Az Európai Unió
Tanácsa

Brüsszel, 2025. április 3.
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2025. április 2.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2025) 148 final
Tárgy:	A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK a ProtectEU-ról: Európai belső biztonsági stratégia

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: COM(2025) 148 final.

Melléklet: COM(2025) 148 final

EURÓPAI
BIZOTTSÁG

Strasbourg, 2025.4.1.
COM(2025) 148 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

a ProtectEU-ról: Európai belső biztonsági stratégia

1. ProtectEU: Európai belső biztonsági stratégia

Minden szabadságunk alapját a biztonság képezi. A demokrácia, a jogállamiság, az alapvető jogok, az európaiak jólléte, a versenyképesség és a jólét – mindez attól függ, hogy képesek vagyunk-e alapvető biztonsági garanciát nyújtani. A biztonsági fenyegetések új korában, amelyben most élünk, az uniós tagállamok azon képessége, hogy garantálják polgáraik biztonságát, minden eddiginél jobban függ a **belső biztonságunk védelmére irányuló egységes európai megközelítéstől**. A változó geopolitikai környezetben Európának továbbra is eleget kell tennie a békére vonatkozó tartós ígéretének.

Az európai biztonsági apparátus kiépítésének első lépései már megtörténtek. Az elmúlt évtizedben javított kollektív cselekvési mechanizmusokkal láttuk el az Uniót a bűnüldözés és az igazságügyi együttműködés, a határbiztonság, a súlyos és szervezett bűnözés elleni küzdelem, a terrorizmus és az erőszakos szélsőségesség elleni küzdelem, valamint az EU kritikus fizikai és digitális infrastruktúrájának védelme terén. Továbbra is kulcsfontosságú a korábban elfogadott jogszabályok és a kidolgozott szakpolitikák megfelelő végrehajtása.

Napjaink fenyegetéseinek jellege, valamint az EU belső és külső biztonsága közötti szoros kapcsolat miatt további lépéseket kell tennünk.

A fenyegetettségi helyzet nyilvánvaló. A **hibrid fenyegetések** és a nyílt hadviselés közötti határvonalak elmosódnak. Oroszország online és offline hibrid hadjáratot indított az EU és partnerei ellen a társadalmi kohézió és a demokratikus folyamatok megzavarása és aláásása, valamint az EU Ukrajnával való szolidaritásának próbára tétele érdekében. Az ellenséges külföldi államok és az állam által támogatott szereplők arra törekszenek, hogy beszivárogjanak kritikus infrastruktúráinkba és ellátási láncainkba és megzavarják azokat, érzékeny adatokat lopjanak, és úgy pozícionálják magukat, hogy a jövőben a lehető legnagyobb fennakadást tudják okozni. A bűncselekményeket szolgáltatásként, a bűnözőket pedig helyettesítőként (proxy) használják fel. Emellett a harmadik országoktól való függőségünk az ellátási láncok tekintetében kiszolgáltatottabbá tesz minket az ellenséges államok hibrid hadjárataival szemben.

Amint azt az Europol által a közelmúltban előterjesztett, a súlyos és szervezett bűnözés általi fenyegetettségről szóló uniós értékelés (SOCTA)[1] is kiemelte, a **szervezett bűnözői hálózatok** – amelyeket az interneten keresztül építenek, és amelyek kihatással vannak a gazdaságunkra és a társadalmunkra – egyre nagyobb teret hódítanak Európában. Ha egyszer a szervezett bűnözés megveti a lábát egy közösségben vagy gazdasági ágazatban, felszámolása szélmalomharccá válik: a legnagyobb fenyegetést jelentő bűnözői hálózatok egyharmada több mint tíz éve aktív. Kriptovaluták és párhuzamos pénzügyi rendszerek segítik ezeket a hálózatokat bűncselekményből származó jövedelmeik tisztára mosásában és elrejtésében.

Európában továbbra is aggasztó a terrorfenyegetettség szintje. Az EU-n kívüli regionális válságok tovagyűrűző hatást fejtenek ki, új motivációt biztosítva a terrorista szereplők számára a teljes ideológiai spektrumban a toborzásra, a mozgósításra és kapacitásaik kiépítésére. Radikalizálódási és toborzási erőfeszítéseik kifejezetten társadalmaink legkiszolgáltatottabb rétegeit, különösen bizonyos fiatalokat céloznak. Ezek az erőfeszítések magányos elkövetők által véghezvitt támadásokat és a rendszerellenes szélsőségesség fellendülését ösztönzik, amelyek célja a demokratikus jogrend megzavarása.

A **technológiai haladás** ugrásszerű fejlődése alapvető eszközöket biztosít biztonsági apparátusunk megerősítéséhez. A kibertámadások és a külföldi információmanipuláció azonban egyre elterjedtebbé válnak, és kiaknázzák az új technológiákat, például a mesterséges

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

intelligenciát. A gyermekek, a fiatalok és az idősek különösen veszélyeztetettek az interneten, az online gyűlölet terjedése pedig veszélyezteti a véleménynyilvánítás szabadságát és a társadalmi kohéziót.

Életünk kevésbé biztonságos, és ezt egyre inkább érzik az európaiak is, akiknek a **biztonságérzete az EU-ban** oly mértékben romlott, hogy a jövőre vonatkozó kérdésre 64 %-uk válaszolta azt, hogy aggódik az EU biztonsága miatt.[2] A vállalkozások is egyre inkább aggódnak; a félretájékoztatás és a dezinformáció, a bűnözés, a tiltott tevékenység és a kiberkémkedés egyaránt a tíz legnagyobb kockázat között szerepel a Világgazdasági Fórum globális kockázatokról szóló 2025. évi jelentésében[3].

Az európaiak számára lehetővé kell tenni, hogy **félelem nélkül élhessék életüket**, akár az utcán, akár otthonukban, akár a nyilvános helyeken, a metróban vagy az interneten. Az EU biztonsággal kapcsolatos munkájának középpontjában az emberek – különösen a gyermekeket, a nőket és a kisebbségeket, köztük a zsidó és muzulmán közösségeket általában aránytalanul sújtó támadásoknak leginkább kiszolgáltatott személyek – védelme áll. Ez elengedhetetlen a reziliens és összetartó társadalmak megteremtéséhez.

A Bizottság **európai belső biztonsági stratégiát** dolgoz ki a fenyegetések elleni hatékonyabb fellépés érdekében az elkövetkező években. A szigorúbb jogi eszköztár, a szorosabb együttműködés és a fokozott információmegosztás révén javítani fogjuk rezilienciánkat, valamint a biztonsági fenyegetések előrejelzésére, megelőzésére, felderítésére és az azokra való hatékony reagálásra irányuló kollektív képességünket. A belső biztonság egységes megközelítése támogathatja a tagállamokat abban, hogy a technológia erejét a biztonság megerősítésére, nem pedig gyengítésére használják fel, előmozdítva eközben a mindenki számára biztonságos digitális teret. Támogatja továbbá, hogy a tagállamok közös választ adjanak az Unió belső biztonságát érintő globális politikai és gazdasági változásokra.

Ezt a stratégiát **három elv** vezérli, amelyek középpontjában a jogállamiság és az alapvető jogok tiszteletben tartása áll.

Először is, célul tűzi ki a biztonság kultúrájának megváltoztatását. A **társadalom egészére kiterjedő megközelítésre** van szükségünk, amelyben valamennyi polgár és érdekelt fél részt vesz, beleértve a civil társadalmat, a kutatást, a tudományos köröket és a magánszervezeteket is. A stratégia keretében végrehajtott intézkedések ezért lehetőség szerint integrált, több érdekelt felet bevonó megközelítést alkalmaznak.

Másodszor, a **biztonsági megfontolásokat be kell építeni valamennyi uniós jogszabályba, szakpolitikába és programba**, beleértve az EU külső fellépéseit is, **és érvényesíteni kell azokat**. A jogszabályokat, szakpolitikákat és programokat a biztonsági szempontok szem előtt tartásával kell kidolgozni, felülvizsgálni és végrehajtani, biztosítva, hogy a biztonság koherens és átfogó megközelítésének előmozdítása érdekében figyelembe vegyék a szükséges biztonsági megfontolásokat.

Végezetül a biztonságos, védett és reziliens Európa **komoly beruházásokat igényel az EU, a tagállamok és a magánszektor részéről**. Az e stratégiában meghatározott prioritások és intézkedések végrehajtásához elegendő emberi és pénzügyi erőforrásra van szükség. A következő többéves pénzügyi kerethez vezető útról szóló közleményben[4] foglaltaknak

[2] Az Eurobarométer FL550. számú gyorsfelmérése: Uniós kihívások és prioritások.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, 17. o.
[4] COM (2025) 46 final.

megfelelően Európának növelnie kell a biztonságra fordított közkiadásokat, és elő kell mozdítania a biztonsági kutatást és beruházásokat, fokozva stratégiai autonómiáját.

Ez a stratégia kiegészíti a **felkészültségi unióról szóló stratégiát**[5], amely integrált, az összes veszélyre kiterjedő megközelítést határoz meg a konfliktusokra, az emberi tevékenység és a természet okozta katasztrófákra és válságokra való felkészültség tekintetében, valamint az **„Európai védelem – Készenlét 2030" fehér könyvet**[6], amely támogatja a védelmi képességek fejlesztését és beszerzését az egész EU-ban a külföldi ellenfelek elrettentése érdekében. A Bizottság javaslatot fog tenni továbbá az **európai demokráciapajzsra** az EU demokratikus rezilienciájának megerősítése érdekében. Ezek a kezdeményezések együttesen egy biztonságos, védett és reziliens EU jövőképét határozzák meg.

Új európai belső biztonsági irányítás

A Bizottság szorosan együtt fog működni a tagállamokkal és az uniós ügynökségekkel annak érdekében, hogy stratégiai és operatív szinten egyaránt korszerűsítse a belső biztonsággal kapcsolatos uniós megközelítést.

Ezt a következők révén éri el:

- **az új és felülvizsgált bizottsági kezdeményezések potenciális biztonsági és felkészültségi vonatkozásainak következetes azonosítása már kezdetektől fogva és a teljes tárgyalási folyamat során,**
- **a Bizottság európai belső biztonsággal foglalkozó projektcsoportjának rendszeres ülései, amelyeket a Bizottságon belüli, ágazatokon átívelő stratégiai együttműködés támogat,**
- **az Európai Biztonsági és Védelmi Főiskola munkáját támogató, a belső biztonsággal kapcsolatos fenyegetettségelemzések ismertetése,**
- **megbeszélések a tagállamokkal a Tanácsban a változó belső biztonsági kihívások alakulásáról a fenyegetettségelemzés alapján, valamint eszmecserék a fő szakpolitikai prioritásokról,**
- **rendszeres jelentéstétel az Európai Parlamentnek és a Tanácsnak a kulcsfontosságú biztonsági kezdeményezések szisztematikus végrehajtásának nyomon követése és támogatása érdekében.**

2. Integrált helyzetismeret és fenyegetettségelemzés

Fel fogjuk vértezni az EU-t az információk megosztásának és kombinálásának új módjaival, és rendszeres uniós belső biztonsági fenyegetettségelemzést fogunk készíteni, hozzájárulva egy átfogó kockázat- és fenyegetésértékeléshez.

A biztonság a **hatékony előrejelzéssel** kezdődik. Az EU-nak átfogó, kellően autonóm és naprakész helyzetismeretre és fenyegetettségelemzésre kell támaszkodnia. A hasznosítható információk – amelyeknek a tagállami hírszerzési információk egyedüli belépési pontjaként szolgáló egységes információelemzési kapacitáson (SIAC) keresztüli további javítására ösztönzik a tagállamokat – létfontosságúak a fenyegetések értékeléséhez és leküzdéséhez, és végső soron alapul szolgálnak a szakpolitikai és jogalkotási intézkedésekhez[7]. Hatékonyabban

[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.
[7] Együtt biztonságosabb – Európa polgári és katonai felkészültségének és készenlétének megerősítése, 23. o.

és jobban együttműködve kell kiaknáznunk a **hírszerzésen alapuló elemzéseket** és **fenyegetésértékeléseket** uniós szinten.

Az uniós szinten és egyes ágazatokra[8] vonatkozóan készített különböző kockázat- és fenyegetésértékelésekre építve a Bizottság **rendszeres uniós belső biztonsági fenyegetettségelemzéseket** fog készíteni a fő biztonsági kihívások azonosítása céljából, hogy információkkal szolgáljon a szakpolitikai prioritásokhoz. Ezek segíteni fognak egy olyan agilis és gyorsan reagáló belső biztonsági politika kialakításában, amely hatékonyan kezeli a változó fenyegetéseket, jobban védi az embereket és a vállalkozásokat a támadásokkal szemben, és lehetővé teszi a célzott szakpolitikai beavatkozások időben történő végrehajtását. Ezek az uniós belső biztonsági fenyegetettségelemzések hozzá fognak járulni a Bizottság és a főképviselő által kidolgozott **átfogó (ágazatokon átívelő, az összes veszélyre kiterjedő) uniós kockázat- és fenyegetésértékeléshez** is, a felkészültségi unióról szóló stratégiában meghatározottak szerint.

A bizalom és a biztonságos adatkezelés elengedhetetlen az információmegosztáshoz, és ehhez megbízható és biztonságos infrastruktúrára van szükség. Az uniós intézményeknek, szerveknek és ügynökségeknek biztosítaniuk kell, hogy képesek legyenek **biztonságos kommunikációs csatornákat** használni az érzékeny és minősített adatok egymás közötti és a tagállamokkal való cseréjére. Az **interoperábilis biztonságos rendszerekbe** és a megbízható technológiába történő beruházások megerősítik az EU autonómiáját, és megerősítik az EU azon képességét, hogy kezelje a válságokat és biztosítsa a működési rezilienciát. Ezzel összefüggésben a Bizottság sürgeti a társjogalkotókat, hogy zárják le az **uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról szóló rendeletjavaslattal** kapcsolatos tárgyalásokat, különösen a nem minősített és minősített érzékeny adatok kezelésére vonatkozó közös keret biztosítása érdekében[9].

Saját működési biztonságának és helyzetismeretének biztosítása érdekében a Bizottság felül fogja vizsgálni szervezeti biztonsági irányítási keretét, és **integrált biztonsági műveleti központot (ISOC)** fog létrehozni az emberek, a tárgyi eszközök és a műveletek valamennyi bizottsági helyszínen történő védelme érdekében. A Bizottság emellett növelni fogja a hibrid fenyegetések azonosítására és mérséklésére szolgáló operatív és elemzési kapacitásait.

A felkészültségi unióról szóló stratégiával összhangban a felkészültségi és biztonsági megfontolásokat beépítik és általánosan érvényesítik az uniós jogszabályokban, szakpolitikákban és programokban. A jogszabályok, szakpolitikák vagy programok felkészültségi és biztonsági szempontú előkészítése vagy felülvizsgálata során a Bizottság következetesen azonosítani fogja az előnyben részesített szakpolitikai alternatíva felkészültségre és biztonságra gyakorolt lehetséges hatásait. Ezt a Bizottság politikai döntéshozóinak rendszeres képzése fogja elősegíteni.

A tagállamok támogatása érdekében a Bizottság megvitatja a Tanáccsal a változó belső biztonsági kihívásokat és a kulcsfontosságú szakpolitikai prioritásokat, és rendszeresen tájékoztatja a Tanácsot a stratégia végrehajtásáról. Emellett a Bizottság folyamatosan tájékoztatja az Európai Parlamentet és az érdekelt feleket, és részt vesz minden releváns intézkedésben.

[8] Az e fenyegetettségelemzés alapjául szolgáló ágazati fenyegetésértékelések közé tartozik a súlyos és szervezett bűnözés általi fenyegetettség uniós értékelése (SOCTA), a terrorizmus helyzetéről és alakulásáról jelentés (TE-SAT), a közös kiberértékelési jelentés (JCAR), valamint a pénzmosás és terrorizmus finanszírozása jelentette fenyegetésekre, kockázatokra és módszerekre vonatkozó, a Bizottság és a Pénzmosás Elleni Hatóság által elvégzendő jövőbeli értékelések.

[9] COM (2022)119 final.

Fő intézkedések

A Bizottság:

- **rendszeres fenyegetettségelemzéseket dolgoz ki és nyújt be az EU belső biztonsági kihívásaira vonatkozóan.**

A Bizottság sürgeti a tagállamokat, hogy:

- **fokozzák a hírszerzési információk SIAC-kal való megosztását és biztosítsák az uniós ügynökségekkel és szervekkel való jobb információmegosztást.**

A Bizottság ösztönzi az Európai Parlamentet és a Tanácsot, hogy:

- **zárja le az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról szóló rendeletjavaslattal kapcsolatos tárgyalásokat.**

3. Az EU biztonsági képességeinek megerősítése

Új bűnüldözési eszközöket fogunk kifejleszteni, például az átalakított Europolt, valamint a biztonságos adatcsere és az adatokhoz való jogszerű hozzáférés koordinálására és biztosítására szolgáló jobb eszközöket.

