Az Európai Unió
Tanácsa

Brüsszel, 2022. május 27.
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2022. május 25.
Címzett:	a Tanács Főtitkársága
Biz. dok. sz.:	COM(2022) 252 final
Tárgy:	A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK a biztonsági unióra vonatkozó stratégia végrehajtásáról szóló negyedik eredményjelentésről

Mellékelten továbbítjuk a delegációknak a COM(2022) 252 final számú dokumentumot.

Melléklet: COM(2022) 252 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.5.25.
COM(2022) 252 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

a biztonsági unióra vonatkozó stratégia végrehajtásáról szóló negyedik eredményjelentésről

I. BEVEZETÉS

Jelenleg Oroszország Ukrajna elleni agresszív háborúja határozza meg az EU biztonsági menetrendjét. A háború nem csupán Ukrajnát fenyegeti, célja az is, hogy visszavesse a globális stabilitást és biztonságot. Az EU-n belül ez számos kockázattal jár a polgárok biztonságára nézve. Az energia- és egyéb nyersanyagellátást illetően új bizonytalanságok merülnek fel, és kritikus infrastruktúrák is kibertámadások célpontjai lehetnek. Az EU belső biztonságát és védelmét a háborús övezetben vegyi, biológiai vagy radiológiai harcanyagok felhasználásával összefüggő esetleges támadások vagy balesetek veszélyeztetik. A háború elől menekülő milliók sebezhetőségét gyorsan kihasználja a szervezett bűnözés a leginkább veszélyben lévő nők és gyermekek kereskedelme révén.

Az EU továbbra is eltökélt és egységes ezekkel az új és potenciális fenyegetésekkel szemben. Bár a háború hatása eddig elsősorban Ukrajna területére korlátozódott, az EU a fenyegetettségi helyzet fokozott nyomon követésével megerősítette *az éberséget és a koordinációt*, és a *felkészültség* biztosítása érdekében a reziliencia növelésére törekszik.

A 2022. március 10–11-i versailles-i nyilatkozatban[1] Európai vezetői hangsúlyozták, hogy fel kell készülni a gyorsan kibontakozó kihívásokra, többek között azáltal, hogy „megvédjük magunkat az egyre növekvő mértékű hibrid hadviseléssel szemben, megerősítve kiberrezilienciánkat, megvédve infrastruktúránkat – különösen a kritikus infrastruktúránkat – és fellépve a dezinformáció ellen”.

A biztonsági unióra vonatkozó keret központi szerepet játszik a biztonság Unió-szerte történő garantálásában. A biztonsági unióra vonatkozó stratégiában[2] meghatározott négy stratégiai prioritás a jelenlegi geopolitikai helyzetben továbbra is közvetlenül releváns e feladat szempontjából: i. időtálló biztonsági környezet; ii. a változó fenyegetések kezelése; iii. az európaiak védelme a terrorizmussal és a szervezett bűnözéssel szemben; valamint iv. erős európai biztonsági ökoszisztéma. A háború rávilágított arra, hogy az EU-nak és tagállamainak teljes mértékben ki kell használniuk a biztonsági unióra vonatkozó stratégia keretében már rendelkezésre álló jogalkotási és szakpolitikai eszközöket, amelyek a tagállamoknak nyújtott uniós támogatás alapjául szolgálnak a szervezett bűnözéstől és a terrorizmustól a kiberbiztonságig és a hibrid fenyegetésekig terjedő kérdések vonatkozásában.

A bel- és igazságügy területén működő európai ügynökségek is fokozták erőfeszítéseiket válaszul az ukrajnai háborúra, és kulcsszerepet játszanak a fenyegetések értékelésében és az operatív válaszlépések támogatásában[3]. A schengeni térség operatív gyakorlatának és kormányzásának folyamatos megerősítése szintén fontos tényező.

A biztonsági unióra vonatkozó stratégia végrehajtásáról szóló negyedik eredményjelentés az Oroszország Ukrajna elleni agresszív háborújának elindítása óta az elmúlt néhány hónapban bekövetkezett fejleményekre összpontosít. Áttekintést nyújt a biztonsági unió valamennyi területén hozott intézkedésekről, és figyelembe veszi az Ukrajnában zajló háborúból eredő potenciális biztonsági fenyegetések miatt jelentkező, felkészültséggel kapcsolatos

[1] https://www.consilium.europa.eu/media/54794/20220311-versailles-declaration-hu.pdf
[2] COM(2020) 605.
[3] Az EU bel- és igazságügyi ügynökségeinek közös jelentése Ukrajnáról | Az Európai Unió Menekültügyi Ügynöksége (europa.eu).

szükségleteket. A biztonsági unióval kapcsolatos egyéb ügyekben elért eredmények a mellékletben találhatók.

II. KIBERBIZTONSÁG ÉS KRITIKUS INFRASTRUKTÚRA

A háború kitörése óta magánszereplők és bűnszervezetek is közölték a nyilvánossággal, hogy kibertevékenységeket folytatnak az egyik vagy a másik fél támogatása érdekében. A hacktivizmus[4] veszélyt jelent az EU-ban a kritikus szolgáltatásokra a továbbgyűrűző hatások kockázata miatt, illetve a hivatalos hálózatokból jövő támadások vagy más, előre nem látható továbbgyűrűző hatások kockázata miatt. Bár a háború eddig nagyrészt hagyományos eszközökkel zajlott, és csak korlátozott mértékű továbbgyűrűző hatásokkal járt, az eszkalálódás valós veszélyt jelent ezen a területen.

Ezért az EU fokozta koordinációját és felkészültségét. A háborúból eredő fenyegetések rávilágítanak arra, hogy ki kell alakítani az információk és a szakértelem megosztásának kultúráját az EU, a tagállamok és a kiberbiztonsági közösségek között. Ez magában foglalja az uniós intézmények, szervek és ügynökségek, valamint a tagállamok közös, integrált helyzetismeretének kialakítását, különösen azon kritikus infrastruktúrák tekintetében, amelyektől a belső piac zavartalan működése függ.

