsági szempontból való tervezés csökkentheti a kockázatokat, a vállalatok és a szélesebb társadalom költségeit, és ezáltal fokozhatja a rezilienciát.

## *1.1. reziliens infrastruktúra és kritikus szolgáltatások*

A **hálózati és információs rendszerek biztonságára vonatkozó** uniós **szabályok** a kiberbiztonsági egységes piac alapját képezik. A Bizottság az átdolgozott kiberbiztonsági irányelv keretében az említett szabályok megreformálását javasolja, hogy fokozza **valamennyi érintett, a gazdaság és a társadalom szempontjából fontos feladatot ellátó ágazat – legyen szó akár a magán-, akár a közszféráról – kiberrezilienciáját**[34]. A felülvizsgálat elengedhetetlen ahhoz, hogy az illetékes hatóságok hatáskörének, biztonsági és eseményjelentési követelményeinek, nemzeti felügyeletének, jogérvényesítésének és kapacitásának összehangolásával csökkenjen a következetlenség a belső piacon.

Az átdolgozott kiberbiztonsági irányelv alapozza meg a stratégiailag fontos ágazatok – beleértve az energiaügyet, közlekedést és egészségügyet – szempontjából is szükséges konkrétabb szabályokat. A biztonsági unióra vonatkozó 2020–2025. évi stratégia értelmében bejelentett következetes megközelítés biztosítása érdekében a javaslat az irányelv átdolgozása mellett a kritikus infrastruktúra rezilienciára vonatkozó jogszabályok felülvizsgálatát is tartalmazza[35]. Az alapvető szolgáltatások folytonossága, illetve a kritikus energetikai infrastruktúra stratégiai ellenőrzése szempontjából fontos szerepet játszanak a digitális összetevőket tartalmazó energetikai technológiák és a kapcsolódó ellátási láncok biztonsága. A Bizottság ezért 2022 végére elfogadandó intézkedéseket javasol, köztük a határokon átnyúló villamosenergia-áramlás kiberbiztonságára vonatkozó szabályokat meghatározó „hálózati szabályozást”. A Bizottság javaslatának megfelelően a pénzügyi ágazatnak is meg kell erősítenie a digitális operatív rezilienciát, és biztosítania kell az infokommunikációs zavarok és veszélyek valamennyi típusával szembeni rezilienciát[36]. A közlekedés terén a Bizottság a légi közlekedés védelméről szóló uniós jogszabályokat kibővítette kiberbiztonsági rendelkezésekkel[37], és valamennyi közlekedési mód vonatkozásában folytatja a kiberreziliencia fokozására irányuló erőfeszítéseit. A **demokratikus folyamatok és intézmények** kiberrezilienciájának megerősítése az Európai Demokráciára vonatkozó

[34] [*a kiberbiztonsági javaslatra való hivatkozás helye*].
[35] [a kritikus gazdálkodó egységek rezilienciájára vonatkozó *irányelvjavaslatra* történő hivatkozás helye].
[36] Rendeletjavaslat a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU és a 909/2014/EU rendelet módosításáról (COM(2020) 595 final).
[37] A Bizottság (EU) 2019/1583 végrehajtási rendelete.

cselekvési terv központi eleme a szabad választások, a demokratikus párbeszéd és a médiapluralizmus védelme és előmozdítása érdekében[38]. Végezetül, a jövőbeli űrprogram keretében az infrastruktúra és a szolgáltatások biztonsága tekintetében a Bizottság folytatni fogja a Galileo kiberbiztonsági stratégia elmélyítését a GNNS-szolgáltatások következő generációja és az űrprogram egyéb új elemeinek tekintetében[39].

### *1.2. Európai kiberpajzs létrehozása*

Az összekapcsoltság terjedése és az egyre kifinomultabb kibertámadások mellett az információmegosztó és -elemző központok fontos feladatot látnak el, többek között ágazati szinten, amikor lehetővé teszik több érdekelt fél között a kibertámadásokkal kapcsolatos információk megosztását[40]. Emellett a hálózati és számítógépes rendszerek folyamatos nyomon követést és elemzést igényelnek a behatolások és rendellenességek valós időben történő észlelése érdekében. Sok magánvállalkozás, állami szervezet és nemzeti hatóság ezért a számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT) és biztonsági műveleti központokat (SOC) hozott létre.

A biztonsági műveleti központok kulcsfontosságú szerepet játszanak az eseménynaplók összegyűjtésében[41] és az általuk megfigyelt kommunikációs hálózatokban bekövetkező gyanús események izolálásában. Ennek során azonosítják a jeleket és mintákat, és veszélyekkel kapcsolatos információkat nyernek ki a megvizsgálandó hatalmas adatmennyiségből. Hozzájárultak a rosszindulatú számítógépes programok tevékenységének észleléséhez, és segítettek megakadályozni a kibertámadásokat. Az ezekben a központokban szükséges munka nagyon megterhelő, és gyors munkatempót igényel, ezért a mesterséges intelligencia és különösen a gépi tanulási technikák felbecsülhetetlen segítséget nyújthatnak a szakembereknek[42].

A Bizottság javasolja a **biztonsági műveleti központok uniós hálózatának[43]** kiépítését, valamint a meglévő központok fejlesztésének és új központok létrehozásának támogatását. Emellett támogatni fogja az ezekben a központokban dolgozók képzését és készségeinek fejlesztését. Az érintett érdekelt felekkel, illetve az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) támogatásával folytatott igényelemzés alapján több mint 300 millió EUR nagyságú összeggel támogathatja a nemzeti és ágazati hálózatok létrehozására irányuló magán- és állami, valamint határokon átnyúló együttműködést,

[38] Közlemény az Európai Demokráciára vonatkozó cselekvési tervről (COM(2020) 790). A terv értelmében a tagállami választási hálózatokból álló európai választási együttműködési hálózat támogatni fogja a közös szakértői csoportok alkalmazását a választási folyamatokat veszélyeztető tényezők, köztük a kiberfenyegetések elhárítása érdekében (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en).

[39] Idetartozik a kormányzati műholdas kommunikációs rendszerre irányuló új kezdeményezés (GOVSATCOM) és az űrhulladékkal kapcsolatos kezdeményezés (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[41] Oly módon, hogy a bűnüldözés és az igazságszolgáltatás bizonyítékként használhassa őket.

[42] Forrás: a Ponemon Institute Research felmérése, Improving the Effectiveness of the SOC, 2019 (A SOC hatékonyságának javítása, 2019); a biztonsági műveleti központokban alkalmazott mesterséges intelligenciáról szóló tanulmányokhoz lásd például az alábbi dokumentumot: Khraisat, A., Gondal, I., Vamplew, P. *et al.* Survey of intrusion detection systems: techniques, datasets and challenges (A behatolások észlelésére szolgáló rendszerek felmérése: technikák, adatok és kihívások), *Cybersecur* 2**,** 20 (2019).

[43] Kidolgozásra vár az ilyen központok irányítására, működési elveire és finanszírozására vonatkozó részletes mechanizmus, illetve annak meghatározása, hogyan fogják kiegészíteni a meglévő struktúrákat, például a digitális innovációs központokat.

beleértve a kkv-ket is, az irányításra, az adatok megosztására és a biztonságra vonatkozó megfelelő rendelkezések alapján.

A tagállamok számára ajánlott társfinanszírozóként részt venni ebben a projektben. A központok így hatékonyabban tudnák megosztani és értelmezni az észlelt jeleket, és a fenyegetésekkel kapcsolatban az információmegosztó és -elemző központokkal, illetve a nemzeti hatóságokkal megosztandó jó minőségű információkat tudnánk előállítani, lehetővé téve ezzel a jobb helyzetismeretet. A cél az, hogy szakaszosan a lehető legtöbb központ csatlakozzon az EU-ban a kollektív ismeretek létrehozása és a bevált gyakorlatok megosztása érdekében. Ezek a központok támogatást fognak kapni az incidensek hatékonyabb észlelése és elemzése, illetve a gyorsabb reagálás érdekében a legmodernebb mesterséges intelligenciák és gépi tanulási képességek révén, amelyet az európai nagy teljesítményű számítástechnika közös vállalkozás által az EU-ban kifejlesztett szuper-számítástechnikai infrastruktúra egészít ki[44].

Ez a hálózat a folyamatos együttműködés révén időben figyelmeztetni tudja a hatóságokat és valamennyi érdekelt felet, beleértve a közös kiberbiztonsági egységet (lásd a 2.1. szakaszt) a kiberbiztonsági eseményekre. **Valódi kiberbiztonsági pajzsként fog szolgálni az EU számára** az őrtornyok szilárd hálózatával, amely még azelőtt képes észlelni a lehetséges fenyegetéseket, hogy azok nagyobb kárt okozhatnának.

### *1.3. Ultrabiztonságos kommunikációs infrastruktúra*

Az űrprogram részét képező uniós kormányzati műholdas kommunikációs rendszer[45] biztonságos és költséghatékony űralapú kommunikációs lehetőséget kínál az EU és tagállamai – beleértve a nemzeti biztonsági szereplőket, valamint az uniós intézményeket, szerveket és ügynökségeket – által irányított, a biztonság és védelem szempontjából kritikus küldetések és műveletek biztosításához.

A tagállamok elkötelezték magukat a Bizottsággal való együttműködés mellett a biztonságos kvantumkommunikációs infrastruktúra (QCI) európai alkalmazása terén[46]. A kvantumkommunikációs infrastruktúra teljesen új megoldást kínál a hatóságoknak a bizalmas információk ultrabiztos, európai technológiával készült, a kibertámadások ellen védelmet biztosító titkosítással történő átvitelére. Két fő részből fog állni: egyrészt a meglévő, a stratégiai helyszíneket nemzeti és határokon átnyúló szinten összekötő szárazföldi száloptikás kommunikációs hálózatokból, másrészt az egész EU-t – beleértve a tengeren túli területeit – lefedő összekapcsolt műholdakból[47]. Az új és biztonságosabb titkosítási módok

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

[45] A GOVSATCOM az Unió űrprogramjának része.

[46] Az EuroQCI nyilatkozatot a legtöbb tagállam aláírta, és a fejlesztésre, illetve az infrastruktúra alkalmazására 2021–2027 között kerül sor a Horizont Európa, a Digitális Európa és az Európai Űrügynökség finanszírozásával, a megfelelő irányítási megállapodások függvényében (https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network).

[47] Az űrkomponens kifejlesztése elengedhetetlen a hosszú távú (> 1000 km) pont-pont összeköttetésekhez, amelyeket a földi infrastruktúra nem képes támogatni. A kvantummechanika jellemzőinek hasznosításával a kvantumkommunikációs infrastruktúra kezdetben lehetővé fogja tenni a felek számára az üzenetek titkosításához és visszafejtéséhez használandó véletlenszerű titkos kulcsok biztonságos megosztását. Emellett magában foglalja a vizsgálati és megfelelőségi infrastruktúra használatát egyrészt annak felmérésére, hogy az európai kvantumkommunikációs eszközök és rendszerek mennyire felelnek meg a kvantumkommunikációs infrastruktúrának, másrészt ezek tanúsításának és hitelesítésének értékelésére a kvantumkommunikációs infrastruktúrába való integrációjukat megelőzően. Úgy kerül kialakításra, hogy a szükséges technológiai

kidolgozására és alkalmazására, valamint a kritikus kommunikáció és adateszközök megvédésére szolgáló új módszerek kidolgozására irányuló kezdeményezés segíthet az érzékeny információk és ezáltal a kritikus infrastruktúrák védelmének biztosításában.

Ebben a tekintetben, illetve a jövőre nézve, a Bizottság meg fogja vizsgálni a multiorbitális biztonságos összeköttetési rendszer lehetséges alkalmazását. A GOVSATCOM-ra és a kvantumkommunikációs infrastruktúrára építve, a legszigorúbb kiberbiztonsági kereten belül a Bizottság integrálni fogja a legújabb technológiákat (kvantum, 5G, MI, pereminformatika), hogy támogassa az olyan, a tervezésből kifolyólag biztonságos szolgáltatásokat, mint például a megbízható, biztonságos és költséghatékony összeköttetés, illetve a kritikus kormányzati tevékenységekkel kapcsolatos titkosított kommunikáció.

