Az Európai Unió
Tanácsa

Brüsszel, 2023. október 18.
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2023. október 18.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2023) 665 final
Tárgy:	A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK a biztonsági unióra vonatkozó uniós stratégia végrehajtásáról szóló hatodik eredményjelentésről

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: COM(2023) 665 final.

Melléklet: COM(2023) 665 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2023.10.18.
COM(2023) 665 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

a biztonsági unióra vonatkozó uniós stratégia végrehajtásáról szóló hatodik eredményjelentésről

I. Bevezetés

Három évvel ezelőtt a Bizottság elfogadta a 2020–2025-ös időszakra szóló, biztonsági unióra vonatkozó stratégiát[1], amely meghatározza az Unió fő prioritásait a biztonság területén. Azóta a stratégia mind a négy pillére keretében jelentős előrehaladást értünk el: mérföldkőnek számító jogszabályokat dolgoztunk ki minden területen, a kritikus szervezetek védelmétől kezdve a kiberreziliencia fokozásáig. Közben azonban folyamatosan változik a biztonsági fenyegetettségi helyzet Európában és a szomszédságunkban egyaránt. Egy franciaországi iskolában és a brüsszeli utcákon az elmúlt napokban elkövetett terrortámadások kíméletlenül emlékeztetnek arra, hogy sürgősen folyatnunk kell biztonsági struktúrának kiigazítását és megerősítését. A kibertámadások jelentette veszély egyre fokozódik, amit az is súlyosbít, hogy rosszindulatú szereplők állást foglalnak a fennálló konfliktusokban. A hibrid fenyegetések, így a dezinformáció előfordulása is egyre gyakoribb. Az Europol megállapította, hogy az Ukrajna elleni orosz agressziós háború az oka annak, hogy jelentős mértékben nőtt az uniós célpontok elleni kibertámadások száma, melyek közt oroszbarát hackercsoportok által koordinált nagyszabású, politikai indíttatású támadások is voltak[2]. Ez az internet-hozzáférés akadályozásában és a kulcsfontosságú szolgáltatások, például az energiahálózatok megszakításában nyilvánult meg.[3]

A biztonsági unióra vonatkozó stratégia célja, hogy felkészítse az EU-t arra, hogy jobban ellenálljon a változó fenyegetettségi helyzetnek. Amikor szembesültünk a világjárvány és a háború okozta válságokkal, az események igazolták a stratégiában alkalmazott megközelítés fontosságát: eltökélt szándékunk, hogy összekössük az EU biztonsági ökoszisztémájában lévő pontokat, és lebontsuk a biztonság kiber- és fizikai dimenzióit egymástól elválasztó falakat, ennek során pedig fellépjünk a szervezett bűnözéssel és a terrorizmussal szemben, és megfékezzük a radikalizálódást.

Az éberség azonban megköveteli, hogy folyamatosan elemezzük, milyen további teendőink vannak polgáraink biztonságának megőrzése érdekében. A stratégia meghatározta azokat a kiemelt területeket, ahol az Unió hozzáadott értéket nyújthat a tagállamok számára az Európában élők biztonságának előmozdításában. A stratégia elfogadása óta már az abban meghatározott összes intézkedéssel foglalkoztunk, és új intézkedéseket építettünk be az aktuális biztonsági kihívásokra való reagálás érdekében.

Összességében a Bizottság 36 jogalkotási kezdeményezést terjesztett elő a biztonsági unióra vonatkozó stratégia keretében. E javaslatok több mint fele esetében az intézményközi tárgyalások már lezárultak szilárd új jogszabályok létrehozásával, amint az a mellékletben található táblázatban szerepel. A Bizottság által javasolt számos kulcsfontosságú kezdeményezéssel kapcsolatban azonban még folyamatban vannak a tárgyalások az Európai Parlamentben és a Tanácsban. Mivel a jelenlegi parlamenti ciklus véget ér a 2024 júniusában sorra kerülő európai választásokkal, gyorsan kell dolgoznunk annak érdekében, hogy

---

1 COM(2020) 605.

2 Elosztott szolgáltatásmegtagadási támadások: lásd az Europol Spotlight jelentését: „Cyber-attacks: the apex of crime-as-a-service” (Kibertámadások: a bűncselekmény mint szolgáltatás csúcsa), 2023. szeptember 13.

3 Az ukrajnai konfliktus során nagymértékben elterjedt a rosszindulatú törlőprogramok használata adatok és rendszerek megsemmisítésére, ami befolyásolta például az internet-hozzáférést az EU-ban több ezer előfizető számára és egy nagy német energiaipari vállalat számára is, amely elvesztette a távellenőrzési hozzáférést több mint 5 800 szélturbinához. „The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict” (A kibertér szerepe az Ukrajna elleni orosz háborúban: Hatása és következményei a fegyveres konfliktus jövőjére nézve), az Európai Parlament tanulmánya, 2023. szeptember – PE 702.594.

megvalósuljanak ezek a folyamatban lévő javaslatok, és a polgárok teljes mértékben részesülhessenek a biztonsági unió nyújtotta előnyökből. A biztonsági unióról szóló jelenlegi, hatodik eredményjelentés középpontjában ezért azoknak a biztonsági unióra vonatkozó, a Bizottság által elfogadott kulcsfontosságú jogalkotási és nem jogalkotási javaslatoknak az ismertetése áll, amelyek véglegesítése és hatékony végrehajtása érdekében további munkára van szükség.

A már elfogadott uniós jogszabályokból származó előnyök csak akkor lesznek érezhetők, ha azokat átültetik a gyakorlatba. A munka során a tagállamok általi helyes és teljes körű átültetésre, végrehajtásra és alkalmazásra kell összpontosítani. 2023-ban a Bizottság továbbra is biztosította a biztonsági unióra vonatkozó uniós stratégia eredményességét azzal, hogy intézményi hatáskörét kihasználva kötelezettségszegési eljárásokat indított minden olyan esetben, amikor a tagállamok nem vagy helytelenül ültették át az uniós jogszabályokat.

Ez a jelentés összefoglalja továbbá azokat az eseteket, amikor a tagállamok és/vagy az uniós ügynökségek tevékenysége a végrehajtás központi eleme. Az uniós ügynökségek döntő szerepet játszanak a biztonsági unióra vonatkozó kezdeményezések végrehajtásának támogatásában, és feladatkörük az elmúlt évek során bővült. A jelentés felvázol néhány olyan fő új feladatot, amelyeket azért határoztak meg, hogy fokozott támogatást nyújtsanak a tagállamoknak a biztonsági unió keretébe tartozó legfontosabb kezdeményezések végrehajtása során.

Emellett a geopolitikai helyzet rávilágított arra, hogy a külső biztonság nagy jelentőséggel bír belső biztonságunk szempontjából. A biztonság területére vonatkozó erősebb uniós belső keret szervesen kapcsolódik a harmadik országokkal való szorosabb partnerségekhez és együttműködéshez. Az EU-nak továbbra is aktívan nyomon kell követnie, hogy a világszintű szerepvállalás miként segíthet annak biztosításában, hogy a polgárok belföldön biztonságban legyenek.

II. Időtálló biztonsági környezet

Kiberbiztonság és a kritikus infrastruktúra rezilienciája

A biztonsági unió keretében az Unió kötelezettséget vállalt arra, hogy minden európai polgár és vállalkozás számára megfelelő online és offline védelmet biztosít, valamint előmozdítja a nyitott, biztonságos és stabil kibertér létrehozását. Az egyre jelentősebb, egyre gyakrabban előforduló és egyre súlyosabb kiberbiztonsági események komoly fenyegetést jelentenek a hálózati és információs rendszerek működésére és a belső piacra. Oroszország Ukrajna elleni agressziós háborúja tovább súlyosbította ezt a fenyegetést, és a jelenlegi geopolitikai feszültségeket súlyosbítja az államhoz kötődő, bűnöző és haktivista szereplők sokaságának tevékenysége. Az Északi Áramlat gázvezetékek ellen tavaly ősszel elkövetett szabotázsakció rávilágított arra, hogy mennyire függenek a reziliens kritikus infrastruktúrától az olyan alapvető ágazatok, mint az energiaágazat, a digitális infrastruktúra, a közlekedés és az űrágazat. Az Észtországban és Finnországban lévő tenger alatti gázvezetéket és adatkábelt érintő közelmúltbeli incidens jól mutatja, hogy magas szintű felkészültségre van szükség az ilyen helyzetek kezeléséhez. Bár a kár oka továbbra is tisztázatlan, és a vizsgálatok még tartanak, a tagállamok és a Bizottság között különböző szinteken megosztott információk biztatóak. A fennakadások nem gyakoroltak közvetlen hatást sem az internetkapcsolatra, sem pedig a gázellátás biztonságára, sem európai, sem helyi szinten. Ez jelzi az elmúlt hónapokban elért eredményeket és a megerősített felkészültség érdekében tett fokozott erőfeszítéseket.

Nélkülözhetetlen tehát egy egyértelmű és szilárd jogi keret e kritikus infrastruktúrák védelmének és rezilienciájának a biztosításához. Ezzel összefüggésben nagy áttörést jelentett az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló felülvizsgált irányelv (NIS 2 irányelv)[4] és a kritikus szervezetek rezilienciájáról szóló irányelv (CER-irányelv)[5] párhuzamos elfogadása, amelyek 2023. január 16-án léptek hatályba. Most nyomatékosan arra kérjük a tagállamokat, hogy mielőbb, de legkésőbb 2024. október 17-ig teljeskörűen ültessék át ezeket az alapvető jogszabályokat annak érdekében, hogy létrejöjjön az Unió kritikus infrastruktúrájának fizikai és kiberfenyegetésekkel szembeni védelmét szolgáló szilárd uniós keret.

2023 júliusában a Bizottság felhatalmazáson alapuló bizottsági rendeletben meghatározta az alapvető szolgáltatásokat a CER-irányelv hatálya alá tartozó 11 ágazatban[6]. A következő lépés az, hogy a tagállamok elvégzik e szolgáltatások kockázatértékelését. A 2022. december 8-i tanácsi ajánlást[7] követően intenzívebbé vált a munka a kritikus infrastruktúrákra vonatkozó, az energiaágazattal kezdődő stressztesztekkel kapcsolatban, valamint a NATO-val és a kulcsfontosságú partnerországokkal folytatott együttműködés megerősítése érdekében. E munka eredményeként 2023 júniusában az EU–NATO munkacsoport jelentést készített a kritikus infrastruktúrák rezilienciájáról, amelyben négy kulcsfontosságú ágazatban (energia, közlekedés, digitális infrastruktúra és űrágazat) feltérképezik a kritikus infrastruktúrákkal kapcsolatos jelenlegi biztonsági kihívásokat, és ajánlásokat fogalmaznak meg a reziliencia fokozására. Az ajánlásokat – többek között a fokozott koordinációra, az információmegosztásra és a gyakorlatokra vonatkozóan – az EU és a NATO személyzete a rezilienciáról szóló strukturált párbeszéd keretében hajtja végre.