Az Ukrajna elleni kibertámadások felróhatósága

Az Ukrajna elleni kibertámadások már az orosz agresszió előtt kezdődtek, és a háború első napjaiban[5] arra irányultak, hogy ellehetetlenítsék az ukrán katonai személyzet felhasználói fiókjait, és megzavarják az alapvető szolgáltatásokat, többek között a határellenőrzést és a telekommunikációt.

2022. január 14-én a főképviselő nyilatkozatot[6] tett az Európai Unió nevében, amelyben elítélte az Ukrajna elleni kibertámadásokat, és újólag megerősítette, hogy az EU egyértelműen támogatja Ukrajnát.

Május 10-én az Európai Unió és tagállamai nemzetközi partnereikkel együtt határozottan elítélték[7] az Ukrajna ellen irányuló február 24-i, rossz szándékú kibertevékenységet, amellyel

[4] Egy közelmúltbeli példa a hacktivizmusra az úgynevezett „protestware” használata rosszindulatú szoftverek orosz IP-címekre való terjesztésére egy népszerű nyílt forráskódú csomag révén, ami az ellátási láncot érintő kockázatokhoz és a nyílt forráskódú közösségbe vetett bizalom elvesztéséhez vezethet. A Bizottság egyértelművé tette, hogy az Oroszország elleni kibertámadások jogellenesek (akkor is, ha azok jó szándékúak).

[5] A Microsoft különjelentése: Oroszország Ukrajnában folytatott kibertámadási tevékenységének áttekintése; Az ukrajnai hibrid háború – A Microsoft véleménye a problémákról.

[6] https://www.consilium.europa.eu/hu/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/

[7] Ukrajna ellen irányuló orosz kiberműveletek: a főképviselőnek az Európai Unió nevében tett nyilatkozata – az Európai Unió Tanácsa (europa.eu).

az Oroszországi Föderáció a Viasat által üzemeltetett KA-SAT műholdas hálózatot vette célba. A kibertámadás súlyos hatással járt, és válogatás nélkül zavarokat és fennakadásokat okozott a kommunikációs csatornákban több ukrajnai hatóságnál, vállalkozásnál és felhasználónál, valamint több uniós tagállamot is érintett.

Éberség és koordináció

Oroszország Ukrajna elleni agresszív háborújának elindítása óta fokozott figyelemmel kísérik a kiberbiztonsági helyzet alakulását a tagállamokban és az uniós intézményekben. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), az Europol Kiberbűnözés Elleni Európai Központja és az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU), valamint az Európai Unió Helyzetelemző Központja (EU INTCEN) mind hozzájárulnak az EU közös helyzetismeretéhez, többek között azáltal, hogy biztosítják a gyanús kibertevékenységek folyamatos felügyeletét, különösen bizonyos ágazatokban, így például az energia, a közlekedés és a légi közlekedés területén, és értékeléseket készítenek, hogy iránymutatást nyújtsanak a megelőző fellépéshez.

Fokozódott a koordináció és az információcsere a kiberbiztonsági hálózatokkal is, köztük az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatával (EU-CyCLONe), amely magában foglalja a nemzeti kiberbiztonsági ügynökségeket, a Bizottságot és az ENISA-t. E megközelítésnek az uniós intézményeken belüli tükrözése érdekében a kiberválsággal foglalkozó munkacsoport – ami egy koordinációs mechanizmus – lehetővé teszi az információk megosztását valamennyi érintett szolgálat, szerv és ügynökség – köztük az ENISA, az Europol Kiberbűnözés Elleni Európai Központja és a CERT EU – között. Folyamatos erőfeszítésekre van szükség a politikai, operatív és technikai szintek közötti kommunikációs csatornák biztosítása, valamint a számítógép-biztonsági eseményekre reagáló csoportok hálózatával (CSIRT-ek hálózata) való együttműködés fokozása érdekében.

Az Europol életbe léptette továbbá az uniós bűnüldözési vészhelyzet-elhárítási protokollt, amely lehetővé teszi a kiberfenyegetések fokozott figyelését és az információk megosztását az érdekelt felek széles körében, hogy átfogó képet lehessen alkotni a kiberhírszerzésről.

A kiberfenyegetéseken túl a tagállamok, az EKSZ és a Bizottság szolgálatai fokozott éberséget tanúsítanak a kritikus infrastruktúrák nem informatikai jellegű, fizikai fenyegetéseknek való kitettsége tekintetében. A kritikus infrastruktúrák és az azokat üzemeltető szervezetek az EU-val szembeni esetleges megtorló intézkedések részeként fizikai kockázatoknak, például az állam vagy az állami dolgozók általi szabotázsnak lehetnek kitéve.

Felkészültség

Most minden eddiginél fontosabb a felkészültség a kiberbiztonság és a kritikus infrastruktúrák biztonsága terén, tekintve Európa fokozott mértékű kitettségét számos veszélynek a háború miatt. A felkészültség fokozására irányuló erőfeszítések számos közvetlen fellépést is magukban foglaltak, köztük olyanokat is, amelyeket már az Ukrajna elleni orosz agresszió előtt előirányoztak. Ezek között szerepelnek gyakorlatok, iránymutatás, jogalkotási intézkedések, a reziliencia növelése a kritikus ágazatokban, valamint a partnerekkel folytatott munka.

Az Európai Unió Tanácsának francia elnöksége az Európai Külügyi Szolgálattal (EKSZ) és az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) közösen 2022 elején EU CyCLES (Cyber Crisis Linking Exercise on Solidarity) címmel forgatókönyv-alapú gyakorlatot szervezett a politikai szintű tájékozottság megteremtése, valamint az operatív és a politikai szintek közötti együttműködés megerősítése érdekében, nagy horderejű kibertámadás esetére.