A változó fenyegetésekkel szembeni hatékony fellépés érdekében az EU-nak fokoznia kell biztonsági képességeit és elő kell mozdítania az innovációt. A belső biztonsági fenyegetések elleni küzdelem elsődleges szereplőiként a bűnüldöző és igazságügyi hatóságoknak megfelelő operatív eszközökre és képességekre van szükségük a gyors és hatékony fellépéshez. Fontos, hogy ezek a hatóságok képesek legyenek a határokon és szolgálatokon átnyúló kommunikációra és koordinációra a hatékony megelőzés, felderítés, nyomozás és büntetőeljárás alá vonás érdekében.

A belső biztonságért felelős uniós ügynökségek és szervek

Az igazságügy, a belügy és a kiberbiztonság területén működő uniós ügynökségek és szervek kulcsszerepet játszanak az EU biztonsági struktúrájában, és ez a szerepük felelősségi körük bővülésével párhuzamosan egye növekszik.

Ma, 25 évvel létrehozása után az **Europol** minden eddiginél központibb szerepet tölt be az EU biztonsági keretrendszerében. Támogatja az összetett, határokon átnyúló nyomozásokat, megkönnyíti az információcserét, innovatív rendfenntartó eszközöket fejleszt ki, és magas szintű szakértelmet biztosít a bűnüldözés számára. Ugyanakkor számos tényező akadályozza az Europolt abban, hogy teljes mértékben kiaknázza operatív potenciálját a határokon átnyúló bűnözés elleni küzdelemre irányuló nyomozási és műveleti tevékenységek támogatása terén: ezen tényezők az erőforrások elégtelen szintjétől addig a tényig terjednek, hogy jelenlegi megbízatása nem terjed ki az olyan új biztonsági fenyegetésekre, mint a szabotázs, a hibrid fenyegetések vagy az információmanipuláció. A Bizottság ezért javasolni fogja az **Europol megbízatásának ambiciózus felülvizsgálatát** annak érdekében, hogy az valóban működőképes rendészeti szervvé váljon, amely jobban támogatja a tagállamokat. A cél az Europol technológiai szakértelmének és a nemzeti bűnüldöző hatóságok támogatására irányuló kapacitásának megerősítése, a más ügynökségekkel és szervekkel, valamint a tagállamokkal való koordináció fokozása, a partnerországokkal és a magánszektorral való stratégiai partnerségek megerősítése, valamint az Europol megerősített felügyeletének biztosítása.

Ezen túlmenően a Bizottság azon fog munkálkodni, hogy **tovább javítsa a belső biztonság terén működő uniós ügynökségek és szervek hatékonyságát és egymást kiegészítő jellegét, és erősítse a zökkenőmentes együttműködést** közöttük.

Értékeli és megerősíti az **Eurojust** megbízatását a hatékonyabb igazságügyi együttműködés érdekében, fokozva az Europollal való kiegészítő jelleget és együttműködést. Ez magában foglalja az Eurojust hatékonyságának növelését, valamint azon képességének fokozását, hogy proaktív támogatást és elemzést nyújtson a tagállamok igazságügyi hatóságainak. Továbbá, tekintettel az **Európai Ügyészségnek** az Unió pénzügyi érdekeit sértő bűncselekmények kivizsgálására és büntetőeljárás alá vonására vonatkozó egyedülálló hatáskörére, a Bizottság meg fogja vizsgálni, hogy miként lehetne a legjobban javítani az Európai Ügyészség uniós források védelmére irányuló kapacitását. Ez magában foglalja az Európai Ügyészség és az Europol közötti együttműködés megerősítését.

Az **ügynökségek közötti hatékony és biztonságos információcsere** elengedhetetlen az együttműködéshez. A 2024. januári együttes nyilatkozatnak[10] megfelelően az Europolnak és a Frontexnek gyors kölcsönös információcserére van szüksége, többek között operatív célokból. Az **eu-LISA** központi szerepet játszik az adatok biztonságos tárolásának és rendelkezésre állásának biztosításában az ügynökségek közötti jobb koordináció és hatékonyabb információcsere érdekében. Az **Európai Unió Alapjogi Ügynöksége** szakértelmet biztosít az alapvető jogok védelme terén a biztonságpolitikák kidolgozása és végrehajtása során.

Az **Európai Unió Pénzmosás és Terrorizmusfinanszírozás Elleni Hatósága (AMLA)** felhatalmazást kapott arra, hogy „találat/nincs találat” alapon összevesse az információkat az Europol, az Európai Ügyészség, az Eurojust és az Európai Csalás Elleni Hivatal által a határokon átnyúló ügyek közös elemzése céljából rendelkezésre bocsátott információkkal.

Az **ENISA** központi szerepet játszik az európai kiberbiztonsági jogszabályok végrehajtásában. A **kiberbiztonsági jogszabály** közelgő **felülvizsgálata** során a Bizottság értékelni fogja az ügynökség hatáskörét, és javaslatot fog tenni annak korszerűsítésére az uniós hozzáadott érték megerősítése érdekében.

Fokozódni fog a vámhatóságok és más bűnüldöző hatóságok közötti együttműködés annak köszönhetően, hogy az uniós vámügyi reformcsomagban javasoltaknak megfelelően létrejön az **Európai Unió vámhatósága** és az **uniós vámügyi adatközpont**. A jövőbeli vámügyi adatközpontból származó információk, valamint az Europoltól, az Eurojusttól, az Európai Ügyészségtől, az OLAF-tól, az AMLA-tól és a Frontextől származó kapcsolódó adatok saját hatáskörükön belül javítani fogják a közös elemzést, és hozzá fognak járulni a koherensebb műveleti tevékenységekhez, különösen a külső határokon. A Bizottság arra ösztönzi a társjogalkotókat, hogy mielőbb zárják le az uniós vámügyi reformról szóló tárgyalásokat, és e célból továbbra is segíteni fogja őket.

Az Európai Ügyészség, az OLAF, az Europol, az Eurojust, az AMLA és a javasolt uniós vámhatóság közötti kiegészítő jelleg fokozása emellett az **EU csalás elleni architektúrája** folyamatban lévő felülvizsgálatának eredményeire fog építeni. A belső biztonság számára előnyös lehet ez a holisztikus megközelítés, amely a büntetőjogi és közigazgatási eszközök jobb felhasználására, az informatikai rendszerek interoperabilitására és a jobb együttműködésre összpontosít.

Kritikus kommunikáció

Napjainkban a **kritikus kommunikációs rendszereket**[11] a legtöbb esetben nemzeti szinten, elszigetelten működtetik. Ez azt jelenti, hogy az elsődleges beavatkozók gyakran nem tudnak kommunikálni partnereikkel, amikor átlépik a határt egy másik tagállamba. Egyes

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

[11] Azaz a bűnüldöző szervek, a határőrök, a vámhatóságok, a polgári védelem, a tűzoltók, az orvosi sürgősségi ellátók és a közbiztonság és védelem egyéb kulcsszereplői által használt hálózatok.

tagállamokban az elsődleges beavatkozók különböző típusai (pl. rendőrség és mentősök) közötti kommunikáció is korlátozott. A legtöbb rendszer szabványai nem felelnek meg a mai követelményeknek a funkcionalitás és a reziliencia tekintetében, ami jelentősen korlátozza az elsődleges beavatkozók reagálási képességét, különösen határokon átnyúlóan.

Az EU válsághelyzetekre való reagálási képességének javítása érdekében a Bizottság jogalkotási javaslatot fog tenni egy **európai kritikus kommunikációs rendszer (EUCCS)** létrehozására, amely összekapcsolja a tagállamok következő generációs kritikus kommunikációs rendszereit az EU-ban. A cél az, hogy az EUCCS három stratégiai pilléren alapuljon: operatív mobilitás, erős reziliencia és stratégiai autonómia. Az EUCCS-kezdeményezés harmonizált követelményeket határoz meg, és elősegíti a tagállamok kritikus kommunikációs rendszereinek korszerűsítését, lehetővé téve azok zökkenőmentes működését. Ezen felül kiterjeszti a rendszer lefedettségét a jövőbeli IRIS^{2} [12] multiorbitális rendszer révén. Az EUCCS technikai képességeit az EU által finanszírozott projektek építik ki, elsősorban az európai technológiaszolgáltatókra támaszkodva, hogy előmozdítsák az EU stratégiai autonómiáját ebben az érzékeny ágazatban.

Jogszerű hozzáférés az adatokhoz

A bűnüldöző és igazságügyi hatóságoknak képesnek kell lenniük a bűncselekmények kivizsgálására és az ellenük való fellépésre. Napjainkban a súlyos és szervezett bűnözés szinte minden formájának van digitális lábnyoma[13]. A bűnügyi nyomozások mintegy 85 %-a esetébenjelenleg elengedhetetlen, hogy a bűnüldöző hatóságok képesek legyenek hozzáférni a digitális információkhoz.[14]

A **hatékony bűnüldözést célzó adathozzáféréssel foglalkozó magas szintű munkacsoport** zárójelentésében[15] kiemelte, hogy a bűnüldöző szervek és az igazságszolgáltatás az elmúlt évtizedben teret vesztettek a bűnözőkkel szemben, mivel utóbbiak más joghatóságokból származó eszközöket és termékeket vesznek igénybe. Ezeket olyan szolgáltatók bocsátják a rendelkezésükre, amelyek az általuk bevezetett intézkedésekkel megfosztják a hatóságokat az egyes büntetőügyekben a jogszerű megkeresésekkel kapcsolatos együttműködés eszközeitől. A bűnüldöző hatóságok és a magánfelek – köztük a szolgáltatók – közötti szisztematikus együttműködés ezért elengedhetetlen az Unióban és azon kívül a legnagyobb fenyegetést jelentő bűnözői hálózatok és egyének felszámolására irányuló jövőbeli erőfeszítésekhez.

Mivel a digitalizáció egyre elterjedtebbé válik, és egyre több új eszközt biztosít a bűnözők számára, alapvető fontosságú egy olyan keret az adatokhoz való hozzáféréshez, amely megfelel a jogszabályok érvényesítéséhez és értékeink védelméhez szükséges igényeknek. Ugyanakkor a kiberbiztonság megőrzése és a felmerülő biztonsági fenyegetésekkel szembeni védelem szempontjából ugyanilyen fontos annak biztosítása, hogy a digitális rendszerek továbbra is biztonságosak maradjanak a jogosulatlan hozzáféréssel szemben. Az ilyen hozzáférési kereteknek tiszteletben kell tartaniuk az alapvető jogokat is, biztosítva többek között a magánélet és a személyes adatok megfelelő védelmét.

Az elmúlt években az EU intézkedéseket hozott mind az **online bűnözés elleni küzdelem, mind pedig a digitális bizonyítékokhoz való hozzáférés megkönnyítése érdekében valamennyi bűncselekmény esetében**, az elektronikus bizonyítékokra vonatkozó szabályok

[12] A rezilienciát, az összekapcsoltságot és a biztonságot szolgáló uniós műholdas infrastruktúra.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52019PC0070.
[15] A hatékony bűnüldözést célzó adathozzáféréssel foglalkozó magas szintű munkacsoport zárójelentése – 2024. 11. 15., 4802e306-c364-4154-835b-e986a9a49281_en.

elfogadásával, amelyek 2026 augusztusától teljeskörűen alkalmazandók lesznek[16]. Ezeket az információk és bizonyítékok cseréjére vonatkozó nemzetközi jogi eszközök egészítik ki. A Bizottság hamarosan javaslatot fog tenni a **számítástechnikai bűnözés elleni új ENSZ-egyezmény** aláírására és megkötésére.

A magas szintű munkacsoport ajánlásainak[17] gyakorlatba ültetése érdekében a Bizottság 2025 első felében **ütemtervet fog előterjeszteni, amelyben meghatározza azokat a jogi és gyakorlati intézkedéseket**, amelyeket az **adatokhoz való jogszerű és hatékony hozzáférés biztosítása** érdekében javasol. Ezen ütemterv végrehajtása során a Bizottság prioritásként fogja kezelni az **adatmegőrzési szabályok** uniós szintű hatásának értékelését és a **titkosításra vonatkozó technológiai ütemterv** elkészítését azon technológiai megoldások azonosítása és értékelése érdekében, amelyek lehetővé tennék a bűnüldöző hatóságok számára, hogy a kiberbiztonság és az alapvető jogok biztosítása mellett jogszerűen hozzáférjenek titkosított adatokhoz.

Operatív együttműködés

A Bizottság együtt fog működni a tagállamokkal, az uniós ügynökségekkel és szervekkel, valamint a partnerországokkal az operatív együttműködés megerősítése érdekében, ami elengedhetetlen a nemzetközi szervezett bűnözés és a terrorizmus elleni küzdelem hatékonyabb megközelítéséhez.

A súlyos és szervezett bűnözés elleni közös fellépés fő uniós kereteként az **Európai Multidiszciplináris Platform a Bűnügyi Fenyegetettség Ellen (EMPACT)** jelentős operatív eredményeket ért el. A következő, 2026–2029-es EMPACT-ciklus lehetőséget kínál e keret további megerősítésére. A legnagyobb fenyegetést jelentő bűnözői hálózatok és egyének felszámolása érdekében az Uniónak észszerűsítenie kell erőfeszítéseit, és azokat a legsürgetőbb prioritásokra kell összpontosítania, fokozva a tagállamok kötelezettségvállalásait és biztosítva az erőforrások hatékony felhasználását.

E célból a Bizottság együtt fog működni a Tanács elnökségeivel és a tagállamokkal az **EMPACT-ban rejlő lehetőségek maximalizálása és a következő, 2026–2029-es EMPACT-ciklus fő prioritásainak kezelése érdekében.** Ezeken a kiemelt területeken a legnagyobb fenyegetést jelentő bűnözői hálózatokkal kapcsolatos hírszerzési információkra, közös nyomozásokra és operatív munkacsoportokra, valamint határozott igazságügyi válaszintézkedésekre, többek között a pénz útjának nyomon követésére vonatkozó elven alapuló megközelítésre van szükség. Ezen túlmenően az Uniónak küzdenie kell a bűnszervezetek általi beszervezés és azok beszivárgása ellen, és meg kell erősítenie a több ügynökség munkájára építő és nemzetközi bűnüldözési együttműködést és képzést.

A Bizottság a **tagállamok és a schengeni társult országok közötti, határokon átnyúló operatív bűnüldözési együttműködés** egyéb formáit is támogatni fogja. A belső határellenőrzés nélküli schengeni térség szoros együttműködést és információcserét igényel a tagállamok bűnüldöző hatóságai között a magas szintű belső biztonság biztosítása érdekében. A bűnüldöző szervek tagjai ma még mindig kihívásokkal szembesülnek a határokon átnyúló megfigyelés vagy sürgős beavatkozások végrehajtása során[18], és a hibrid fenyegetések elleni

[16] Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról, (HL L 191., 2023.7.28.).

[17] A Tanács következtetései a hatékony bűnüldözést szolgáló adathozzáférésről (2024. december 12.) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/hu/pdf.

[18] Az operatív bűnüldözési együttműködésről szóló, 2022. június 9-i (EU) 2022/915 tanácsi ajánlás tagállami hatásának bizottsági értékelésében (5909/25) foglaltak szerint.

küzdelemhez szintén megerősített határokon átnyúló együttműködésre van szükség. A közös stratégiai jövőkép kialakítása érdekében létre kell hozni az **operatív bűnüldözési együttműködés jövőjével foglalkozó magas szintű munkacsoportot**.

A bűnüldöző hatóságok közötti hatékony adatcsere szintén elengedhetetlen a hatékony határokon átnyúló együttműködéshez. Létrehozását követően az **interoperabilitási architektúra** hatékony hozzáférést biztosít a bűnüldöző hatóságok és az Europol számára a kulcsfontosságú információkhoz. Ugyanakkor az EU-nak és tagállamainak prioritásként kell kezelniük a két- és többoldalú információcserét a **Prüm II. rendelet**[19] jogi és technikai végrehajtása révén, az eu-LISA-val és az Europollal együttműködésben. Ez lehetővé teszi az ujjlenyomatok, DNS-profilok, gépjármű-nyilvántartási adatok, arcképmások és rendőrségi nyilvántartási adatok uniós útválasztókon keresztüli biztonságos automatizált cseréjét. Nemzeti szinten a tagállamoknak végre kell hajtaniuk az **információcseréről szóló irányelvet**[20], javítva a zökkenőmentes, határokon átnyúló információáramlást lehetővé tevő információcsere-csatornákat, ugyanakkor biztosítva azok integrációját az uniós szintű rendszerekkel, például a SIENA-val[21].