Ezzel párhuzamosan, 2023. szeptember 6-án a Bizottság a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák zavaraira való koordinált, uniós szintű reagálásról szóló tervről szóló tanácsi ajánlásra irányuló javaslatot[8] fogadott el. 2023. október 4-én a tervről folytatott, forgatókönyvön alapuló vita formájában gyakorlatot szerveztek, hogy teszteljék, hogy a terv hogyan működne a gyakorlatban, és ezzel hozzájáruljanak a javaslatról a Tanácsban folyó tárgyalásokhoz.

A Tanács felhívására[9] a Bizottság, a főképviselő és a Kiberbiztonsági Együttműködési Csoport kockázatértékeléseket végez és kockázati forgatókönyveket dolgoz ki a kiberbiztonság perspektívájából. Ez a munka első körben a távközlési és a villamosenergia-ágazatra összpontosul. Az összes érintett – polgári és katonai – ügynökség és hálózat bevonásával most először jön létre egy átfogó és inkluzív uniós szintű értékelés. Ez kiegészíti majd a NIS 2 irányelv keretében a kritikus ellátási láncokra vonatkozóan végzett összehangolt biztonsági kockázatértékeléseket, valamint a kritikus infrastruktúrák kockázatértékeléseit és stressztesztjeit az energiaágazatban, a digitális infrastruktúra ágazatában, a hírközlési és a közlekedési ágazatban, valamint az űrágazatban. A koordináció és a koherencia érdekében ezeknek a tevékenységeknek egymásra kell épülniük egy egységes megközelítés kialakítása

---

4 (EU) 2022/2555 irányelv (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2018/1972 irányelv módosításáról (NIS 2 irányelv).

5 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.

6 C(2023) 4878.

7 A Tanács ajánlása (2022. december 8.) a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről.

8 COM(2023) 526.

9 Az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetések és az EU kiberbiztonsági képességeinek megerősítésére irányuló 2022. március 9-i nevers-i felhívás.

érdekében, és iránymutatással kell szolgálniuk jövőbeli gyakorlatok kidolgozásához. Ezen intézkedések sikere most már a tagállamok aktív szerepvállalásán múlik.

A gazdaságok és a társadalmak működése egyre nagyobb mértékben támaszkodik az űrrel kapcsolatos szolgáltatásokra és adatokra, különösen a biztonság és védelem területén. Az űr egyre inkább vitatott stratégiai terület, és különösen az Ukrajna elleni orosz inváziót követően megnőtt a jelentősége a biztonság szempontjából. Az uniós biztonsági és védelmi űrstratégia elfogadására 2023 márciusában került sor azzal a céllal, hogy megerősítsük űrbeli stratégiai helyzetünket és autonómiánkat. Az e stratégiából eredő kulcsfontosságú intézkedésként az Európai Bizottság 2024-ben uniós űrjogszabályra vonatkozó javaslatot nyújt be, amely szabályozza az EU-ban folytatott űrtevékenységek biztonságát, fenntarthatóságát és rezilienciáját/védelmét.

A külső dimenziót tekintve a biztonságos infrastruktúra a globális gazdaság és ellátási láncok rezilienciájának alapját képezi[10], ezért az EU Global Gateway stratégiája erős biztonsági dimenziót foglal magában. Hasonlóképpen, tekintettel az EU és a partnerországok infrastruktúrája közötti összeköttetésekre, elengedhetetlen a további nemzetközi együttműködés a globális kiberreziliencia megerősítéséhez, valamint a szabad, nyitott, biztonságos és védett kibertér támogatásához.

A kiberrezilienciáról szóló jogszabály

Az európai kiberbiztonság szempontjából központi jelentőségű annak biztosítása, hogy a fogyasztók és a vállalkozások biztonságos digitális termékekre támaszkodhassanak. A Bizottság a kiberrezilienciáról szóló jogszabályra irányuló, 2022. szeptember 15-én elfogadott javaslatában[11] igyekezett kezelni ezt az igényt. A jogszabály kötelező horizontális kiberbiztonsági követelményeket vezetne be a digitális elemeket tartalmazó termékekre vonatkozóan öt éven keresztül vagy a termék teljes élettartama alatt (attól függően, hogy melyik a rövidebb időszak). Megteremtené a digitális elemeket tartalmazó biztonságos termékek tervezésének és fejlesztésének feltételeit, biztosítva azt, hogy a hardver- és szoftvertermékeket a lehető legkevesebb sebezhetőséggel hozzák forgalomba. Ez kulcsfontosságú mérföldkő lenne az európai kiberbiztonsági előírások javítása terén valamennyi területen, és valószínűleg nemzetközi referenciaponttá válik, egyértelmű előnyöket biztosítva az Unió kiberbiztonsági ipara számára a globális piacokon. 2023 júliusában az Európai Parlament és a Tanács is elfogadta saját álláspontját, és a tárgyalásoknak gyors ütemben kell haladniuk.

A kiberbiztonsági tanúsítás döntő szerepet játszik az IKT-termékekbe és -szolgáltatásokba vetett bizalom növelésében is, lehetővé téve a fogyasztók, a vállalkozások és a hatóságok számára, hogy megfelelő szintű kiberbiztonság mellett megalapozott döntéseket hozzanak. A kiberbiztonsági tanúsítással kapcsolatos munka jól halad, és a közös kritériumokon alapuló uniós kiberbiztonsági tanúsítási rendszert bizottsági eljárás keretében értékelik. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) jelenleg dolgozik a számításifelhő-szolgáltatásokra vonatkozó javaslati európai kiberbiztonsági tanúsítási rendszer (EU Cloud Security Certification Scheme – EUCS) előkészítésén, és az jelenleg megbeszélések tárgyát képezi az európai kiberbiztonsági tanúsítási csoportban. A különböző ágazatok, fogyasztók és szolgáltatók szakértőivel folytatott intenzív munkának olyan szilárd jogi és technikai megközelítést kell eredményeznie, amely biztosítja a szükséges biztonsági garanciákat, az uniós joggal, a nemzetközi kötelezettségvállalásokkal és a WTO-kötelezettségekkel összhangban. Emellett az ENISA az EU5G javaslati rendszer és az európai digitális személyiadat-tárca (EUIDW) előkészítésén is dolgozik. Az IKT-termékek, az IKT-

[10] JOIN(2021) 30.
[11] COM(2022) 454.

szolgáltatások és az IKT-folyamatok általános biztonságának növelése érdekében elengedhetetlenül fontos, hogy az összes tagállam összehangolt erőfeszítéseket tegyen.

Az uniós intézmények, szervek és ügynökségek információbiztonságáról és kiberbiztonságáról szóló rendeletek

A 2022 márciusában együttesen javasolt, az Unió saját intézményeinek kiberbiztonságát és információbiztonságát szabályozó rendeletek eltérő ütemben haladtak. Tavaly júniusban politikai megállapodás született a kiberbiztonsági rendeletről, lehetővé téve valamennyi uniós intézmény, szerv, hivatal és ügynökség kiberbiztonsági helyzetének megerősítését, és tükrözve azt, hogy az EU nagy jelentőséget tulajdonít e javaslat gyors végrehajtásának. Ebben a helyzetben különösen aggasztó, hogy az információbiztonságra vonatkozó párhuzamos javaslat, amely elengedhetetlen ahhoz, hogy teljessé váljon az uniós intézményekre, szervekre és ügynökségekre vonatkozó szilárd jogi keret, nem várt módon lassan halad előre. Mindkét javaslatot még az európai parlamenti választások előtt el kell fogadni annak érdekében, hogy az európai közigazgatás hiteles és reziliens legyen a jelenlegi geopolitikai környezetben. Az Unió valamennyi intézményére, szervére és ügynökségére vonatkozó információbiztonsági szabályok és előírások minimális készlete jogbiztonságot teremtene valamennyi érintett fél számára, és következetes védelmet biztosítana az adataikat fenyegető, folyamatosan változó fenyegetésekkel szemben, legyenek azok EU-minősített vagy nem minősített adatok. Ezek az új szabályok együttesen stabil alapot biztosítanának az uniós intézmények, szervek és ügynökségek között és a tagállamokkal folytatott biztonságos információcseréhez, az információáramlás védelmét szolgáló szabványosított gyakorlatok és intézkedések révén. Ilyenként pedig reagálnak a Tanács azon többszöri felhívására, hogy fokozni kell az uniós intézmények, szervek és ügynökségek rezilienciáját, és jobban kell védeni az uniós döntéshozatali folyamatot a rosszindulatú beavatkozásokkal szemben.

A kiberbiztonsági szolidaritásról szóló jogszabály

A már meglévő erős stratégiai, szakpolitikai és jogalkotási keretre építve a Bizottság 2023 április 18-án elfogadta a javasolt kiberbiztonsági szolidaritásról szóló jogszabályt[12], amely további erősítené a kiberfenyegetések felderítését, valamint a rezilienciát és a felkészültséget az EU kiberbiztonsági ökoszisztémájának minden szintjén. Ezek a célkitűzések három fő intézkedés révén valósulnának meg:

(1) ***Európai kiberbiztonsági pajzs*** létrehozása közös észlelési és helyzetismereti képességek kialakítása és javítása érdekében. Ez nemzeti biztonsági műveleti központokból és határokon átnyúló biztonsági műveleti központokból állna.
(2) ***Kiberbiztonsági vészhelyzeti mechanizmus*** létrehozása, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, az azokra való reagálásban és az azonnali helyreállításban. A biztonsági eseményekre való reagáláshoz nyújtott támogatás magában foglalná az uniós kiberbiztonsági tartalékot, amely rendelkezésre állna az uniós intézmények, szervek, hivatalok és ügynökségek számára, valamint a Digitális Európa programhoz társult harmadik országok számára, amennyiben erről rendelkezik a Digitális Európa programhoz való társulásukról szóló megállapodás.
(3) A ***kiberbiztonsági események európai felülvizsgálati mechanizmusának*** létrehozása bizonyos jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálatára és

[12] COM(2023) 209.

értékelésére. A kiberbiztonsági eseményeket követő felülvizsgálati jelentést az ENISA koordinálná és készítené el.

A Tanácsban és az Európai Parlamentben elkezdődtek a megbeszélések. A tárgyalások lezárása az Európai Parlament jelenlegi mandátumának lejárta előtt jelentős lendületet adna az uniós polgárok és vállalkozások védelmére irányuló erőfeszítéseknek.