Az ENISA és a CERT-EU februárban **iránymutatásokat** tett közzé arról, hogy hogyan fokozható az EU rezilienciája és felkészültsége[8]. Ezek arra ösztönzik az EU-ban működő valamennyi köz- és magánszektorbeli szervezetet, hogy a kiberbiztonsági kultúra jelentős mértékű javítása érdekében fogadják el a kiberbiztonsággal kapcsolatos legjobb gyakorlatok minimális körét. Márciusban a CERT-EU nyomonkövetési technikai iránymutatást tett közzé az ENISA támogatásával[9], továbbá biztonsági iránymutatást a Signal alkalmazás konfigurációjának megerősítéséhez[10], amely számos gyakorlati ajánlást tartalmaz a szervezetek számára kiberbiztonsági helyzetük javítására vonatkozóan.

Jogalkotási kezdeményezések

A jelenlegi helyzet rávilágít arra, hogy sürgősen **végre kell hajtani a meglévő jogszabályokat**, és fel kell gyorsítani **a függőben lévő kezdeményezések elfogadását**.

A Bizottság támogatja a tagállamokat a **kiberbiztonsági irányelv** (NIS-irányelv)[11] végrehajtásában, amely előírja a tagállamok számára, hogy rendelkezzenek a szükséges képességekkel, például egy számítógép-biztonsági eseményekre reagáló csoporttal (CSIRT), és jelöljenek ki illetékes hatóságokat. Alapot biztosít továbbá a tagállamok közötti hatékony együttműködéshez. A társjogalkotók által a **NIS 2 irányelvvel**[12] kapcsolatban elért politikai megállapodás további áttörést jelent a szilárd uniós felkészültségi keret biztosítása terén.

NIS 2 irányelv – a felkészültség további megerősítése

- A hálózati és információs rendszerekről szóló új irányelv orvosolni fogja a korábbi kiberbiztonsági irányelv hiányosságait, hogy hozzáigazítsa azt a jelenlegi igényekhez, és időtállóvá tegye. Minimumszabályokat állapít meg a szabályozási keretre vonatkozóan, és meghatározza az egyes tagállamok megfelelő hatóságai közötti hatékony együttműködést szolgáló mechanizmusokat.
- Kiterjeszti a szabályok alkalmazási körét új, a gazdaság és a társadalom számára kritikus fontosságú ágazatokra (például a gyógyszerek és orvostechnikai eszközök ágazatára vagy az élelmiszeriparra). Az irányelv hatálya alá kerül minden közepes és nagy méretű szervezet, amely azokban az ágazatokban működik, vagy olyan szolgáltatásokat nyújt, amelyekre az irányelv kiterjed. A hatály kiterjed a központi kormányzatok közigazgatási szervezeteire (kivéve az igazságszolgáltatást, a parlamenteket és a központi bankokat) és a regionális szintű közigazgatási szervekre is. Ezen túlmenően a tagállamok dönthetnek

[8] Boosting your Organisation's Cyber Resilience (Hogyan növelheti szervezete kiberrezilienciáját) – Közös kiadvány, 2022.02.14.

[9] Security Guidance 2022-01 – Cybersecurity mitigation measures against critical threats (Biztonsági iránymutatás 2022-01 – Kiberbiztonsági kockázatcsökkentő intézkedések a kritikus fenyegetésekkel szemben).

[10] CERT-EU Biztonsági iránymutatás 22-002 – A Signal alkalmazás megerősítése.

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

[12] COM(2020) 823.

úgy, hogy az irányelvet helyi szinten is alkalmazzák az ilyen szervezetekre.

- A NIS 2 irányelv a kiberbiztonsági kockázatkezelési intézkedések alapját képezi, és hivatalosan létrehozza az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe), amely támogatást nyújt a nagy horderejű kiberbiztonsági események összehangolt kezeléséhez.
- A javaslat emellett pontosabb rendelkezéseket vezet be az események bejelentésének folyamatára, a bejelentések tartalmára és a határidőkre vonatkozóan, valamint rendelkezik a végrehajtást biztosító jogorvoslatokról és szankciókról.
- A tagállamoknak az irányelv hatálybalépésétől számítva 21 hónap áll rendelkezésükre, hogy a rendelkezéseket beépítsék a nemzeti jogukba.

A NIS 2 irányelv terén elért eredményeket követően a lehető leghamarabb le kell zárni **a kritikus fontosságú szervezetek rezilienciájáról szóló irányelvjavaslattal**[13] kapcsolatos tárgyalásokat, amely irányelv – miután sor került annak elfogadására és végrehajtására – várhatóan növelni fogja a kritikus fontosságú szervezetek rezilienciáját számos fenyegetéssel – többek között a terrortámadásokkal, belső fenyegetésekkel vagy szabotázzsal – szemben. Alapvető fontosságú továbbá, hogy a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv célkitűzéseinek szintje megfeleljen a bizottsági javaslatban meghatározott szintnek, és hogy továbbra is fennmaradjon az összhang a NIS 2 irányelv kapcsán kötött politikai kompromisszummal. Mindezek az intézkedések együttesen fokozzák a rezilienciát és a felkészültséget azáltal, hogy koherensebb és szilárdabb rendszert hoznak létre, többek között a biztonsági eseményekre és válságokra való nemzeti reagálási tervek révén. Ezek részét képezték a **közös kiberbiztonsági egység** létrehozásáról szóló tavalyi bizottsági ajánlásnak[14] is, amely meghatározta, hogy a kiberbiztonsági ökoszisztéma különböző szereplőinek (diplomáciai, rendőrségi, polgári és adott esetben védelmi szereplők) hogyan kell együttműködniük operatív szinten. A jelenlegi fenyegetettségi helyzet rávilágít a kulcsszereplők közötti hatékony együttműködés értékére.