A határokon átnyúló hatékony együttműködés a **közös uniós bűnüldözési kultúra** előmozdításán is múlik. E cél eléréséhez elengedhetetlenek a közös képzések, a kiválósági központok és a mobilitási programok. A Bizottság meg fogja vizsgálni, hogy az EU miként tudja a legjobban támogatni a tagállami hatóságok képzését, a **CEPOL**-ra mint a bűnüldözési képzéssel foglalkozó uniós ügynökségre támaszkodva.

A határbiztonság megerősítése

A külső határok rezilienciájának és biztonságának megerősítése elengedhetetlen a hibrid fenyegetésekkel – például a migráció fegyverként való felhasználásával – szembeni fellépéshez, a fenyegető szereplők és áruk EU-ba való belépésének megelőzéséhez, valamint a határokon átnyúló bűnözés és a terrorizmus elleni hatékony küzdelemhez. A **tervek szerint 2026-ban továbbfejlesztik a Schengeni Információs Rendszert (SIS)** annak érdekében, hogy a tagállamok a harmadik országok által az Europollal megosztott adatok alapján bevihessék a terrorizmusban és egyéb súlyos bűncselekményekben részt vevő harmadik országbeli állampolgárokra – többek között a külföldi terrorista harcosokra – vonatkozó figyelmeztető jelzéseket.

A nagy méretű uniós információs rendszerek **interoperabilitásának** javítása alapvető információkkal fogja ellátni a tagállamokat a külső határokat átlépő vagy átlépni szándékozó, harmadik országokból származó egyénekről, segítve a hatóságokat a tagállamok területére való belépés engedélyezési feltételeinek értékelésében[22] A Bizottság továbbra is szorosan együtt fog működni a tagállamokkal és az eu-LISA-val e rendszerek – nevezetesen a **betáplálási-kiadási**

[19] Az Európai Parlament és a Tanács (EU) 2024/982 rendelete (2024. március 13.) az adatoknak a rendőrségi együttműködés céljából történő automatizált kereséséről és cseréjéről, valamint a 2008/615/IB és a 2008/616/IB tanácsi határozat, továbbá az (EU) 2018/1726, az (EU) 2019/817 és az (EU) 2019/818 európai parlamenti és tanácsi rendelet módosításáról (Prüm II rendelet) (HL L 2024/982, 2024.4.5.).

[20] Az Európai Parlament és a Tanács (EU) 2023/977 irányelve (2023. május 10.) a tagállamok bűnüldöző hatóságai közötti információcseréről és a 2006/960/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 134., 2023.5.22., 1. o.).

[21] Biztonságos Információcsere Hálózati Alkalmazás.

[22] A betáplálási-kiadási rendszer (EES) lehetővé teszi a tagállamok számára, hogy azonosítsák a harmadik országbeli állampolgárokat a schengeni térség külső határain, és rögzítsék be- és kilépéseiket, lehetővé téve az engedélyezett tartózkodási időt túllépő személyek szisztematikus azonosítását. A harmadik országbeli állampolgároknak a külső határokra való megérkezését megelőzően az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) és a vízuminformációs rendszer (VIS) lehetővé teszi a tagállamok számára annak előzetes értékelését, hogy egy harmadik országbeli állampolgár jelenléte az EU területén biztonsági kockázatot jelentene-e.

rendszer (EES), az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) és a felülvizsgált vízuminformációs rendszer (VIS) – gyors megvalósítása céljából, azok zökkenőmentes működésének és biztonsági előnyeinek biztosítása érdekében.

A határbiztonság további fokozása és a változó fenyegetésekkel szembeni uniós együttműködés megerősítése érdekében a **Bizottság javasolni fogja a Frontex megerősítését**. Az Európai Határ- és Parti Őrség létszámának idővel meg kell háromszorozódnia, azaz 30 000 főre kell emelkednie. Az Ügynökséget fejlett megfigyelési és helyzetismereti technológiával kell felszerelni, beleértve az európai integrált határigazgatás szempontjából releváns hírszerzési technológiákat, valamint a 2027-ig telepítendő, megbízható uniós Föld-megfigyelési kormányzati szolgáltatásokhoz való hozzáférést. Ennek tovább kell erősítenie a határokon átnyúló bűnözés külső határokon történő felderítésére, megelőzésére és az ellene folytatott küzdelemre irányuló képességet, valamint meg kell erősítenie a tagállamoknak a visszaküldések végrehajtásához nyújtott támogatást, különösen a biztonsági kockázatot jelentő harmadik országbeli állampolgárok tekintetében.

Az **okmányokkal és személyazonossággal való visszaélés** megkönnyíti a migránscsempészést, az emberkereskedelmet, az illegális bűnözői mozgásokat és a tiltott áruk kereskedelmét. A **többszörös személyazonosságot észlelő rendszer (MID)**[23] – amint működőképessé válik – javítani fogja a nemzeti hatóságok azon képességét, hogy azonosítsák a többszörös személyazonosságot használó személyeket, és fellépjenek a személyazonossággal való visszaélés ellen. A Bizottság meg fogja vizsgálni, hogy miként lehetne fokozni az uniós polgárok és harmadik országbeli állampolgárok számára kiállított úti és tartózkodási okmányok biztonságát. Emellett a Bizottság értékelni fogja, hogy az európai digitális személyiadat-tárcák, amelyeket 2026 végéig kell bevezetni az európai digitális személyazonossági keret keretében, hogyan járulhatnak hozzá az úti okmányok biztonságának fokozásához és a személyazonosság-ellenőrzés javításához. Ez kiegészíti a digitális utazási igazolványokra és az „EU Digital Travel" alkalmazásra[24] vonatkozó javaslatokat.

Az **utazási információk** kulcsfontosságúak a hatóságok számára a bűnözők, terroristák és más, biztonsági fenyegetést jelentő személyek mozgásának azonosításához és kivizsgálásához. Bár létezik a kereskedelmi légi közlekedési információkra vonatkozó uniós keret[25], a más közlekedési módokból származó adatok bűnüldözési célú feldolgozása széttagolt. Következésképpen a bűnözők és a terroristák az egyéb közlekedési módokat kihasználhatják észrevétlen illegális tevékenységek folytatására. A Bizottság együtt fog működni a tagállamokkal és a közlekedési ágazattal az **utazási információs keret megerősítése** érdekében azáltal, hogy megvizsgálja egy olyan uniós szabályozás lehetőségét, amely előírja a magánrepülőgépek üzemeltetői számára az utasadatok gyűjtését és továbbítását, értékeli az utasnyilvántartási adatállomány kezelésére vonatkozó szabályokat, és értékeli a tengeri utazási információk feldolgozása észszerűsítésének módjait. A közúti közlekedés tekintetében a Bizottság értékelni fogja az **automatikus rendszámfelismerő (ANPR) rendszerek** kiterjesztett használatát, és növelni fogja a SIS-szel való szinergiák lehetőségeit.

[23] A többszörös személyazonosságot észlelő rendszer az (EU) 2019/818 rendelettel és az (EU) 2019/817 rendelettel bevezetett interoperabilitási elemek egyike.
[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047.
[25] Az (EU) 2016/681 irányelvvel (a továbbiakban: PNR-irányelv), valamint az (EU) 2025/12 rendelettel és az (EU) 2025/13 rendelettel (a továbbiakban: API-rendeletek) létrehozott utasnyilvántartási adatállomány (PNR) és előzetes utasinformációs (API) keret.

Előrejelzés, innováció és képességorientált megközelítés

A Bizottság a nemzeti szinten azonosított bevált gyakorlatokra támaszkodva **átfogó, uniós szintű előrejelzési megközelítést** fog kidolgozni a **belső biztonságra vonatkozóan**. Ez a megközelítés támogatni fogja a szakpolitikai döntéshozatalt, és iránymutatást nyújt az uniós finanszírozású releváns biztonsági kutatásba és innovációba történő beruházásokhoz.

A **kutatás és az innováció döntő szerepet játszik a belső biztonságban** azáltal, hogy megoldásokat dolgoz ki az újonnan felmerülő – többek között a technológiával való visszaélésből eredő – fenyegetések leküzdésére[26]. Az EU-nak az uniós finanszírozású biztonsági kutatás és innováció[27] révén továbbra is be kell ruháznia a biztonsági fenyegetések kezelésére szolgáló innovatív eszközök és megoldások fejlesztésébe, miközben tiszteletben tartja az uniós szabályokat és az alapvető jogokat. A Bizottságnak támogatnia kell a kutatásról a hasznosításra való átállást e modern képességek hatékony elterjedésének biztosítása érdekében, prioritásként kezelve az olyan **modern technológiákat**, mint a mesterséges intelligencia. Ennek a megközelítésnek magában kell foglalnia az MI-rendszerek és más technikai képességek bűnüldöző és igazságügyi hatóságok általi használatának javítását célzó képzést. Emellett adott esetben a technológiák kettős felhasználásában rejlő lehetőségeket mindkét irányban ki kell aknázni (a polgári technológia védelmi célú felhasználása, illetve a védelmi technológia polgári célú felhasználása)[28].

A kutatás gyakorlati és szakpolitikai integrálását a **belső biztonság uniós innovációs központja**[29] elnevezésű, innovációs laboratóriumok alkotta hálózat fogja segíteni, amely a legújabb innovációs frissítéseket és hatékony megoldásokat kínál az EU-ban és a tagállamokban működő belső biztonsági szereplők munkájának támogatására. Az Europol hatékonyságának növeléséhez meg kell erősíteni az Europol-eszköztárat (ETR), amely lehetővé teszi az Europol számára a fejlett technológiák operatív azonosítását, fejlesztését, közös beszerzését és alkalmazását. Emellett a Bizottság a Közös Kutatóközpontjában **biztonsági kutatási és innovációs kampuszt** hoz létre, amely összefogja a kutatókat, hogy lerövidítse a kutatási eredményektől az innovációig, a fejlesztésig és a sikeres megvalósításig tartó ciklust, miközben csökkenti a fejlesztési, tesztelési és validálási költségeket.

Európai Kutatási Térségünk természeténél fogva együttműködésen alapul, ezért ki van téve a külföldi beavatkozásnak és a dezinformációnak. A kutatásbiztonság fokozásáról szóló tanácsi ajánlás[30] elfogadását követően a Bizottság és a tagállamok intézkedéseket hoznak az érintett szereplők megerősítése érdekében, többek között egy kutatásbiztonsággal foglalkozó szakértői központ létrehozása révén.

Fő intézkedések

A Bizottság elfogadja a következőket:

- **jogalkotási javaslat az Europol 2026-ra valóban működőképes bűnüldöző hatósággá alakításáról,**

[26] Lásd a Bizottság Közös Kutatóközpontjának „Emerging risks and opportunities for EU internal security from new technologies” (Az EU belső biztonságát fenyegető, az új technológiákból eredő kockázatok és lehetőségek) című jelentését: https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] Study on strengthening EU- funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025 (Tanulmány az uniós finanszírozású biztonsági kutatás és innováció megerősítéséről – Az EU által finanszírozott polgári biztonsági kutatás és innováció 20 éve) – 2025, https://data.europa.eu/doi/10.2837/0004501.

[28] A Niinistö-jelentésben foglaltak szerint.

[29] A belső biztonság európai innovációs központja | Europol.

[30] HL C/2024/3510, 2024.5.30.

- **jogalkotási javaslat az Eurojust 2026-ra történő megerősítéséről,**
- **jogalkotási javaslat a Frontex szerepének és feladatainak 2026-ra történő megerősítéséről,**
- **jogalkotási javaslat az európai kritikus kommunikációs rendszer 2026-ban történő létrehozásáról.**

A Bizottság:

- **2025-ben ütemtervet terjeszt elő, amelyben meghatározza a bűnüldöző szervek adatokhoz való jogszerű és hatékony hozzáférésével kapcsolatos további lépéseket,**
- **2025-ben hatásvizsgálatot készít az uniós szintű adatmegőrzési szabályok adott esetben elvégzendő naprakésszé tétele céljából,**
- **2026-ban a titkosításra vonatkozó technológiai ütemtervet terjeszt elő azon technológiai megoldások azonosítása és értékelése céljából, amelyek lehetővé teszik a bűnüldöző hatóságok számára az adatokhoz való jogszerű hozzáférést,**
- **egy magas szintű munkacsoport létrehozására fog törekedni az operatív bűnüldözési együttműködés megerősítése érdekében,**
- **2026-ban biztonsági kutatási és innovációs kampuszt hoz létre a Közös Kutatóközpontban.**

A Bizottság a tagállamokkal és az érintett uniós ügynökségekkel együttműködve:

- **megerősíti az EMPACT architektúráját,**
- **az interoperabilitási architektúra gyors bevezetésén és a Prüm II rendelet végrehajtásán fog munkálkodni,**
- **megerősíti az utazási információs keretet.**

A Bizottság sürgeti a tagállamokat, hogy:

- **ültessék át és hajtsák végre teljeskörűen az információcseréről szóló irányelvet.**

4. Reziliencia a hibrid fenyegetésekkel és más ellenséges cselekményekkel szemben

A kritikus infrastruktúrák védelmének fokozása, a kiberbiztonság megerősítése, a közlekedési csomópontok és kikötők biztosítása, valamint az online fenyegetések elleni küzdelem révén növeljük a hibrid fenyegetésekkel szembeni rezilienciát.

Nőtt az EU biztonságát aláásó ellenséges cselekmények gyakorisága és kifinomultsága, és a rosszindulatú szereplők jelentősen bővítették arzenáljukat. Az EU-t, annak tagállamait és partnereit célzó hibrid hadjáratok intenzívebbé váltak, és a kritikus infrastruktúrákat célzó szabotázscselekményeket, gyújtogatást, kibertámadásokat, a választásokba történő beavatkozást, külföldi beavatkozást és információmanipulációt, többek között dezinformációt, valamint a migráció fegyverként való felhasználását is magukban foglalják. Politikai és operatív szerepük, valamint az általuk kezelt információk jellege miatt a támadások az uniós intézményeket, szerveket és hivatalokat (a továbbiakban: uniós szervezetek) sem kímélik.

Az EU-nak **fokoznia kell rezilienciáját**, hatékonyan kell alkalmaznia a jelenlegi eszközöket, és új módszereket kell kidolgoznia az állami és nem állami szereplőktől eredő, folyamatosan változó fenyegetésekkel való szembeszállásra, mind most, mind a jövőben.

Kritikus infrastruktúra

Komoly aggodalomra adnak okot a **kritikus infrastruktúrákat** fenyegető veszélyek, többek között az olyan hibrid fenyegetések, mint a szabotázs és a rossz szándékú kibertevékenységek,

különösen a tagállamokat összekötő infrastruktúra – legyen szó energiarendszer-összekötőkről vagy határokon átnyúló kommunikációs kábelekről – és a közlekedés tekintetében. Oroszország Ukrajna elleni agressziós háborúja óta fokozódtak a kritikus infrastruktúrákat célzó szabotázsok, különösen 2024-ben, amelyek számos tagállamot érintettek. Az ilyen cselekmények hatékony előrejelzéséhez, felderítéséhez, megelőzéséhez és az azokra való hatékony reagáláshoz elengedhetetlen a bűnüldöző, biztonsági és kiberbiztonsági szolgálatok, a katonai és polgári védelem, valamint a magánszereplők közötti együttműködés.

A gazdaság és a társadalom számára létfontosságú alapvető szolgáltatások folyamatosságának biztosításához alapvető fontosságú a kritikus szervezetek sebezhetőségének csökkentése és rezilienciájának megerősítése. Ezért e tekintetben döntő fontosságú a **kritikus szervezetek rezilienciájáról (CER) szóló irányelv**[31] és az **Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelv (NIS 2)**[32] valamennyi tagállam általi időben történő átültetése és helyes végrehajtása.