Kiberkészségek Akadémiája

A kiberfenyegetések fokozódásával az EU-nak sürgősen szüksége van olyan szakemberekre, akik megfelelő készségekkel és kompetenciákkal rendelkeznek ahhoz, hogy megelőzzék, felderítsék és elhárítsák a kibertámadásokat, illetve megvédjék az EU-t azokkal szemben. Az EU kiberbiztonsági munkaerőigénye jelenleg 883 000 szakemberre becsülhető, míg 2022-ben 260 000 és 500 000 között volt a betöltetlen álláshelyek száma. A társadalom egészét ösztönözni kell arra, hogy segítsenek betölteni ezt a hiányt, viszont például 2022-ben a kiberbiztonsági végzettséggel rendelkezők mindössze 20 %-a, és az információs és kommunikációs technológiában jártas szakemberek csupán 19 %-a volt nő. A készségek 2023-as európai évének keretében a Bizottság 2023. április 18-án elfogadta a kiberbiztonsági szakemberhiány megszüntetése érdekében a Kiberkészségek Akadémiájának létrehozására irányuló kezdeményezést[13], amelyet a tagállamok üdvözöltek[14]. A Kiberkészségek Akadémiája összefogná a kiberbiztonsági készségekkel kapcsolatos meglévő kezdeményezéseket, és javítaná a koordinációt. A Bizottság arra ösztönzi a tagállamokat, a regionális és helyi hatóságokat, valamint az európai közintézményeket, hogy fogadjanak el a kiberbiztonsági készségekre irányuló célzott stratégiákat vagy kezdeményezéseket, vagy pedig építsék be a kiberbiztonsági készségeket szélesebb körű releváns stratégiákba vagy kezdeményezésekbe (pl. kiberbiztonság, digitális készségek, foglalkoztatás stb.). A magánszektorbeli érdekelt felek bevonása szintén elengedhetetlen lesz a kiberbiztonsági készséghiány és a kapcsolódó munkaerőhiány csökkentéséhez Európában.

Pilóta nélküli légi járművek

A nyilvános tereket és a kritikus infrastruktúrákat fenyegető másik növekvő veszélyt a pilóta nélküli légi járművek rosszindulatú használata jelenti. A pilóta nélküli légi járművekhez kötődő biztonsági események gyakoribbá váltak az Unión belül és kívül egyaránt, és az elhárításukra kifejlesztett megoldások kulcsfontosságú eszközt jelentenek az Unióban a bűnüldöző hatóságok és más közigazgatási szervek számára, valamint a kritikus infrastruktúrákat üzemeltető magánszereplők számára. Ugyanakkor a személyzet nélküli légi járművek jogszerű használata jelentősen hozzájárul a zöld és digitális kettős átálláshoz.[15] A 2022 novemberében elfogadott 2.0-s drónstratégiában foglaltaknak megfelelően a Bizottság a mai napon közleményt fogad el a pilóta nélküli légi járművek jelentette potenciális fenyegetések elhárításának módjáról, amelyet a kulcsfontosságú technikai szempontokra vonatkozó gyakorlati iránymutatást tartalmazó két kézikönyv támaszt alá[16]. A kezdeményezés célja átfogó és harmonizált szakpolitikai keret biztosítása az alkalmazandó szabályok közös értelmezésének kialakításával a pilóta nélküli légi járművek jelentette lehetséges fenyegetések leküzdése érdekében, valamint a gyors technológiai fejlődéshez való, szükség szerinti alkalmazkodás céljából. A Bizottság felkéri a tagállamokat és az érintett magánszereplőket, hogy szorosan működjenek együtt a Bizottsággal a kezdeményezés teljes körű végrehajtása érdekében.

[13] COM(2023) 207.
[14] A Tanács következtetései (2023. május 22.) az EU kibervédelmi politikájáról.
[15] COM(2022) 652.
[16] COM(2023) 659.

Tengeri védelem és a légi közlekedés védelme

Az olyan illegális tevékenységek, mint a kalóztevékenység, a tengeren elkövetett fegyveres rablások, a migránscsempészés, az emberkereskedelem, a fegyver- és kábítószer-kereskedelem, valamint a terrorizmus továbbra is kihívást jelentenek a tengeri védelem számára, és ezeket súlyosbítják az újonnan felmerülő fenyegetések, köztük a hibrid és a kibertámadások. A Bizottság és a főképviselő 2023. március 10-én közös közleményt fogadott el, amelyben aktualizálták az EU tengeri védelmi stratégiáját[17], amelyet most az aktualizált cselekvési tervvel összhangban kell végrehajtani.

A légi közlekedés védelme területén a Bizottság 2023. február 2-án szolgálati munkadokumentumot fogadott el „A megerősített és reziliensebb légiközlekedés-védelmi politika felé”[18] címmel, amely ambiciózus programot tartalmaz 1. a légi közlekedés védelmére vonatkozó szabályozási szerkezet korszerűsítésére, 2. az innovatívabb megoldások kifejlesztésének és alkalmazásának előmozdítására; és 3. a légiközlekedés-védelmi alapkövetelmények olyan módon történő aktualizálására, hogy az uniós repülőterek teljes mértékben kihasználhassák az új és élvonalbeli technológiák előnyeit a legmagasabb prioritású fenyegetések kezelése érdekében. Tizennégy kiemelt intézkedést kell végrehajtani két éven belül.

A Bizottság felszólítja az Európai Parlamentet és a Tanácsot, hogy sürgősen, de még mindenképpen a jelenlegi Európai Parlament megbízatásának lejárta előtt zárják le a tárgyalásokat az alábbi dokumentumok vonatkozásában:

- a kiberrezilienciáról szóló jogszabályra irányuló javaslat,
- a kiberbiztonsági szolidaritásról szóló jogszabályra irányuló javaslat,
- rendeletjavaslat az uniós intézmények, szervek és ügynökségek információbiztonságáról.

A Bizottság felszólítja a tagállamokat, hogy:

- kezeljék prioritásként a kritikus szervezetek rezilienciájáról szóló irányelv átültetését, valamint az energiaágazatbeli kritikus infrastruktúrák stressztesztelését,
- fogadják el a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák zavaraira való koordinált, uniós szintű reagálásról szóló tervről szóló tanácsi ajánlást,
- teljeskörűen és sürgősen ültessék át a NIS 2 irányelvet az alapvető és fontos szervezetek kiberbiztonságának fokozása érdekében,
- aktívan vegyenek részt a kiberbiztonsági kockázatértékelések elvégzésében, valamint a kritikus infrastruktúrákra és ellátási láncokra vonatkozó kockázati forgatókönyvek kidolgozásában,
- kövessék a Kiberkészségek Akadémiáját határozott európai szintű szerepvállalással és a kiberbiztonsági készségekre irányuló célzott nemzeti stratégiákkal vagy kezdeményezésekkel, bevonva a kulcsfontosságú érdekelt feleket, köztük a regionális és helyi hatóságokat,
- működjenek együtt az érintett magánszereplőkkel és a Bizottsággal a drónok jelentette potenciális fenyegetések elhárításáról szóló közleményben felsorolt valamennyi intézkedés végrehajtásának biztosítása érdekében,
- hajtsák végre az Európai Unió tengeri védelmi stratégiájához kapcsolódó cselekvési tervet, és rendszeresen számoljanak be az elért eredményekről,

[17] JOIN(2023) 8.
[18] SWD(2023) 37.

- hajtsák végre a légi közlekedés védelmének fokozása érdekében meghatározott 14 kiemelt intézkedést.

III. Az újonnan felmerülő fenyegetések kezelése

Az új geopolitikai feszültségek könyörtelenül igazolták, hogy az EU előtt álló biztonsági kihívások nem csupán fokozódnak, de egyre kiszámíthatatlanabbak, és sok esetben a fenyegetések hibrid jellege is súlyosbítja őket. A védelemi intézkedéseknek a társadalmi és technológiai változásokkal is lépést kell tartaniuk. A Covid19-világjárvány felerősítette a kiberbűnözők lehetőségeit, és különösen fokozódott a gyermekek szexuális bántalmazását ábrázoló online anyagok jelentette veszély. A bűnözők és a rosszindulatú szereplők mindig készen állnak a technológiai fejlődés kiaknázására. Az ilyen, gyakran összetett és többdimenziós fenyegetésekkel szemben határozott és egységes uniós fellépésre van szükség.

Rendelet a gyermekek online szexuális bántalmazása elleni küzdelemről

Az Europol internetes szervezett bűnözés általi fenyegetettségről szóló értékelése feltárta, hogy 2022-ben gyakoribbá vált és súlyosbodott a gyermekek szexuális kizsákmányolása és bántalmazása, és az elkövetők továbbra is kihasználták a technikai lehetőségeket tevékenységeik és személyazonosságuk elleplezése érdekében[19].A vállalatok általi önkéntes felderítésen és jelentéstételen alapuló jelenlegi rendszer elégtelennek bizonyult a gyermekek védelmére. Egy ideiglenes rendelet lehetővé teszi a vállalatok általi önkéntes felderítést és jelentéstételt, amennyiben az jogszerű az általános adatvédelmi rendelet értelmében. Ez a rendelet 2024 augusztusában hatályát veszti. 2022 májusában a Bizottság rendeletjavaslatot[20] terjesztett elő az online szolgáltatásokkal való, a gyermekek szexuális bántalmazása céljából történő visszaélések elleni fellépésre vonatkozóan. A javasolt keret nagy hangsúlyt fektet a megelőzésre. A vállalatok kötelesek lennének értékelni a rendszereiken keresztül a gyermekek szexuális bántalmazásának kockázatát, és megelőző intézkedéseket hozni. Végső eszközként, kizárólag jelentős kockázat esetén, a nemzeti bíróságok vagy a független közigazgatási hatóságok célzott felderítést elrendelő határozatokat bocsáthatnak ki a szolgáltatók számára. Egy új, független uniós központ előmozdítaná a szolgáltatók erőfeszítéseit azzal, hogy szakértői hátteret biztosít, megbízható információkat szolgáltat az azonosított anyagokról, fogadja és elemzi a gyermekek online szexuális bántalmazásáról a szolgáltatóktól érkező jelentéseket a téves bejelentések azonosítása érdekében, valamint támogatást nyújt az áldozatoknak. Alapvető fontosságú, hogy az új szabályokat a lehető leghamarabb elfogadják és végrehajtsák a gyermekek további bántalmazással szembeni védelme, az anyagok újbóli online felbukkanásának megakadályozása, valamint az elkövetők bíróság elé állítása érdekében. Folyamatban vannak a tárgyalások a Tanácsban és a Parlamentben azzal a céllal, hogy még a Parlament megbízatásának lejárta előtt megállapodás szülessen a javaslatról.

Irányelv a nők elleni erőszak és a kapcsolati erőszak elleni küzdelemről

A nők elleni – többek között a kapcsolati erőszakkal összefüggésben elkövetett – online erőszak az ilyen erőszak új formájaként jelent meg, amely az interneten és az informatikai eszközökön keresztül az egyes tagállamokon túlra is átterjed. 2022 márciusában a Bizottság javaslatot tett a nők elleni erőszak és a kapcsolati erőszak elleni küzdelemről szóló irányelvre, beleértve az

[19] Europol (2023), Az internetes szervezett bűnözés általi fenyegetettség értékelése (IOCTA), 2023.
[20] COM (2022) 209.

online erőszakra vonatkozó konkrét szabályokat, valamint a védelem, az igazságszolgáltatáshoz való jog és a megelőzés terén fennálló hiányosságok orvoslására irányuló intézkedéseket. Az irányelv mielőbbi elfogadása és végrehajtása további eszközöket biztosítana a tagállamok számára a bűnözés e formája elleni küzdelemhez. A társjogalkotók 2023 júliusában intézményközi tárgyalásokat kezdtek, és arra törekszenek, hogy még az Európai Parlament jelenlegi megbízatásának lejárta előtt lezárják a tárgyalásokat.