A Bizottság továbbra is nyomon követi az **5G-hálózat** kiberbiztonsági eszköztárának végrehajtását[15]. Ezzel összefüggésben a Kiberbiztonsági Együttműködési Csoport május 11-én jelentést fogadott el az Open RAN biztonságáról[16]. Emellett továbbra is együttműködik a tagállamokkal annak érdekében, hogy az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont teljes mértékben működőképessé váljon.

A Bizottság 2022. március 22-én javaslatot tett **az uniós intézmények, szervek, hivatalok és ügynökségek egységes kiberbiztonságát és információbiztonságát biztosító intézkedések meghatározására irányuló új szabályokra.** Ezek a szabályok javítják az uniós közigazgatás rezilienciáját, valamint a kiberfenyegetésekre és -eseményekre való reagálási képességét. E tevékenységek közös keretbe helyezésével erősödik az intézményközi együttműködés, és minimálisra csökken a kockázatoknak való kitettség. A javasolt, **uniós intézmények, szervek, hivatalok és ügynökségek kiberbiztonságáról szóló rendelet**[17] megerősíti a CERT-EU megbízatását, és egy új intézményközi kiberbiztonsági testület létrehozását

[13] COM(2020) 829.
[14] Ajánlás a közös kiberbiztonsági egység létrehozásáról | Európa digitális jövőjének megtervezése (europa.eu).
[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[16] Kiberbiztonsági Együttműködési Csoport, Jelentés az Open RAN kiberbiztonságáról, 2022. május 11.
[17] COM(2022) 122.

eredményezi, fokozza a kiberbiztonsági képességeket, továbbá ösztönzi a rendszeres érettségi értékeléseket és a jobb kiberhigiéniát. A javasolt **információbiztonsági rendelet**[18] minimális információbiztonsági szabályokat és előírásokat határoz meg az összes uniós intézmény, szerv, hivatal és ügynökség információinak biztonságos kezelésére és cseréjére vonatkozóan az információikat fenyegető, folyamatosan változó fenyegetésekkel szembeni fokozott és következetes védelem biztosítása érdekében. A Bizottság felkéri az Európai Parlamentet és a Tanácsot, hogy minél előbb fogadják el ezeket az intézkedéseket.

A Bizottság mostanra befejezte a digitális termékek **kiberrezilienciáját** fokozó intézkedésekről szóló nyilvános konzultációját, és javaslatot készít, amelynek közzétételére idén ősszel kerül majd sor[19]. Ebben foglalkozik a digitális termékek és a kiegészítő szolgáltatások sebezhetőségével, amelyek – bár lehetőségeket teremtenek az uniós gazdaságok és társadalmak számára – új kihívásokhoz is vezetnek, hiszen minél inkább összefügg minden mindennel, egy kiberbiztonsági esemény annál könnyebben érinti az egész rendszert, ezáltal pedig zavart okoz a gazdasági és társadalmi tevékenységekben.

2022. március 9-én a telekommunikációért felelős uniós miniszterek egyhangúlag elfogadták az EU kiberbiztonsági képességeinek megerősítésére irányuló nevers-i felhívást, amely tartalmazza „a Bizottság által létrehozandó új kiberbiztonsági szükséghelyzeti válaszalap létrehozását”[20]. A Bizottság mérlegeli a meglévő források legjobb felhasználását a megelőző és válaszintézkedések támogatása érdekében.

Kritikus fontosságú ágazatok

Az EU **energiaellátásának** biztonsága kritikus fontosságú a polgárok jólléte és gazdaságaink zavartalan működése szempontjából, és a jelenlegi helyzet rávilágított arra, hogy ebben az ágazatban egyértelmű kiberbiztonsági szabályokra van szükség. A Bizottság jelenleg dolgozik a villamos energiáról szóló rendeletben[21] előírt, a határokon átnyúló villamosenergia-áramlás kiberbiztonságára vonatkozó üzemi és kereskedelmi szabályzaton, hogy szabályokat állapítson meg a kockázatértékelésekre, a közös minimumkövetelményekre, a tervezésre, a nyomon követésre, a jelentéstételre és a válságkezelésre vonatkozóan. Oroszország Ukrajna elleni agresszív háborújának elindítása óta a kiberbiztonsági üzemi és kereskedelmi szabályzat célkitűzései még nagyobb jelentőséggel bírnak. A Bizottság emellett strukturális együttműködést indított az ENISA, a villamosenergia-piaci ENTSO[22], a földgázpiaci ENTSO[23] és az Energiaközösség között az energiaágazat kiberbiztonsági helyzetének folyamatos felügyelete terén.

Az EU arra törekszik, hogy megvédje partnerei biztonságát anélkül, hogy saját magát új kockázatoknak tenné ki. 2022 márciusában, kockázatcsökkentő intézkedések elfogadását

---

[18] COM(2022) 119.

[19] A kiberrezilienciáról szóló jogszabály – a digitális termékekre és a kiegészítő szolgáltatásokra vonatkozó új kiberbiztonsági szabályok (europa.eu).

[20] 08/03/2022 - Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances (economie.gouv.fr).

[21] Az Európai Parlament és a Tanács (EU) 2019/943 rendelete (2019. június 5.) a villamos energia belső piacáról (HL L 158., 2019.6.14., 54. o.). Az Energiaszabályozók Együttműködési Ügynöksége jelenleg vizsgál egy javaslatot.

[22] Villamosenergia-piaci Átvitelirendszer-üzemeltetők Európai Hálózata.

[23] Földgázpiaci Szállításirendszer-üzemeltetők Európai Hálózata.

követően sor került Ukrajna és Moldova villamosenergia-hálózatainak a kontinentális európai hálózattal való vészhelyzeti szinkronizálására, elsősorban a kiberbiztonság tekintetében.