A gyors előrehaladás biztosítása érdekében a Bizottság a **kritikus szervezetek rezilienciájával foglalkozó csoporttal és a Kiberbiztonsági Együttműködési Csoporttal** együttműködve támogatni fogja a tagállamokat a kritikus szervezetek azonosításában[33], valamint az alapvető szolgáltatásokkal kapcsolatos nemzeti stratégiákra és kockázatértékelésekre vonatkozó bevált gyakorlatok cseréjében. Amennyiben a kritikus infrastruktúrák zavarai számottevő határokon átnyúló hatással járnak, a **kritikus infrastruktúrákra vonatkozó uniós terv** fogja koordinálni az uniós szintű válaszlépéseket. A Bizottság arra ösztönzi a Tanácsot, hogy mielőbb fogadja el az **uniós kiberbiztonsági tervet**, amely tovább erősíti a koordinációt a válságkezeléssel összefüggésben, elősegítve a hatóságok közötti szorosabb együttműködést a fizikai és digitális reziliencia terén. A 2023. évi sikeres energiaágazati stressztesztet követően a Bizottság ösztönözni fogja az **önkéntes stressztesztet** a belső biztonság szempontjából kulcsfontosságú egyéb ágazatokban. Emellett a Bizottság **uniós szintű áttekintést** fog nyújtani az alapvető szolgáltatásokat érintő, **határokon átnyúló és ágazatközi kockázatokról**, hogy támogassa a tagállamok kockázatértékeléseit, és alapul szolgáljon egy átfogó uniós szintű kockázatértékeléshez. A felkészültségi unióról szóló stratégiával összhangban a Bizottság együtt fog működni a tagállamokkal azon további ágazatok és szolgáltatások azonosítása érdekében, amelyek nem tartoznak a jelenlegi jogszabályok hatálya alá, és amelyek esetében fellépésre lehet szükség.

A **kritikus infrastruktúrák rezilienciájával foglalkozó EU-NATO munkacsoport** kiváló együttműködést mozdított elő a bevált gyakorlatok megosztása, valamint az energia-, a közlekedési, a digitális infrastruktúra és az űrágazat rezilienciájának fokozása terén. Ez a munka a **rezilienciáról szóló EU-NATO strukturált párbeszéd** keretében folytatódik. Az **uniós hibrid eszköztár** stabil támogatást nyújt a tagállamoknak és a partnereknek a hibrid fenyegetésekre való felkészüléshez és az ellenük való fellépéshez. A **hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatok**[34] kérésre személyre szabott, rövid távú segítséget nyújtanak a tagállamoknak, a különböző uniós misszióknak és partnereknek. Ezen túlmenően

[31] 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.

[32] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).

[33] Az irányelv hatálya alá tartozó ágazatok az energia, a közlekedés, a bankszektor, a pénzügyi piaci infrastruktúra, az egészségügy, az ivóvíz, a szennyvíz, a digitális infrastruktúra, a közigazgatás, az űrkutatás, az élelmiszer-termelés, -feldolgozás és -elosztás.

[34] A biztonság és a védelem területére vonatkozó uniós stratégiai iránytű, 2022, 22. o.

a Bizottság szakértői tevékenységek[35] révén elő fogja mozdítani a szabotázs elleni küzdelem terén folytatott uniós együttműködést, beleértve egy a szakértőknek szóló **célzott közös munkaprogramot** az információcsere észszerűsítése és az ellenintézkedések feltérképezése érdekében.

A **tenger alatti kábeleket** érintő váratlan európai események rávilágítanak arra, hogy határozottabb intézkedésekre és egyértelműbb válaszlépésekre van szükség. A **kábelbiztonságra vonatkozó uniós cselekvési tervben**[36] foglaltaknak megfelelően a Bizottság és a főképviselő együtt fognak működni a tagállamokkal, az uniós ügynökségekkel és a partnerekkel, például a NATO-val a tenger alatti kábeleket fenyegető veszélyek megelőzése, felderítése, az azokra való reagálás és az ilyen fenyegetésektől való elrettentés érdekében. A fenyegetések integrált helyzetképének kialakítása érdekében a Bizottság együtt fog működni a tagállamokkal annak érdekében, hogy önkéntes alapon tengermedencénként kidolgozzák a tenger alatti kábelek integrált felügyeleti mechanizmusát és alkalmazzák azt, kezdve egy skandináv/balti regionális központtal.

Kiberbiztonság

A gyakran a többdimenziós és hibrid fenyegetések szélesebb körének részét képező **rossz szándékú kibertevékenységek** tartós jellege folyamatos figyelmet és fellépést igényel európai szinten. Az elmúlt években az Unió számos olyan kiberbiztonsági jogszabályt fogadott el, amelyek megerősítik az uniós kritikus ágazatokban működő NIS 2 szervezetek, valamint az uniós szervezetek kiberrezilienciáját[37], javítják a digitális termékek biztonságát (a kiberrezilienciáról szóló jogszabály), valamint létrehozzák a felkészültség és a biztonsági eseményekre való reagálás támogatásának keretét (a kiberszolidaritásról szóló jogszabály). 2025 januárjában a Bizottság elfogadta a **kórházak és az egészségügyi szolgáltatók kiberbiztonságára vonatkozó európai cselekvési tervet**[38] a fenyegetések felderítésének, az azokra való felkészültségnek és a válságokra való reagálásnak a javítása érdekében. Ennek teljes körű végrehajtása kulcsfontosságú. Ugyanakkor az új fenyegetések és fejlemények kezelése érdekében fokoznunk kell intézkedéseinket, különösen az információcsere, az ellátási lánc biztonsága, a zsarolóvírusok és a kibertámadások, valamint a technológiai szuverenitás területén.

Emellett a végrehajtáshoz meg kell szüntetni a jelenlegi, 299 000 főt kitevő kiberbiztonsági készséghiányt. A Bizottság a készségek uniója[39] keretében együtt fog működni a tagállamokkal a kiberbiztonsági munkaerő bővítése érdekében, különösen az új Kiberkészségek Akadémiájának segítségével. A STEM (a természettudományok, a technológia, a műszaki tudományok és a matematika) oktatási stratégiai terv[40] hozzájárul az uniós tehetségbázis és Európa kiberbiztonsági munkaerőpiaci igényekre való reagálásának javításához.

Rezilienciájának fokozásával párhuzamosan az EU továbbra is teljes mértékben ki fogja használni a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai

[35] Az uniós védelmi biztonsági tanácsadók, a robbanóanyag-mentesítési európai hálózat (EEODN), az Atlasz-hálózat, az EU kiemelt kockázatú nyilvános terek biztonságával foglalkozó hálózata (EU HRSN), a vegyi, biológiai, radiológiai és nukleáris anyagokkal foglalkozó biztonsági tanácsadó csoport, a kritikus szervezetek rezilienciájával foglalkozó csoport (CERG).

[36] JOIN (2025) 9 final.

[37] Az Európai Parlament és a Tanács (EU, Euratom) 2023/2841 rendelete (2023. december 13.) az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról (HL L, 2023/2841, 2023.12.18.).

[38] https://digital-strategy.ec.europa.eu/hu/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

[39] COM (2025) 90 final.

[40] COM (2025) 89 final.

intézkedések keretét (**a kiberdiplomáciai eszköztárat**) az állami és nem állami szereplőktől eredő kiberfenyegetések megelőzése, az ilyen fenyegetésektől való elrettentés és az azokra való reagálás érdekében.

Az IKT-ellátási láncok biztonsága

Az **5G kiberbiztonsággal kapcsolatos eszköztár** megfelelő keretet biztosít az 5G hálózatok védelméhez, de a tagállamok jelenleg elégtelenül hajtják végre azt. Továbbra is elfogadhatatlan biztonsági kockázatok állnak fenn, különösen a magas kockázatú szolgáltatók helyettesítése tekintetében. Az IKT-ellátási lánc biztonságára vonatkozó harmonizált megközelítés kezelheti a belső piacnak a különböző nemzeti szintű megközelítések által okozott jelenlegi széttagoltságát, elkerülheti a kritikus függőségeket és csökkentheti IKT-ellátási láncaink magas kockázatú beszállítókkal kapcsolatos kockázatait, ily módon biztosítva kritikus infrastruktúráinkat.

E megközelítéssel összhangban a **kiberbiztonsági jogszabály közelgő felülvizsgálata** során a Bizottság szélesebb körben fogja vizsgálni az IKT-ellátási láncok és infrastruktúra biztonságát és rezilienciáját. Emellett a Bizottság javasolni fogja az **európai kiberbiztonsági tanúsítási keretrendszer** javítását annak biztosítása érdekében, hogy a jövőbeli tanúsítási rendszereket időben el lehessen fogadni, és azok reagálni tudjanak a szakpolitikai igényekre.

A meglévő vagy folyamatban lévő ágazati értékelésekre[41] építve a Bizottság a tagállamokkal együtt **stratégiai tervet dolgoz ki az összehangolt kiberbiztonsági kockázatértékelésekre** vonatkozóan.

A felhőalapú és távközlési szolgáltatások a kritikus infrastruktúrák, a vállalkozások és a hatóságok ellátási láncainak egyik sarokkövévé váltak. A Bizottság intézkedéseket fog hozni annak érdekében, hogy arra ösztönözze a kritikus szervezeteket, hogy olyan **felhőalapú és távközlési szolgáltatásokat** válasszanak, amelyek **megfelelő szintű kiberbiztonságot kínálnak**, figyelembe véve nemcsak a technikai kockázatokat, hanem a stratégiai kockázatokat és függőségeket is.

Zsarolóvírusok és kibertámadások

Az EU-ban és világszerte továbbra is komoly kihívást jelentenek a **zsarolóvírusok**; egy jelentés 2031-re több mint 250 milliárd EUR-ra becsüli az azokkal kapcsolatos globális éves költségeket[42]. Mind a **NIS 2 irányelv**, mind a **kiberrezilienciáról szóló jogszabály** jelentősen javítani fogja a szervezetek kiberbiztonsági helyzetét, ami költségesebbé teszi a zsarolóvírus-hálózatok számára a támadásaik végrehajtását. Emellett a Bizottság szorosan együtt fog működni a tagállamokkal annak biztosítása érdekében, hogy több zsarolóvírus-támadást, különösen folyamatos fenyegetést jelentő támadást és váltságdíjfizetést jelentsenek a bűnüldöző hatóságoknak, megkönnyítve a nyomozásokat.

A kibertámadások megelőzése és megállítása érdekében az EU-nak az Europol és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) égisze alatt meg kell erősítenie a bűnüldöző hatóságok, a kiberbiztonsági hatóságok és szervezetek, valamint a magánfelek közötti információcserét.

Az Europolnak és az Eurojustnak tovább kell építkeznie a váltságdíjfizető programok felszámolása terén elért eredményeire, támogatva a bűnüldözési együttműködést. E célból a

[41] Például az 5G hálózatokkal, a távközléssel, a villamos energiával, a megújuló energiával és az összekapcsolt járművekkel kapcsolatosan.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

bűnüldözésnek maximálisan ki kell használnia az együttműködési mechanizmusokat, beleértve az **Europol nemzetközi zsarolóvírus-reagálási modelljét** és a **zsarolóvírusok elleni nemzetközi kezdeményezést (CRI)**[43], az ENISA-nak és az Europolnak pedig együtt kell működnie a különböző típusú zsarolóvírusokat dekódoló eszközök adattárának[44] bővítése érdekében.

Technológiai szuverenitás

A kiberbiztonság és a technológiai szuverenitás szorosan összefügg egymással, és a technológiai függőségekkel prioritásként kell foglalkozni. Az Uniónak **irányító szerepet kell vállalnia az új technológiák fejlesztésében és bevezetésében**, a Bizottságnak pedig **a képességek javításán** kell dolgoznia az olyan **stratégiai technológiák** terén, mint a mesterséges intelligencia, a kvantumtechnológia, a fejlett konnektivitás, a felhő- és a pereminformatika, valamint a dolgok internete[45] olyan jövőbeli kezdeményezések révén, mint az MI-kontinens cselekvési terv, a kvantumstratégia és más kezdeményezések[46]. A Bizottság továbbra is támogatni fogja a legújabb, nemzetközileg elfogadott **internetprotokollok** időben történő bevezetését, amelyek elengedhetetlenek a fokozott kiberbiztonsággal rendelkező, méretezhető és hatékony internet fenntartásához. További intézkedésekre van szükség a **rádióspektrummal kapcsolatos kihívások** – például a GNSS-spoofing (jelhamisítás), a zavarás, az ellátási lánc kockázataival és függőségeivel, például a kvantumérzékelési technológiák használatával és a rádiófrekvenciás megfigyelési kapacitás fejlesztésének feltárásával kapcsolatos kihívások – kezelése érdekében is.

A **posztkvantum-kriptográfiai** (PQC) megoldások bevezetése az új kvantumkorszakban kulcsfontosságú lesz az érzékeny kommunikáció és az inaktív adatok megóvása, valamint a digitális személyazonosság védelme szempontjából. A posztkvantum-kriptográfiára való átállás összehangolt végrehajtási ütemtervéről szóló 2024. évi ajánlás[47] alapján a Bizottság együttműködik a tagállamokkal ezen átállás előmozdítása érdekében. E tekintetben a tagállamoknak azonosítaniuk kell a kritikus szervezetek magas kockázatú eseteit, és a lehető leghamarabb, de legkésőbb 2030 végéig biztosítaniuk kell e magas kockázatú esetek kvantumbiztonságos titkosítását. A Bizottság emellett az **IRIS²**, az Unió biztonságos konnektivitási programja részeként a tagállamokkal és az Európai Űrügynökséggel (ESA) együtt a kvantum-kulcsszétosztáson (QKD) alapuló **európai kvantumkommunikációs infrastruktúra (EuroQCI)**[48] fejlesztésén és bevezetésén dolgozik. Mindkét kezdeményezés végső soron az adatok biztonságos továbbítását és az információk biztonságos tárolását teszi lehetővé a szervezetek számára.

A **kvantumtechnológiák** kulcsszerepet fognak játszani a biztonsági alkalmazásokban is: a **kvantumstratégia** részeként **ütemtervet** fognak kidolgozni a **biztonsági alkalmazásokban található kvantumszenzorokra** vonatkozóan. Hasonlóképpen, a Bizottság azon dolgozik, hogy kvantumbiztossá tegye szervezeti biztonsági szempontból kritikus rendszereit, köztük minősített informatikai rendszereit is.

Vállalkozásbarát kiberbiztonsági keret

[43] https://counter-ransomware.org/.
[44] Elérhető a No More Ransom projekten keresztül, https://www.nomoreransom.org/hu/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] pl. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, a Kvantum vezérprogramа Kvantum vezérprogram kezdőlapja | Kvantum vezérprogram, a 3C-hálózatok (COM(2024) 81 final) és a kábelbiztonságra vonatkozó uniós cselekvési terv (JOIN(2025) 9 final).
[47] Ajánlás a posztkvantum-kriptográfiára való átállás összehangolt végrehajtási ütemtervéről |Európa digitális jövőjének alakítása.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

A kiberbiztonsági jogszabály közelgő felülvizsgálata lehetőséget kínál az **uniós kiberbiztonsági jogszabályok egyszerűsítésére**, összhangban a versenyképességi iránytűvel. A Bizottság szorosan együtt fog működni a tagállamokkal a NIS 2 irányelvben, a kiberrezilienciáról szóló jogszabályban és a kiberszolidaritásról szóló jogszabályban meghatározott horizontális kiberbiztonsági keret gyors, koherens és vállalkozásbarát végrehajtásának biztosítása érdekében, előmozdítva az egyszerűséget és a koherenciát, valamint elkerülve az uniós és nemzeti jogszabályokban foglalt kiberbiztonsági szabályok széttöredezettségét vagy átfedéseit.

Az online szolgáltatásokhoz való biztonságos hozzáférés lehetővé tétele és a digitális biztonság EU-szerte történő megerősítése érdekében az **európai digitális személyazonossági keret** 2026 vége előtt valamennyi uniós polgár és lakos számára megbízható digitális személyiadat-tárcát kínál. A közeljövőbeli **európai üzleti tárca** elő fogja segíteni a vállalkozások és a közigazgatási szervek közötti biztonságos, határokon átnyúló interakciókat. Mindkettő előfeltétele az adatközpontú egységes piac biztonságos és hatékonyabb működésének, olyan eszközökkel, mint az egységes digitális kapu, az e-számlázás, az e-közbeszerzés és a digitális termékútlevél.

Online biztonság

Az európai emberek biztonságát és védelmét veszélyeztető és az EU demokratikus szféráját célzó legsúlyosabb hibrid fenyegetések némelyike online jelenik meg. E fenyegetések közé tartoznak a jogellenes tevékenységek és a jogellenes online tartalmak, a mesterségesen felerősített információmanipuláció, a megtévesztő információk és a külföldi információmanipuláció és beavatkozás.