5G kiberbiztonság

Az 5G hálózatok biztonsága a Bizottság egyik fő prioritása és a biztonsági unióra vonatkozó stratégia alapvető eleme. Az 5G hálózatok olyan központi infrastruktúrák, amelyek a belső piac működéséhez, valamint az alapvető társadalmi és gazdasági funkciók működtetéséhez nélkülözhetetlen szolgáltatások széles körének az alapját képezik. 2023. június 15-én a Kiberbiztonsági Együttműködési Csoportban képviselt uniós tagállami hatóságok a Bizottság és az ENISA támogatásával közzétették az 5G kiberbiztonsággal kapcsolatos uniós eszköztár végrehajtásáról szóló második eredményjelentést. A jelentés szerint 24 tagállam fogadott el vagy készít elő olyan jogalkotási intézkedéseket, amelyek jogosultságot adnak a nemzeti hatóságoknak a beszállítók értékelésére és korlátozások bevezetésére, 10 tagállam pedig már bevezette ezeket a korlátozásokat. További intézkedésekre van azonban szükség az Unió egészét érintő sebezhetőségek elkerülése érdekében, amelyek szerte az Unióban súlyos negatív hatást gyakorolhatnak az egyéni felhasználók és a vállalatok biztonságára, valamint az Unió kritikus infrastruktúrájára. A tagállamoknak késedelem nélkül végre kell hajtaniuk az eszköztárat. Ugyanezen a napon a Bizottság közleményt fogadott el az eszköztár tagállamok általi végrehajtásáról, valamint az EU saját intézményi kommunikációs és finanszírozási tevékenységeiről. Ebben hangsúlyozta, hogy mély aggodalommal töltik el azok a kockázatok, amelyeket a mobilhálózati kommunikációs berendezések egyes beszállítói, a Huawei és a ZTE jelentenek az Unió biztonságára nézve. Ezzel összefüggésben a Bizottság intézkedéseket foganatosít annak elkerülésére, hogy az intézményi kommunikáció ki legyen téve a Huawei-t és a ZTE-t beszállítóként használó mobilhálózatoknak. A beszerzésekből kizárják az olyan új konnektivitási szolgáltatásokat, amelyek az említett beszállítók berendezéseire támaszkodnak, és a Bizottság együtt fog működni a tagállamokkal és a távközlési szolgáltatókkal, hogy ezeket a beszállítókat fokozatosan kiszorítsák a bizottsági helyszínek meglévő konnektivitási szolgáltatásaiból. A Bizottság emellett valamennyi vonatkozó uniós finanszírozási programban és eszközben érvényesíteni kívánja ezt a döntést, az uniós joggal teljes összhangban.

Adatokhoz való hozzáférés a hatékony bűnüldözés érdekében

Napjaink digitális korában szinte minden bűncselekménynek van digitális eleme. A technológiákat és az eszközöket bűnügyi célokra is felhasználják, köztük azokat is, amelyek ahhoz szükségesek, hogy kielégítsék a kiberbiztonság, az adatvédelem és a magánélet védelme iránti társadalmi igényt. Emiatt egyre nagyobb problémát jelent a hatékony bűnüldözés fenntartása az EU-ban a közbiztonság védelme, valamint a bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében, és bár uniós és nemzeti szinten is jelentős erőfeszítésekre került sor, többek között jogszabályok, valamint kapacitásépítés és innovációs kezdeményezések révén, még mindig vannak jogi és technikai kihívások. A Bizottság a Tanács elnökségével együttműködve a hatékony bűnüldözés érdekében létrehozta az adatokhoz való hozzáféréssel foglalkozó magas szintű munkacsoportot, hogy együttműködési platformot biztosítson az érdekelt felek és a szakértők széles köre számára a bűnüldözési szakemberek előtt álló kihívások (pl. titkosítás, adatmegőrzés, 5G és szabványosítás) feltárása érdekében. A Bizottság azt várja a magas szintű munkacsoporttól, hogy 2024 júniusáig – többek között a kiberbiztonság és az adatvédelem perspektívájából – fogalmazzon meg kiegyensúlyozott, szilárd és megvalósítható ajánlásokat, amelyek tükrözik e

kérdések összetettségét. A tagállamokat és a részt vevő szakértőket ezért arra ösztönözzük, hogy aktívan vegyenek részt ebben a folyamatban, és törekedjenek arra, hogy hatékony, jogszerű és általánosan elfogadott megoldásokat találjanak.

Hibrid fenyegetések

Egy olyan geopolitikai környezetben, amelyben a hibrid fenyegetések egyre összetettebbé és kifinomultabbá válnak, az EU-nak a biztonság és a védelem területére vonatkozó stratégiai iránytűje[21] (stratégiai iránytű) az Unió előtt álló fenyegetésekre és kihívásokra vonatkozó közös értékelést, valamint stratégiai cselekvési tervet bocsátott rendelkezésre. Az államok és a nem állami szereplők rossz szándékú kibertevékenységének fokozódása – többek között az Ukrajna elleni háborúval összefüggésben – még inkább rávilágított a kibertér mint kül- és biztonságpolitikai terület jelentőségére. A rosszindulatú fellépések és a dezinformáció potenciális kockázata különös éberséget tesz szükségessé a választási időszakokban, így a 2024-es európai parlamenti választások közeledtével is.

Tekintettel a tovagyűrűző hatások magas kockázatára, az EU folytatja a kiberkapacitás-építési tevékenységek fejlesztését, és támogatja a harmadik országokkal való partnerségeket – például célzott kiberpárbeszédek révén – annak érdekében, hogy aktívan elősegítse általános rezilienciáját. A hibrid fenyegetésekről szóló, 2023. szeptember 14-én közzétett hetedik eredményjelentésben[22] leírtaknak megfelelően sor került számos eszköz kifejlesztésére, felülvizsgálatára és megerősítésére, hogy az Unió még inkább képes legyen hatékonyan kezelni a hibrid fenyegetéseket. Ezek közé tartoznak a következők:

- uniós hibrid eszköztár a hibrid fenyegetésekre és hadjáratokra való összehangolt és megalapozott reagálás keretének biztosítása érdekében,
- a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatok létrehozására irányuló, folyamatban lévő munka, a tagállamok, a partnerországok, valamint a közös biztonság- és védelempolitikai (KBVP) missziók és műveletek számára rövid távú, testre szabott támogatás nyújtása érdekében,
- a hibrid fenyegetésekkel szembeni fellépés uniós operatív protokollja[23], amely leírja a hibrid fenyegetésekkel és hadjáratokkal foglalkozó uniós folyamatokat és struktúrákat,
- a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete[24] (kiberdiplomáciai eszköztár), amely lehetővé teszi a tartós kiberfenyegetésben részt vevő fenyegető szereplőkkel szembeni hosszú távú, testre szabott, koherens és összehangolt stratégiák kidolgozását,
- a külföldi információmanipuláció és beavatkozás kezelésére szolgáló eszköztár a külföldi információmanipuláció és beavatkozás megelőzésére, megakadályozására és az arra való reagálásra szolgáló meglévő uniós eszközök megerősítése érdekében,
- az uniós kibervédelmi politika[25], amelynek célja az uniós kibervédelmi képességek megerősítése, a helyzetismeret javítása és a rendelkezésre álló védelmi lehetőségek teljes körének összehangolása a reziliencia megerősítése, a kibertámadásokra való reagálás, valamint a szolidaritás és a kölcsönös segítségnyújtás biztosítása érdekében.

A Bizottság ezért arra ösztönzi a tagállamokat, hogy folytassák és fokozzák együttműködésüket ezen a területen azzal, hogy biztosítják a fent említett eszköztárak hatékony végrehajtását, többek között rendszeres gyakorlatok révén, továbbá azzal, hogy megállapodásra jutnak a hibrid fenyegetéseket kezelő gyorsreagálású csapatok koncepciója

[21] A 7371/22. sz. tanácsi dokumentum.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 2023. június 8-i 10289/23. sz. dokumentum.
[25] JOIN(2022) 49.

tekintetében, ami iránymutatásul szolgál majd a csapatok létrehozása érdekében teendő további lépésekhez.

Mesterséges intelligencia a bűnüldözéssel összefüggésben

A mesterséges intelligencia (MI) nagyon rövid idő alatt a mindennapi élet megszokott elemévé vált. A mesterséges intelligencia használatának a kiberbűnözésre és a kiberbiztonságra gyakorolt hatásai még nem teljesen ismertek, de egyértelműen új kihívásokat fognak jelenteni. Bár a mesterséges intelligencia hasznos lehet, ha biztonságos és ellenőrzött módon használják, rosszindulatú szereplők kezében veszélyessé válhat, például ha segíti a bűnözőket személyazonosságuk elrejtésében olyan bűncselekmények során, mint a terrorizmus vagy gyermekek szexuális bántalmazása. Ezért alapvető fontosságú, hogy a hatóságok lépést tartsanak a fejlődéssel az erőszak megelőzése és a visszaélésekre való reagálás érdekében[26]. A mesterséges intelligenciáról szóló jogszabályra irányuló javaslatról folytatott tárgyalások célja e kérdések kezelése. Ezek a tárgyalások kulcsfontosságú szakaszba léptek, mivel a társjogalkotók most vitatják meg azokat a technikai és politikai kérdéseket, amelyek meghatározzák az ezzel a technológiával való együttműködést az elkövetkező években. Alapvető fontosságú, hogy kiegyensúlyozott megoldásokat találjunk, különösen a nagy kockázatú alkalmazások tekintetében, többek között a bűnüldözés területén.

A Bizottság felszólítja az Európai Parlamentet és a Tanácsot, hogy sürgősen, de még mindenképpen a jelenlegi Európai Parlament megbízatásának lejárta előtt zárják le az intézményközi tárgyalásokat az alábbi, függőben lévő javaslatok vonatkozásában:

- rendeletjavaslat a gyermekek online szexuális bántalmazása elleni küzdelemről,
- irányelvjavaslat a nők elleni erőszak és a kapcsolati erőszak elleni küzdelemről,
- rendeletjavaslat a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (a mesterséges intelligenciáról szóló jogszabály).

A Bizottság felszólítja a tagállamokat, hogy:

- haladéktalanul gondoskodjanak az 5G kiberbiztonsággal kapcsolatos uniós eszköztár teljes körű végrehajtásáról,
- támogassák a hatékony bűnüldözés érdekében az adatokhoz való hozzáféréssel foglalkozó magas szintű munkacsoport munkáját, hogy egyértelmű, szilárd és megvalósítható ajánlásokat fogalmazzon meg a jelenlegi és a várható kihívások arányos kezeléséhez,
- a főképviselővel együttműködve tegyenek lépéseket az uniós hibrid eszköztár, a felülvizsgált kiberdiplomáciai eszköztár és a külföldi információmanipuláció és beavatkozás kezelésére szolgáló eszköztár hatékony végrehajtásának biztosítása érdekében, többek között rendszeres gyakorlatok révén, és a globális dinamikát figyelembe véve,
- jussanak megállapodásra a hibrid fenyegetéseket kezelő gyorsreagálású csapatok koncepciója tekintetében.