### *1.4. A következő generációs széles sávú mobilhálózatok biztonságának biztosítása*

Az **5G hálózatok és a hálózatok jövőbeli generációi** által lehetővé tett fejlett és innovatív alkalmazásokat használó uniós állampolgárok és vállalatok számára biztosítani kell a legmagasabb biztonsági szabvány előnyeit. A tagállamok – a Bizottsággal együtt, illetve az ENISA támogatásával – a 2020. januári 5G uniós eszköztárral[48] az 5G kiberbiztonság olyan átfogó és objektív, kockázatalapú megközelítését dolgozták ki, amely a lehetséges kockázatcsökkentési tervek értékelésén és a leghatékonyabb intézkedések azonosításán alapul. Az EU továbbá megerősíti az 5G-vel és a későbbi hálózatokkal kapcsolatos kapacitását, hogy elkerülje a függőséget, illetve előmozdítsa a fenntartható és sokrétű ellátási láncot.

2020 decemberében a Bizottság jelentést tett közzé az 5G hálózatok kiberbiztonságáról szóló, 2019. március 26-i bizottsági ajánlás hatásairól[49]. A jelentés arról tanúskodik, hogy az eszköztár elfogadása óta jelentős előrelépésre került sor, és a legtöbb tagállam jó úton halad afelé, hogy a közeljövőben az eszköztár nagy részét alkalmazza, bár ahogy a 2020 júliusában közzétett eredményjelentésben már szerepel, eltérésekre került sor, és egyes hiányosságok megszüntetése még nem történt meg[50].

2020 októberében az Európai Tanács felszólította az EU-t és a tagállamokat, hogy a legnagyobb mértékben alkalmazzák az 5G kiberbiztonsági eszköztárat, és a közös objektív kritériumok alapján az uniós koordinált kockázatértékelésben kritikusként és érzékenyként azonosított legfontosabb eszközök vonatkozásában alkalmazzák a nagy kockázatnak kitett beszállítókra vonatkozó releváns korlátozásokat[51].

A jövőre nézve az EU-nak és tagállamainak biztosítaniuk kell egyrészt az azonosított kockázatok megfelelő és koordinált csökkentését – különös tekintettel a nagy kockázatnak kitett beszállítóknak való kitettség minimalizálására, illetve az ilyen beszállítóktól való nemzeti és uniós szintű függés elkerülésére vonatkozó célkitűzésre –, másrészt az új jelentős fejlemények vagy kockázatok figyelembevételét. A tagállamok felkérést kaptak, hogy a

érettségi szint elérésével további alkalmazásokat is támogasson. A jelenlegi OpenQKD kísérleti projekt (https://openqkd.eu/) e vizsgálati és megfelelőségi infrastruktúra előfutára.

[48] Közlemény – Az 5G biztonságos kiépítése az EU-ban – Az uniós eszköztár alkalmazása (COM(2020) 50).

[49] A Bizottság jelentése az 5G hálózatok kiberbiztonságáról szóló, 2019. március 26-i bizottsági ajánlás hatásairól, 2020. december 15.

[50] A kiberbiztonsági együttműködési csoport 2020. július 24-i jelentése az eszköztár végrehajtásáról.

[51] EUCO 13/20, Az Európai Tanács rendkívüli ülése (2020. október 1–2.) – Következtetések.

digitális kapacitásba és az összeköttetésbe való beruházásaik során a legteljesebb mértékben használják az eszköztárat.

A 2019. évi ajánlás hatásairól szóló jelentés alapján a Bizottság arra ösztönzi a tagállamokat, hogy gyorsítsák fel az eszköztár főbb intézkedéseinek 2021 második negyedévére történő végrehajtására irányuló erőfeszítéseket. Arra is felszólította a tagállamokat, hogy folytassák az előrehaladás közös nyomon követését és a megközelítések további összehangolásának biztosítását. Uniós szinten három fő célkitűzés támogatja ezt a folyamatot: a kockázatcsökkentési megközelítések további uniós közelítésének biztosítása, a folyamatos ismeretcsere és kapacitásépítés támogatása, valamint a reziliens ellátási láncok és egyéb uniós stratégiai biztonsági célkitűzések előmozdítása. E közlemény erre a célra szolgáló függeléke konkrét cselekvéseket tartalmaz az említett fő célkitűzések elérésével kapcsolatban.

A Bizottság az ENISA támogatásával továbbra is szorosan együttműködik a tagállamokkal a célkitűzések elérése és a cselekvések megvalósítása érdekében (lásd a mellékletet).

Az EU 5G eszköztárral kapcsolatos megközelítése emellett olyan nem uniós országok érdeklődését is felkeltette, amelyek jelenleg dolgozzák ki a kommunikációs hálózataik biztosítására vonatkozó megközelítéseiket. A Bizottság szervezeti egységei az Európai Külügyi Szolgálattal és az uniós küldöttségek hálózatával együtt készen állnak arra, hogy átfogó, objektív és kockázatalapú megközelítésükről szükség esetén további információkat nyújtsanak a hatóságoknak világszerte.

### *1.5. A biztonságos dolgok internete*

Minden csatlakoztatott dolognak vannak gyenge pontjai, amelyek kijátszása potenciálisan széles körű következményekkel jár. A belső piaci szabályok biztosítékokat tartalmaznak a nem biztonságos termékekkel és szolgáltatásokkal szemben. A Bizottság már dolgozik azon, hogy **a kiberbiztonsági jogszabály értelmében átlátható biztonsági megoldásokat és tanúsítást** kínáljon, illetve a teljesítmény romlása nélkül előmozdítsa a biztonságos termékeket és szolgáltatásokat[52]. 2021 első negyedévében fogadja el az első uniós gördülő munkaprogramját (amelyet azután legalább háromévente aktualizál), hogy lehetővé tegye az ipar, a nemzeti hatóságok és a szabványügyi testületek számára, hogy időben felkészüljenek a jövőbeli európai kiberbiztonsági tanúsítási rendszerekre[53]. Ahogy a dolgok internete bővül, az érvényesíthető szabályokhoz szigorításra van szükség az általános reziliencia biztosítása és a kiberbiztonság fokozása érdekében egyaránt.

A Bizottság meg fogja vizsgálni egy átfogó megközelítés lehetőségét, beleértve a lehetséges **új horizontális szabályokat a belső piacon forgalomba hozott valamennyi csatlakoztatott**

[52] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (Európai Uniós Kiberbiztonsági Ügynökség), valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról és az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). A kiberbiztonsági jogszabály támogatja az uniós szintű ikt-tanúsítást az európai kiberbiztonsági tanúsítási keretrendszerrel az önkéntes európai kiberbiztonsági tanúsítási rendszerek létrehozása érdekében az ikt-termékek, az ikt-szolgáltatások és az ikt-folyamatok megfelelő kiberbiztonsági szintjének az Unióban történő biztosítása céljából, valamint abból a célból, hogy csökkentse a belső piac széttagoltságát az Unión belüli kiberbiztonsági tanúsítási rendszerek tekintetében. Ezzel párhuzamosan a kiberbiztonsági „osztályozással” foglalkozó vállalatok székhelye általában az EU-n kívül található, korlátozott átláthatóság és felügyelet mellett (https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings).

[53] A kiberbiztonsági jogszabály 47. cikkének (5) bekezdése értelmében.

**termék és a kapcsolódó szolgáltatások kiberbiztonságának javítása érdekében**[54]. Az ilyen szabályok magukban foglalhatják **a csatlakoztatott eszközök gyártóira vonatkozó új gondossági kötelezettséget**, hogy megszüntessék a szoftverek sebezhetőségét, ideértve a szoftverek további használatát és a biztonsági frissítéseket, valamint az eszközök élettartamának végén a személyes és egyéb érzékeny adatok törlésének biztosítását. Ezek a szabályok előmozdítanák az elavult szoftverek frissítéséhez való jogra vonatkozó, a körforgásos gazdaságról szóló cselekvési tervben szereplő kezdeményezést, és kiegészítenék a konkrét terméktípusokra vonatkozóan folyamatban levő olyan intézkedéseket, mint például az egyes vezeték nélküli termékek piacra jutása tekintetében javasolandó kötelező követelmények (a rádióberendezésekre vonatkozó irányelv[55] értelmében vett felhatalmazáson alapuló jogi aktus elfogadásával) és 2022 júliusától valamennyi új járműtípus esetében a gépjárművekre vonatkozó kiberbiztonsági szabályok végrehajtására vonatkozó célkitűzés[56]. Emellett a kiberbiztonsági szempontokkal közvetlenül nem foglalkozó általános termékbiztonsági szabályok javasolt átdolgozásán alapulnának[57].

### *1.6. Nagyobb globális internetes biztonság*

Számos alapvető protokoll és támogató infrastruktúra biztosítja világszerte az internet működését és integritását[58]. Idetartozik a DNS és annak hierarchikus és delegált zónarendszere, amely a hierarchia legfelső szintjén a világháló alapját képező gyökérzónával és 13 DNS gyökérszerverrel[59] kezdődik. A Bizottság **– uniós finanszírozással – vészhelyzeti tervet kíván kidolgozni, amely a globális DNS gyökérrendszer integritását és elérhetőségét befolyásoló szélsőséges forgatókönyvekkel foglalkozik**. Az ENISA-val, a tagállamokkal, a két uniós DNS gyökérszerver üzemeltetőjével[60] és a több érdekelt felet tömörítő közösséggel együttműködve értékelni fogja az említett üzemeltetők szerepét annak biztosításában, hogy az internet minden körülmények között világszerte elérhető maradjon.

Ahhoz, hogy egy ügyfél elérjen egy adott doménnéven található erőforrást az interneten, a(z) (általában egy egységes erőforrás-helymeghatározó, vagyis URL iránti) lekérdezést IP-címmé kell alakítani, vagyis „fel kell oldani” a DNS névszerverekre való hivatkozással. Az EU-ban azonban az emberek és a szervezetek egyre inkább csak néhány publikus DNS címfeloldótól függnek, amelyeket nem uniós gazdálkodó egységek üzemeltetnek. A DNS címfeloldás

[54] A Tanács következtetései horizontális intézkedésekre szólítanak fel a csatlakoztatott eszközök kiberbiztonságával kapcsolatban; 13629/20, 2020. december 2.
[55] A 2014/53/EU irányelv.
[56] A 2020 júniusában elfogadott ENSZ-előírást követi http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
[57] A jelenlegi általános termékbiztonsági szabályok (a 2001/95/EK irányelv) átdolgozása; emellett olyan javasolt módosított szabályok is tervben vannak, amelyek a gyártók felelősségére vonatkoznak digitális kontextusban az uniós felelősségi keretszabályozás hatályán belül.
[58] „A nyílt internet nyilvános alkotóelemei – nevezetesen a főbb protokolljai és infrastruktúrája, amelyek globális közjavak – biztosítják az internet egészének alapvető funkcióit és támogatják annak normál működését. Az ENISA-nak támogatnia kell az internet nyilvános alapelemei, többek között, de nem kizárólag a kulcsfontosságú protokollok (különösen a DNS, a BGP és az IPv6) biztonságos és stabil működését, a doménnévrendszer működését (például az összes legfelső szintű domain működését), valamint a gyökérzóna működését” (a kiberbiztonsági jogszabály (23) preambulumbekezdése).
[59] https://www.iana.org/domains/root/servers
[60] A Netnod által Svédországban üzemeltetett i.root-servers és a RIPE NCC által Hollandiában üzemeltetett k.root-servers.

néhány vállalatnál összpontosul[61], ami sebezhetővé teszi a feloldási folyamatot a valamely főbb szolgáltatót érintő jelentős események esetében, és megnehezíti az uniós hatóságok számára a lehetséges rosszindulatú kibertámadások, illetve a nagyobb geopolitikai és műszaki incidensek kezelését[62].