A **digitális szolgáltatásokról szóló rendelet** szigorú végrehajtása rendkívül fontos egy olyan biztonságos és hozzáférhető online környezet biztosításához, amelyben a szereplők elszámoltathatóak, és amely a hibrid fenyegetésekkel szemben is reziliens. A digitális szolgáltatásokról szóló rendelet arra kötelezi az online óriásplatformokat és a nagyon népszerű online keresőprogramokat üzemeltető szolgáltatókat, hogy végezzenek kockázatértékelést, és vezessenek be kockázatcsökkentő intézkedéseket a szolgáltatásaik szerkezetéből, működéséből vagy használatából eredő rendszerszintű kockázatok tekintetében. E kockázatok közé tartozhatnak a civil párbeszédre és a választási folyamatokra, valamint a közbiztonságra gyakorolt negatív hatások, mint a rossz szándékú külföldi állami szereplők széles körű beavatkozása például a választási folyamatokba. Fontos a tagállamok illetékes hatóságainak képzése a jogellenes online tartalmak azonnali eltávolítására szolgáló jogi eszközök használatáról, különös tekintettel a nemi alapú online erőszakra. A digitális szolgáltatásokról szóló rendelet válságreagálási mechanizmust ír elő, amely akkor aktiválható, ha olyan rendkívüli körülmények merülnek fel, amelyek az Unióban vagy annak jelentős részében a közbiztonságot vagy a közegészséget érintő komoly fenyegetéshez vezethetnek. E mechanizmus kiegészítése érdekében a Bizottság és a digitális szolgáltatási koordinátorként kijelölt illetékes nemzeti hatóságok kidolgozták a **digitális szolgáltatásokról szóló rendelet biztonsági eseményekre való önkéntes reagálási keretét**. A digitális szolgáltatási koordinátorok lépéseket tettek a választások integritásának védelme érdekében is, például választási kerekasztal-beszélgetések és stressztesztek[49] szervezésével. A digitális szolgáltatásokról szóló rendelet a politikai reklámtevékenységről szóló rendelettel[50] együtt egyike a demokrácia és a demokratikus folyamatok integritásának védelméhez kapcsolódó

[49] A digitális szolgáltatásokról szóló rendelet választási eszköztára a digitális szolgáltatási koordinátorok számára 2025 https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Az Európai Parlament és a Tanács (EU) 2024/900 rendelete (2024. március 13.) a politikai reklámtevékenység átláthatóságáról és célzott folytatásáról (HL L 2024/900, 2024.3.20.).

számos elemnek, amelyek ki vannak téve annak, hogy ellenséges szereplők célpontjai legyenek, többek között digitális eszközök és a közösségi média révén.

A **külföldi információmanipuláció és beavatkozás** kezelésére szolgáló eszköztár végrehajtása szintén fontos elem, amely kulcsfontosságú uniós szintű támogatást nyújt. A digitális jártasság és a médiaműveltség, valamint a kritikus gondolkodás támogatása szintén központi szerepet játszik ezekben az erőfeszítésekben[51].

A migráció fegyverként való felhasználása elleni küzdelem

Oroszország Belarusz segítségével és határozott támogatásával szándékosan fegyverként használta fel a migrációt, és jogellenesen megkönnyítette az EU külső határai felé irányuló migrációs áramlatokat azzal a céllal, hogy destabilizálja társadalmainkat és aláássa az Európai Unió egységét. Ez nemcsak a tagállamok nemzetbiztonságát és szuverenitását veszélyezteti, hanem a schengeni térség biztonságát és integritását, valamint az Unió egészének biztonságát is. Az Európai Tanács a 2024. októberi következtetéseiben hangsúlyozta: nem engedhetjük meg, hogy Oroszország és Belarusz, vagy bármely más ország visszaéljen értékeinkkel – többek között a menedékjoggal –, valamint aláássa demokráciánkat.

Amint az a migráció fegyverként való felhasználásáról szóló 2024. évi bizottsági közleményben is szerepel, az Unió az erőteljes politikai támogatás mellett pénzügyi, operatív és diplomáciai intézkedéseket is hozott, beleértve a származási és tranzitországokkal való együttműködést is, hogy hatékonyan kezelje ezeket a fenyegetéseket[52]. Ez a válasz magában foglalja a Tanács által létrehozott új keret alkalmazását az olyan fellépésekben és politikákban részt vevő személyek és szervezetek – vagyoni eszközök befagyasztása és utazási tilalmak bevezetése révén történő – szankcionálására, mint például a migráció Oroszország általi fegyverként való felhasználása[53]. Az EU szükség esetén továbbra is alkalmazni fogja ezt a keretet, és támogatni fogja a tagállamokat e fenyegetés elleni küzdelemben.

Közlekedésbiztonság

A tengeri kikötők, repülőterek és szárazföldi infrastruktúra kulcsfontosságú be- és kilépési pontok. Alapvető szerepet játszanak az EU gazdaságában és társadalmában, és alapvető fontosságúak a katonai mobilitás szempontjából. Ezek a közlekedési csomópontok és eszközök azonban a külső fenyegetések és a bűnözői tevékenységek elsődleges célpontjai is. A közelmúltbeli események, többek között a légi teherszállítás biztonságának megsértése és a vasúti infrastruktúra elleni támadások rávilágítanak a súlyos kockázatokra. A **fuvarozók** egyszerre lehetnek a rosszindulatú szereplők célpontjai és eszközei. A meglévő uniós jogi eszközök javították a légi közlekedés védelmét[54], ugyanakkor a polgári repülés magas fenyegetettségi szintje szükségessé teszi az események előrejelzését és az érintett tagállamokkal való gyors konzultációt. A Bizottság együtt fog működni a tagállamokkal a légiközlekedés-védelem területén meglévő végrehajtási jogszabályoknak a **légi közlekedési eseményekre** vonatkozó minősített adatok megosztása céljából történő módosítása érdekében. Emellett a Bizottság **szabályozási intézkedéseket** fog fontolóra venni az olyan új fenyegetések kezelése érdekében, mint a **légi árufuvarozást érintő események**, valamint a légiközlekedés-védelmi előírások megerősítése érdekében. Ez magában foglalja a **légiközlekedés-védelmi jogszabályok (AVSEC)** megerősítését is annak érdekében, hogy lehetővé váljon az azonnali

[51] Digitális oktatási cselekvési terv (2021–2027) – Európai oktatási térség.
[52] COM (2024) 570 final.
[53] A Tanács (EU) 2024/2642 rendelete (2024. október 8.) az Oroszország destabilizáló tevékenységeire tekintettel hozott korlátozó intézkedésekről, ST/8744/2024/INIT (HL L, 2024/2642, 2024.10.9.).
[54] Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól (HL L 97., 2008.4.9., 72. o.).

reagálási intézkedések meghozatala az uniós repülőterek egyszeri védelmi ellenőrzési területének fenntartása mellett.

Az **Európai Kikötők Szövetségére** épülő, jövőbeni **európai kikötőstratégia** kidolgozása során a Bizottság meg fogja vizsgálni, hogy miként lehetne tovább erősíteni a tengeri védelemre vonatkozó jogszabályokat a felmerülő fenyegetések hatékony kezelése, a kikötők védelme és az uniós ellátási lánc biztonságának fokozása érdekében. E célból a Bizottság biztosítani fogja annak határozott végrehajtását, és a nemzeti gyakorlatok harmonizálásán és a kikötői biztonsági háttérellenőrzések megerősítésén fog dolgozni. A légi árufuvarozásra vonatkozóan létrehozott védelmi protokollok kidolgozása mellett a Bizottság együtt fog működni a tagállamokkal és a magánszektorral e jegyzőkönyveknek a tengeri szállítási láncok biztosítása érdekében történő kiterjesztése érdekében.

A javasolt uniós vámhatóság az EU-ba belépő, onnan kilépő és az EU-n áthaladó árukkal kapcsolatos **vámügyi információk** alapján elemezni és értékelni fogja a kockázatokat annak érdekében, hogy támogassa a tagállamokat a nemzetközi ellátási láncok rosszindulatú szereplők általi kihasználásának megelőzésében. Az EU tengeri védelmi stratégiájával[55] összhangban a készülő **európai óceánügyi paktum** kulcsszerepet fog játszani az EU körüli és azon kívüli tengeri medencék tengeri védelmének fokozásában, többek között a többcélú tengeri műveletek és gyakorlatok bővítésének ösztönzése révén.

Az ellátási láncok rezilienciája

Európának csökkentenie kell a harmadik országok technológiáira való támaszkodását, ami függőséghez és biztonsági kockázatokhoz vezethet. A Bizottság célja, hogy enyhítse az egyetlen külföldi beszállítóktól való függőséget, csökkentse ellátási láncaink magas kockázatú beszállítókkal kapcsolatos kockázatait, és biztosítsa a kritikus infrastruktúrát és az ipari kapacitást az EU területén, a **versenyképességi iránytűben**[56] és a **tisztaipar-megállapodásban**[57] meghatározottak szerint. A Bizottság elő fogja mozdítani a **belső biztonságot szolgáló iparpolitikát** azáltal, hogy az uniós iparágakkal a kulcsfontosságú ágazatokban (pl. közlekedési csomópontok, kritikus infrastruktúrák) együttműködve olyan biztonsági megoldásokat állít elő, mint a felderítő berendezések, a biometrikus technológiák és a drónok, amelyek beépített biztonsági jellemzőket tartalmaznak. Az **uniós közbeszerzési szabályok felülvizsgálata** során a Bizottság értékelni fogja, hogy a védelmi és biztonsági beszerzésekről szóló 2009. évi irányelvben[58] foglalt biztonsági megfontolások elegendőek-e a bűnüldöző és a kritikus szervezetek rezilienciájával kapcsolatos igények kielégítéséhez.

A Bizottság támogatni fogja a tagállamokat a **közvetlen külföldi befektetések átvilágításában** és a logisztikai központok berendezéseinek beszerzésében, biztosítva a kritikus infrastruktúra és technológia biztonságát.

A **belső piaci szükséghelyzetről és rezilienciáról szóló jogszabály (IMERA)** alkalmazásának megkezdését követően segíteni fogja az EU-t a kritikus ellátási láncokat, valamint az áruk, a szolgáltatások és a személyek szabad mozgását megzavaró válságok kezelésében. Lehetővé teszi a gyors válságkoordinációt, a válság szempontjából releváns áruk és szolgáltatások meghatározását, és eszköztárat biztosít azok rendelkezésre állásának biztosításához. Ezen túlmenően a Bizottság a tagállamokkal szoros együttműködésben javaslatot fog tenni egy, a

[55] JOIN (2023) 8 final.
[56] COM (2025) 30 final.
[57] COM (2025) 85 final.
[58] Az Európai Parlament és a Tanács 2009/81/EK irányelve a honvédelem és biztonság területén egyes építési beruházásra, árubeszerzésre és szolgáltatásnyújtásra irányuló, ajánlatkérő szervek vagy ajánlatkérők által odaítélt szerződések odaítélési eljárásainak összehangolásáról (HL L 216., 2009.8.20.).

szállítási és ellátási lánc védelmére vonatkozó, több ügynökség munkájára építő riasztási mechanizmus létrehozására, amely garantálja a fenyegetések előrejelzéséhez és leküzdéséhez szükséges releváns információk biztonságos és időben történő megosztását.

Emellett a kritikus fontosságú nyersanyagokról szóló jogszabály és a „nettó zéró" iparról szóló jogszabály végrehajtásával a fenntarthatósági, reziliencia- és európai preferenciakritériumok fokozott alkalmazása az uniós közbeszerzésben elő fogja mozdítani a vezető piacok fejlődését. A megerősített kereskedelmi kapcsolatok – például nyersanyag-partnerségek és a tiszta gazdaságot szolgáló kereskedelmi és beruházási partnerségek révén – hozzá fognak járulni az ellátási láncok diverzifikálásához.

A vegyi, biológiai, radiológiai és nukleáris fenyegetésekkel szembeni reziliencia és felkészültség

Oroszország Ukrajna elleni agressziós háborúja növelte a **vegyi, biológiai, radiológiai és nukleáris (CBRN) fenyegetések** kockázatát. A CBRN-anyagok esetleges beszerzésének és fegyverként való felhasználásának kezelése érdekében a Bizottság célzott képzések és gyakorlatok révén támogatni fogja a tagállamokat és a partnerországokat. A Bizottság emellett az új **CBRN-felkészültségi és -reagálási cselekvési terv** keretében fokozni fogja a CBRN-felkészültségi és -reagálási képességeket a fenyegetések rangsorolása, az ellenintézkedésekhez nyújtott innovációfinanszírozás, a rescEU-képességek és az egészségügyi ellenintézkedések felhalmozása révén. Az **egészségügyi ellenintézkedésekre vonatkozó uniós stratégia** támogatni fogja továbbá az egészségügyi ellenintézkedések kidolgozását a kutatástól a gyártásig és a forgalmazásig, hogy megvédje az EU-t a világjárványoktól és a CBRN-fenyegetésektől.

A Covid19-világjárvány tapasztalataira építve az EU megerősítette az uniós közegészség-védelmi keretet[59]. A Bizottság uniós népegészségügyi referencialaboratóriumokat jelöl ki az uniós és nemzeti felügyeleti és gyorsészlelési kapacitások megerősítése érdekében. Az egészségbiztonsággal kapcsolatos felkészültségre, megelőzésre és reagálásra vonatkozó uniós tervet 2025-ben teszik közzé.

Fő intézkedések

A Bizottság:

- **2025-ben értékeli és felülvizsgálja a kiberbiztonsági jogszabályt,**
- **a felhőszolgáltatások kiberbiztonsági szempontból biztonságos használatát biztosító intézkedéseket dolgoz ki,**
- **2025-ben javaslatot tesz egy európai kikötőstratégiára,**
- **2026-ban felülvizsgálja az uniós védelmi és biztonsági közbeszerzési szabályokat,**
- **2026-ban új CBRN-felkészültségi és -reagálási cselekvési tervet terjeszt elő,**

A Bizottság, a tagállamokkal együttműködve:

- **kidolgozza és kiépíti az európai kvantumkommunikációs infrastruktúrát (EuroQCI),**
- **biztosítja a digitális szolgáltatásokról szóló rendelet hatékony végrehajtását,**
- **fellép a migráció fegyverként való felhasználása ellen,**
- **létrehoz egy a légiközlekedés-védelmi eseményeket kezelő rendszert,**
- **a szállítási és ellátási lánc védelmére vonatkozó, több ügynökség munkájára építő riasztási mechanizmus létrehozásán fog dolgozni.**

[59] Különösen a határokon át terjedő súlyos egészségügyi veszélyekről szóló (EU) 2022/2371 rendelet révén.

A Bizottság sürgeti a Tanácsot, hogy:

- **fogadja el az uniós kiberbiztonsági tervről szóló tanácsi ajánlást.**

A Bizottság sürgeti a tagállamokat, hogy:

- **ültessék át és hajtsák végre teljeskörűen a CER- és NIS 2 irányelvet.**

5. A súlyos és szervezett bűnözés elleni háló szorosabbra fűzése

Segíteni fogjuk a szervezett bűnözés felszámolását azzal, hogy szigorúbb szabályokat javaslunk a szervezett bűnözési hálózatok elleni küzdelemre, többek között a nyomozásokra vonatkozóan, valamint azt, hogy az EU-ban élő fiatalok kevésbé legyenek kitéve a bűnözésbe való beszervezés veszélyének, és fokozzuk a bűnözés eszközeihez és a bűncselekményekből származó javakhoz való hozzáférés megakadályozására irányuló intézkedéseket.

A szervezett bűnözés kihasználja a változó környezetet, és exponenciálisan terjed. Kiaknázza a fejlett technológiákban rejlő lehetőségeket, több joghatóságon átívelően tevékenykedik, és szoros kapcsolatai vannak az EU határain túl is. Tekintettel ezekre az összetett, transznacionális fenyegetésekre, létfontosságú az uniós szintű koordináció és támogatás.

Bűnmegelőzés

A fiatalok szervezett bűnözésbe való beszervezése egyre nagyobb aggodalomra ad okot az EU-ban. A szervezett bűnözés elleni küzdelemhez a bűnözés **kiváltó okait** kell kezelni azáltal, hogy a társadalom egészére kiterjedő megközelítés révén oktatást és a bűnözéssel szemben alternatívát kínálunk. A Bizottság támogatni fogja a biztonsági megfontolásoknak az uniós oktatási, szociális, foglalkoztatási és regionális politikákba való beépítését. Az EU **elő fogja mozdítani a tényeken alapuló**, a helyi körülményekhez igazított **bűnmegelőzési politikákat**[60].