[26] Lásd például az Europol 2023. április 17-én közzétett jelentését: ChatGPT - the impact of Large Language Models on Law Enforcement (ChatGPT – a nagy nyelvi modellek hatása a bűnüldözésre).

IV. Az európaiak védelme a terrorizmussal és a szervezett bűnözéssel szemben

Mindig fennáll annak a kockázata, hogy a globális vagy helyi események újabb terrorista akciókat idéznek elő. Ezzel párhuzamosan a szervezett bűnözés és a kábítószer-kereskedelem az EU biztonságát fenyegető legsúlyosabb veszélyek közé tartozik. Az e fenyegetések elleni küzdelem során tett közös uniós erőfeszítések fokozása érdekében folyamatban van a közös munka a szervezett bűnözés elleni küzdelemre irányuló uniós stratégia[27], az emberkereskedelem elleni küzdelemre irányuló uniós stratégia[28], az EU kábítószer elleni programja és cselekvési terve[29], valamint EU terrorizmus elleni programja[30] végrehajtása terén. Ugyanakkor a szervezett bűnözés és a kábítószer-kereskedelem terén tapasztalható, aggasztóan súlyosbodó helyzetre való reagálás érdekében a tagállamoknak és az EU-nak még intenzívebben kell dolgozniuk a szervezett bűnözői hálózatokkal szembeni kollektív fellépés megerősítése és a bűncselekmények áldozatainak jobb védelme érdekében; e jelentéssel egyidejűleg sor kerül a kábítószer-kereskedelem és a szervezett bűnözés elleni küzdelemre vonatkozó uniós ütemterv közzétételére[31].

A terrorizmus elleni küzdelem területén az EU megerősíti külső eszköztárát[32], és teljeskörűen kihasználja a terrorizmus elleni küzdelemről folytatott magas szintű párbeszédeket és az Unió küldöttségein szolgálatot teljesítő terrorizmusellenes/biztonsági szakértők hálózatát, továbbá multilaterális fórumokon vesz részt, többek között a terrorizmus elleni küzdelem világfórumának (GCTF) társelnökeként.

Kábítószer-kereskedelem

A Kábítószer és a Kábítószerfüggőség Európai Megfigyelőközpontja 2024 júliusától életbe lépő új megbízatásával az EU felkészültebb lesz egy olyan összetett biztonsági és egészségügyi probléma kezelésére, amely emberek millióit érinti az EU-ban és világszerte. Emellett a Bizottság felülvizsgálja[33] a kábítószer-prekurzorokról szóló rendeleteket[34] a 2020. évi értékelésben[35] azonosított fő kihívások kezelése érdekében, amely kiemelte, hogy a tiltott kábítószerek kínálatának csökkentése érdekében foglalkozni kell a dizájner prekurzorok[36] jelentette kihívásokkal.

Ugyanakkor azonban, tekintettel a tiltott kábítószerek rendelkezésre állásának példátlan mértékű növekedésére Európában, a nemzetközi partnerekkel együttműködve fokozni kell a kábítószer-kereskedelem elleni küzdelmet. A tagállamok és az EU részéről további intézkedésekre van szükség a bűnözői hálózatok felszámolása és a bűncselekmények áldozatainak jobb védelme érdekében. A Bizottság a mai napon a kábítószer-kereskedelem és a szervezett bűnözés elleni küzdelemre vonatkozó uniós ütemtervet terjeszt elő. Ebben 17 fellépést határoz meg négy kiemelt területen: a logisztikai központok rezilienciájának megerősítése az Európai Kikötők Szövetségével, a bűnözői hálózatok felszámolása, a

[27] COM(2021)170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM (2020) 795.
[31] COM (2023) 641.
[32] A stratégiai iránytűben, valamint a terrorizmus és az erőszakos szélsőségesség általi folyamatosan változó fenyegetettség külső dimenziójának kezeléséről szóló, 2022 júniusában elfogadott tanácsi következtetésekben foglalt felhívásnak megfelelően.
[33] Kábítószer-prekurzorok – uniós jogszabályok (felülvizsgált szabályok) (europa.eu).
[34] 273/2004/EK rendelet a kábítószer-prekurzorokról, valamint a Tanács 111/2005/EK rendelete a kábítószer-prekurzoroknak a Közösség és harmadik országok közötti kereskedelme nyomon követésére vonatkozó szabályok megállapításáról.
[35] COM(2020) 768.
[36] A kábítószer elleni program és cselekvési terv 23. fellépése, COM(2020) 606.

megelőzésre irányuló erőfeszítések fokozása és a nemzetközi partnerekkel való együttműködés elősegítése. Ezeket az intézkedéseket 2024-ben és 2025-ben kell végrehajtani.

Tűzfegyverek

A tűzfegyverek tiltott kereskedelme segíti a szervezett bűnözést az EU-n belül és annak szomszédságában egyaránt. Becslések szerint az EU-ban 35 millió illegális tűzfegyvert tartanak polgári személyek, és a Schengeni Információs Rendszerben mintegy 630 000 lopott vagy elvesztett tűzfegyvert tartanak nyilván. A gyors csomagkézbesítés lehetőségével és az új technológiák, pl. a 3D nyomtatás fejlődésével a tűzfegyverek tiltott kereskedelme az ellenőrzés elkerülését célzó új formákat ölt. Oroszország Ukrajna elleni agressziós háborúja szintén növelte a tűzfegyverek elterjedésének kockázatát. 2022 októberében a Bizottság javaslatot fogadott el a polgári célú tűzfegyverek behozatalára, kivitelére és továbbítására vonatkozó hatályos jogszabályok aktualizálásáról, hogy megszüntesse a meglévő szabályokban rejlő kiskapukat, amelyek növelhetik az EU-ba becsempészett, illetve oda átirányított tűzfegyverek számát[37]. Középtávon ezek az új szabályok segítenek csökkenteni az embargók kijátszásának kockázatát a polgári felhasználásra szánt tűzfegyverek kivitele esetén, és fokozni fogják az ilyen típusú tűzfegyverek nem uniós országokból történő behozatalának ellenőrzését. Mindkét társjogalkotónak el kell még fogadnia a javaslattal kapcsolatos álláspontját annak érdekében, hogy a jelenlegi Parlament megbízatásának lejárta előtt megállapodásra jussanak erről a javaslatról.

Emberkereskedelem

Az emberkereskedelem a szervezett bűnözés különösen súlyos formája, és az alapvető jogok súlyos megsértését jelenti. Elsősorban szexuális kizsákmányolás és munkaerő-kizsákmányolás céljából kereskednek az áldozatokkal az EU-ban, de koldulásra kényszerítés, bűnözésre kényszerítés céljából és más célokból is. A Bizottság 2022 decemberében javaslatot tett az emberkereskedelem elleni irányelv módosítására[38] olyan aktualizált szabályokkal, amelyek célja a jelenlegi jogi keret hiányosságainak orvoslása. Elfogadását követően a felülvizsgált irányelv hatálya kiterjedne a kényszerházasságra és az illegális örökbefogadásra, és kifejezett rendelkezést tartalmazna az emberkereskedelem online dimenziójára vonatkozóan. Magában foglalná továbbá az elkövetőkre vonatkozó kötelező szankciórendszer bevezetését, és hivatalossá tenné a nemzeti áldozatkezelési mechanizmusok létrehozását az áldozatok kilétének korai megállapítása, segítése és támogatása, valamint határokon átnyúló ügyekben az áldozatok segítségnyújtási és támogató szolgáltatásokhoz irányításának javítása érdekében. Az emberkereskedelem áldozatai által nyújtott szolgáltatások tudatos igénybevétele bűncselekménynek minősülne, és kötelezővé válna az emberkereskedelemre vonatkozó adatok éves szintű gyűjtése és az Eurostat általi közzététele. A Tanács 2023 júniusában elfogadta általános megközelítését, míg az Európai Parlamentnek még el kell fogadnia álláspontját. Gyorsan kell cselekedni annak érdekében, hogy még a jelenlegi Parlament megbízatásának lejárta előtt megállapodás szülessen.

Környezeti bűnözés

A környezeti bűnözés globális fenyegetéssé vált, amely a becslések szerint évente 5–7 %-kal nő. Az elérhető jelentős nyereség, a tagállamok közötti joghézagok és a felderítés alacsony kockázata mind vonzza a szervezett bűnözést. Az Europol szerint vannak arra utaló jelek, hogy az e tevékenységekből származó bevételeket a terrorizmus finanszírozására használják fel. 2021 decemberében a Bizottság javaslatot fogadott el a környezet büntetőjog általi védelméről szóló

[37] COM (2022) 480.
[38] COM(2022) 732.

2008. évi irányelv felváltására. A javaslat a környezeti bűncselekmények kategóriáira vonatkozó fogalommeghatározások pontosítására és aktualizálására, valamint a természetes és jogi személyekre vonatkozó hatékony, visszatartó erejű és arányos szankciótípusok és -szintek meghatározására összpontosít. Az új bűncselekmények közé tartoznak az illegális erdőirtással, a vegyi anyagokra vonatkozó uniós jogszabályok megsértésével, a felszíni vagy felszín alatti vizek illegális kivételével és az illegális hajó-újrafeldolgozással kapcsolatos büntetendő cselekmények. A javaslat célja, hogy jelentősen megerősítse a jogérvényesítési láncot, valamint a tagállami hatóságok és az uniós ügynökségek és szervek közötti, határokon átnyúló együttműködést. Az Európai Parlament és a Tanács már elfogadta a javaslattal kapcsolatos álláspontját, és folyamatban vannak a tárgyalások, amelyeket az év végéig le kellene zárni. A vadon élő állatok és növények jogellenes kereskedelme elleni felülvizsgált cselekvési tervet[39] végre kell hajtani a megelőzés és a jogérvényesítés további megerősítése érdekében.

Vagyonvisszaszerzés és elkobzás

A bűnözők megfosztása illegális bevételeiktől kulcsfontosságú a szervezett bűnözés felszámolásához. Ezért az EU-ban a bűnüldöző hatóságok bankszámla-információkhoz való hozzáférésének biztosításáról szóló javaslat[40] mellett (amelyről 2023 júniusában született politikai megállapodás) a Bizottság 2022 májusában a vagyonvisszaszerzésről és elkobzásról szóló javaslatot[41] terjesztett elő, hogy megerősítse a vagyon felkutatására, azonosítására, befagyasztására, elkobzására és kezelésére szolgáló képességeket. A javaslat kulcsfontosságú rendelkezései a pénzügyi nyomozásokkal kapcsolatos követelményekre, a vagyonvisszaszerzési hivatalok további hatásköreire és eszközeire, valamint a bűncselekmények szélesebb körére kiterjedő hatékonyabb befagyasztási és elkobzási intézkedésekre vonatkoznak. Az egyik új bűncselekmény, amely esetében ezeket az intézkedéseket alkalmazni kellene, az uniós korlátozó intézkedések megsértése. 2022 decemberében a Bizottság külön javaslatot fogadott el az uniós korlátozó intézkedések megsértésére vonatkozó büntetőjogi fogalommeghatározások és szankciók harmonizálására vonatkozóan. Az uniós korlátozó intézkedések hatékony végrehajtása és érvényesítése továbbra is kiemelt prioritás a Bizottság számára, amit megerősít a Bizottság által Oroszország Ukrajna elleni agressziós háborúja nyomán létrehozott „Freeze and Seize" munkacsoport munkája. Az Európai Parlament és a Tanács mindkét javaslat tekintetében elfogadta saját álláspontját azzal a céllal, hogy idén év végéig megállapodás szülessen.