A háború és a szankciók számos kihívást jelentenek az uniós **közlekedés** számára is, az uniós polgári légi közlekedést érintő biztonsági kockázatoktól és a konfliktusövezetekben ragadt kamionsofőröktől kezdve az ukrán közlekedési infrastruktúra megsemmisüléséig, az ellátási láncok elvágásáig és a globális élelmezésbiztonság veszélyeztetéséig. Az Európai Unió Repülésbiztonsági Ügynöksége – szoros együttműködésben a Bizottsággal és az Eurocontrollal (Európai Szervezet a Légi Közlekedés Biztonságáért) – a háború kezdete óta azt tanácsolja az üzemeltetőknek, hogy ne használják Ukrajna légterét, és kerüljék a légtér használatát Belarusz Oroszországgal és Ukrajnával való határától 100 tengeri mérföldön belül.

A Bizottság továbbá azon dolgozik, hogy megerősítse az uniós közlekedési ágazat felkészültségét és rezilienciáját. A május 23-án elfogadott új közlekedési vészhelyzeti terv[24] tanulságokat von le a Covid19-világjárványból és az Ukrajna elleni orosz katonai agresszióból egyaránt. 10 intézkedésből álló eszköztárat javasol, amely iránymutatást nyújt az EU-nak és tagállamainak a vészhelyzeti válságreagálási intézkedések bevezetése során, ideértve a minimális konnektivitás biztosítását, a kiber- és hibrid fenyegetésekkel szembeni reziliencia megteremtését, valamint a nemzetközi partnerekkel a válsághelyzetekre való felkészültség és reagálás terén folytatott együttműködés fokozását. Kiemeli továbbá a reziliencia rendszeres tesztelésének fontosságát a különböző válságforgatókönyvek tekintetében, összefogva az érintett uniós ügynökségeket és más szereplőket, és a meglévő folyamatokra építve.

Az **uniós egészségügyi biztonsági** keret értelmében a korai figyelmeztető és gyorsreagáló rendszeren alapuló információcserét – ideértve az Ukrajnából történő egészségügyi evakuáláshoz nyújtott támogatást is – meg kell védeni a kibertámadásokkal szemben, ezért a rendszer biztonságát megerősítik.

Együttműködés a partnerekkel

Az EU továbbra is együttműködik nemzetközi partnereivel a kibertérben tanúsított rossz szándékú magatartások megelőzése, visszaszorítása, megakadályozása és elhárítása érdekében. Oroszország Ukrajna elleni agresszív háborúja okán minden eddiginél fontosabbá vált az együttműködés ezen a területen. E tekintetben az EKSZ – partnereivel, köztük az USA-val és a NATO-val együttműködve – a helyzetismeret megosztásán és az Ukrajnát célzó rossz szándékú kibertevékenységekre való reagálás, valamint az Ukrajnának és a régió többi szereplőjének nyújtott támogatás koordinálásán dolgozik a komplementaritás biztosítása és az átfedések elkerülése érdekében.

Az EU–USA Kereskedelmi és Technológiai Tanács keretében is intenzívebbé vált az USA-val folytatott szoros együttműködés. A májusi párizsi miniszteri találkozót követő együttes nyilatkozatban[25] hangsúlyozták, hogy az EU–USA Kereskedelmi és Technológiai Tanács központi szerepet tölt be a megújított transzatlanti partnerségben, amely az EU és az USA közös intézkedéseinek koordinálását szolgálja az Ukrajna elleni orosz agresszióval szemben. Mindkét fél egyetértett abban, hogy az ellátási láncok rezilienciájának javítását célzó szoros együttműködés fontosabb, mint valaha. Létrehozták továbbá a harmadik országok

[24] COM(2022) 21.

[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108

biztonságos és reziliens digitális infrastruktúrájának közfinanszírozásával foglalkozó munkacsoportot, amelynek feladata, hogy előkészítse harmadik országbeli digitális projektek Európai Unió és az Egyesült Államok általi közös közfinanszírozását közös, átfogó elvek alapján.

A 2022 márciusában elfogadott stratégiai iránytű (lásd a VII. szakaszt) tovább fogja erősíteni az uniós kiberdiplomáciai eszköztárat, és továbbfejleszti az uniós kibervédelmi szakpolitikát a kibertámadásokra való hatékonyabb felkészülés és reagálás érdekében, egy szélesebb körű stratégia részeként, amely arra irányul, hogy megerősítse az EU képességét a válságokra való reagálásra és érdekeinek megvédésére.

Kiberbiztonsági támogatás Ukrajnának és a szomszédos országoknak

Az EU már a háború előtt is támogatta Ukrajna kiberrezilienciáját. Az EU és Ukrajna között már 2021 júniusában sor került az első kiberdialógusra, és „az EU a digitális Ukrajnáért” (EU4Digital Ukraine) programon keresztül az EU 25 millió EUR értékben támogatást nyújtott a kiberbiztonsághoz és a reziliens digitális átálláshoz. Egy további, 1,5 millió EUR összegű ikerintézményi program segíti majd Ukrajna kiberbiztonsági intézményeinek az uniós normákhoz igazítását.

A háború kitörése óta az EU szorgalmazza az uniós és ukrán kiberszakértők közötti együttműködést, és koordinálja a technikai segítségnyújtást, valamint berendezések, szoftverek és a kapcsolódó szolgáltatások biztosítását Ukrajna kiberrezilienciájának és kibervédelmének megerősítése érdekében.

Emellett az EU azon dolgozik, hogy felmérje a Moldovának, Grúziának és a Nyugat-Balkánnak nyújtott lehetséges középtávú támogatást. 2022. március 3–4-én közös értékelő misszióra került sor Moldovában a kiberbiztonsági igények felmérése céljából, amelynek eredményeként célzott válságreagálási intézkedést fogadtak el az ország kiberbiztonságának gyors megerősítése érdekében. Hasonló gyorsreagálási támogatás előkészítése zajlik számos nyugat-balkáni ország számára, amelyek az uniós szankciókhoz való csatlakozásuk okán különösen veszélyeztetettnek tekinthetők. Folyamatban van a Moldovának az Európai Békekereten keresztül nyújtandó esetleges további támogatás értékelése is.