Az online szolgáltatások igénybe vevőinek, különösen a kiskorúaknak többek között a gyermekek szexuális bántalmazásával, az emberkereskedőkkel és a bűncselekmények vagy erőszakos szélsőségesség céljából történő online toborzással szembeni védelme érdekében a **digitális szolgáltatásokról szóló rendelet** szerinti intézkedések előírják a kiskorúak számára hozzáférhető online platformokat üzemeltető szolgáltatók számára, hogy kezeljék a kockázatokat, és lépjenek fel a jogellenes online tartalmakkal, többek között a gyűlöletbeszéddel szemben. A Bizottság a **kiskorúak védelméről szóló iránymutatások** kiadását tervezi, hogy segítse az online platformokat üzemeltető szolgáltatókat a magánélet védelme, a biztonság és a védettség magas szintjének a kiskorúak számára történő biztosításában az interneten. Az iránymutatások az Unióban működő valamennyi digitális szolgáltatásra vonatkozó ajánlásokat fognak tartalmazni a kiskorúak online védelmének fokozása érdekében. A Bizottság azt tervezi továbbá, hogy 2025-ben előmozdítja a **magánélet védelmét szolgáló uniós életkor-ellenőrzési** megoldást, hogy lefedje az EUDI személyiadat-tárca 2026 végi bevezetése előtti időszakot. A Bizottság emellett elő fog terjeszteni egy az internetes megfélemlítés elleni cselekvési tervet is.

A Bizottság továbbra is támogatni fogja az online platformokkal és más érintett szereplőkkel való, több érdekelt felet bevonó önkéntes együttműködést, többek között az uniós internetfórumon és a digitális szolgáltatásokról szóló rendelet szerinti célzott magatartási kódexeken, például a jogellenes online gyűlöletbeszéd felszámolására vonatkozó 2025. évi magatartási kódexen keresztül. A cél a figyelemfelkeltés, a jelenlegi és jövőbeni fenyegetésekre

[60] https://www.eucpn.org/.

való közös reagálás, valamint a mérséklési intézkedésekkel kapcsolatos bevált gyakorlatok kidolgozása és megosztása.

Helyi szinten a szervezett bűnözés hatása rávilágít arra, hogy regionális megoldásokra van szükség a kiszolgáltatottság és az illegális tevékenységek vonzerejének csökkentése érdekében. Az EU városfejlesztési menetrendje a városok biztonsági kihívásaival foglalkozik majd, az „Uniós városok a radikalizálódás ellen" kezdeményezésre építve. A Bizottság az Európai Regionális Fejlesztési Alapon keresztül támogatni fogja a tagállamokat a városi és regionális biztonság növelésében.

Az erősebb oktatási alapok és készségek megalapozzák a reziliens és összetartó társadalmakat. A **készségek uniója**, valamint az **az integrációról és a befogadásról szóló cselekvési terv** révén az Unió azon fog munkálkodni, hogy az emberek ellenállóbbá váljanak a félretájékoztatással és a dezinformációval, valamint a radikalizálódással és a bűnözésbe való beszervezéssel szemben.

A gyermekeknek az erőszak minden formájával – többek között a bűnözéssel, a fizikai vagy lelki bántalmazással, legyen akár online, akár offline – szembeni védelme alapvető uniós célkitűzés. A különösen veszélyeztetett csoportok – például a gyermekek, akik egyre inkább ki vannak téve a toborzásnak és a radikalizálódásnak, a gyermekcsábításnak és a gyermekek szexuális bántalmazásának, az internetes megfélemlítésnek, a dezinformációnak és más fenyegetéseknek – sajátos szükségleteinek kezelése érdekében az EU **cselekvési tervet** fog kidolgozni **a gyermekek bűnözés elleni védelméről**, amely egyaránt kiterjed az online és offline dimenzióra. A terv koherens és összehangolt megközelítést fog meghatározni, amely a rendelkezésre álló kereteken és eszközökön – többek között a gyermekek szexuális bántalmazásának megelőzésével és az ellene folytatott küzdelemmel foglalkozó jövőbeli uniós központon, valamint más uniós szerveken és ügynökségeken – alapul, és javaslatokat fog tenni abban az esetben, ha továbbra is hiányosságok állnak fenn.

A bűnözői hálózatok és támogatóik felszámolása

Fokozni kell a nagy kockázatot jelentő bűnözői hálózatok, a bűnszervezetek vezetői és a támogatók elleni küzdelmet. Bár a közelmúltban elért sikerek figyelemre méltóak[61], az elavult szabályok és a bűnözői hálózatok következetlen meghatározásai akadályozzák a hatékony büntető igazságszolgáltatási reagálást és a határokon átnyúló együttműködést. A Bizottság felül fogja vizsgálni az e területre vonatkozó elavult jogszabályokat, és a válaszintézkedések megerősítése érdekében javaslatot fog tenni a **szervezett bűnözésre vonatkozó jogi keret megújítására**.

A közigazgatási végrehajtás kiegészítheti a bűnüldözést, és gyorsabb eredményeket hozhat – amint azt az Európai Ügyészség és az Európai Csalás Elleni Hivatal (OLAF) a **határokon átnyúló csalások és az EU pénzügyi érdekeit sértő bűncselekmények kezelése** során bizonyította. A támogatásokkal visszaélő csalók olyan ágazatokra összpontosítanak, mint a megújuló energia, a kutatási programok és a mezőgazdasági ágazat[62]. A Bizottság meg fogja vizsgálni, hogy miként lehetne koordinálni a büntetőjogi és közigazgatási eszközök használatát, fokozva az együttműködést az Europollal, az Eurojusttal és az Európai Ügyészséggel. A Bizottság továbbra is támogatni fogja a **közigazgatási megközelítés** szélesebb körű

[61] Beleértve a közelmúltbeli EMPACT-ügyeket is.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

alkalmazását annak érdekében, hogy a helyi és egyéb közigazgatási hatóságok képesek legyenek megakadályozni a bűnözői hálózatok beszivárgását[63].

Az EU a **korrupció** elleni küzdelem jogi keretének megerősítésén dolgozik[64]. Az Európai Parlamentnek és a Tanácsnak mielőbb le kell zárnia a Bizottság által javasolt aktualizált korrupcióellenes keretről szóló tárgyalásokat. A Bizottság uniós korrupcióellenes stratégiát fog előterjeszteni az integritás előmozdítása, valamint az e területen működő valamennyi érintett hatóság és érdekelt fél közötti koordináció megerősítése érdekében.

A tűzfegyverek kulcsfontosságú szerepet játszanak a szervezett bűnözői csoportok által elkövetett erőszak fokozódásában. A Bizottság közös büntetőjogi normákat fog javasolni a tűzfegyverek tiltott kereskedelmére vonatkozóan. A **tűzfegyverek tiltott kereskedelmére vonatkozó új uniós cselekvési terv** a legális piac védelmére, a bűncselekményeknek a jobb hírszerzési információkon alapuló visszaszorítására, valamint a nemzetközi együttműködés megerősítésére fog összpontosítani, különös tekintettel Ukrajnára és a Nyugat-Balkánra.

A bűncselekményekben használt, illegálisan forgalmazott pirotechnikai termékek a megelőzés és a nyomonkövethetőség javítását célzó intézkedéseket tesznek szükségessé. A Bizottság jelenleg értékeli a pirotechnikai termékekről szóló irányelvet, és a **pirotechnikai termékek kereskedelmére vonatkozó büntetőjogi szankciókat** is mérlegelni fog.

A pénz útjának nyomon követése

A **pénz útjának nyomon követése** döntő fontosságú a szervezett bűnözés és a terrorizmus elleni küzdelemben, de továbbra is nagy kihívást jelent. A szervezett bűnözés és a pénzmozgások közötti kapcsolat intenzív és együttes erőfeszítéseket tesz szükségessé a bűnözői hálózatok finanszírozási forrásokhoz való hozzáférésének felszámolása, valamint az emberek, a vállalkozások és az állami költségvetések jobb védelme érdekében.

Az EU az új pénzmosás elleni szabályokkal – többek között az **Európai Unió Pénzmosás és Terrorizmusfinanszírozás Elleni Hatóságának (AMLA)**[65] létrehozásával – fokozta erőfeszítéseit. Az AMLA, az OLAF, az Európai Ügyészség, az Eurojust és az Europol közötti együttműködés elengedhetetlen a hatékony pénzügyi nyomozások végrehajtásához. A Bizottság támogatni fogja – mind az ügynökségek közötti együttműködést elősegítő, mind a magánszektort bevonó – **partnerségek** létrehozását.

A szervezett bűnözés mögött álló pénzügyi motivációk felszámolásához elengedhetetlen a vagyoni eszközök lefoglalása és a bűncselekményből származó haszon elkobzása. A **vagyonvisszaszerzésre és -elkobzásra** vonatkozóan nemrégiben elfogadott szigorúbb szabályokat[66] a tagállamoknak haladéktalanul át kell ültetniük, és teljes mértékben ki kell használniuk a bennük rejlő lehetőségeket. A pénzmosás elleni uniós keretet megkerülő párhuzamos pénzügyi rendszerek – köztük a kriptoalapú rendszerek – elleni küzdelemhez innovatív intézkedésekre, a bevált gyakorlatok tagállamok közötti megosztására, valamint az Europol és az Eurojust fokozott támogatására is szükség van. A Bizottság meg fogja vizsgálni egy új, az egész EU-ra kiterjedő rendszer megvalósíthatóságát a szervezett bűnözésből származó nyereség és a terrorizmus finanszírozásának nyomon követésére, valamint ösztönözni

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Javaslat – Az Európai Parlament és a Tanács irányelve a korrupció elleni küzdelemről, a 2003/568/IB tanácsi kerethatározat és az Európai Közösségek tisztviselőit és az Európai Unió tagállamainak tisztviselőit érintő korrupció elleni küzdelemről szóló egyezmény felváltásáról, valamint az (EU) 2017/1371 európai parlamenti és tanácsi irányelv módosításáról, COM(2023) 234 final, Brüsszel, 2023.5.3.

[65] https://www.amla.europa.eu/index_en.

[66] Az Európai Parlament és a Tanács (EU) 2024/1260 irányelve (2024. április 24.) a vagyonvisszaszerzésről és -elkobzásáról (HL L, 2024/1260, 2024.5.2.).

fogja a **pénzügyi információs egységektől** a bűnüldöző hatóságok felé történő időszerű és kibővített információáramlást. A Bizottság meg fogja vizsgálni, hogy miként lehetne bezárni a kiskapukat, támogatja a tagállamokat a kapacitásépítésben, és tovább fog dolgozni azon harmadik országokkal folytatott együttműködés megerősítésén, amelyeket a bűnözők rejtett banki műveletekre használnak fel.

A súlyos bűncselekmények elleni küzdelem

A bűnözői hálózatok felszámolása mellett a súlyos bűncselekmények elleni küzdelem célzott erőfeszítéseket igényel. Annak érdekében, hogy megerősítsük a nagyon jelentős pénzügyi károkat[67] okozó **online csalás** elleni küzdelemre való képességünket, a Bizottság támogatni fogja a megelőző intézkedéseket és a hatékonyabb bűnüldözési intézkedéseket, és együtt fog működni a tagállamokkal és az érdekelt felekkel az áldozatok támogatása és védelme érdekében, többek között azáltal, hogy segítséget nyújt pénzeszközeik visszaszerzéséhez. Ezeket az erőfeszítéseket az **online csalásról szóló cselekvési terv** fogja formalizálni.

A **gyermekek szexuális bántalmazása** elleni küzdelemre irányuló 2020–2025-ös uniós stratégiára[68] építve a Bizottság támogatni fogja a társjogalkotókat a gyermekek online szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre, valamint a gyermekek szexuális bántalmazása és kizsákmányolása elleni bűnüldözési intézkedések hatékonyabbá tételére irányuló két jogalkotási javaslat[69] véglegesítésében. Mivel 2026 áprilisáig ideiglenes szabályok vannak érvényben, alapvető fontosságú egy állandó jogi keret létrehozása, és a Bizottság arra ösztönzi a társjogalkotókat, hogy kezdjenek tárgyalásokat a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról szóló rendelettervezetről. Felkérjük továbbá a társjogalkotókat, hogy folytassák a tárgyalásokat a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekek szexuális bántalmazását ábrázoló anyagok elleni küzdelemről szóló irányelvről, amely szabályozási minimumokat fog megállapítani a bűncselekményi tényállások meghatározására és a szankciókra vonatkozóan a gyermekek szexuális kizsákmányolása területén.

Az EU legveszélyesebb bűnözői hálózatainak fele erőszakos **kábítószer-kereskedelemmel** foglalkozik. Bár az EU a közelmúltban – különösen az **Európai Unió Kábítószer-ügynöksége** megbízatásának kiterjesztésével – fokozta az e bűncselekmény elleni küzdelmet[70], további intézkedésekre van szükség. A Bizottság szorosan együtt fog működni a tagállamokkal annak érdekében, hogy javaslatot tegyen egy új, **kábítószer elleni uniós stratégiára**. Felül fogja vizsgálni továbbá a **kábítószer-prekurzorokra vonatkozó jogi keretet**, és javaslatot fog tenni a **kábítószer-kereskedelem elleni uniós cselekvési tervre** az útvonalak és az üzleti modellek felszámolása érdekében. Az **Európai Kikötők Szövetségének** a kikötővédelem megerősítésére irányuló **köz-magán társulását** kiterjesztik a kisebb és belvízi kikötőkre is, és biztosítják a tengeri védelmi szabályok érvényesítését. Felismerve a kábítószer-kereskedelem súlyos helyi hatásait, a Bizottság továbbra is támogatni fogja a kiegyensúlyozott, tényeken alapuló és multidiszciplináris kábítószer-ellenes politikát, amely felkészült a kábítószerek, különösen a szintetikus opioidok hirtelen beáramlására.

[67] A csalás elleni 2024. évi globális jelentés.
[68] COM (2020) 607 final.
[69] COM (2022) 209 final és COM (2024) 60 final.
[70] COM (2023) 641 final.

Az emberek kizsákmányolása elleni küzdelem érdekében az EU új szabályokat[71] fogadott el, és az **emberkereskedelem elleni küzdelemre vonatkozó megújított uniós stratégiát** (2026–2030) fog bevezetni, amely a megelőzéstől a büntetőeljárásig valamennyi szakaszra kiterjed, különös tekintettel az áldozatok támogatására uniós és nemzetközi szinten egyaránt.

A **migránsok csempészése** elleni küzdelem terén a Bizottság – kulcsfontosságú partnereivel közösen – vezető szerepet fog betölteni a migránscsempészés elleni új globális szövetségen keresztül, az Europollal, az Eurojusttal és a Frontexszel együttműködve, az online dimenzióra is kiterjedően. Az embercsempészet elleni küzdelemre vonatkozó bizottsági javaslatokat[72] haladéktalanul el kell fogadni és végre kell hajtani. Emellett a **fuvarozókra vonatkozó eszköztár**[73] elfogadását követően a Bizottság fokozta a külföldi hatóságok és üzemeltetők bevonását, és továbbra is együtt fog működni a légi közlekedési ágazattal és a polgári légiközlekedési szervezetekkel[74] annak érdekében, hogy felhívja a figyelmet a légi úton történő migránscsempészésre[75].

A **környezeti bűnözés** hosszú távon veszélyezteti a környezetet, a közegészséget és a gazdaságokat. A Bizottság támogatni fogja a tagállamokat a környezeti bűnözésről szóló irányelv[76] végrehajtásában, és támogatni fogja az operatív hálózatokat és intézkedéseket ezen a területen[77]. Alapvető fontosságú a határozott végrehajtás. Emellett az Európa Tanács nemrégiben elfogadott, a környezet büntetőjog általi védelméről szóló egyezménye[78] hozzá fog járulni a környezeti bűnözés elleni küzdelemre irányuló határozott és hasonló erőfeszítések biztosításához, mind Európában, mind azon kívül.

A büntető igazságszolgáltatás válaszintézkedései

A bűnözés és a terrorizmus mindenkit érinthet, ami elengedhetetlenné teszi a bűncselekmények **áldozatai** jogainak támogatását és védelmét a károk csökkentése, valamint az általános biztonság és a hatóságokba vetett bizalom növelése érdekében. Az áldozatok jogairól szóló irányelvre építve a Bizottság új, az **áldozatok jogairól szóló uniós stratégiát** fog bevezetni.

Az **uniós büntető igazságszolgáltatási rendszereknek** hatékony eszközökre van szükségük a felmerülő fenyegetések kezeléséhez. Ennek elérése érdekében a Bizottság elindította az **uniós büntető igazságszolgáltatás jövőjével foglalkozó magas szintű fórumot**. Ez a fórum a tagállamokat, az Európai Parlamentet, az uniós ügynökségeket és szerveket, valamint más érdekelt feleket tömörít. Célja annak megvitatása, hogy miként biztosítható, hogy büntető igazságszolgáltatási rendszereink hatékonyak, méltányosak és reziliensek maradjanak a változó

[71] (EU) 2024/1712 irányelv (2024. június 13.) az emberkereskedelem megelőzéséről és az ellene folytatott küzdelemről, valamint az áldozatok védelméről szóló 2011/36/EU irányelv módosításáról (HL L, 2024/1712, 2024.6.24.).