A pénzmosás elleni küzdelemről szóló jogalkotási csomag

A pénzmosás összekapcsolódik gyakorlatilag minden olyan bűnözői cselekménnyel, amely bűncselekményből származó jövedelmet termel az EU-ban[42], és ezért kulcsfontosságú tényező a bűnözés elleni küzdelemben az EU-ban. 2021 júliusában a Bizottság ambiciózus javaslatokat terjesztett elő a pénzmosás és a terrorizmusfinanszírozás megelőzésére irányuló uniós intézkedések megerősítésére[43], négy jogalkotási javaslattal, amelyek célja a bűnözők által a pénzügyi rendszeren keresztül az illegális pénzeszközök tisztára mosására vagy terrorista tevékenységek finanszírozására tett kísérletek megelőzésének és felderítésének megerősítése. A csomag négy kezdeményezésének egyikét, amely a kriptoeszköz-átruházások

[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM (2022) 245.
[42] Europol, Enterprising criminals – Europe's fight against the global networks of financial and economic crime (Vállalkozószellemű bűnözők: Európa küzdelme a pénzügyi és gazdasági bűnözés globális hálózatai ellen), 2020.
[43] COM(2021) 420.

nyomonkövethetőségének biztosítására irányul, a társjogalkotók 2023 májusában elfogadták[44]. Ez a rendelet 2024. december 30-án lép hatályba, amikorra valamennyi kriptoeszköz-szolgáltatónak adatokat kell gyűjtenie és tárolnia a kriptoeszköz-átruházások kezdeményezőjére és kedvezményezettjére vonatkozóan. A további három javaslat célja i. pénzmosás elleni új uniós hatóság létrehozása annak érdekében, hogy biztosítsa a következetesen magas színvonalú felügyeletet a belső piacon, a legkockázatosabb, határokon átnyúló szervezetek esetében is, támogatva és koordinálva a pénzügyi információs egységek munkáját, ii. harmonizált szabályok meghatározása a magánszektorra vonatkozóan, bevezetve a szolgáltatások és áruk ellenértékeként történő nagy összegű készpénzfizetésekre vonatkozó uniós szintű 10 000 EUR-s korlátot, valamint iii. az illetékes hatóságok hatásköreinek és együttműködési eszközeinek megerősítése. Ez a csomag várhatóan jelentősen fokozza majd az EU képességét arra, hogy fellépjen a pénzmosás ellen és megvédje az uniós polgárokat a terrorizmussal és a szervezett bűnözéssel szemben. A három kiemelt javaslatot jelenleg tárgyalják a társjogalkotók, azzal a céllal, hogy még a mostani Parlament megbízatásának lejárta előtt megállapodás szülessen ezzel kapcsolatban.

A Bizottság felszólítja az Európai Parlamentet és a Tanácsot, hogy sürgősen, de még mindenképpen a jelenlegi Európai Parlament megbízatásának lejárta előtt zárják le az intézményközi tárgyalásokat az alábbi, függőben lévő javaslatok vonatkozásában:

- irányelvjavaslat a vagyonvisszaszerzésről és elkobzásról,
- irányelvjavaslat az uniós korlátozó intézkedések megsértésére vonatkozó büntetőjogi fogalommeghatározások és szankciók harmonizálásáról,
- irányelvjavaslat az emberkereskedelem elleni küzdelemről,
- irányelvjavaslat a környezet védelmének büntetőjog általi javításáról,
- a pénzmosás elleni csomagra irányuló javaslat,
- javaslat a polgári célú tűzfegyverek behozatalára, kivitelére és továbbítására vonatkozó hatályos jogszabályok aktualizálására.

A Bizottság felszólítja a tagállamokat, valamint az uniós ügynökségeket és szerveket, hogy:

- működjenek együtt a kábítószer-kereskedelem és a szervezett bűnözés elleni küzdelemre vonatkozó uniós ütemtervben foglalt 17 fellépés 2023-ban és 2024-ben történő végrehajtása érdekében.

V. Erős európai biztonsági ökoszisztéma

Az elmúlt években a biztonsági fenyegetések egyre inkább határokon átnyúló jellegűvé váltak, ami minden szinten további szinergiákat és szorosabb együttműködést tesz szükségessé. A biztonsági unióra vonatkozó stratégia elfogadása óta fontos kezdeményezések indultak a határokon átnyúló együttműködés maximalizálása, a külső határokon és a schengeni térségen belül rendelkezésre álló eszközök és eljárások egyszerűsítése és korszerűsítése, valamint a bűnüldöző és igazságügyi hatóságok közötti információcsere fokozása érdekében a szervezett bűnözés elleni küzdelem hatékonyabbá tétele érdekében. Ennek fényében az adatcserére vonatkozó interoperabilitási keret hatékony végrehajtása fontos pillére a biztonság fokozásának

[44] (EU) 2023/1113 rendelet (2023. május 31.) a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az (EU) 2015/849 irányelv módosításáról.

és a határokon átnyúló fenyegetésekre adott hatékony európai reagálásnak, miközben garantálja az Unión belüli szabad mozgást.

Fokozott információcsere a schengeni térségen belül: előzetes utasinformáció (API), utasnyilvántartási adatállomány (PNR) és Prüm II

A Bizottság által az előzetes utasinformációkra vonatkozóan 2022 decemberében elfogadott két javaslat[45] fokozná az Unió belső biztonságát azáltal, hogy a tagállamok bűnüldöző hatóságai számára további eszközöket biztosít a súlyos bűncselekmények és a terrorizmus elleni küzdelemhez. Például az EU-n belüli járatokra vonatkozó előzetes utasinformációk a légi utasokra vonatkozó utasnyilvántartási adatállománnyal együtt alkalmazva, lehetővé tennék a tagállamok bűnüldöző hatóságai számára, hogy célzottabb beavatkozásokkal jelentősen növeljék nyomozásaik hatékonyságát. Fontos, hogy a javasolt szabályokat a lehető leghamarabb elfogadják: ez nemcsak a szervezett bűnözés és a terrorizmus elleni küzdelmet támogatná, hanem jelentősen csökkentené az összes utazó szisztematikus ellenőrzésének szükségességét a belső határellenőrzések ideiglenes visszaállítása esetén, megkönnyítve a légi közlekedést és a szabad mozgást. Az Európai Bizottság 2023. szeptember 6-án azt ajánlotta, hogy a Tanács engedélyezze a Svájccal, Izlanddal és Norvégiával a PNR-adatok továbbításáról szóló megállapodásokra irányuló tárgyalásokat. E három ajánlás elfogadása támogatná az EU következetes és hatékony külső PNR-politikáját.

A prümi adatcseréket a rendőrség napi szinten használja a szervezett bűnözés, a kábítószerek, a terrorizmus, a szexuális kizsákmányolás és az emberkereskedelem elleni küzdelem során. A rendőrségi együttműködés céljából történő automatizált adatcseréről szóló rendeletre irányuló javaslat („Prüm II")[46] felülvizsgálja a jelenleg hatályos prümi keretet az EU-ban az információs hiányosságok megszüntetése, valamint a bűncselekmények megelőzésének, felderítésének és kivizsgálásának előmozdítása érdekében. A rendőrségi együttműködés céljából történő automatizált adatcserére vonatkozó felülvizsgált szabályok kiegészítik a jelenlegi megbízatás során a rendőrségi együttműködésre vonatkozóan előterjesztett javaslatokat, a határokon átnyúló operatív együttműködés megerősítéséről szóló, már elfogadott tanácsi ajánlás és a bűnüldöző hatóságok közötti információcseréről szóló irányelv mellett. E kapcsolódó eszközök gyors elfogadása és végrehajtása javítaná, megkönnyítené és felgyorsítaná a bűnüldöző hatóságok közötti adatcserét, és elősegítené a bűnözők azonosítását.

Teljes mértékben interoperábilis határigazgatási rendszer a biztonságos, erős, digitális és egységes schengeni térség érdekében

A belső határok nélküli, jól működő schengeni térség a tagállamok közötti kölcsönös bizalmon alapul. Ez pedig a hatékony ellenőrzéseken nyugszik, akár az Unió külső határain, akár a tagállamok területén alkalmazott alternatív intézkedések formájában. A Schengeni határellenőrzési kódex Bizottság által javasolt módosítása[47] ismerteti, hogy a tagállamok hogyan használhatják eredményesebben a belső határellenőrzés alternatíváit, amelyek magas szintű biztonságot nyújthatnak. A schengeni térségen belüli magas és arányos biztonsági szint biztosítása érdekében fontos, hogy sor kerüljön a Schengeni határellenőrzési kódex módosításának elfogadására és teljes körű végrehajtására. Folyamatban van az uniós információs rendszerek új struktúrájának kidolgozása a nemzeti hatóságok által a biztonság és a határigazgatás terén végzett munka hatékonyabb támogatása érdekében. Ez magában foglalja

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.
[47] COM(2021) 891.

a megújított Schengeni Információs Rendszert, az Európai Utasinformációs és Engedélyezési Rendszert, a határregisztrációs rendszert, a vízuminformációs rendszer frissítését, valamint az interoperabilitási keretet a rendszerek teljes biztonságban történő összekapcsolása érdekében. Miután teljesen elkészül az új architektúra, átfogóbb és megbízhatóbb biztonsági információkkal szolgálhat a nemzeti hatóságok számára. Az interoperabilitási keret valamennyi eleme alapvető fontosságú, ami azt jelenti, hogy valamely elem vagy valamely tagállam késedelme mindenki más számára is késlelteti a bevezetést. A határregisztrációs rendszer technikai fejlesztésének késedelmét a lehető legkisebbre kell csökkenteni annak érdekében, hogy a határregisztrációs rendszer minél előbb működésbe léphessen, és az interoperabilitási keret valamennyi kulcsfontosságú elemét be lehessen vezetni.

Az előszűrésről szóló javaslat[48] növelné a schengeni térségen belüli biztonságot azzal, hogy egységes szabályokat hoz létre azon harmadik országbeli állampolgárok azonosítására vonatkozóan, akik nem teljesítik a Schengeni határellenőrzési kódexben említett beutazási feltételeket, valamint a külső határokon végzendő egészségügyi és biztonsági ellenőrzéseket ír elő rájuk vonatkozóan. A javasolt Eurodac-rendszer támogatná ezeket a célkitűzéseket, jelezve, amikor az előszűrést követően úgy tűnik, hogy egy adott személy veszélyt jelenthet a belső biztonságra. Ez azután megkönnyítené a menekültügy és a migráció kezeléséről szóló javasolt rendelet végrehajtását. A Bizottság arra ösztönzi a társjogalkotókat, hogy mihamarabb, még a jelenlegi jogalkotási időszak vége előtt zárják le az e javaslatokról szóló tárgyalásokat.