A piaci koncentrációval kapcsolatos biztonsági problémák csökkentésére való tekintettel a Bizottság arra fogja ösztönözni az érintett érdekelt feleket, köztük az uniós vállalatokat, internetszolgáltatókat és böngészőszolgáltatókat, hogy fogadjanak el stratégiát a DNS címfeloldás diverzifikálására. A Bizottság emellett hozzá kíván járulni ahhoz, hogy egy nyilvános **európai DNS címfeloldási szolgáltatás** kidolgozásának támogatásával gondoskodjon a biztonságos internetes összeköttetésről. A DNS4EU kezdeményezés alternatív, európai szolgáltatást fog kínálni a globális internet elérésére. A DNS4EU átlátható lesz, megfelel a legújabb biztonsági és adatvédelmi szabványoknak és szabályoknak, valamint a magánélet védelmére vonatkozó beépített, illetve alapértelmezett szabványoknak és szabályoknak, és az Európai Ipariadat- és Számításifelhő-szövetség[63] részét fogja képezni.

A Bizottság emellett – a tagállamokkal és az iparral együtt – **fel fogja gyorsítani a legfontosabb internetes szabványok, köztük az IPv6[64], illetve a DNS-re, az útválasztásra és az e-mailek biztonságára vonatkozó, jól működő internetes biztonsági szabványok és bevált gyakorlatok elterjesztését[65]**, nem zárva ki olyan, a piac irányítását szolgáló szabályozási intézkedéseket sem, mint az IPv4 hatályvesztésére vonatkozó európai rendelkezés, ha nem történik megfelelő előrehaladás e téren. Az EU (például az Afrikára vonatkozó uniós stratégia[66] keretében) elő fogja mozdítani az ilyen szabványok alkalmazását a partnerországokban, hogy támogassa a globális és nyílt internet fejlődését, és ellensúlyozza a zárt, ellenőrzésalapú internetmodelleket. Végezetül a Bizottság mérlegelni fogja az internetes forgalommal kapcsolatos összesített adatok következetesebb nyomon követésére és összegyűjtésére, valamint a lehetséges zavarokkal kapcsolatos tanácsadásra szolgáló mechanizmus szükségességét[67].

### *1.7. Megerősített jelenlét a technológiai ellátási láncban*

A 2021–2027 közötti többéves pénzügyi keretben a kiberbiztonságos digitális átalakulás tervezett pénzügyi támogatásával az EU egyedülálló lehetőséget kapott arra, hogy az

[61] Consolidation in the DNS resolver market – how much, how fast how dangerous? (A DNS címfeloldási piac koncentrációja – milyen mértékű, milyen gyors, milyen veszélyes?) Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services (Az internetes entrópia csökkenésének bizonyítéka – a redundancia hiánya a főbb honlapok és szolgáltatások általi DNS címfeloldásban).

[62] Arra utaló bizonyítékok is vannak, hogy a DNS adatok profilalkotási célokra is használhatók, ami hatással van a magánélethez és az adatok védelméhez való jogra.

[63] Joint Declaration: Building the next generation cloud for businesses and the public sector in the EU (Együttes nyilatkozat: A következő generációs felhő kiépítése az uniós vállalkozások és magánszektor számára) (https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe).

[64] Az IPv6 protokoll az IPv4 címek terén mutatkozó súlyos ellátási hiány és a költségek emelkedése miatt mára jobban teret hódított, elterjedtsége azonban nem egyenletes az EU-n belül.

[65] Az ilyen szabványok közé tartoznak a DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE, valamint olyan útválasztási előírások és bevált gyakorlatok, mint az útválasztási biztonságra vonatkozóan közösen elfogadott előírások (MANRS).

[66] Közös közlemény – Az Afrikával kapcsolatos átfogó stratégia felé, 2020.3.9. (JOIN(2020) 4 final).

[67] Egy ilyen „internet-megfigyelőközpont” az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont tevékenységi körébe tartozhat; az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló rendeletjavaslat (COM(2018) 630 final).

eszközeit összegyűjtve előmozdítsa ipari stratégiáját[68] és vezető szerepét a digitális technológiák és a kiberbiztonság terén a digitális ellátási láncban (beleértve az adatokat és a felhőt, a következő generációs processzortechnológiákat, az ultrabiztonságos összeköttetést és a 6G hálózatokat) az értékeinek és prioritásainak megfelelően. A közszféra beavatkozásának az uniós közbeszerzési keretszabályozás és a közös európai érdeket szolgáló fontos projektek által biztosított eszközökön kell alapulnia. Ezen túlmenően magánberuházásokat tehet lehetővé a köz- és magánszféra közötti partnerségeken keresztül (többek között a szerződéses kiberbiztonsági köz-magán társulás tapasztalataira és annak az Európai Kiberbiztonsági Szervezet révén történő végrehajtására építve), illetve a kkv-ket vagy az ipari szövetségeket támogató kockázati tőke és a technológiai kapacitásokra vonatkozó stratégiák révén.

Emellett kiemelt figyelmet fog kapni a technikai támogatási eszköz[69], illetve az, hogy a kkv-k – különösen azok, amelyek nem tartoznak az átdolgozott kiberbiztonsági irányelv hatálya alá – a leghatékonyabban használják a legújabb kiberbiztonsági eszközöket, többek között a Digitális Európa program keretében a digitális innovációs központok releváns tevékenységei révén. A cél az, hogy a tagállamok hasonló mértékű beruházásokat tegyenek, amelyet az ipar is kiegészít ugyanilyen mértékű beruházásokkal a tagállamokkal közösen irányított partnerség keretében a javasolt **Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontban és a koordinációs központok hálózatában (CCCN)**. A CCCN kulcsfontosságú szerepet fog játszani az ipari és tudományos közösségek hozzájárulásával az uniós kiberbiztonsági technológiai szuverenitás megteremtésében, az olyan érzékeny infrastruktúrák biztosítására szolgáló kapacitásépítésben, mint az 5G, továbbá a világ más részein a legfontosabb technológiák iránti függőség csökkentésében.

A Bizottság – potenciálisan a CCCN-nel együtt – támogatni kívánja egy kiberbiztonsági mesterképzési program kidolgozását, és hozzá kíván járulni a 2020 utáni időszakra vonatkozó közös európai kiberbiztonsági kutatási és innovációs menetrendhez. A CCCN-en keresztüli beruházások emellett a kiberbiztonsági kiválósági központok hálózatai közötti kutatási-fejlesztési együttműködésre építenének, összehozva Európa legjobb kutatócsoportjait az iparral a közös kutatási menetrendek kidolgozása és végrehajtása érdekében, az Európai Kiberbiztonsági Szervezet ütemtervének megfelelően[70]. A Bizottság továbbra is az ENISA és az Europol kutatómunkájára épít, és – a Horizont Európa keretében – továbbra is támogatja, hogy az egyéni internetes innovátorok a magánéletet megillető védelmet megerősítő és biztonságos kommunikációs technológiákat dolgozzanak ki nyílt forrású szoftverek és hardverek alapján, ahogy jelenleg is teszi az Újgenerációs Internet kezdeményezés keretében.

### *1.8. Kiberkészségekkel rendelkező uniós munkaerő*

A munkaerő készségeinek fejlesztésére, a legjobb kiberbiztonsági tehetségek kibontakozására, vonzására és megtartására, valamint a világszínvonalú kutatásba és innovációba való beruházásokra irányuló uniós erőfeszítések a kiberfenyegetésekkel szembeni általános védelem fontos részét képezik. Ez a terület nagy lehetőségeket kínál. Különös figyelmet kell fordítani a sokoldalúbb tehetségek vonzására és megtartására. Az átdolgozott digitális oktatási cselekvési terv fokozni fogja az egyének, különösen a gyermekek és a fiatalok, valamint a szervezetek, elsősorban a kkv-k kiberbiztonsági

[68] Közlemény – Új európai iparstratégia (COM(2020) 102 final).
[69] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0409:FIN
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies

tudatosságát[71]. Emellett elő fogja mozdítani a nők részvételét a tudományban, technológiában, mérnöki tudományokban, matematikában, oktatásban és ikt-munkákban, valamint a digitális készségek át- és továbbképzésében. Ezenfelül a Bizottság az Europol keretébe működő EUIPO (az Európai Unió Szellemi Tulajdoni Hivatala), az ENISA, a tagállamok és a magánszektor közreműködésével figyelemfelkeltő eszközöket és iránymutatást fog kidolgozni, hogy növelje az uniós vállalkozások rezilienciáját **a szellemi tulajdon kibertechnológiával elkövetett lopásával szemben**[72].

Az oktatásnak, beleértve a szakképzést, a tudatosságot és a gyakorlatokat, szintén tovább kell fokoznia az uniós szintű kiberbiztonságot és fejlesztenie kell a kibervédelmi készségeket. Ennek érdekében a releváns uniós szereplők, például az ENISA, az Európai Védelmi Ügynökség (EDA), valamint az Európai Biztonsági és Védelmi Főiskola (ESDC)[73] szinergiákra törekszik a tevékenységei között.

***Stratégiai kezdeményezések***

Az EU-nak biztosítania kell az alábbiakat:

- az átdolgozott kiberbiztonsági irányelv elfogadása;
- a biztonságos dolgok internetére vonatkozó szabályozási intézkedések;
- a kiberbiztonsági CCCN beruházások (mindenekelőtt a Digitális Európa program, a Horizont Európa és a helyreállítási eszköz) révén akár 4,5 milliárd EUR összegű állami és magánberuházás 2021–2027 között;
- a mesterséges intelligenciát használó biztonsági műveleti központok uniós hálózata és a kvantumtechnológiákon alapuló ultrabiztonságos kommunikációs infrastruktúra;
- a kiberbiztonsági technológiák széles körű elfogadása a kkv-knak nyújtott támogatás révén a digitális innovációs központok keretében;
- az uniós DNS címfeloldási szolgáltatás kifejlesztése, amely biztonságos és nyílt alternatívát kínál az uniós polgároknak, vállalkozásoknak és közigazgatásoknak az internet-hozzáférésre; és
- az 5G eszköztár végrehajtásának befejezése 2021 második negyedévére (lásd a mellékletet).

## 2. OPERATÍV KAPACITÁSÉPÍTÉS A MEGELŐZÉS, ELRETTENTÉS ÉS REAGÁLÁS ÉRDEKÉBEN

A kiberbiztonsági események, függetlenül attól, hogy bűnözők, állami vagy egyéb nem állami szereplők véletlenül vagy szándékosan idézik elő őket, óriási károkat okozhatnak. A nagyságuk és összetettségük miatt – gyakran harmadik fél szolgáltatások, hardverek és szoftverek alkalmazásával érik el végső céljukat – az uniós kollektív fenyegetési környezet nehezen kezelhető az információk következetes és átfogó megosztása és a közös reagálásra irányuló együttműködés nélkül. Az EU arra törekszik, hogy **a szabályozási eszközök, a**

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[72] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2187
[73] A kiberoktatással, -képzéssel, -értékeléssel és -gyakorlattal kapcsolatos platformon (ETEE).

**mozgósítás és az együttműködés teljes körű alkalmazásával** támogassa a tagállamokat a polgáraik, valamint a gazdasági és nemzetbiztonsági érdekeik megvédésében, maradéktalanul tiszteletben tartva az alapvető jogokat és szabadságokat, valamint a jogállamiságot. Számos, hálózatokból, uniós intézményekből, szervekből és ügynökségekből, valamint tagállami hatóságokból álló közösség feladata a kiberfenyegetések megakadályozása, visszaszorítása, a kiberfenyegetésektől való elrettentés és a kiberfenyegetésekre való reagálás az eszközeik és kezdeményezéseik alkalmazásával[74]. E közösségek közé tartoznak i. a kiberbiztonsági hatóságok, például a CSIRT-ek, illetve a katasztrófareagálás, ii. a bűnüldöző és igazságügyi hatóságok, iii. a kiberdiplomácia, illetve iv. a kibervédelem.

### *2.1. Közös kiberbiztonsági egység*

A közös kiberbiztonsági egység a különböző uniós kiberbiztonsági közösségek együttműködésére szolgáló virtuális és fizikai platform lenne, amely a főbb, határokon átnyúló kiberbiztonsági események és fenyegetések elleni küzdelemre szolgáló operatív és technikai együttműködésre összpontosít.