[72] COM (2023) 755 final és COM (2023) 754 final.

[73] A kereskedelmi szállítóeszközöknek az EU-ba irányuló illegális migráció megkönnyítésére történő használatának kezelésére szolgáló eszköztár.

[74] Beleértve a Nemzetközi Polgári Repülési Szervezetet (ICAO).

[75] A Bizottság támogatni fogja továbbá az emberkereskedelmet vagy migránscsempészést elősegítő vagy abban részt vevő fuvarozókkal szembeni intézkedésekről szóló rendelet véglegesítését, COM(2021) 753 final.

[76] Az Európai Parlament és a Tanács (EU) 2024/1203 irányelve (2024. április 11.) a környezet büntetőjog általi védelméről (HL L, 2024/1203, 2024.4.30.).

[77] A környezeti jog alkalmazására és végrehajtására létrehozott EU-hálózat (IMPEL), az Európai Környezetvédelmi Ügyészhálózat (ENPE), az EnviCrimeNet és a Bírák Európai Környezetvédelmi Fóruma (EUFJE).

[78] A környezet büntetőjog általi védelmével foglalkozó szakértői bizottság (PC-ENV) – a bűnügyi problémákkal foglalkozó európai bizottság.

kihívások közepette, miközben megerősítik az igazságügyi együttműködést és fokozzák a kölcsönös bizalmat, többek között a digitalizáció révén[79].

Fő intézkedések

A Bizottság:

- **2026-ban jogalkotási javaslatot terjeszt elő a szervezett bűnözésre vonatkozó szabályok korszerűsítésére vonatkozóan,**
- **2025-ben jogalkotási javaslatot terjeszt elő a kábítószer-prekurzorokra vonatkozó jogi keret felülvizsgálatára vonatkozóan,**
- **2025-ben jogalkotási javaslatot terjeszt elő a tűzfegyverek tiltott kereskedelmére irányuló közös büntetőjogi normákra vonatkozóan,**
- **értékeli, hogy szükség van-e a pirotechnikai termékekről és a polgári felhasználású robbanóanyagokról szóló irányelvek felülvizsgálatára,**
- **értékeli, hogy szükség van-e az európai nyomozási határozat és az európai elfogatóparancs további megerősítésére,**
- **2026-ban új uniós stratégiát terjeszt elő az emberkereskedelem elleni küzdelemre vonatkozóan,**
- **2026-ban előterjeszti az áldozatok jogairól szóló új uniós stratégiát,**
- **2027-ig előterjeszti a gyermekek bűnözés elleni védelméről szóló uniós cselekvési tervet,**
- **2025-ben előterjeszti a kábítószer-kereskedelem elleni uniós cselekvési tervet,**
- **2026-ban előterjeszti a tűzfegyverek tiltott kereskedelmére vonatkozó uniós cselekvési tervet,**
- **2025-től kezdődően fokozatosan bővíti az Európai Kikötők Szövetségét,**
- **2026-ban elfogadja a digitális szolgáltatásokról szóló rendelethez kapcsolódó, a kiskorúak védelmére vonatkozó iránymutatásokat,**
- **2026-ban előterjeszti az internetes megfélemlítés elleni uniós cselekvési tervet.**

A Bizottság sürgeti a tagállamokat, hogy:

- **2026 végéig teljeskörűen ültessék át a vagyonvisszaszerzésre és -elkobzásra vonatkozó új szabályokat, és teljes mértékben használják ki a bennük rejlő lehetőségeket,**
- **alkalmazzák az adminisztratív megközelítést a bűnözés beszivárgása elleni küzdelemben,**
- **hozzanak létre a pénzmosás elleni köz-magán társulásokat,**
- **ültessék át és hajtsák végre teljeskörűen a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről és azok megelőzéséről szóló irányelvet.**

A Bizottság sürgeti az Európai Parlamentet és a Tanácsot, hogy:

- **folytassák a tárgyalásokat a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról szóló rendeletről, valamint a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekek szexuális bántalmazását ábrázoló anyagok elleni küzdelemről szóló irányelvről,**
- **zárják le a korrupció elleni küzdelemről szóló irányelvről folytatott tárgyalásokat.**

[79] Nevezetesen az online adatcsere útján történő e-igazságügyi kommunikáció (eCODEX) és a Harmadik Országbeli Állampolgárok Európai Bűnügyi Nyilvántartási Információs Rendszerének (ECRIS-TCN) létrehozása révén.

6. A terrorizmus és az erőszakos szélsőségesség elleni küzdelem

Átfogó terrorizmusellenes programot fogunk bevezetni a radikalizálódás megelőzése, az online és nyilvános terek biztosítása, a finanszírozási csatornák felszámolása, valamint a támadásokra azok bekövetkeztekor történő reagálás érdekében.

A terrorfenyegetés szintje továbbra is magas az EU-ban. Ez szorosan összefügg a geopolitikai események tovagyűrűző hatásaival, az új technológiákkal és a terrorizmus finanszírozásának új eszközeivel. Biztosítanunk kell, hogy az EU megfelelően felkészüljön a fenyegetések előrejelzésére, (az offline, valamint az online) radikalizálódás megelőzésére, a polgárok és a nyilvános terek támadásoktól való megvédésére, valamint a támadásokra azok bekövetkeztekor történő hatékony reagálásra. 2025-ben előterjesztik a **terrorizmus és az erőszakos szélsőségesség megelőzésére és leküzdésére vonatkozó új uniós menetrendet**, amely meghatározza az EU jövőbeli fellépését. Az új menetrenddel összhangban az EU és a Nyugat-Balkán 2025-ben aláírja a terrorizmus és az erőszakos szélsőségesség megelőzéséről és leküzdéséről szóló új **közös cselekvési tervet**.

A radikalizálódás megelőzése és az emberek online védelme

A szervezett bűnözés elleni küzdelemhez hasonlóan a terrorizmus és az erőszakos szélsőségesség elleni küzdelem is a **kiváltó okok kezelésével** kezdődik. A **radikalizálódásmegelőzési uniós tudásközpont** egy új, **átfogó megelőzési eszköztárral** fogja fokozni a gyakorló szakembereknek és a politikai döntéshozóknak nyújtott támogatását, hogy lehetővé tegye a korai azonosítást és a kiszolgáltatott helyzetben lévő személyekre, különösen a kiskorúakra összpontosító beavatkozásokat. A radikalizálódásra gyakran a börtönökben kerül sor, és a Bizottság – annak érdekében, hogy támogassa a tagállamokat e probléma kezelésében – új ajánlásokat fog kiadni.

A terroristák és erőszakos szélsőségesek online platformokat használnak terrorista és káros tartalmak terjesztésére, pénzeszközök gyűjtésére és toborzásra. A kiszolgáltatott helyzetben lévő felhasználókat, különösen a kiskorúakat riasztó mértékben radikalizálják az interneten. Az **online terrorista tartalomról szóló rendelet** fontos szerepet játszott az online terrorista tartalmak terjedése elleni küzdelemben, lehetővé téve a legszörnyűbb és legveszélyesebb anyagok gyors eltávolítását[80]. A Bizottság jelenleg értékeli a rendelet működését, és fel fogja mérni, hogyan lehetne a legjobban megerősíteni ezt a keretet.

A terrortámadásokkal kapcsolatos közös és gyors bűnüldözési és technológiai iparági válaszlépésekre vonatkozó **uniós válságkezelési protokoll** módosításra kerül annak érdekében, hogy biztosítani lehessen a méretezhetőséget és a rugalmasságot a terrortámadások egyre növekvő online dimenziójára való reagálás érdekében. Az uniós internetfórum továbbra is a technológiai ágazattal való önkéntes együttműködés fő eszköze lesz a terrorista és káros online tartalmak elleni küzdelem érdekében. A Bizottság emellett olyan nemzetközi kezdeményezésekben is részt vesz, mint a Christchurch Call Foundation és a terrorizmus elleni globális fórum (GIFCT).

A terrorizmus finanszírozása elleni küzdelem

A terroristák közösségi finanszírozási kampányokkal, kriptoeszközökkel, neobankok vagy online fizetési platformok révén finanszírozzák tevékenységüket. A bűnüldöző szerveknek fel kell deríteniük és ki kell vizsgálniuk ezeket a pénzmozgásokat. Ehhez eszközökre és szakértelemre van szükség. A **terrorizmusellenes pénzügyi nyomozók hálózata (Counter-**

[80] 2024. december 31-ig 1 426 eltávolítási végzést adtak ki a terrorista tartalmak eltávolítására vagy az azokhoz való hozzáférés letiltására, amelyek nagy többsége dzsihadista terrorista tartalmakra, de azok mellett jobboldali terrorista tartalmakra is irányult.

terrorism Financial Investigators' Network) kulcsszerepet játszik ebben. A Bizottság meg fogja vizsgálni egy **új**, az EU-n belüli és a SEPA-tranzakciókra, a kriptoeszköz-átutalásokra, az online és az elektronikus fizetésekre kiterjedő, a **terrorizmusfinanszírozás nyomon követésére szolgáló uniós szintű rendszer** létrehozását, amely kiegészíti a terrorizmus finanszírozásának felderítését célzó programról (TFTP) szóló EU–USA megállapodást.

Az uniós költségvetést **meg kell védeni az olyan visszaélésektől, amelyek célja a radikális/szélsőséges nézetek előmozdítása** a tagállamokban. A felülvizsgált **költségvetési rendelet** immár az uniós finanszírozásból való kizárás egyik okaként tartalmazza a „megkülönböztetésre, gyűlöletre vagy erőszakra való felbujtás" miatti ítéletet. A Bizottság tovább fogja vizsgálni az eszköztár teljes körű kihasználásának legjobb módját, többek között a potenciális kedvezményezettek kiválasztásakor. Az uniós költségvetés védelme a nemzeti hatóságokkal, az uniós ügynökségekkel és szervekkel való szoros együttműködésen és információmegosztáson is múlik.

A támadásokkal szembeni védelem

A radikalizálódás megelőzésébe történő befektetéseken túl a polgárok védelmének fontos eleme a terroristák és bűnözők támadások elkövetéséhez szükséges eszközökhöz való hozzáférésének korlátozása. Fellépésre van szükség mind a terroristák által használt eszközökkel kapcsolatban, mind pedig a támadások kockázatának kitett célpontok védelme érdekében.

A tűzfegyverekkel kapcsolatos intézkedések mellett a Bizottság **felül fogja vizsgálni a robbanóanyag-prekurzorokra vonatkozó szabályokat** is, hogy azok a magas kockázatú vegyi anyagokra is kiterjedjenek. A terrortámadások leggyakoribb célpontjai továbbra is a **nyilvános terek**, különösen a magányos elkövetők esetében. A polgárok támadásokkal szembeni védelme érdekében meg kell erősíteni az **uniós védelmi biztonsági tanácsadói programot**, hogy a tagállamok kérésére és az uniós költségvetésből a Belső Biztonsági Alap keretében finanszírozva elvégezzék a nyilvános terek, a kritikus infrastruktúrák és a magas kockázatú események sebezhetőségi értékelését. Az EU törekedni fog arra, hogy bővítse a nyilvános terek védelmére rendelkezésre álló finanszírozást. A Bizottság célzott iránymutatások és eszközök – például a nyilvános terek védelmével foglalkozó tudásközpont[81] – révén támogatást nyújt a tagállami hatóságoknak és a magánszereplőknek, és 2020 óta 70 millió EUR-t bocsátott rendelkezésre a nyilvános terek védelmének támogatására.

A Bizottság olyan követelmények bevezetését is meg fogja vizsgálni, miszerint a szervezeteknek a nyilvánosan hozzáférhető helyszíneken biztonsági intézkedéseket kelljen mérlegelniük, illetve alkalmazniuk a helyi hatóságokkal és a magánpartnerekkel való együttműködés révén.

Tekintettel a nyilvánvaló sebezhetőségekre, az **antiszemitizmus elleni küzdelemre és a zsidó élet előmozdítására vonatkozó uniós stratégia (2021–2030)** továbbra is iránymutatásul szolgál a zsidó közösség védelmére irányuló bizottsági fellépésekhez. A Bizottság továbbá biztosítani fogja, hogy megfelelő eszközök álljanak rendelkezésre, amelyek támogatják a tagállamokat a **muszlimellenes gyűlölet** elleni küzdelemben.

A **drónok** kémkedésre és támadásokra való használata egyre nagyobb biztonsági kihívást jelent. A Bizottság ki fogja dolgozni a **drónelhárítási rendszerek harmonizált tesztelési**

[81] A nyilvános terek védelmével foglalkozó tudásközpont.

módszertanát, létrehozza a **drónelhárítási kiválósági központot**, és értékeli, hogy szükséges-e harmonizálni a tagállamok jogszabályait és eljárásait[82].

Külföldi terrorista harcosok

Az EU külső határaira visszatérő vagy ott belépő külföldi terrorista harcosok azonosításához szükség van a terrorista fenyegetést jelentő személyekre vonatkozó adatokra. E célból a Bizottság az Europollal együtt meg fogja erősíteni **együttműködését a kulcsfontosságú harmadik országokkal az olyan személyek** – köztük a külföldi terrorista harcosok – **életrajzi és biometrikus adatainak megszerzése** érdekében, akik terrorfenyegetést jelenthetnek, amelyeket azután az alkalmazandó uniós és nemzeti jogi keretekkel teljes összhangban be lehet illeszteni a Schengeni Információs Rendszerbe. Ezért alapvető fontosságú, hogy a tagállamok minden meglévő eszközt felhasználjanak. Ez magában foglalja az összes releváns információ bevitelét a **Schengeni Információs Rendszerbe**, a biometrikus ellenőrzések fokozását, valamint valamennyi személy kötelező szisztematikus ellenőrzését az EU külső határain[83]. Emellett a Frontex által kidolgozott **közös kockázati mutatók** továbbra is segíteni fogják a tagállamok határellenőrző hatóságait abban, hogy azonosítsák és értékeljék a potenciális külföldi terrorista harcosok gyanús utazásainak kockázatát.

Továbbá annak biztosítása érdekében, hogy a tagállamok továbbra is hozzáférjenek a Dáis/ISIL által elkövetett bűncselekményekkel kapcsolatos elszámoltathatóság előmozdítását célzó ENSZ-nyomozócsoport (UNITAD) által a külföldi terrorista harcosok büntetőeljárás alá vonása céljából gyűjtött **harctéri bizonyítékokhoz**, a Bizottság az Eurojusttal együtt értékelni fogja annak lehetőségét, hogy ezeket a bizonyítékokat az Eurojust legsúlyosabb nemzetközi bűncselekményekre vonatkozó bizonyítékok adatbázisában tárolják. Emellett az új európai **terrorizmusellenes igazságügyi nyilvántartás** továbbra is támogatni fogja a tagállamok igazságszolgáltatási szerveit a terrorizmussal kapcsolatos ügyekben a határokon átnyúló kapcsolatok gyors azonosításában.

Fő intézkedések

A Bizottság:

- **2025-ben elfogadja a terrorizmus és az erőszakos szélsőségesség megelőzésére és leküzdésére vonatkozó új uniós menetrendet,**
- **2025-ben aláírja a terrorizmus és az erőszakos szélsőségesség megelőzéséről és leküzdéséről szóló új közös cselekvési tervet a Nyugat-Balkánnal,**
- **új, átfogó megelőzési eszköztárat dolgoz ki az uniós tudásközpont segítségével,**
- **2026-ban értékeli az online terrorista tartalomról szóló rendelet alkalmazását,**
- **2025-ben módosítja az uniós válságkezelési protokollt,**
- **2026-ban jogalkotási javaslatot terjeszt elő a robbanóanyag-prekurzorok forgalomba hozataláról és felhasználásáról szóló rendeletre vonatkozóan,**
- **megvizsgálja a terrorizmus finanszírozásának nyomon követésére szolgáló új uniós rendszer megvalósíthatóságát.**

A Bizottság sürgeti a tagállamokat, hogy:

- **javítsák a biometrikus ellenőrzéseket és végezzenek kötelező szisztematikus ellenőrzéseket az EU külső határain,**

[82] A 2023. évi drónelhárítási közleményben (COM(2023) 659 final) foglalt kulcsfontosságú intézkedések nyomán.

[83] A Schengeni határellenőrzési kódexszel és az előszűrésről szóló rendelettel teljes összhangban.