A korrupció elleni küzdelem

A korrupció rendkívül káros a demokráciáinkra, a gazdaságra és a biztonságunkra nézve, mivel segíti a szervezett bűnözést és az ellenséges külföldi beavatkozást. A korrupció sikeres megelőzése és az ellene folytatott küzdelem alapvető fontosságú mind az uniós értékek védelme és az uniós politikák hatékonyságának biztosítása, mind pedig a jogállamiság, valamint a kormányzati szereplők és a közintézmények iránti bizalom fenntartása szempontjából. Amint azt Ursula von der Leyen elnök az Unió helyzetéről szóló 2022. évi beszédében bejelentette, a Bizottság 2023. május 3-án korrupcióellenes intézkedéscsomagot[49] fogadott el**.** A korrupció elleni küzdelemről szóló irányelvre irányuló bizottsági javaslat megerősített szabályokat tartalmaz a korrupció bűncselekménnyé nyilvánítására és a szankciók Unió-szerte történő harmonizálására vonatkozóan. Lehetővé teszi továbbá a hatékony nyomozást és büntetőeljárás alá vonást, továbbá nagy hangsúlyt fektet a megelőzésre és a feddhetetlenség kultúrájának kialakítására, ahol a korrupció nem tolerálható. Az Európai Parlamentben és a Tanácsban megkezdődtek a tárgyalások a javaslatról. Emellett felkérjük a tagállamokat, hogy hajtsák végre a 2023. július 5-én elfogadott 2023. évi jogállamisági jelentés korrupcióellenes pilléréből eredő ajánlásokat. A főképviselőnek a Bizottság által támogatott javaslata továbbá közös kül- és biztonságpolitikai (KKBP) célzott szankciórendszert javasol a súlyos korrupciós cselekmények elleni globális fellépés érdekében.

Az áldozatokat megillető jogok megerősítése

A Bizottság 2023. július 12-én javaslatot tett az áldozatok jogairól szóló irányelv módosítására az áldozatok információhoz, támogatáshoz és védelemhez való hozzáférésének, büntetőeljárásban való részvételének és kárenyhítéshez való hozzájutásának megerősítése érdekében. A felülvizsgálat egyik általános célkitűzése a magas szintű biztonsághoz való hozzájárulás biztonságosabb környezet megteremtésével az áldozatok számára, a

[48] COM(2020) 612.
[49] COM(2023) 234.

bűncselekmények bejelentésének ösztönzése és a megtorlástól való félelem csökkentése érdekében.

A Bizottság felszólítja az Európai Parlamentet és a Tanácsot, hogy sürgősen, de még mindenképpen a jelenlegi Európai Parlament megbízatásának lejárta előtt zárják le az intézményközi tárgyalásokat az alábbi, függőben lévő javaslatok vonatkozásában:

- javaslat a Prüm II rendeletre,
- az előzetes utasinformációkra (API) vonatkozó javaslatok,
- a korrupció elleni küzdelemre és különösen a közös kül- és biztonságpolitikai (KKBP) célzott szankciórendszer létrehozására irányuló javaslatok,
- a Schengeni határellenőrzési kódexről szóló rendelet módosítására irányuló javaslat,
- irányelvjavaslat az áldozatokat megillető jogokról,
- az előszűrésre vonatkozó javaslat.

A Bizottság felszólítja a tagállamokat, hogy:

- biztosítsák a határregisztrációs rendszer mielőbbi hatálybalépését az információcsere uniós architektúrájának teljes körű megvalósítása érdekében.

VI. Végrehajtás

Európa egészének biztonsága közös felelősség, amelyben minden szereplőnek részt kell vállalnia, így a Bizottságnak és a társjogalkotóknak új, erős, átfogó és gyakorlati szabályok elfogadásával, a tagállamoknak e szabályok időben történő végrehajtásával és alkalmazásával, végül pedig a különböző hatóságoknak, szervezeteknek és érdekelt feleknek is a konkrét ügyekben végzett tevékenységekkel. A bel- és igazságügy, valamint a kiberbiztonság területén működő uniós ügynökségek szintén kulcsszerepet játszanak, ami tovább fokozódott felelősségi köreik közelmúltbeli kiterjesztésével.

Az uniós finanszírozás kedvezményezettjeinek fokozott átvilágítása

Az uniós költségvetés végrehajtása során a Bizottság feladata annak biztosítása, hogy az uniós finanszírozás kedvezményezettjei tiszteletben tartsák az uniós értékeket. Azok a mechanizmusok és kontrollrendszerek, amelyek meghatározzák, hogy ki részesülhet uniós finanszírozásban, már most is szilárdak, és a költségvetési rendelet átdolgozásáról folyó tárgyalások során is arra törekszenek, hogy erősebb jogi eszközöket biztosítsanak a Bizottságnak ahhoz, hogy szükség esetén fellépjen. Emellett a Bizottság jelenleg olyan módszereken dolgozik, amelyekkel tovább fokozható az uniós finanszírozás jelenlegi és potenciális jövőbeli kedvezményezettjeinek átvilágítása, és e munka során tökéletesíti az uniós értékek tiszteletben tartásával kapcsolatos kötelezettségekre és az uniós értékek megsértésével járó következményekre vonatkozó iránymutatást. Ez pontosítja mind a kedvezményezettek, mind pedig az uniós szintű ellenőrzéseket végzők feladatait, és inspirációként szolgálhat a nemzeti szinten kidolgozandó iránymutatáshoz. A finanszírozási feltételek megsértése esetén a Bizottság most is és a jövőben is habozás nélkül leállítja az együttműködést az érintett projekt kedvezményezettjeivel, és szükség esetén visszafizetteti a pénzeszközöket. Fontos, hogy a tagállamok proaktívan megosszák az információkat a Bizottsággal, amikor tudomásuk van lehetséges kockázatokról az uniós finanszírozást kérelmező szervezetekkel kapcsolatban.

Kötelezettségszegések

A biztonság területén a Bizottság számos kötelezettségszegési eljárást folytatott le. 2023-ban például igen sok kötelezettségszegési ügyben indult vizsgálat az online terrorista tartalom terjesztéséről szóló 2021. évi rendelet szerinti kötelezettségek teljesítésének elmulasztása miatt (16 tagállam)[50], 2022 és 2023 folyamán pedig 20 tagállam kapott kiegészítő felszólító levelet a gyermekek szexuális bántalmazása elleni küzdelemről szóló 2011. évi irányelv[51] helytelen végrehajtása miatt. Még mindig jelentős számú kötelezettségszegési ügy van folyamatban amiatt, hogy a nemzeti jogszabályok nem felelnek meg a terrorizmus elleni küzdelemről szóló 2017. évi irányelvnek[52], továbbá a pénzügyi és egyéb információk bizonyos bűncselekmények megelőzése, felderítése, nyomozása és büntetőeljárás alá vonása céljából történő felhasználását megkönnyítő szabályok[53] átültetésének elmulasztása miatt. Egyéb olyan területek, ahol kötelezettségszegési eljárások vannak folyamatban, többek között a tűzfegyverekre vonatkozó jogszabályok, a kábítószerekben használt pszichoaktív anyagokra, a készpénz-helyettesítő fizetési eszközökkel kapcsolatos csalás és hamisítás elleni küzdelemre, a pénzmosás elleni küzdelemre, a bűnügyi nyilvántartások uniós tagállamok közötti cseréjére vonatkozó szabályok, valamint az áldozatok jogairól szóló irányelv. Az elfogadott kezdeményezéseket és intézkedéseket végrehajtó tagállamok (technikai és pénzügyi) támogatást kaptak, és a Bizottság továbbra is készen áll arra, hogy együttműködjön a tagállamokkal a végrehajtás optimalizálása érdekében.

Ellenőrzés a schengeni értékelési és monitoringmechanizmus keretében, valamint annak új irányítási rendszere

A schengeni értékelési és monitoringmechanizmus továbbra is hozzájárul a belső ellenőrzések nélküli térség biztonságának fokozását célzó schengeni szabályok hatékony végrehajtásához. 2023-ban sor került a megerősített schengeni értékelési és monitoringmechanizmus keretében végzett első értékelésekre, amelyek lehetővé tették az EU-n belüli biztonságra és védelemre határokon átnyúló hatást gyakorló stratégiai sebezhetőségek időben történő azonosítását és orvoslását. Emellett a Bizottság 2023-ban tematikus schengeni értékelést kezdett, hogy megvizsgálja az EU-ba irányuló kábítószer-kereskedelem elleni küzdelem terén hasonló kihívásokkal szembesülő tagállamok gyakorlatait, különös figyelmet fordítva a nagy volumenű kábítószer-kereskedelemre. Ezek az értékelések fokozottan és átfogóbb megközelítéssel összpontosítottak a schengeni térség biztonsági elemeire. Az időszakos, tematikus és be nem jelentett schengeni értékelések eredményei alapján a Tanács 2023 júniusában meghatározta a 2023–2024-es schengeni ciklus prioritásait. Ezek tartalmazzák azokat a kiemelt területeket, ahol további ösztönzésre van szükség a biztonságosabb és erősebb schengeni térség kialakításához. E prioritások hatékony és gyors végrehajtása a Schengen Tanács fokozott szakpolitikai koordinációjával együtt tovább erősíti a szervezett bűnözés elleni küzdelmet, és maximalizálja a határokon átnyúló operatív együttműködést.

Az uniós ügynökségek és szervek szerepe

A partnerség kulcsfontosságú a biztonsági unióval kapcsolatos kezdeményezések végrehajtásához, mivel a konkrét eredmények eléréséhez szükség van a különböző nemzeti és

[50] (EU) 2021/784 rendelet az online terrorista tartalom terjesztésével szembeni fellépésről.

[51] 2011/93/EU irányelv a gyermekek szexuális bántalmazása elleni küzdelemről.

[52] Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról.