A közös kiberbiztonsági egység fontos lépés lenne az **európai kiberbiztonsági válságreagálási keret** megteremtése felé. Ahogy a Bizottság elnökének politikai iránymutatásában[75] szerepel, az egységnek lehetővé kell tennie a tagállamok, valamint az uniós intézmények, szervek és ügynökségek számára a meglévő struktúrák, erőforrások és kapacitások teljes körű kihasználását, és **a megosztás szükségességére** vonatkozó szemlélet előmozdítását. Biztosítaná az eszközöket a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló 2017. évi ajánlás („tervezet”) megvalósítása terén eddig elért haladás megszilárdításához[76]. Emellett lehetőséget nyújtana a tervezet architektúrájával kapcsolatos együttműködés további megerősítésére, illetve a különösen a kiberbiztonsági együttműködési csoportban és a CyCLONe hálózatban elért eredmények felhasználására.

Ezzel kezelhető lenne **két nagy hiányosság**, amely jelenleg fokozza a sebezhetőséget és csökkenti az Uniót érintő, határokon átnyúló fenyegetésekre és eseményekre adott válaszok hatékonyságát. Először, a polgári, diplomáciai, bűnüldözési és védelmi kiberbiztonsági **közösségek** még nem rendelkeznek olyan közös térrel, ahol strukturált együttműködést folytathatnának, és elősegíthetnék az operatív és technikai együttműködést. Másodszor, a releváns kiberbiztonsági érdekelt felek még nem tudták teljes mértékben kihasználni a meglévő hálózatokon és közösségeken belül az operatív együttműködésben és a kölcsönös segítségnyújtásban rejlő **lehetőségeket**. Idetartozik, hogy nincs olyan platform, amely lehetővé tenné a magánszektorbeli operatív együttműködést. Az egységnek javítania kellene

[74] Beleértve az operatív együttműködés és a válságkezelés terén az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) által biztosított támogatást, a CSIRT-ek hálózatát, a CyCLONe (Cyber Crises Liaison Organisation Network) hálózatot (az átdolgozott kiberbiztonsági irányelvre vonatkozó javaslat értelmében EU-CyCLONe), a kiberbiztonsági együttműködési csoportot; a rescEU-t, a Kiberbűnözés Elleni Európai Központot, az Europolon belül működő, a kiberbűnözéssel foglalkozó közös akciócsoportot és a bűnüldözési vészhelyzet-elhárítási protokollt, az Európai Unió Helyzetelemző Központját (EU INTCEN) és a kiberdiplomáciai eszköztárat, az egységes információelemzési kapacitást (SIAC), az állandó strukturált együttműködés (PESCO) keretében a kiberbiztonsági projekteket, mindenekelőtt a „Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén” projektet.

[75] Ambiciózusabb Unió: Programom Európa számára, Politikai iránymutatás a hivatalba lépő következő Európai Bizottság számára (2019–2024). Előterjesztette: Ursula von der Leyen, európai bizottsági elnökjelölt.

[76] Ajánlástervezet (C(2017) 6100 final, 2017.9.13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról.

és fel kellene gyorsítania az együttműködést, és lehetővé kellene tennie az EU számára a nagyszabású kiberbiztonsági eseményekre és válságokra való reagálást.

A közös kiberbiztonsági egység nem további, önálló szerv lenne, és a nemzeti kiberbiztonsági hatóságok vagy az uniós résztvevők illetékességét és hatáskörét sem érintené. Az egység inkább olyan védőhálóként működne, amelyben a résztvevők számíthatnának a többi résztvevő támogatására és szakértelmére, különösen akkor, ha különböző kiberbiztonsági közösségeknek kell szorosan együttműködniük. Ugyanakkor a legújabb események azt mutatják, hogy az EU-nak fokoznia kell célkitűzései szintjét és készültségét a kiberfenyegetési környezet kezelése érdekében. A közös kiberbiztonsági egységhez való hozzájárulásuk részeként az uniós szereplők (a Bizottság, illetve az uniós ügynökségek és szervek) ezért készek lesznek jelentősen növelni erőforrásaikat és kapacitásukat, hogy fokozzák készültségüket és rezilienciájukat.

A közös kiberbiztonsági egység három fő célt szolgálna. Először, biztosítaná a kiberbiztonsági közösségek **felkészültségét**, másodszor, az információmegosztás révén biztosítaná a folyamatos megosztott **helyzetismeretet**, harmadszor pedig megerősítené a koordinált **választ** és a helyreállítást. E célkitűzések elérése érdekében az egységnek olyan jól meghatározott **elemekre és célokra** kellene építenie, mint például a **biztonságos és gyors információmegosztás** biztosítása, a résztvevők közötti **együttműködés** javítása, beleértve a tagállamok és a releváns uniós gazdálkodó egységek közötti interakciót, az **elfogadott ipari bázissal rendelkező** strukturált **partnerségek** létrehozása, valamint a **külső partnerekkel való együttműködéssel** kapcsolatos koordinált megközelítés elősegítése. Ennek érdekében az elérhető nemzeti és uniós szintű kapacitások feltérképezése alapján az egység lehetővé tehetné az együttműködési keret kidolgozását.

Ahhoz, hogy a közös kiberbiztonsági egység az uniós kiberbiztonsági operatív együttműködés központi elemévé válhasson, a Bizottság együtt fog működni a tagállamokkal és az érintett uniós intézményekkel, szervekkel és ügynökségekkel, beleértve az ENISA-t, a CERT-EU-t és az Europolt, hogy előmozdítsa a **fokozatos és inkluzív megközelítést**, teljes mértékben tiszteletben tartva az érintettek illetékességét és megbízatását. E megközelítéssel összhangban az egység hozzájárulhatna egy adott kiberbiztonsági közösség alkotóelemei közötti további együttműködéshez, amennyiben azok szükségesnek tartják azt.

A közös kiberbiztonsági egység létrehozása tekintetében négy fő lépésre történt javaslat:

- *meghatározás* az elérhető nemzeti és uniós szintű kapacitások feltérképezésével;
- *felkészülés* a strukturált együttműködési és segítségnyújtási keret létrehozásával;
- *alkalmazás* a keretrendszer végrehajtásával a résztvevők erőforrásaira támaszkodva, hogy a közös kiberbiztonsági egység megkezdhesse működését;
- *bővítés* a koordinált reagálási kapacitás megerősítésével az ipar és a partnerek bevonása mellett.

A tagállamokkal, valamint az uniós intézményekkel, szervekkel és ügynökségekkel folytatott konzultáció[77] eredménye alapján a Bizottság – a főképviselő bevonásával, a főképviselő

[77] A tagállamokkal, valamint az uniós intézményekkel, szervekkel és ügynökségekkel 2020 júliusa és novembere között folytatott konzultáció (többek között a nemzeti kiberbiztonsági hatóságok vezetőinek részvételével zajló Blue OLEx20 gyakorlat során).

hatáskörének megfelelően – 2021 februárjáig bemutatja **a közös kiberbiztonsági egység meghatározására, felkészülésére, alkalmazására és bővítésére** vonatkozó folyamatot, mérföldköveket és határidőket.

### *2.2. A kiberbűnözés kezelése*

Az online eszközöktől való függésünk exponenciálisan növelte a számítógépes bűnözők támadási felületét, és olyan helyzetet eredményezett, amelyben szinte minden bűncselekménytípus nyomozásának van digitális eleme. Továbbá, a társadalmunk alapvető részét fenyegetik a számítógépes bűnözők és azok, akik számítógépes eszközöket használnak jogellenes tevékenységük megtervezésére és végrehajtására. Ezért mindez szorosan összefügg az EU általános biztonsági politikájával, ahogy azt a biztonsági unióra vonatkozó 2020. évi stratégia kiberbiztonsági elemei és a terrorizmus elleni uniós program is tükrözik[78].

A számítástechnikai bűnözés hatékony kezelése kulcsfontosságú szerepet játszik a kiberbiztonság biztosításában: az elrettentés nem érhető el kizárólag reziliencia révén, hanem szükség van az elkövetők azonosítására és büntetőeljárás alá vonására is. Ezért elengedhetetlen a kiberbiztonsági szereplők és a bűnüldözés közötti együttműködés és információcsere támogatása. Uniós szinten az Europol és az ENISA ezért már szoros együttműködést épített ki, amelynek keretében közös konferenciákat és műhelytalálkozókat szervezett, és közös jelentéseket készített a Bizottságnak, a tagállamoknak és egyéb érdekelt feleknek a kiberbiztonsági fenyegetésekről és a technológiai kihívásokról. A Bizottság ezt az integrált megközelítést a továbbiakban is támogatni fogja annak érdekében, hogy átfogó információkon alapuló, koherens és hatékony válasz születhessen.

E válasz egyik fontos elemeként az uniós és nemzeti hatóságoknak ki kell bővíteniük és fejleszteniük kell a bűnüldözési kapacitást a kiberbűnözéssel kapcsolatos nyomozások érdekében, maradéktalanul tiszteletben tartva az alapvető jogokat, illetve törekedve a különböző jogok és érdekek közötti szükséges egyensúlyra. Az EU-nak tudnia kell kezelni a kiberbűnözést a célnak megfelelő, teljeskörűen végrehajtott jogszabályok révén, különös tekintettel a gyermekek online szexuális zaklatása elleni küzdelemre, valamint a digitális nyomozásra, beleértve a darkneten folytatott illegális tevékenységeket. A bűnüldöző hatóságokat teljes mértékben fel kell szerelni ahhoz, hogy képesek legyenek digitális nyomozások végzésére. A Bizottság ezért a bűnüldöző hatóságok digitális képességeit javító cselekvési tervet fog előterjeszteni, felruházva ezeket a hatóságokat a szükséges készségekkel és eszközökkel. Emellett az Europol tovább fogja fejleszteni szakértői központ szerepét, hogy támogassa a nemzeti bűnüldözési hatóságokat a számítógépek által lehetővé tett és a számítógépekkel összefüggő bűncselekmények elleni küzdelemben, hozzájárulva a közös kriminalisztikai szabványok meghatározásához (az Europol innovációs laboratóriuma és központja révén).Mindezen tevékenységekhez azonban a tagállamok megfelelő mértékű részvételére van szükség. Ajánlott, hogy ehhez igénybe vegyék a Belső Biztonsági Alap nemzeti programjait, illetve javasoljanak projekteket a pályázati felhívások keretében a tematikus eszköz részeként.

A Bizottság az összes megfelelő eszközt igénybe fogja venni – beleértve a kötelezettségszegési eljárást – az információs rendszerek elleni támadásokról szóló, 2013. évi

[78] Communication A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 2020.12.9. (COM(2020) 795 final).

irányelv[79] teljes körű átültetésének és végrehajtásának biztosításához, ideértve a tagállami statisztikák biztosítását. Hatékonyabban fog fellépni a doménnevekkel való visszaélések megakadályozása terén, ideértve adott esetben a jogellenes tartalmak terjesztésére irányuló visszaéléseket, és a pontos regisztrációs adatok elérhetőségére törekszik, aminek érdekében továbbra is együttműködik a Bejegyzett Nevek és Számok Internetszervezetével (ICANN) és az internetes irányítási rendszer egyéb érdekelt feleivel, mindenekelőtt az ICANN kormányzati tanácsadó bizottságának közbiztonsági munkacsoportja révén. Az átdolgozott kiberbiztonsági irányelvben szereplő javaslat ennek megfelelően a doménnevek és regisztrációs adatok (WHOIS-adatok) pontos és hiánytalan adatbázisainak működtetésére irányul, és jogszerű hozzáférést biztosít az ilyen adatokhoz a DNS biztonságának, stabilitásának és rezilienciájának biztosításához szükséges mértékben.

A Bizottság emellett továbbra is azon dolgozik, hogy biztosítsa a megfelelő csatornákat, és egyértelművé tegye a szabályokat a nyomozások során az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférés érdekében (a nyomozások 85 %-ában szükség van erre, és az összes megkeresés 65 %-a más joghatóság alá tartozó szolgáltatókhoz érkezik) az elektronikus bizonyítékokról szóló csomag és gyakorlati intézkedések elfogadásának és azt követő végrehajtásának elősegítésével[80]. Az elektronikus bizonyítékokra vonatkozó javaslatoknak az Európai Parlament és a Tanács általi gyors elfogadása kulcsfontosságú ahhoz, hogy a szakemberek hatékony eszközt kapjanak a kezükbe. Az elektronikus bizonyítéknak olvashatónak kell lennie, ezért a Bizottság továbbra is azon dolgozik, hogy támogassa a bűnüldözési kapacitást a digitális nyomozások területén, beleértve a titkosítást a bűnügyi nyomozásokban, teljes mértékben betöltve az alapvető jogok és a kiberbiztonság védelmére irányuló feladatát.