III. SZERVEZETT BŰNÖZÉS ÉS TERRORIZMUS

Oroszország Ukrajna elleni agresszív háborúja miatt emberek milliói kényszerültek arra, hogy elhagyják otthonukat, amelynek eredményeképp rendkívüli mértékben fokozódott az EU külső határait átlépő személyek mozgása. Május 18-ig közel 6 millióan érkeztek az EU-ba Ukrajnából és Moldovából, mostanáig pedig 2,8 millióan kérték nyilvántartásba vételüket arra, hogy átmeneti védelmet kapjanak az EU-ban. Az EU arra törekszik, hogy a lehető leggyorsabban és legrugalmasabban befogadja a háború elől menekülőket, anélkül, hogy veszélyeztetné az EU külső határainak biztonságát. Az EU példátlan intézkedéseket hozott annak érdekében, hogy átmeneti védelmet nyújtson a háború elől menekülőknek, és elkötelezett amellett, hogy minden újonnan érkező személyt megkülönböztetés nélkül kezeljen. Ugyanakkor nem szabad figyelmen kívül hagyni azokat a potenciális kockázatokat, amelyek az emberek ilyen nagy számban történő mozgásából adódhatnak, és az EU – az érintett uniós ügynökségek határozott támogatásával – továbbra is éberen figyeli a szervezett bűnözés és a terrorizmus terén zajló fejleményeket.

Erős schengeni rendszer a fokozott fenyegetések idején

A magas szintű biztonság biztosítása a **schengeni** térségben és az EU-n belül soha nem volt olyan fontos, mint az EU külső határának túloldalán zajló háborúból eredő fokozott fenyegetések légkörében.

A 2021. júniusi stratégiában meghatározott, a schengeni térségre vonatkozó ambiciózus menetrend megvalósítása érdekében a Bizottság májusban elfogadta a schengeni rendszer helyzetéről szóló első jelentést[26]. Az éves schengeni ciklus új kormányzási modellt biztosít a schengeni térség számára, amelynek keretében sor kerül a schengeni rendszer helyzetének rendszeres állapotfelmérésére. Ez elősegíti a hiányosságok gyors azonosítását és a hatékony nyomonkövetési eljárásokat a schengeni térség erősebbé és reziliensebbé tétele érdekében.

Ez az első jelentés elismeri, hogy fokozni kell a kulcsfontosságú uniós szintű kezdeményezések végrehajtására irányuló erőfeszítéseket, ideértve az összes utas külső határokon történő szisztematikus ellenőrzését a Frontex és az Europol megbízatásának, valamint a határokon átnyúló rendőrségi együttműködés javasolt és rendelkezésre álló eszközeinek teljes körű kihasználásával.

A belső biztonság és a határigazgatás javítására irányuló erőfeszítések lényeges eleme a határigazgatást, a migrációt és a biztonságot szolgáló uniós információs rendszerek új architektúrája és interoperabilitása. Döntő fontosságú lesz az interoperabilitási keret valamennyi elemének az elfogadott határidőkkel összhangban történő hatékony végrehajtása.

Éberség és koordináció

A tagállamok közötti és a harmadik országokkal folytatott szorosabb bűnüldözési együttműködés kulcsfontosságú az újonnan megjelenő bűnügyi és terrorizmus általi fenyegetettségekkel kapcsolatos tájékoztatás érdekében, valamint azokkal a bűnözői hálózatokkal és egyénekkel szembeni fellépés érdekében, akik esetleg megpróbálnak hasznot húzni az Ukrajna elleni háborúból. A tagállamok és az operatív partnerek aktívan megosztják a rendelkezésre álló releváns információkat és bűnüldözési operatív információkat az Europollal, amely összeveti és elemzi az információkat, majd végrehajtható operatív hírszerzési tájékoztatókat készít, például korai figyelmeztető értesítéseket és fenyegetésértékeléseket, amelyeket megosztanak a partnerekkel.

Szervezett bűnözés

A szervezett bűnözés már most is módot talál a jelenlegi helyzet kihasználására. A kezdeti információelemzés során számos területen azonosítottak bűnözési mintákat, így az emberkereskedelem, az importált és exportált árukra vonatkozó hamis árunyilatkozatok, az online csalás, a kiberbűnözés és a tiltott fegyverkereskedelem terén. Bizonyítékok állnak rendelkezésre arra vonatkozóan is, hogy kiberbűnözők elhitetik magukról, hogy Ukrajna

[26] COM(2022) 301.

számára gyűjtenek adományokat, és így lopnak pénzt és kriptovalutát[27]. Előfordulhat, hogy a jelenlegi helyzet miatt egyes ukrán bűnszervezetek megkísérelnek áttelepülni az EU-ba, hogy ott folytassák tevékenységeiket.

A Bizottság és a Tanács francia elnöksége együttműködött az uniós bel- és igazságügyi ügynökségekkel, különösen az Europollal annak érdekében, hogy mozgósítsa a Bűnügyi Fenyegetettség Elleni Európai Multidiszciplináris Platformot (**EMPACT**) a már létező vagy kialakulóban lévő, súlyos és szervezett bűnözés általi fenyegetettség értékelése, előrejelzése, megelőzése és leküzdése érdekében. 2022. április 7-én az Europol adott otthont az EMPACT találkozójának, amelyen az uniós tagállamok és az uniós biztonsági közösség képviselői és szakértői vettek részt, hogy foglalkozzanak az Ukrajnában zajló háború következtében megjelent, súlyos és szervezett bűnözés általi fenyegetésekkel. A megvitatott konkrét lépések között szerepelt még több hírszerzési információ gyűjtése, vészhelyzeti operatív intézkedések végrehajtása és a meglévők átirányítása, valamint ad hoc együttes fellépési napok.