- **teljeskörűen használják ki az európai terrorizmusellenes igazságügyi nyilvántartást.**

7. Az EU mint erős globális szereplő a biztonság terén

Az EU biztonságának javítása érdekében fokozni fogjuk az operatív együttműködést a kulcsfontosságú régiókkal, például a bővítési és szomszédsági partnereinkkel, Latin-Amerikával és a földközi-tengeri térséggel kialakított partnerségek révén. A nemzetközi együttműködés során figyelembe fogjuk venni az EU biztonsági érdekeit, többek között az uniós eszközök és intézkedések mozgósítása révén.

Az elmúlt évek megmutatták az EU külső és belső biztonsága közötti alapvető összefüggést. Az Ukrajna elleni orosz agressziós háború, a gázai konfliktus, a szíriai helyzet és a világszerte újonnan kialakuló konfliktusok súlyos tovagyűrűző hatást gyakoroltak az EU belső biztonságára. A globális instabilitás által a belső biztonságra gyakorolt hatás ellensúlyozása érdekében az **EU-nak aktívan meg kell védenie biztonsági érdekeit** azáltal, hogy kezeli a külső fenyegetéseket, felszámolja az emberkereskedelmi útvonalakat, és védi a stratégiai jelentőségű folyosókat, például a kereskedelmi útvonalakat. Ezzel egyidejűleg az EU továbbra is erős szövetségese lesz partnerországainak, és együtt fog működni a globális biztonság fokozása és a fenyegetésekkel szembeni kölcsönös reziliencia kiépítése érdekében.

Az elmúlt években az EU jelentős lépéseket tett a biztonsági együttműködés fokozása érdekében. Operatív bűnüldözési és igazságügyi együttműködési megállapodásokat, valamint más típusú megállapodásokat kötött partnerországaival. A Tanács tárgyalási irányelveivel összhangban aktívan törekszik további nemzetközi megállapodások megkötésére, valamint az uniós ügynökségek és szervek által támogatott kapacitásépítési kezdeményezések indítására. A Globális Európa – Szomszédsági, Fejlesztési és Nemzetközi Együttműködési Eszköz szintén kulcsfontosságú a partnerországok biztonságának megerősítésében.

A **szabályokon alapuló multilaterális rend** a globális biztonság megerősítésének sarokköve. A biztonsággal kapcsolatos párbeszédek, beleértve a tematikus párbeszédeket is, elengedhetetlenek ezen erőfeszítések megerősítéséhez. A **biztonság és a védelem területére vonatkozó stratégiai iránytű** végrehajtása, valamint a két- és többoldalú együttműködési keretek, például a stabilizációs és társulási megállapodások és a társulási megállapodások, valamint az olyan szervezetekkel folytatott együttműködések, mint az ENSZ és a NATO, kulcsfontosságúak a hatékony biztonsági megoldások kidolgozásához. Az EU továbbra is részt fog venni a többoldalú fórumokon[84], és fokozni fogja együttműködését az érintett nemzetközi és regionális szervezetekkel és keretekkel, többek között a NATO-val, az Egyesült Nemzetek Szervezetével, az Európa Tanáccsal, az Interpollal, a G7-ekkel, az EBESZ-szel és a civil társadalommal.

Regionális együttműködés

Politikai és geostratégiai szükségszerűség, hogy az EU továbbra is rendíthetetlenül támogassa **Ukrajnát**, és erősítse az **uniós bővítési országok** biztonságát és rezilienciáját. Az EU biztonsága támogatásának együtt kell járnia a **tagjelölt országoknak az EU biztonsági architektúrájába való gyorsított integrációjával**, a regionális együttműködésük megszilárdításával párhuzamosan. A Bizottság az EU bővítési politikáját arra fogja felhasználni, hogy támogassa az uniós tagjelölt és potenciális tagjelölt országok kapacitásait a fenyegetésekre való reagálás, az operatív együttműködés és az információcsere fokozása,

[84] A terrorizmus elleni küzdelem világfóruma, a Dáis elleni nemzetközi koalíció, a terrorizmus elleni globális fórum (GIFCT), a Christchurch Call Foundation, a szintetikus kábítószerek jelentette fenyegetések kezelésével foglalkozó nemzetközi koalíció.

valamint az uniós elvekkel, jogszabályokkal és eszközökkel való összhang biztosítása érdekében. Az Előcsatlakozási Támogatási Eszköz (IPA III), valamint Ukrajna, Moldova és a Nyugat-balkáni Reform- és Növekedéstámogató Eszköz kulcsfontosságúak a biztonság megerősítéséhez mind a tagjelölt, mind a potenciális tagjelölt országokban.

Az EU emellett folytatni fogja a **szomszédságpolitikai partnereknek** az EU biztonsági architektúrájába történő integrációját. Az **új földközi-tengeri paktum** és a **Fekete-tengerre vonatkozó**, küszöbön álló **stratégiai megközelítés** révén az Unió törekedni fog arra, hogy a biztonsággal kapcsolatos rendszeres magas szintű párbeszédek révén folytassa a regionális együttműködés és a kétoldalú átfogó stratégiai partnerségek kiépítését, adott esetben biztonsági dimenzióval. Meg kell erősíteni az Észak-Afrikával, a **Közel-Kelettel és a Perzsa-öböl térségével** folytatott operatív együttműködést, különösen a terrorizmus elleni küzdelem, a pénzmosás, a tűzfegyverek tiltott kereskedelme, valamint a kábítószer-előállítás és -kereskedelem – különösen a kaptagon – elleni küzdelem területén.

A terrorista és bűnözői tevékenységek térnyerésének, valamint annak a **szubszaharai Afrikára, nevezetesen a Szahel-övezetre, Afrika szarvára és Nyugat-Afrikára** gyakorolt lehetséges tovagyűrűző hatásainak kezelése érdekében az EU meg fogja erősíteni az Afrikai Uniónak, a regionális gazdasági közösségeknek és a régió országainak nyújtott támogatást. Az EU tengeri védelmi stratégiájával[85] összhangban az EU meg fogja erősíteni az együttműködést a **Guineai-öbölben, a Vörös-tengeren és az Indiai-óceánon** az illegális kereskedelem és a kalózkodás elleni küzdelem érdekében, támogatva az Afrikán belüli és a regionális együttműködést, valamint támogatva a tengeri jelenlétek koordinálásának uniós koncepcióját (CMP) és a tengeri elemző és műveleti központ kábítószerekkel foglalkozó részlegét (MAOC-N).

Latin-Amerikával és a Karib-térséggel az EU meg fogja erősíteni az operatív együttműködést a nagy kockázatot jelentő bűnözői hálózatok felszámolása és büntetőeljárás alá vonása, valamint a tiltott tevékenységek és kereskedelmi útvonalak felszámolása érdekében, megerősítve az olyan együttműködési kereteket, mint az EU-CLASI (Latin-amerikai Belső Biztonsági Bizottság) és az EU-CELAC kábítószerekkel kapcsolatos koordinációs és együttműködési mechanizmus. A prioritások között szerepelni fognak a logisztikai központok rezilienciája és partnerségei, valamint a pénzt útjának nyomon követésére vonatkozó elven alapuló megközelítések. Az EU továbbra is támogatni fogja az Amerika rendőrségei közösségének (AMERIPOL) fejlesztését, hogy az az Europol regionális megfelelőjévé váljon, és megerősítse a tagállamok és a régió közötti igazságügyi együttműködést. Az EU emellett együtt fog működni **Dél- és Közép-Ázsiával** a terrorizmussal, a tiltott áruk – többek között a kábítószerek – kereskedelmével, az emberkereskedelemmel és a migránscsempészéssel kapcsolatos közös biztonsági kihívások terén.

Emellett az EU támogatni fogja a harmadik országok regionális együttműködési kereteit annak érdekében, hogy további segítséget nyújtson számukra a tiltott kereskedelem forrásnál történő felszámolásához, összhangban a teljes bűnözői ellátási láncért való megosztott felelősség elvével. Ezen túlmenően az EU a **harmadik országok kikötőiben végzett közös ellenőrzések** koordinálása révén hozzá fog járulni a külföldi logisztikai csomópontok biztonságának megerősítéséhez.

Operatív együttműködés

A **Global Gateway** támogatni fogja a fenntartható és magas színvonalú infrastrukturális projekteket a digitális, az éghajlat- és az energia-, a közlekedési, az egészségügyi, az oktatási és a kutatási ágazatban. A Bizottság – adott esetben – biztonsági megfontolásokat is be fog

[85] JOIN (2023) 8 final.

építeni a Global Gateway jövőbeli beruházásaiba. Ez magában foglalja az EU és partnerországai stratégiai autonómiája szempontjából kritikus fontosságú kezdeményezéseket, például a biztonsági értékeléseket és kockázatcsökkentő intézkedéseket tartalmazó infrastrukturális projekteket.

A Bizottság további **megállapodásokat** fog kötni az EU és harmadik országok között az Europollal és az Eurojusttal, különösen a latin-amerikai országokkal **való együttműködésről**.

Emellett a nem uniós országok **EMPACT**-ban való proaktív részvétele az egyik leghatékonyabb eszköz az operatív együttműködés megerősítésére. Az EU továbbra is ösztönözni fogja a harmadik országok – különösen a Nyugat-Balkán, a keleti szomszédság, a szubszaharai Afrika, Észak-Afrika, a Közel-Kelet, Latin-Amerika és a Karib-térség országainak – bevonását a keretbe. A bűnözés elleni küzdelem terén a harmadik országokkal folytatott együttműködés fokozására szolgáló másik eszköz a tagállamok közötti és az Europol által koordinált operatív munkacsoportok, amelyekben harmadik országok is részt vehetnek. A Bizottság továbbá arra törekszik, hogy lezárja az **EU és az Interpol közötti** nemzetközi megállapodásra[86] irányuló tárgyalásokat, biztosítva a globális biztonsági fenyegetések egységesebb megközelítését és a transznacionális bűncselekmények elleni küzdelmet.

Az **Uniónak az „Európa együtt" megközelítés keretében jelen kell lennie a helyszínen**. Az Unió és a tagállamok szakmai személyzete döntő szerepet játszik annak biztosításában, hogy az Unió külső tevékenysége jól tájékozott, összehangolt és reagálóképes legyen. E megközelítés következő szintre emelése érdekében a Bizottság – a külügyi és biztonságpolitikai főképviselő támogatásával – megerősíti az **összekötő hálózatokat**, és a tagállamok operatív igényeivel összhangban megkönnyíti a regionális **Europol és Eurojust összekötő tisztviselők** kiküldését.

Az EU szorosabb operatív bűnüldözési és igazságügyi együttműködésre fog törekedni, elő fogja mozdítani a valós idejű információmegosztást és a közös műveleteket a harmadik országokban működő **közös nyomozócsoportokon** keresztül, az Europol és az Eurojust támogatásával. A Bizottság támogatni fogja a tagállamokat abban is, hogy **közös fúziós központokat** hozzanak létre, amelyek összefogják a szakértőket és a helyi bűnüldöző szerveket a stratégiai jelentőségű harmadik országokban.

Közös kül- és biztonságpolitikai (KKBP) eszközök

A **közös biztonság- és védelempolitikai (KBVP) missziókban** rejlő lehetőségeket szintén teljes mértékben ki fogják használni az EU belső biztonságát fenyegető külső fenyegetések jobb azonosítása és kezelése érdekében, a Tanács által meghatározott megbízatásukkal összhangban. A harmadik országok kapacitásainak kiépítése érdekében az Unió külügyi és biztonságpolitikai főképviselője és a Bizottság célzott finanszírozási eszközökkel fogja támogatni a KBVP-fellépéseket, és meg fogja vizsgálni az összes megfelelő finanszírozási lehetőséget.

Az **uniós korlátozó intézkedések** a KKBP jól bevált eszközei, amelyeket a terrorizmus elleni küzdelemben is alkalmaznak. A külügyi és biztonságpolitikai főképviselő, a tagállamok vagy a Bizottság javaslatai alapján a Tanács értékelhetné, hogy az EU meglévő autonóm korlátozó intézkedéseit (a terroristák uniós jegyzéke) hogyan lehetne hatékonyabbá, eredményesebbé, működőképesebbé és agilisabbá tenni. Ezen felül a KKBP célkitűzéseivel összhangban fontolóra vehetik a bűnözői hálózatokat célzó további korlátozó intézkedések feltárását.

Vízumpolitika és információcsere

Az EU vízumpolitikája kulcsfontosságú eszköz a harmadik országokkal való együttműködéshez és határaink biztosításához azáltal, hogy ellenőrzi az EU-ba való belépést és

[86] A Tanács (EU) 2021/1312 határozata (2021. július 19.) és a Tanács (EU) 2021/1313 határozata (2021. július 19.).

meghatározza annak feltételeit. A Bizottság a jövőbeni európai vízumpolitikai stratégia révén teljeskörűen beépíti a **biztonsági megfontolásokat az uniós vízumpolitikába**. A Bizottság együtt fog működni a társjogalkotókkal a vízummentesség-felfüggesztési mechanizmus felülvizsgálatára és észszerűsítésére irányuló javaslat elfogadása érdekében, különös tekintettel a vízummentességi rendszerrel való visszaélés konkrét eseteire[87]. A Bizottság arra ösztönzi a harmadik országokat, hogy osszák meg egymással a biztonsági kockázatot jelentő személyekről szóló információkat, amelyeket az uniós információs rendszerekbe és adatbázisokba visznek be.

A szakpolitikai koordináció és a felfelé irányuló erőfeszítések megvalósítása, valamint a hatékonyabb, gyorsabb és gördülékenyebb együttműködés lehetővé tétele érdekében a Bizottság azon fog munkálkodni, hogy **adatáramlási megállapodásokat** kössön, és feltárja, hogy az alapvető jogokkal és az adatvédelmi szabályokkal összhangban miként lehetne **javítani** a megbízható harmadik országokkal bűnüldözési és határigazgatási célokból folytatott **információcserét**.

Fő intézkedések

A Bizottság:

- **nemzetközi együttműködési megállapodásokat köt az EU és a kiemelt harmadik országok között az Europollal és az Eurojusttal való együttműködésről,**
- **ösztönzi a partnerországok EMPACT-ban való részvételét a szervezett bűnözés és a terrorizmus elleni küzdelem érdekében,**
- **támogatja az uniós ügynökségeket és szerveket a partnerországokkal való munkamegállapodások kialakításában és megerősítésében,**
- **még inkább figyelembe veszi a biztonsági megfontolásokat az uniós vízumpolitikában a készülő vízumstratégia révén,**
- **megerősíti a megbízható harmadik országokkal bűnüldözési és határigazgatási célokból folytatott információcserét.**

A Bizottság, a külügyi főképviselővel együttműködve:

- **teljeskörűen kihasználja a közös biztonság- és védelempolitika (KBVP) polgári misszióit,**
- **2027-ig közös ellenőrzéseket koordinál a harmadik országok kikötőiben.**

A Bizottság, a külügyi főképviselővel és a tagállamokkal együttműködve:

- **megerősíti az összekötő hálózatokat és az együttműködést az „Európa együtt” megközelítés keretében,**
- **2025-től kezdődően közös operatív csoportokat és fúziós központokat hoz létre harmadik országokban.**

A Bizottság sürgeti az Európai Parlamentet és a Tanácsot, hogy:

- **zárja le a vízummentesség-felfüggesztési mechanizmus felülvizsgálatáról szóló tárgyalásokat.**

[87] COM (2023) 642.

8. Következtetés

A bizonytalanság világában javítani kell az Unió képességét a biztonsági fenyegetések előrejelzésére, megelőzésére és az azokra való reagálásra.

Nem elég csak akkor reagálni a válságokra, amikor azok bekövetkeznek. Bővítenünk kell ismereteinket, hogy teljes képet kapjunk a változó fenyegetésekről, valamint annak biztosítása érdekében, hogy eszközeink és képességeink megfeleljenek a feladatnak.

Az e stratégiában részletezett átfogó intézkedéscsomag hozzá fog járulni ahhoz, hogy az Unió erősebbé váljon a világban: olyan Unióvá, amely képes előre jelezni, megtervezni és kezelni saját biztonsági szükségleteit, hatékonyan reagálni a belső biztonságát fenyegető veszélyekre, felelősségre vonni az elkövetőket, valamint megvédeni nyitott, szabad és virágzó társadalmait és demokráciáit.

Ehhez a belső biztonsággal kapcsolatos gondolkodásmódunk megváltoztatására van szükség. Azon fogunk dolgozni, hogy elősegítsük egy olyan új uniós biztonsági kultúra kialakulását, amelyben a biztonsági megfontolások minden jogszabályunkban, szakpolitikánkban és programunkban – a kezdetektől a végrehajtásig – szerepet kapnak, és amely révén a szakpolitikai területek közötti együttműködés lehetővé teszi számunkra, hogy úttörő szerepet játszhassunk.

Ez nem csupán egy intézmény, kormány vagy szereplő feladata. Ez egy közös európai vállalkozás.