### *2.3. Uniós kiberdiplomáciai eszköztár*

Az EU arra használja **kiberdiplomáciai eszköztárát**[81], hogy megakadályozza és visszaszorítsa a rosszindulatú kibertevékenységeket, elrettentsen tőlük, és reagáljon rájuk. A kibertámadások elleni célzott korlátozó intézkedésekre vonatkozó jogi keret 2019 májusában történt bevezetését[82] követően e rendszer értelmében 2020 júliusában az EU hat olyan egyént és három szervezetet sorolt fel, aki/amelyek felelősek voltak az EU-t és tagállamait érintő kibertámadásokért vagy részt vettek azokban[83]. 2020 október további két

[79] A 2013/40/EU irányelv az információs rendszerek elleni támadásokról.

[80] COM(2018) 225 és 226; C(2020) 2779 final. Mindenekelőtt a SIRIUS projekt további finanszírozásban részesült a közelmúltban a Partnerségi Eszköz keretében, hogy fejlessze a nyomozások során az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférést lehetővé tevő csatornákat (a súlyos bűncselekményekkel kapcsolatos nyomozások mintegy 85 %-ában szükség van erre, és az összes megkeresés 65 %-a más joghatóság alá tartozó szolgáltatókhoz érkezik), és nemzetközi szinten kompatibilis szabályokat hozzon.

[81] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82] A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről (HL L 129I., 2019.5.17., 13. o.) és a Tanács (EU) 2019/796 rendelete
(2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről (HL L 129I., 2019.5.17., 1. o.).

[83] A Tanács (KKBP) 2020/1127 határozata (2020. július 30.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról (ST/9564/2020/INIT) (HL L 246., 2020.7.30., 12–17. o.) és a Tanács (EU) 2020/1125 végrehajtási rendelete (2020. július 30.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (EU) 2019/796 rendelet végrehajtásáról (ST/9568/2020/INIT) (HL L 246., 2020.7.30., 4–9. o.).

személy és egy szervezet került fel erre a listára[84]. A rosszindulatú kibertámadások esetén, ideértve azokat, amely lassan fejtik ki hatásukat, hatékony és átfogó közös uniós diplomáciai választ kell adni az uniós szinten elérhető intézkedések teljes skálájának felhasználásával.

A gyors és hatékony közös uniós diplomáciai válaszhoz megbízható közös helyzetismeretre, valamint arra van szükség, hogy gyorsan közös uniós állásfoglalást lehessen kiadni. Az Unió külügyi és biztonságpolitikai főképviselője elő fogja mozdítani és segíteni a **tagállamok uniós kiberhírszerzési munkacsoportjának** létrehozását az Európai Unió Helyzetelemző Központján (EU INTCEN) belül, hogy támogassa a kiberfenyegetésekkel és -tevékenységekkel kapcsolatos stratégiai hírszerzési együttműködést. Ez a munka tovább támogatja az uniós helyzetismeretet és a közös diplomáciai válasszal kapcsolatos döntéshozatalt. A munkacsoportnak a helyzetismeret felmérése érdekében be kell vonnia a meglévő struktúrákat[85], többek között szükség esetén a hibrid és külföldi beavatkozás szélesebb körű veszélyével kapcsolatos struktúrákat.

A rosszindulatú kibertevékenységek megakadályozására és visszaszorítására, az ezektől való elrettentésre és az ezekre való reagálásra vonatkozó képesség megerősítése érdekében a főképviselő – a Bizottság bevonásával, a Bizottság hatáskörének megfelelően – javaslatot fog benyújtani az EU-nak a **kibertevékenységektől való elrettentéssel kapcsolatos megközelítésének** további meghatározásáról. A kiberdiplomáciai eszköztár keretében eddig végzett munka alapján a megközelítésnek hozzá kell járulnia a felelős állami magatartáshoz és együttműködéshez a kibertérben, és irányt kell mutatnia a legjelentősebb hatással járó kibertámadások (mindenekelőtt a kritikus infrastruktúrát, a demokratikus intézményeket és folyamatokat érintő támadások[86], az ellátási láncok elleni támadások és a kibertechnológiával elkövetett szellemitulajdon-lopás) elleni küzdelem vonatkozásában. A megközelítésnek fel kell vázolnia, hogyan használhatják az EU és tagállamai a politikai, gazdasági, diplomáciai, jogi és kommunikációs eszközöket a rosszindulatú kibertevékenységek ellen, és ki kell térnie arra, hogyan mozdíthatják elő a rosszindulatú kibertevékenységek elkövetőinek felderítésére vonatkozó képességüket. A főképviselő emellett – a Tanáccsal és a Bizottsággal együtt – arra törekszik, hogy **a kiberdiplomáciai eszköztár keretében további intézkedéseket** vizsgáljon meg, beleértve a korlátozó intézkedésekre vonatkozó további lehetőségeket és **a minősített többségi szavazás lehetőségét a kibertámadások esetében alkalmazott horizontális szankciókra vonatkozó rendszer értelmében történő listázás tekintetében**. Ezenkívül az EU-nak további erőfeszítéseket kell tennie **a nemzetközi partnerekkel** – beleértve a NATO-t – **való együttműködés megerősítésére**, hogy előmozdítsa a fenyegetési környezet közös értelmezését, együttműködési mechanizmusok jöjjenek létre, és azonosítsák az együttműködésen alapuló diplomáciai válaszokat.

A főképviselő – a Bizottság bevonásával – továbbá javasolni fogja a **kiberdiplomáciai eszköztár végrehajtására vonatkozó iránymutatás[87]** aktualizálását, többek között a

[84] A Tanács (KKBP) 2020/1537 határozata (2020. október 22.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról (HL L 351I., 2020.10.22., 5. o.) és a Tanács (EU) 2020/1536 végrehajtási rendelete (2020. október 22.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (EU) 2019/796 rendelet végrehajtásáról (HL L 351I., 2020.10.22., 1–4. o.).

[85] Például az egységes információelemzési kapacitást (SIAC) és szükség esetén a PESCO keretében indított releváns projekteket, valamint a 2018. évi riasztási rendszert, amely azért jött létre, hogy támogassa a dezinformáció kezelésére szolgáló átfogó uniós megközelítést.

[86] Mindenekelőtt az Európai Demokráciára vonatkozó cselekvési terv értelmében vett kezdeményezésekkel való szinergiákra törekedve.

[87] 13007/17.

döntéshozatali eljárás fokozott hatékonyságra való tekintettel, és továbbra is rendszeresen szervez a kiberdiplomáciai eszköztárral kapcsolatos gyakorlatokat és értékeléseket. Az EU-nak emellett jobban **integrálnia kell a kiberdiplomáciai eszköztárat az uniós válságkezelési mechanizmusokba**, és szinergiákra kell törekednie a hibrid fenyegetések, a dezinformáció és a külföldi beavatkozás elleni erőfeszítések terén a hibrid fenyegetésekkel szembeni fellépés közös kerete[88] és az Európai Demokráciára vonatkozó cselekvési terv értelmében. Ebben az összefüggésben az EU-nak foglalkoznia kell egyrészt a kiberdiplomáciai eszköztár, másrészt az EUSZ 42. cikke (7) bekezdésének és az EUMSZ 222. cikkének lehetséges alkalmazása közötti kapcsolattal[89].

### *2.4. A kibervédelmi képességek fejlesztése*

Az EU-nak és tagállamainak fokozniuk kell a kibertámadások megakadályozására és a reagálásra vonatkozó képességüket a 2016. évi uniós globális stratégiából eredő uniós célkitűzésnek megfelelően[90]. Ennek érdekében a főképviselő – a Bizottsággal együttműködve – be fogja mutatni **a kibervédelmi szakpolitikai keret (CDPF) felülvizsgálatát**, hogy tovább fokozza az uniós[91] szereplők közötti, valamint a tagállamokkal való és tagállamok közötti koordinációt és együttműködést, többek között a közös biztonság- és védelempolitikai (KBVP) missziók és műveletek vonatkozásában. A kibervédelmi szakpolitikai keret alapul szolgál majd a leendő stratégiai iránytűhöz[92], biztosítva a kiberbiztonság és kibervédelem további integrálását a szélesebb körű biztonsági és védelmi menetrendbe.

Az EU 2018-ban műveleti területként azonosította a kiberteret[93]. Az Európai Unió Katonai Bizottsága által kiadandó **„A kibertérre mint műveleti területre vonatkozó katonai jövőkép és stratégia”** című dokumentumnak részletesebben meg kell határoznia, hogy a kibertér mint műveleti terület hogyan teszi lehetővé az uniós közös biztonság- és védelempolitikai missziókat és műveleteket. A **katonai CERT-hálózat**[94], amelyet az Európai Védelmi Ügynökség (EDA) jelenleg épít ki, még inkább hozzá fog járulni a tagállamok közötti együttműködés jelentős fokozásához. Emellett az űrprogram keretében a kritikus űrinfrastruktúra kiberbiztonságának biztosítása érdekében sor fog kerülni Az Európai Unió Űrprogramügynöksége és különösen a Galileo Biztonsági Megfigyelőközpont megerősítésére, és a megbízatását kiterjesztik az űrprogram egyéb kritikus elemeire.

Az EU-nak és tagállamainak további lendületet kell biztosítaniuk **a legmodernebb kibervédelmi kapacitások kidolgozásához** különböző uniós szakpolitikák és eszközök alkalmazásával, mindenekelőtt a kibervédelmi szakpolitikai keret révén, illetve adott esetben az EDA munkájára építve. Ehhez nagy hangsúlyt kell fektetni olyan alapvető technológiák kifejlesztésére és használatára, mint az MI, a titkosítás és a kvantum-számítástechnika.

---

[88] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[89] Kölcsönös védelmi záradék, illetve szolidaritási záradék.

[90] A Tanács következtetései (14149/16) a biztonság és védelem terén az uniós globális stratégia végrehajtásáról.

[91] Mindenekelőtt az EKSZ, beleértve az Európai Unió Katonai Törzsét (EUKT), az Európai Biztonsági és Védelmi Főiskola (EBVF), a Bizottság és az uniós ügynökségek, elsősorban az Európai Védelmi Ügynökség (EDA).

[92] A Tanács következtetései a biztonság és védelem terén, 2020. június 17. (8910/20).

[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

[94] Az uniós katonai CERT-hálózat felállítása a 2018. évi kibervédelmi szakpolitikai keretben azonosított célkitűzésre adott válasz, és az uniós tagállamok katonai CERT-jei közötti aktív interakció és információcsere előmozdítására irányul.

A 2018. évi uniós képességfejlesztési prioritásokkal[95] összhangban, illetve a koordinált éves védelmi szemléről (CARD) szóló első teljes jelentés[96] megállapításai alapján az EU-nak továbbra is elő kell mozdítania a tagállamok közötti, **a kibervédelmi kutatással, innovációval és képességfejlesztéssel** kapcsolatos együttműködést, arra ösztönözve a tagállamokat, hogy teljes mértékben használják ki az **állandó strukturált együttműködésben (PESCO)[97]** és az **EDF-ben[98]** rejlő lehetőségeket.

A leendő, 2021. első negyedévében bemutatandó, **a polgári, védelmi és űripar közötti szinergiákról szóló bizottsági cselekvési terv** olyan cselekvéseket fog tartalmazni, amely tovább támogatják a szinergiákat a programok, technológiák, innováció és induló innovatív vállalkozások szintjén a vonatkozó programok irányításának megfelelően[99].

Emellett szinergiákat és felhasználói felületeket kell létrehozni a más keretekben indult kibervédelmi kezdeményezések között, ideértve a tagállamok kiberbiztonsági együttműködési projektjeit[100] a PESCO keretében, továbbá az uniós kiberbiztonsági struktúrákkal az információmegosztás és a kölcsönös támogatás érdekében.