A **CELBET** (Keleti és Dél-keleti Szárazföldi Vámhatárok Szakértői Csoport) – az Európai Bizottság által finanszírozott együttműködési projekt – megbízatása keretében nyomon követi a határon zajló fejleményeket, melynek során operatív támogatást és iránymutatást nyújt a vámtisztviselőknek, és figyelemmel kíséri az Ukrajnával közös uniós határon (Lengyelország, Szlovákia, Magyarország és Románia) lévő határátkelőhelyeken történő vámhatósági lefoglalásokat.

Bűnözői és terrorista tevékenység

Bár Ukrajna orosz megszállásával kapcsolatban az EU-ban még nem jelentkezett közvetlen terrorveszély, egyértelműen éberségre van szükség.

A bűnözői és a terrorista tevékenység megnövekedett kockázata rávilágít annak fontosságára, hogy a tagállamok használják a megfelelő uniós adatbázisokat – például a Schengeni Információs Rendszert –, szükség esetén adatokat rögzítsenek bennük, és betekintsenek azokba az EU-ba belépő személyek ellenőrzése során. Ez segít annak biztosításában, hogy a külső határokon azonosítsák azokat a személyeket, akik veszélyt jelentenek az EU belső biztonságára. Az eu-LISA, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökség, továbbra is biztosítja az uniós határigazgatási rendszerek teljes körű rendelkezésre állását és hatékonyságát. A tagállamoknak szóló iránymutatás[28] tisztázta, hogy miként kell egyensúlyt teremteni az érkezések külső határnál történő zökkenőmentes kezelésének szükségessége és a szükséges biztonsági ellenőrzések elvégzése között.

Felkészültség

[27] A Google fenyegetettségelemző csoportja olyan fenyegető szereplők növekvő számával szembesült, akik csalétekként használják az ukrajnai háborút adathalászati és rosszindulatú szoftvereket terjesztő kampányaik során. Az internetes biztonsággal foglalkozó Cyren vállalat kutatói arról számolnak be, hogy egyre nagyobb számban fordulnak elő kriptocsalások, amelyek során hamis adományozási weboldalak használatával húznak hasznot a konfliktusból.

[28] A Bizottság közleménye – Operatív iránymutatás a külső határok igazgatására vonatkozóan az EU és Ukrajna közötti határátlépések megkönnyítése érdekében (2022/C 104 I/01).

Az iránymutatás és a koordináció mellett az uniós ügynökségek személyzetének kiküldése révén is fokozták az EU felkészültségét.

Az **Europol** műveleti csapatokat telepített az Ukrajnával szomszédos uniós tagállamokba. Ezek a csapatok az Europol tagállamokból származó vendégtisztjeiből, valamint az Europol Magyarországon, Litvániában, Lengyelországban, Romániában, Szlovákiában, továbbá Moldovában dolgozó szakértőiből állnak[29]. Az Europol vendégtisztjei elkülönített helyen történő biztonsági ellenőrzések lefolytatásával támogatják a nemzeti hatóságokat az EU külső határain. Az Europol szakértői által nyújtott támogatás abból áll, hogy információkat gyűjtenek és értékelnek a terror- és bűnügyi fenyegetettség felderítése, a nyomozások támogatása, valamint az EU-ba való belépés megkísérlésével kockázatot jelentő személyek azonosítása érdekében. Ezek a műveleti csapatok információkat gyűjtenek, amelyek bekerülnek a tagállamok rendelkezésére álló bűnügyi fenyegetésértékelésekbe. Az ilyen információgyűjtési tevékenység lehetővé teszi az Europol számára, hogy előre jelezze a fejleményeket és összehangolja operatív tevékenységeit az uniós tagállamokkal az ukrajnai háborúból hasznot húzni kívánó bűnözői csoportok tevékenységeire való reagálás során, valamint hogy építsen az ukrán bűnüldöző hatósággal az Europol hollandiai székhelyén jelen lévő ukrán összekötő tisztviselőn keresztül folytatott aktív együttműködésre.

Az **Európai Határ- és Partvédelmi Ügynökség (Frontex)** is jelen van a tagállamokban és az EU-val szomszédos országokban a határellenőrzési műveletek támogatása érdekében: jelenleg több mint 2 100 kiküldött határőr teljesít szolgálatot az EU területén, a Nyugat-Balkánon és Moldovában. Az **Európai Menekültügyi Támogatási Hivatal (EASO)** közel 750 alkalmazottat telepített az EU déli tagállamaiba és Litvániába az operatív tevékenységek támogatása, a befogadási kapacitások megerősítése és a menekültügyi eljárások előmozdítása érdekében.

A jelenlegi **prümi határozatra**[30] építve, amely keretet biztosít a tagállamok számára a bűnüldöző szervek tagjainak bevetéséhez közös műveletek – például közös járőrszolgálatok – végzése céljából, a Bizottság és az Európai Unió Tanácsának francia elnöksége közös levelet küldött valamennyi tagállamnak, amelyben kérték a szükségletek meghatározását, valamint azt, hogy küldjenek ki rendőrtiszteket annak érdekében, hogy közös járőrszolgálatokat indítsanak a háború miatti tömeges határátlépések által leginkább érintett uniós frontországokban. A Bizottság ezeket a kiküldéseket a rendőrségi együttműködést támogató eszköz keretében fogja finanszírozni.

Az emberkereskedelem kezelése

Az EU a háború első napjai óta gyorsan reagál a bűnözői tevékenység azon meghatározott területén jelentkező kockázatokra, amely hasznot húzhat az EU-ban biztonságot kereső emberek hatalmas áradatából. Alapvető fontosságú megfékezni az emberkereskedőket, akiknek a célpontjai kiszolgáltatott helyzetben lévő, menekülő emberek, többnyire **nők és gyermekek**, akiket hazug ajánlatokkal hálóznak be, például utaztatást vagy szállást ígérve nekik.