[53] Az Európai Parlament és a Tanács (EU) 2019/1153 irányelve (2019. június 20.) a pénzügyi és egyéb információk bizonyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása céljából történő felhasználásának megkönnyítését szolgáló szabályok megállapításáról, valamint a 2000/642/IB tanácsi határozat hatályon kívül helyezéséről.

európai hatóságok és szervek munkájára. Például az EMPACT (Európai Multidiszciplináris Platform a Bűnügyi Fenyegetettség Ellen) lehetővé teszi a tagállamok strukturált multidiszciplináris együttműködését az összes uniós intézmény, szerv és hivatal (pl. Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA) támogatásával. Az EMPACT által többek között az erre a célra létrehozott operatív munkacsoportokon keresztül végzett műveletek koordinálják a tagállamoknak és az operatív partnereknek a bűnözői hálózatok és a súlyos bűncselekmények elleni küzdelemre irányuló erőfeszítéseit. Csak 2022-ben az EMPACT eredményeképp összesen 9 922 letartóztatásra, több mint 180 millió EUR értékű vagyon és pénz lefoglalására, 9 263 esetben nyomozás indítására, 4 019 áldozat azonosítására, több mint 62 tonna kábítószer lefoglalására, 51 nagy értékű célpont (High Value Targets (HVT)) azonosítására és 12 letartóztatására, valamint az Ukrajna elleni agressziós háborúval összefüggésben végrehajtott műveletekre került sor, különösen az emberkereskedelem és a tűzfegyverekkel kapcsolatos fenyegetések kezelése érdekében.[54]

A Frontex, az Európai Tengerészeti Biztonsági Ügynökség (EMSA) és az Európai Halászati Ellenőrző Hivatal (EFCA) tovább erősíti együttműködését a parti őrségi feladatok terén annak érdekében, hogy támogassák a nemzeti hatóságokat a tengeri biztonság és védelem fokozásában. Ezek az ügynökségek jelentős mértékben hozzájárulnak majd az Európai Unió tengeri védelmi stratégiájának végrehajtásához.

A biztonsági unióval kapcsolatos számos kezdeményezés új felelősségi körökkel és feladatokkal ruházta fel az érintett ügynökségeket, aminek olykor az emberi erőforrásokat érintő vonzatai vannak.

Európai Uniós Kiberbiztonsági Ügynökség (ENISA)

A kiberbiztonság fokozását célzó felkészültséget és a biztonsági eseményekre való reagálást illetően a Bizottság rövid távú intézkedést vezetett be a tagállamok támogatása érdekében, és forrásokat csoportosított át a Digitális Európa programból az **Európai Uniós Kiberbiztonsági Ügynökséghez (ENISA)** a jelentős kiberbiztonsági eseményekre való felkészültség és reagálási kapacitások megerősítése céljából. A kiberszolidaritásról szóló jogszabályra irányuló, 2023 áprilisában elfogadott javaslat erre az intézkedésre épül, és a társjogalkotók általi elfogadást követően az ENISA-t további feladatokkal bízhatja meg, például a jövőbeli uniós kiberbiztonsági tartalék működtetésével és igazgatásával, vagy a nagyszabású kiberbiztonsági eseményeket követő esemény-felülvizsgálati jelentés elkészítésével. A kiberrezilienciáról szóló jogszabályjavaslat szerint az ENISA feladata lenne, hogy fogadja a gyártóktól a digitális elemeket tartalmazó termékek sebezhetőségeiről és az e termékek biztonságát befolyásoló biztonsági eseményekről szóló értesítéseket, amelyeket az ENISA-nak továbbítania kell majd a megfelelő CSIRT-ekhez vagy a tagállamok megfelelő egyedüli kapcsolattartó pontjaihoz. Az ENISA-nak továbbá kétévente technikai jelentést kell készítenie a digitális elemeket tartalmazó termékek kiberbiztonsági kockázataival kapcsolatban kialakuló tendenciákról, és be kell nyújtania azt a Kiberbiztonsági Együttműködési Csoportnak.

Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont

[54] 2022. évi EMPACT tájékoztatók: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

Az **Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont** a nemzeti koordinációs központok hálózatával együtt az Unió új szerve, amely támogatja az innovációt és az iparpolitikát a kiberbiztonság területén. Ez az ökoszisztéma megerősíti a kiberbiztonsági technológiai közösség kapacitásait, megőrzi a kutatási kiválóságot és fokozza az uniós ipar versenyképességét ezen a területen. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok stratégiai beruházási döntéseket hoznak, és egyesítik az Uniótól, a tagállamoktól és közvetett módon az ipartól származó erőforrásokat a technológiai és ipari kiberbiztonsági kapacitások javítása és megerősítése érdekében. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak tehát kulcsszerepet kell játszania a Digitális Európa és a Horizont Európa program ambiciózus kiberbiztonsági célkitűzéseinek megvalósításában.

Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont már felvette a szükséges személyzete több mint felét, és hamarosan fel fogja venni ügyvezető igazgatóját. A már folyamatban lévő munka kiterjed a Digitális Európa program kiberbiztonsági részére, valamint a technológiafejlesztésre és -alkalmazásra vonatkozó új stratégiai menetrendre[55], amely kiemelt intézkedéseket határoz meg a következőkre vonatkozóan: a kkv-k támogatása a stratégiai kiberbiztonsági technológiák, szolgáltatások és folyamatok fejlesztése és használata során; szakemberek támogatása és számuk növelése; valamint a kutatási, fejlesztési és innovációs szakértelem megerősítése a tágabb európai kiberbiztonsági ökoszisztémában.

Europol

Teljesen új megbízatásával az **Europol** megfelelőbb eszközökkel fog rendelkezni arra, hogy támogassa a tagállamokat a szervezett bűnözés elleni küzdelemben. A kábítószer-kereskedelem elleni küzdelem kulcsfontosságú prioritás, tekintettel annak növekvő jelentőségére és az uniós polgárok biztonságára gyakorolt fokozódó negatív hatására. Az Európai Unió Tanácsának 2023. május 15-i felhatalmazása óta a Bizottság aktívan dolgozik azon, hogy Bolíviával, Brazíliával, Ecuadorral, Mexikóval és Peruval a személyes adatoknak az Europollal való cseréjéről szóló nemzetközi megállapodásokat kössön a súlyos bűncselekmények és a terrorizmus megelőzése, valamint az ellenük való küzdelem céljából.

Eurojust

A határokon átnyúló súlyos és összetett bűncselekmények széles köre elleni küzdelemben a nemzeti hatóságoknak nyújtott igazságügyi támogatás terén szerzett több mint 20 éves tapasztalattal az **Eurojust** megszilárdította pozícióját a szabadságon, a biztonságon és a jog érvényesülésén alapuló uniós térségben. Az átfogó együttműködés megerősítése érdekében a Bizottság tárgyalásokat folytat az Eurojust és 13 harmadik ország[56] közötti együttműködést előmozdító nemzetközi megállapodásokról a személyes adatoknak a szervezett bűnözés és a terrorizmus elleni küzdelem céljából történő cseréjét illetően. A tárgyalások már lezárultak Örményországgal és Libanonnal, folyamatban vannak Algériával és Kolumbiával, és megkezdődtek Bosznia-Hercegovinával. A Bizottság arra ösztönzi az Európai Parlamentet és a Tanácsot, hogy még a parlamenti ciklus vége előtt véglegesítsék a megállapodások megkötését ezekkel az országokkal a transznacionális igazságügyi együttműködés megerősítése és a határokon átnyúló bűnözés elleni küzdelem kiszélesítése érdekében.

Európai Ügyészség

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_en

[56] Algéria, Argentína, Bosznia-Hercegovina, Brazília, Egyiptom, Izrael, Jordánia, Kolumbia, Libanon, Marokkó, Örményország, Törökország és Tunézia.

Műveleti tevékenységeinek 2021. júniusi megkezdése óta az **Európai Ügyészség (EPPO)** hatékony eszköznek bizonyult a közös uniós eszköztárban az Unió általános költségvetését érintő bűncselekmények kivizsgálására és büntetőeljárás alá vonására, ideértve a bűnszervezetben való részvételhez kapcsolódó bűncselekményeket, amikor a hangsúly az Unió általános költségvetése elleni bűncselekményeken van. A Bizottság arra ösztönzi azokat a tagállamokat, amelyek még nem vesznek részt az Európai Ügyészségre irányuló megerősített együttműködésben, hogy ezt mielőbb tegyék meg annak érdekében, hogy az Európai Ügyészség teljeskörűen kibontakoztathassa lehetőségeit az uniós adófizetők pénzének védelme terén.

EUDA

A társjogalkotók által 2023 júniusában elfogadott új megbízatással a Kábítószer és a Kábítószerfüggőség Európai Megfigyelőközpontja (EMCDDA) teljes jogú ügynökséggé alakul át – az **Európai Unió Kábítószerügyi Ügynöksége (EUDA*)* –, amely megerősített szerepet tölt be. Az ügynökség képes lesz arra, hogy átfogóbb módon felmérje a tiltott kábítószerek jelentette új egészségügyi és biztonsági kihívásokat, és hatékonyabban hozzájáruljon a tagállami és nemzetközi szintű munkához. Az ügynökség fő feladata továbbra is az adatok gyűjtése, elemzése és terjesztése lesz, de a megerősített megbízatás lehetővé teszi az ügynökség számára, hogy általános egészségügyi és biztonsági fenyegetésértékelési képességeket fejlesszen ki az újonnan megjelenő fenyegetések – köztük a politoxikomán droghasználat – azonosítása érdekében, megerősítse együttműködését a nemzeti kapcsolattartó pontokon keresztül, és létrehozza az ügynökség számára forenzikus és toxikológiai információkat biztosító laboratóriumok hálózatát. Ez segíteni fogja az ügynökséget abban, hogy riasztást adjon ki, amikor különösen veszélyes anyagok jelennek meg a piacon, és figyelemfelkeltő tevékenységet folytasson.

A Bizottság felszólítja az Európai Parlamentet és a Tanácsot, hogy sürgősen, de még mindenképpen a jelenlegi Európai Parlament megbízatásának lejárta előtt zárják le az intézményközi tárgyalásokat az alábbi, függőben lévő javaslatok vonatkozásában:

- a költségvetési rendelet átdolgozására irányuló javaslat.

A Bizottság felszólítja a tagállamokat, hogy:

- proaktívan osszák meg az információkat a Bizottsággal, amikor tudomásuk van lehetséges kockázatokról az uniós finanszírozást kérelmező szervezetekkel kapcsolatban,
- mielőbb hajtsák végre a 2023–2024-es schengeni ciklus prioritásait egy biztonságosabb és erősebb schengeni térség érdekében,
- foglalkozzanak a velük szemben indított, folyamatban lévő kötelezettségszegési eljárásokkal az érintett jogszabályok megfelelő átültetésének biztosítása érdekében.

VII. Következtetés

Az elmúlt három évben folyamatos és határozott erőfeszítéseket tettünk azon törekvésünk megvalósítása érdekében, hogy biztonsági uniót teremtsünk az Európai Unió számára. Hatalmas előrelépések történtek a biztonságpolitika valamennyi területén. A folyamatosan változó fenyegetések valósága most arra sarkall bennünket, hogy megújult erővel folytassuk fáradozásunkat. A jogalkotási kerettel kapcsolatos munkát kellő időben, még a parlamenti

ciklus vége előtt, 2024 tavaszáig le kell zárni. A tagállamok állandó feladata az új jogszabályok átültetése, végrehajtása és alkalmazása. A végrehajtás összehangolt erőfeszítéseket kíván meg, adott esetben az uniós ügynökségek támogatásával, és sok esetben egyre szorosabb együttműködésre van szükség nemzetközi partnereinkkel.

Csak az összes érintett fél együttes és határozott erőfeszítésével érhetjük el az EU-ban azt a biztonsági és védelmi szintet, amit a polgárok elvárnak, és a jelenlegi körülmények között minden szereplő számára elsődleges fontossággal kell bírnia annak, hogy részt vállaljon az EU biztonságának megerősítésében.