***Stratégiai kezdeményezések***

Az EU-nak

- létre kell hoznia az európai kiberbiztonsági válságreagálási keretet, és ki kell dolgoznia a közös kiberbiztonsági egység létrehozásának folyamatát a kapcsolódó mérföldkövekkel és határidőkkel;
- folytatnia kell a kiberbűnözéssel kapcsolatos menetrend végrehajtását a biztonsági unióra vonatkozó stratégia keretében;
- elő kell mozdítania és segítenie az EU INTCEN-en belül a tagállamok kiberhírszerzési munkacsoportjának létrehozását;
- elő kell mozdítania a kibertevékenységektől való elrettentésre vonatkozó uniós megközelítést, hogy megakadályozza és visszaszorítsa a rosszindulatú kibertevékenységeket, elrettentsen tőlük, és reagáljon rájuk;
- felül kell vizsgálnia a kibervédelmi szakpolitikai keretet;
- elő kell segítenie „A kibertérre mint műveleti területre vonatkozó katonai jövőkép és stratégia” című uniós dokumentum kidolgozását a KBVP katonai missziói és műveletei

[95] 2018 júniusában a tagállamok az EDA irányítóbizottságában megállapodtak az uniós szintű védelmi együttműködés irányításában.
[96] A védelmi miniszterek 2020 novemberében az EDA irányítóbizottságában jóváhagyták. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)
[97] Jelenleg számos kiberbiztonsági PESCO projekt fut, mindenekelőtt „A kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform”, „a Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén”, az Uniós Kiberakadémia és Innovációs Központ, valamint A Kiber- és az Információs Terület Koordinációs Központja (CIDCC).
[98] Az Európai Védelmi Alap keretében a Bizottság már azonosította az olyan potenciális, együttműködésen alapuló kibervédelmi kutatási-fejlesztési fellépések lehetőségét, amelyek célja az együttműködés, az innovációs kapacitás és a védelmi ipar versenyképességének megerősítése.
[99] Például a Horizont Európa, a Digitális Európa és az EDF.
[100] https://pesco.europa.eu/

vonatkozásában;

- támogatnia kell a polgári, védelmi és űripar közötti szinergiákat; és
- meg kell erősítenie az űrprogram keretében a kritikus űrinfrastruktúrák kiberbiztonságát.

## 3. A GLOBÁLIS ÉS NYÍLT KIBERTÉR ELŐMOZDÍTÁSA

Az EU-nak folytatnia kell a nemzetközi partnerekkel annak érdekében folytatott munkát, hogy egyrészt előmozdítsa a jogállamiságon, emberi jogokon, alapvető szabadságokon és demokratikus értékeken alapuló kibertér politikai modelljét és jövőképét, amely globális társadalmi, gazdasági és politikai fejlődést eredményez, másrészt hozzájáruljon a biztonsági unióhoz. A nemzetközi együttműködés elengedhetetlen a globális, nyílt, stabil és biztonságos kibertérhez. Ehhez az EU-nak folytatnia kell a harmadik országokkal, a nemzetközi szervezetekkel és a több érdekelt felet tömörítő közösséggel folytatott munkát, hogy koherens és holisztikus nemzetközi kiberpolitikát dolgozzon ki és hajtson végre, figyelembe véve az új technológiák, a belső biztonság, valamint a külföldi biztonsági és védelmi politikák közötti egyre nagyobb összekapcsoltságot. Az EU alapvető demokratikus értékeken, valamint a jogállamiság és az alapvető jogok tiszteletben tartásán alapuló erős gazdasági és kereskedelmi egységként továbbá egyedülálló vezető szerepet játszik a nemzetközi előírások és szabványok meghatározásában és előmozdításában.

### *3.1. Az EU vezető szerepe a kibertérre vonatkozó szabványok, előírások és keretrendszerek terén*

#### *A nemzetközi szabványosítás fokozása*

A kibertérrel kapcsolatos jövőképének nemzetközi szinten való előmozdítása és megvédése érdekében az EU-nak **fokoznia kell a nemzetközi szabványosítási folyamatokban való részvételét és vezető szerepét, és jobban képviseltetnie kell magát a nemzetközi és európai szabványosítási szervekben és egyéb szabványosítási szervezetekben**[101]. Mivel a digitális technológiák gyors ütemben fejlődnek, a nemzetközi szabványok egyre fontosabb szerepet játszanak a hagyományos szabályozási erőfeszítések kiegészítésében olyan területeken, mint az MI, a felhő, a kvantum-számítástechnika és a kvantumkommunikáció. A harmadik országok egyre nagyobb mértékben alkalmazzák a nemzetközi szabványosítást a politikai és ideológiai menetrendjük előmozdítására, ami gyakran nem felel meg az uniós értékeknek. Emellett egyre nagyobb az egymással versengő nemzetközi szabványosítási keretrendszerek kockázata, ami töredezettséghez vezet.

A kialakulóban lévő technológiák és az alapvető internetes architektúra területén az uniós értékekkel összhangban lévő nemzetközi szabványok elengedhetetlenek ahhoz, hogy az internet globális és nyílt maradjon, továbbá a technológiák emberközpontúak és magánélet-központúak legyenek, illetve a használatuk jogszerű, biztonságos és etikus legyen. A jövőbeli szabványosítási stratégia részeként az EU-nak meg kell határoznia a **nemzetközi szabványosítási célkitűzéseit**, illetve proaktív és koordinált figyelemfelkeltő tevékenységet

[101] Például a Nemzetközi Szabványügyi Szervezet (ISO), a Nemzetközi Elektrotechnikai Bizottság (IEC), a Nemzetközi Távközlési Egyesület (ITU), az Európai Szabványügyi Testület (CEN), az Európai Elektrotechnikai Szabványügyi Bizottság (CENELEC), az Európai Távközlési Szabványügyi Intézet (ETSI), az Internet-mérnöki Munkacsoport (IETF), a Harmadik Generációs Partneri Projekt (3GPP) és a Villamos- és Elektronikai Mérnökök Intézete (IEEE).

kell folytatnia, hogy nemzetközi szinten előmozdítsa ezeket. Nagyobb együttműködésre és tehermegosztásra kell törekedni a hasonló gondolkodású partnerekkel és az európai érdekelt felekkel.

***A felelős állami magatartás előmozdítása a kibertérben***

Az EU folytatja a nemzetközi partnerekkel való együttműködését az olyan globális, nyílt, stabil és biztonságos kibertér előmozdítása és támogatása érdekében, amelyben **tiszteletben tartják a nemzetközi jogot, mindenekelőtt az Egyesült Nemzetek Alapokmányát**[102] és **a felelős állami magatartásra vonatkozó önkéntes, nem kötelező érvényű normákat, szabályokat és elveket**[103]. A kibertérben a nemzetközi biztonságról szóló hatékony többoldalú vita lehetőségének romlásával egyértelműen szükség van arra, hogy az EU és a tagállamok proaktívabb szerepet vállaljanak az ENSZ-ben és az egyéb releváns nemzetközi fórumokon folytatott megbeszéléseken. Az EU a legjobb helyzetben van ahhoz, hogy **előmozdítsa, koordinálja és egységesítse a tagállami álláspontokat a nemzetközi fórumokon**, és **ki kell dolgoznia a nemzetközi jog kibertérben való alkalmazására vonatkozó uniós álláspontot**. A főképviselő – a tagállamokkal együtt – emellett arra törekszik, hogy előmozdítsa az inkluzív és konszenzuson alapuló javaslatokat **a kibertérben gyakorolt felelős állami magatartás előmozdítására irányuló cselekvési programra**[104] vonatkozó politikai kötelezettségvállalás tekintetében az ENSZ-ben. Az ENSZ Közgyűlése[105] által támogatott meglévő vívmányokra építve a cselekvési program az együttműködésre és a bevált gyakorlatok cseréjére szolgáló platformot kínál az ENSZ-ben, és javasolja a felelős állami magatartásra vonatkozó előírások gyakorlati alkalmazására és a kapacitásépítés előmozdítására irányuló mechanizmus kidolgozását. A főképviselő továbbá arra törekszik, hogy megerősítse és előmozdítsa a **bizalomépítő intézkedések** végrehajtását a tagállamok között, többek között a bevált gyakorlatok regionális és többoldalú szinten való megosztásával és a régiókon átnyúló együttműködéshez való hozzájárulással.

A fokozott globális összekapcsoltság nem vezethet cenzúrához, tömeges megfigyeléshez, az adatvédelem megsértéséhez, illetve a polgári társadalom, a tudományos közösség és az állampolgárok elnyomásához. Az EU-nak továbbra is vezető szerepet kell játszania **az emberi jogok és alapvető szabadságjogok** online védelme és előmozdítása terén. Ennek érdekében az EU-nak még inkább elő kell mozdítania a nemzetközi emberi jogi normáknak és előírásoknak[106] való megfelelést, végre kell hajtania az emberi jogokra és a demokráciára vonatkozó 2020–2024-es uniós cselekvési tervet[107], és elő kell mozdítania az online és offline véleménynyilvánítás szabadságáról szóló uniós emberi jogi iránymutatásokat[108], **új lendületet adva az uniós eszközök gyakorlati alkalmazásának**. Az EU-nak folyamatos erőfeszítéseket kell tennie **az olyan kérdésekkel foglalkozó emberijog-védők, civil**

---

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] A nemzetközi biztonság összefüggésében az információs és távközlési technológiák területén végbemenő fejleményekkel foglalkozó kormányzati szakértői csoportok releváns, az ENSZ Közgyűlése által támogatott 2015., 2013. és 2010. évi jelentésének megfelelően.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] A nemzetközi biztonság összefüggésében az információs és távközlési technológiák területén végbemenő fejleményekkel foglalkozó kormányzati szakértői csoportok releváns, az ENSZ Közgyűlése által támogatott 2015., 2013. és 2010. évi jelentésének megfelelően.

[106] Mindenekelőtt az ENSZ Alapokmánya és Az Emberi Jogok Egyetemes Nyilatkozata.

[107] https://www.consilium.europa.eu/en/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

**társadalom és tudományos közösség védelmére, mint például a kiberbiztonság, az adatvédelem, a felügyelet és az online cenzúra**. Ennek érdekében az EU-nak további gyakorlati útmutatást kell nyújtania, elő kell mozdítania a bevált gyakorlatokat, és fokozni kell a kialakulóban lévő technológiákkal való visszaélések megakadályozására irányuló erőfeszítéseket, mindenekelőtt szükség esetén diplomáciai intézkedések használatával és az ilyen technológiák kivitelének ellenőrzésével. Az EU-nak emellett folytatnia kell a társadalom legveszélyeztetettebb tagjainak online védelmére irányuló küzdelmet a gyermekek szexuális zaklatása és kizsákmányolása elleni hatékonyabb védelmet biztosító jogszabályok, illetve egy gyermekjogi stratégia előterjesztésével.

***A számítástechnikai bűnözésről szóló budapesti egyezmény***

Az EU továbbra is támogatja azokat a harmadik országokat, amelyek csatlakozni kívánnak **az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményéhez**, és arra törekszik, hogy véglegesítse **a budapesti egyezmény második kiegészítő jegyzőkönyvét**, amely intézkedéseket és biztosítékokat tartalmaz a bűnüldözési és igazságszolgáltatási hatóságok, illetve más országokban a hatóságok és a szolgáltatók közötti nemzetközi együttműködés javítására, és e jegyzőkönyv vonatkozásában a Bizottság részt vesz az EU nevében folytatott tárgyalásokon[109]. A kiberbűnözésre vonatkozó új, uniós szintű jogi eszközre vonatkozó jelenlegi kezdeményezés azzal a kockázattal jár, hogy növeli az osztályok számát, és lelassítja azokat a nemzeti reformokat és a kapcsolódó kapacitásépítési erőfeszítéseket, amelyekre nagy szükség van, potenciálisan akadályozva a kiberbűnözés elleni hatékony nemzetközi együttműködést: az EU szerint nincs szükség a kiberbűnözésre vonatkozó új, uniós szintű jogi eszközre. Az EU továbbra is részt vesz **a kiberbűnözéssel kapcsolatos többoldalú információcserében**, hogy az inkluzív jelleg és az átláthatóság révén, továbbá az elérhető szakértelem figyelembevételével biztosítsa az emberi jogok és az alapvető szabadságok tiszteletben tartását azzal a céllal, hogy mindenki számára hozzáadott értéket biztosítson.

### *3.2. Együttműködés a partnerekkel és a több érdekelt félből álló közösséggel*

Az EU-nak **meg kell erősítenie és ki kell terjesztenie a harmadik országokkal folytatott kiberbiztonsági párbeszédet**, hogy előmozdítsa a kibertérre vonatkozó értékeit és jövőképét, megossza a bevált gyakorlatokat, és hatékonyabb együttműködésre törekedjen. Az EU emellett **strukturált információcserét** fog folytatni olyan **regionális szervezetekkel**, mint az Afrikai Unió, az ASEAN regionális fórum, az Amerikai Államok Szervezete, illetve az Európai Biztonsági és Együttműködési Szervezet. Az EU-nak ugyanakkor arra kell törekednie, hogy a közös érdekű ügyekre építve minden lehetséges esetben közös megegyezésre jusson a partnerekkel. Az EU-nak – az uniós küldöttségekkel és adott esetben világszerte a tagállamok nagykövetségeivel együttműködve – létre kell hoznia egy informális **uniós kiberdiplomáciai hálózatot**, hogy előmozdítsa a kibertérre vonatkozó uniós jövőképet, biztosítsa az információcserét, és rendszeresen koordinálja a kibertérben történő fejleményeket[110].

A 2016. július 8-i[111] és a 2018. július 10-i[112] együttes nyilatkozatra építve az EU-nak folytatnia kell **az EU és a NATO közötti együttműködés** előmozdítását, mindenekelőtt a

[109] A Tanács 2019. júniusi határozata (9116/19).
[110] Adott esetben a tagállami külügyminisztériumokat tömörítő informális uniós digitális diplomáciai hálózat tevékenységét is hasznosíthatja.
[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/

kibervédelmi interoperabilitási követelmények vonatkozásában. Ebben az összefüggésben az EU-nak továbbra is arra kell törekednie, hogy a releváns KBVP struktúrák betagozódjanak a NATO Federated Mission Networking kezdeményezésébe, szükség esetén lehetővé téve a hálózati interoperabilitást a NATO-val és a partnerekkel. Emellett jobban fel kell térképezni az EU és a NATO közötti, az oktatással, képzéssel és gyakorlatokkal kapcsolatos együttműködést, többek között szinergiákra törekedve az Európai Biztonsági és Védelmi Főiskolával, illetve a NATO együttműködésen alapuló kibervédelmi kiválósági központjával.

Az értékeivel összhangban az EU határozottan támogatja és előmozdítja **a több érdekelt félre kiterjedő internetirányítási modellt**. Egyetlen gazdálkodó egység, kormány vagy nemzetközi szervezet sem törekedhet az internet ellenőrzésére. Az EU-nak továbbra is részt kell vennie a fórumokon[113] az együttműködés fokozása, valamint az alapvető jogok és szabadságok, mindenekelőtt a méltósághoz, a magánélethez, a véleménynyilvánítás szabadságához és az információszabadsághoz való jog védelme érdekében. A kiberbiztonsággal kapcsolatos, több érdekelt félre kiterjedő együttműködés előmozdítása érdekében a Bizottság és a főképviselő – a hatáskörének megfelelően – meg kívánja erősíteni az érdekelt felekkel – beleértve a magánszektort, a tudományos közösséget és a polgári társadalmat – való **rendszeres és strukturált információcserét**, kihangsúlyozva, hogy a kibertér összekapcsolt jellegéhez szükség van a valamennyi érdekelt fél közötti információcserére, és sajátos feladataik vannak a globális, nyílt, stabil és biztonságos kibertér fenntartása tekintetében. Ezek az erőfeszítések értékes hozzájárulást nyújtanak a lehetséges főbb uniós szintű fellépésekhez.

### *3.3. A globális kapacitás megerősítése a globális reziliencia fokozása érdekében*

Annak biztosítása érdekében, hogy valamennyi ország előnyére tudja fordítani az internet és a technológiák által kínált társadalmi, gazdasági és politikai előnyöket, az EU továbbra is támogatja a partnereit kiberrezilienciájuk és arra irányuló kapacitásuk megerősítésében, hogy felderítsék és büntetőeljárás alá vonják a kiberbűnözést, és kezelni tudják a kiberfenyegetéseket. Az általános koherencia biztosítása érdekében az EU-nak ki kell dolgoznia az **uniós külső kiberkapacitás-építési menetrendet** az ilyen erőfeszítések irányítására a külső kiberkapacitás-építésre vonatkozó iránymutatásnak[114], illetve a 2030-ig tartó időszakra vonatkozó fenntartható fejlődési menetrendnek[115] megfelelően. A menetrendnek hasznosítania kell a tagállamok, valamint a releváns uniós intézmények, szervek és ügynökségek szakértelmét, továbbá a kezdeményezéseket, ideértve az uniós kiberkapacitás-építő hálózatot[116] a megbízatásuknak megfelelően. Létre kell hozni a releváns uniós intézményi érdekelt feleket tömörítő **uniós kiberkapacitás-építési testületet**, amely nyomon követi az előrehaladást, valamint a további szinergiák és a lehetséges hiányosságok azonosítását. Ez a testület támogathatja továbbá a tagállamokkal, illetve az állami és magánszektorbeli partnerekkel és egyéb releváns nemzetközi szervekkel folytatott fokozott együttműködést az erőfeszítések koordinálásának biztosítása és az erőfeszítések megkettőzésének elkerülése érdekében.

---

[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Például a Bejegyzett Nevek és Számok Internetszervezete (ICANN) és az Internetirányítási Fórum (IGF).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

Az **uniós kiberkapacitás-építésnek** továbbra is a Nyugat-Balkánra és az uniós szomszédságra, valamint a gyors digitális fejlődést tapasztaló partnerországokra kell összpontosítania. Az uniós erőfeszítéseknek támogatniuk kell a partnerországok jogszabályainak és szakpolitikáinak kidolgozását a releváns uniós kiberdiplomáciai szakpolitikáknak és előírásoknak megfelelően. Ebben az összefüggésben a digitalizáció terén folytatott uniós kapacitásépítési erőfeszítéseknek standard elemként magukban kell foglalniuk a kiberbiztonságot. Ennek érdekében az EU-nak ki kell dolgoznia az uniós digitális és külső kiberkapacitás-építési erőfeszítésekért felelős uniós munkavállalók képzési programját. Az EU-nak emellett segítséget kell nyújtania ezeknek az országoknak a társadalmi fejlődésüket, illetve a **demokratikus rendszereik integritását és biztonságát** fenyegető rosszindulatú kibertevékenységek által jelentett egyre növekvő kihívás kezeléséhez az Európai Demokráciára vonatkozó cselekvési tervnek megfelelően. Az uniós tagállamok, valamint a releváns uniós ügynökségek és harmadik országok közötti egymástól való tanulás különösen hasznos lehet ebben a tekintetben.

Végezetül, a polgári KBVP területére vonatkozó 2018. évi paktum[117] összefüggésében a polgári KBVP missziók is hozzájárulhatnak a szélesebb körű uniós válaszhoz a kiberbiztonsági kihívások kezelése terén, mindenekelőtt a partnerországokon belül a jogállamiság, valamint a bűnüldözés és a polgári hatóságok kapacitásának megerősítésével.

***Stratégiai kezdeményezések***

Az EU-nak

- meg kell határoznia a nemzetközi szabványosítási folyamatok célkitűzéseit, és elő kell mozdítania őket nemzetközi szinten;
- elő kell mozdítania a kibertérben való nemzetközi biztonságot és stabilitást, mindenekelőtt az EU és a tagállamai által az ENSZ-nél a kibertérben gyakorolt felelős állami magatartás előmozdítására irányuló cselekvési programra vonatkozóan benyújtott javaslat révén;
- gyakorlati iránymutatást kell nyújtania az emberi jogok és az alapvető szabadságok kibertérben való alkalmazásához;
- hatékonyabb védelmet kell biztosítania a gyermekek szexuális zaklatása és kizsákmányolása ellen, illetve gyermekjogi stratégiát kell előterjesztenie;
- meg kell erősítenie és elő kell mozdítania a számítástechnikai bűnözésről szóló budapesti egyezményt, többek között a budapesti egyezmény második kiegészítő jegyzőkönyvével kapcsolatos munka révén;
- ki kell terjesztenie a harmadik országokkal, valamint a regionális és nemzetközi szervezetekkel folytatott uniós kiberbiztonsági párbeszédet, többek között egy informális uniós kiberdiplomáciai hálózat révén;
- meg kell erősítenie a több érdekelt felet tömörítő közösséggel való információcserét, mindenekelőtt a magánszektorral, a tudományos közösséggel és a polgári társadalommal folytatott rendszeres és strukturált információcserével; és

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/en/pdf

- javaslatot kell tennie egy uniós külső kiberkapacitás-építési menetrendre és egy uniós kiberkapacitás-építési testületre.

## III. KIBERBIZTONSÁG AZ UNIÓS INTÉZMÉNYEKBEN, SZERVEKBEN ÉS ÜGYNÖKSÉGEKNÉL

Tekintettel jelentős politikai szerepükre, a rendkívül érzékeny kérdések koordinálására irányuló kritikus küldetéseikre, valamint a jelentős összegű közpénzek kezelésében játszott szerepükre, **az uniós intézmények, szervek és ügynökségek a kibertámadások**, különösen a kiberkémkedés **rendszeres célpontjai**. Ugyanakkor a kiberreziliencia szintje, valamint a rosszindulatú kibertevékenységek észlelésére és a reagálásra való képesség jelentősen eltér az említett szervezeteknél az érettség tekintetében. Ezért következetes és egységes szabályozással javítani kell a kiberbiztonság általános szintjét.

**Az információbiztonság területén** előrelépés történt az **EU-minősített adatok, valamint a nem minősített érzékeny adatok védelmére vonatkozó szabályok** nagyobb konzisztenciája terén. Ugyanakkor a minősített információs rendszerek interoperabilitása továbbra is korlátozott, ami megakadályozza az információk gördülékeny átadását a különböző szervezetek között. További előrehaladásra van szükség az EU-minősített adatok és a nem minősített érzékeny adatok kezelésére vonatkozó intézményközi megközelítés lehetővé tétele érdekében, ami interoperabilitási modellként is szolgálhat a tagállamokban. A tagállamokkal folytatott eljárások egyszerűsítése érdekében ki kell dolgozni egy alapforgatókönyvet is. Az EU-nak emellett tovább kell fejlesztenie arra vonatkozó képességét, hogy biztonságosan kommunikáljon a releváns partnerekkel, a lehető legnagyobb mértékben a meglévő mechanizmusokra és eljárásokra támaszkodva.

A biztonsági unióra vonatkozó stratégiának megfelelően a Bizottság ezért 2021-ben javaslatokat fog tenni **az információbiztonságra vonatkozó közös, kötelező érvényű szabályokra, valamint a valamennyi uniós intézmény, szerv és ügynökség kiberbiztonságára vonatkozó közös, kötelező érvényű szabályokra** a kiberbiztonság terén folyamatban lévő uniós intézményközi megbeszélések alapján[118].

A távmunkával kapcsolatos jelenlegi és jövőbeni tendenciák is további beruházásokat igényelnek a biztonságos berendezésekbe, infrastruktúrákba és eszközökbe, hogy lehetővé váljon az érzékeny és minősített dokumentumokkal folytatott távmunka.

Ezenfelül az egyre ellenségesebb kiberfenyegetési környezet, valamint az uniós intézményeket, szerveket és ügynökségeket érintő kifinomultabb és gyakoribbá váló kibertámadások szükségessé teszik a nagyobb beruházásokat a magasabb szintű kiberérettség elérése érdekében. Jelenleg folyik egy kibertudatossági program kidolgozása valamennyi uniós intézmény, szerv és ügynökség vonatkozásában a munkavállalók tudatossága és a kiberhigiénia növelése, illetve a közös kiberbiztonsági kultúra támogatása érdekében.

Szükség van **a CERT-EU hatékonyabb finanszírozási mechanizmussal való megerősítésére**, hogy jobban tudjon segíteni az uniós intézményeknek, szerveknek és ügynökségeknek az új kiberbiztonsági szabályok alkalmazásában és a kiberreziliencia

[118] A rendszeres uniós intézményközi kiberbiztonsági megbeszélések az uniós intézmények digitális átalakulásával kapcsolatos lehetőségekkel és kihívásokkal kapcsolatos szélesebb körű információcsere részét képezik.

fejlesztésében. A CERT-EU megbízatását azért is meg kell erősíteni, hogy stabil eszközökkel rendelkezzen e célkitűzések elérésére.

***Stratégiai kezdeményezések***

1. Az uniós intézmények, szervek és ügynökségek információbiztonságáról szóló rendelet
2. Az uniós intézményekre, szervekre és ügynökségekre vonatkozó közös kiberbiztonsági szabályokról szóló rendelet
3. A CERT-EU új jogi alapja a megbízatása és a finanszírozása megerősítéséhez

## IV. KÖVETKEZTETÉSEK

E stratégia összehangolt végrehajtása hozzá fog járulni egy kiberbiztonságos digitális évtizedhez az EU számára, a biztonsági unió megvalósításához és az EU helyzetének globális megerősítéséhez.

Az EU-nak elő kell mozdítania a világszínvonalú megoldásokra vonatkozó szabványokat és normákat, az alapvető szolgáltatások és a kritikus infrastruktúrák vonatkozásában a kiberbiztonsági szabványokat, valamint az új technológiák kifejlesztését és alkalmazását. Az internetet használó minden szervezet és egyén része a kiberbiztonságos digitális átalakulást biztosító megoldásnak.

A Bizottság és a főképviselő – a hatáskörének megfelelően – nyomon fogja követni az e stratégia terén elért előrehaladást, és értékelési követelményeket fog kidolgozni. A nyomon követéshez hozzájárulnak az ENISA jelentései és a biztonsági unióról szóló rendszeres bizottsági jelentések. Az eredmények hozzá fognak járulni a digitális évtized leendő célkitűzéseinek eléréséhez[119]. A Bizottság és a főképviselő – a hatáskörének megfelelően – továbbra is tartja a kapcsolatot a tagállamokkal, hogy olyan gyakorlati intézkedéseket azonosítson, amelyek szükség esetén összekötik a négy uniós kiberbiztonsági közösséget a kritikus infrastruktúra és a belső piac rezilienciája, az igazságszolgáltatás és a bűnüldözés, a kiberdiplomácia és a kibervédelem terén. A Bizottság és a főképviselő emellett továbbra is szerepet vállal a több érdekelt felet magában foglaló közösségben, kihangsúlyozva, hogy minden internethasználó személynek részt kell vállalnia a globális, nyílt, stabil és biztonságos kibertér fenntartásában, ahol mindenki biztonságban élheti digitális életét.

[119] A Bizottság 2021. évi munkaprogramjának megfelelően.

# Függelék: Az 5G hálózatok kiberbiztonságával kapcsolatos következő lépések

Az 5G hálózatok kiberbiztonságáról szóló bizottsági ajánlás[120] felülvizsgálatának eredményei alapján az uniós szintű koordinált erőfeszítések következő lépésében az alábbi táblázatban szereplő három kulcsfontosságú célkitűzésre, valamint a tagállami hatóságok, a Bizottság és az ENISA által végrehajtandó, rövid és középtávú főbb cselekvésekre kell összpontosítani.

A következő szakasz első prioritása **az eszköztár nemzeti szintű végrehajtásának befejezése és a 2020. júliusi eredményjelentésben azonosított problémák kezelése**. Ebben az összefüggésben az eszköztár néhány stratégiai intézkedése szempontjából előnyös lenne a **fokozott koordináció vagy információcsere** a kiberbiztonsági munkafolyamatban – ahogy az eredményjelentésben szerepel –, ami potenciálisan a **bevált gyakorlatok vagy iránymutatás** kidolgozásához vezetne. A technikai intézkedések tekintetében az ENISA további támogatást nyújthatna az eddigi munkája alapján, részletesebben megvizsgálva egyes témákat, illetve **elkészítve a mobilhálózat-üzemeltetőkre vonatkozó 5G kiberbiztonsági követelményekről szóló valamennyi releváns iránymutatás átfogó áttekintését**.

Másodszor, a tagállamok hangsúlyozták, hogy milyen fontos lépést tartani a fejleményekkel **a technológia, az 5G architektúra, a fenyegetések és az 5G használati esetek és alkalmazások, valamint a külső tényezők alakulásának folyamatos nyomon követésével,** hogy **azonosítani és kezelni lehessen az új vagy kialakulóban lévő kockázatokat**. Továbbá, a kezdeti kockázatelemzés számos vonatkozását alaposabban meg kell vizsgálni, mindenekelőtt annak biztosítása érdekében, hogy a teljes 5G ökoszisztémára kitérjen, beleértve a hálózati infrastruktúra és az 5G ellátási lánc valamennyi releváns részét. Az eszköztár kidolgozására rugalmas és alakítható eszközként került sor, de szükség esetén, középtávon lépéseket lehet tenni a bővítésére vagy módosítására, hogy átfogó és naprakész maradjon.

Harmadszor, további **uniós szintű cselekvésekre** van szükség az eszköztár célkitűzéseinek támogatása és kiegészítése, valamint ezeknek a releváns uniós és bizottsági szakpolitikákba való teljes körű integrálása érdekében, mindenekelőtt a Bizottság által az eszköztárról szóló, 2020. január 29-i közleményben[121] bejelentett cselekvések utánkövetéseként számos területen (például a biztonságos 5G hálózatok uniós finanszírozása, az 5G és az azt követő technológiákba való beruházások, piacvédelmi eszközök és verseny az 5G ellátási piac torzulásának elkerülésére stb.).

**A vezető szereplőknek 2021 elején adott esetben el kell fogadniuk az alábbiakban meghatározott főbb cselekvésekre vonatkozó részletes intézkedéseket és határidőket.**

| **1. kulcsfontosságú célkitűzés: A hatékony uniós kockázatcsökkentésre vonatkozó nemzeti megközelítések közelítésének biztosítása** | | |
|---|---|---|
| **Területek** | **Főbb rövid és középtávú cselekvések** | **Vezető szereplők** |
| **Az eszköztár** | Az eszköztárra vonatkozó következtetésekben ajánlott | Tagállami |

[120] Az 5G hálózatok kiberbiztonságáról szóló, 2019. március 26-i (EU) 2019/534 bizottsági ajánlás hatásairól szóló bizottsági jelentés.

[121] A Bizottság közleménye (COM(2020) 50) – Az 5G biztonságos kiépítése az EU-ban – Az uniós eszköztár alkalmazása, 2020. január 29.

| | | |
|---|---|---|
| **tagállamok általi végrehajtása** | intézkedések végrehajtásának befejezése 2021 második negyedévére, rendszeres értékeléssel a kiberbiztonsági munkafolyamatban | hatóságok |
| **A beszállítókra vonatkozó stratégiai intézkedésekkel kapcsolatos információk és bevált gyakorlatok cseréje** | Az információcsere fokozása és a lehetséges bevált gyakorlatok mérlegelése, különös tekintettel az alábbiakra:<br>- korlátozások a nagy kockázatnak kitett beszállítók esetében (SM03) és a kihelyezett szolgáltatások nyújtásával kapcsolatos intézkedések (SM04);<br>- az ellátási láncok biztonsága és rezilienciája, különösen a BEREC által az SM05–SM06 kapcsán végzett felmérés utánkövetéseként. | Tagállami hatóságok, Bizottság |
| **Kapacitásépítés és technikai intézkedésekkel kapcsolatos iránymutatás** | Technikai deep-dive, valamint közös iránymutatás és eszközök kidolgozása, beleértve az alábbiakat:<br>- az 5G biztonságra vonatkozó biztonsági ellenőrzések és bevált gyakorlatok átfogó és dinamikus mátrixa;<br>iránymutatás az eszköztár kiválasztott technikai intézkedéseinek végrehajtása tekintetében. | ENISA, tagállami hatóságok |
| **2. kulcsfontosságú célkitűzés: A folyamatos ismeretcsere és kapacitásépítés támogatása** | | |
| **Területek** | **Főbb rövid és középtávú cselekvések** | **Vezető szereplők** |
| **Az ismeretek folyamatos bővítése** | Ismeretszerző tevékenységek szervezése a technológiával és a kapcsolódó kihívásokkal (nyílt architektúrák, az 5G jellemzői – például virtualizáció, konténerizáció, szeletelés stb.), a fenyegetési környezet változásaival, valós eseményekkel stb. kapcsolatban | ENISA, tagállami hatóságok, egyéb érdekelt felek |
| **Kockázatértékelések** | A naprakész nemzeti kockázatértékelésekről szóló információk frissítése és cseréje | Tagállami hatóságok, Bizottság, ENISA |
| **Közös uniós finanszírozású projektek az eszköztár végrehajtásának támogatására** | Az eszköztár végrehajtását támogató projektek pénzügyi támogatása uniós finanszírozás felhasználásával, mindenekelőtt a Digitális Európa program keretében (például kapacitásépítési projektek a nemzeti hatóságok számára, próbapadok vagy egyéb fejlett kapacitások stb.) | Tagállami hatóságok, Bizottság |
| **Az érdekelt felek együttműködése** | Az 5G kiberbiztonságban érintett nemzeti hatóságok (például a kiberbiztonsági együttműködési csoport, a kiberbiztonsági hatóságok, a távközlést szabályozó hatóságok) közötti, illetve a magán érdekelt felekkel folytatott együttműködés elősegítése | Tagállami hatóságok, Bizottság, ENISA |
| **3. kulcsfontosságú célkitűzés: Az ellátási láncok rezilienciájának előmozdítása és egyéb uniós stratégiai biztonsági célkitűzések** | | |
| **Területek** | **Főbb rövid és középtávú cselekvések** | **Vezető szereplők** |
| **Szabványosítás** | Konkrét cselekvési terv kidolgozása és végrehajtása annak érdekében, hogy az EU nagyobb mértékben képviseltesse magát a szabványügyi testületekben a kiberbiztonsági szabványügyi alcsoport által végzett munka következő lépésének részeként konkrét biztonsági célkitűzések elérése céljából, ideértve a beszállítók diverzifikációját elősegítő interoperábilis interfészek előmozdítását | Tagállami hatóságok |

| | | |
|---|---|---|
| **Az ellátási láncok rezilienciája** | – Az 5G ökoszisztéma és ellátási lánc mélyreható elemzése a legfontosabb eszközök és a potenciális kritikus függőségek hatékonyabb azonosítása és nyomon követése érdekében<br>– Annak biztosítása, hogy az 5G piac és ellátási lánc működése megfeleljen az uniós kereskedelmi és versenypolitikai szabályoknak és célkitűzéseknek a Bizottság január 29-i közleményének megfelelően, és a közvetlen külföldi befektetések átvilágítása kiterjedjen az 5G értékláncot potenciálisan érintő beruházási fejlesztésekre, figyelembe véve az eszköztár célkitűzéseit<br>– A meglévő és várható piaci tendenciák nyomon követése, illetve a kockázatok és lehetőségek felmérése a nyílt RAN terén, mindenekelőtt független tanulmány segítségével | Tagállami hatóságok, Bizottság |
| **Tanúsítás** | A legfontosabb 5G alkotóelemekre és a beszállítók folyamataira vonatkozó releváns jelölt tanúsítási rendszerek előkészítésének megkezdése a technikai sebezhetőséggel kapcsolatos egyes kockázatok kezelésének elősegítése érdekében az eszköztár kockázatcsökkentési tervének megfelelően | Bizottság, ENISA, nemzeti hatóságok, egyéb érdekelt felek |
| **Uniós kapacitások és biztonságos hálózatbővítések** | – Beruházások a K+I-be és a kapacitásokba, mindenekelőtt az intelligens hálózatokkal és szolgáltatásokkal kapcsolatos partnerség elfogadásával<br>– Az uniós finanszírozási programokra és a (külső és belső) pénzügyi eszközökre vonatkozó releváns biztonsági feltételek végrehajtása a január 29-i bizottsági közleménynek megfelelően | Tagállamok, Bizottság, az 5G iparágban érdekelt felek |
| **Külső vonatkozások** | Kedvező válaszok az olyan harmadik országoktól érkező megkeresésekre, amelyek szeretnék megérteni és esetlegesen használni az EU által kidolgozott eszköztárral kapcsolatos megközelítést | Tagállamok, Bizottság EKSZ, uniós küldöttségek |