[29] Május 3-ig az Europol 1 Europol alkalmazottat és 3 vendégtisztet küldött Szlovákiába, 1 Europol tisztviselőt Lengyelországba, 1 Europol tisztviselőt és 4 vendégtisztet Romániába, valamint 2 vendégtisztet Magyarországra. 1 Europol alkalmazott és 2 vendégtiszt tevékenykedik Moldovában.

[30] 2008/615/JHA, 2008/616/JHA.

Márciusban az Europol és az Eurojust korai előrejelző értesítéseket küldött az illetékes nemzeti hatóságoknak az emberkereskedelem és az Ukrajnából érkező áldozatok kizsákmányolásának potenciális veszélyére vonatkozóan. Az Eurojust segít fokozni az információcserét és felgyorsítani az igazságügyi együttműködést többek között Ukrajnával is, és az emberkereskedelmi ügyekben folytatott nyomozásokat koordináció céljából az ügynökség hatáskörébe utalták.

Az emberkereskedelem elleni küzdelem uniós koordinátora találkozókat tartott a nemzeti előadók vagy azzal egyenértékű mechanizmusok uniós hálózatával, a bel- és igazságügyi ügynökségekkel és az emberkereskedelem elleni uniós civil társadalmi platformmal, hogy megvitassák a visszaélések megelőzéséhez és leküzdéséhez, valamint az áldozatok védelméhez szükséges intézkedéseket. Több tagállamban vizsgálat indult potenciális ügyekben.

Az EU gyors és határozott lépéseket tett annak érdekében, hogy összehangolt választ adjon az EU segítségére szoruló embereket fenyegető valós veszélyre. Az átmeneti védelemről szóló irányelvet az ukrajnai háború elől menekülők támogatása érdekében végrehajtó tagállamoknak gyorsan operatív iránymutatást[31] nyújtott többek között az emberkereskedelem jelentette kihívást illetően. A 2022. március 28-án a Bel- és Igazságügyi Tanács elé terjesztett, az Ukrajna elleni háború elől menekülők fogadásának erőteljesebb európai koordinációjához szolgáló tízpontos terv[32] részeként az emberkereskedelem elleni küzdelem uniós koordinátora az uniós ügynökségekkel és a tagállamokkal együttműködésben közös emberkereskedelem elleni tervet[33] dolgozott ki az emberkereskedelem megelőzésére és az áldozatok megsegítésére vonatkozóan. Különös figyelmet fordítanak azoknak a szervezeteknek és magánszemélyeknek (köztük önkénteseknek) a nyilvántartásba vételére, akik szállást, szállítást és egyéb segítséget kívánnak nyújtani, valamint a háttérellenőrzések végzésére. A Bizottság felvette a kapcsolatot az Európai Unió Menekültügyi Ügynökségével is, hogy elősegítse az emberkereskedelem áldozatainak felderítését a befogadóállomásokon végzett egészségügyi vizsgálatok során. A kísérő nélküli vagy a hozzátartozóiktól elszakított gyermekek különösen ki vannak téve a bántalmazás, a szexuális kizsákmányolás vagy a bűnözésre kényszerítés veszélyének. A fent említett operatív iránymutatás emellett segítséget nyújt a tagállamoknak a gyermekek és különösen a kísérő nélküli kiskorúak érkezésének kezeléséhez, fogadásához és támogatásához. A kockázatnak kitett személyek tájékoztatása érdekében a Bizottság külön honlapot hozott létre, amelynek egyik oldala gyakorlati tanácsokat tartalmaz arra vonatkozóan, hogy hogyan kerüljék el az emberkereskedőket.

Míg a felkészültség fokozására irányuló intézkedésekre kifejezetten a háborúból fakadó új körülményekre adott válaszként került sor, más kulcsfontosságú intézkedések olyan **jogalkotási kezdeményezésekből** erednek, amelyek folyamatban voltak már Oroszország Ukrajna elleni agresszív háborúja előtt is.

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - HU - EUR-Lex (europa.eu).

[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en

[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en

A Bizottság üdvözli az **Europol** módosított megbízatásáról szóló, 2022. februári megállapodást[34], amely a végrehajtását követően lehetővé teszi az Europol számára, hogy hatékonyabban támogassa a tagállamokat a szervezett bűnözés és a terrorizmus elleni küzdelem során. Ezt követően az ügynökség megfelelő eszközökkel és biztosítékokkal fog rendelkezni ahhoz, hogy támogassa a rendőri erőket a nagy adathalmazok elemzésében a bűncselekmények kivizsgálása során, valamint a számítástechnikai bűnözés elleni küzdelmet szolgáló úttörő módszerek kidolgozásában. Ezek a változások megerősített adatvédelmi keretet, valamint erősebb parlamenti felügyeletet és elszámoltathatóságot vonnak maguk után.

A Bizottság által 2021. december 8-án előterjesztett és jelenleg tárgyalás alatt álló, **rendőrségi együttműködésre** vonatkozó csomag[35] erősíteni fogja a tagállamok bűnüldöző szerveinek tagjai közötti együttműködést azáltal, hogy gyorsabbá, egyszerűbbé és biztonságosabbá teszi az adatcserét, valamint javítja és hatékonyabbá teszi a helyszíni operatív rendőrségi együttműködést. A Bizottság felkéri az Európai Parlamentet és a Tanácsot, hogy minél előbb fogadják el ezt a csomagot.

Elfogadásukat és végrehajtásukat követően e jogalkotási javaslatok támogatni fogják a bűnüldözést a határokon átnyúló szervezett bűnözés elleni küzdelemben. Ez különösen fontos lehet abban az esetben, ha a jelenlegi helyzet miatt az ukrán bűnszervezetek esetleg megkísérelnek áttelepülni az EU-ba, hogy ott folytassák a tevékenységeiket.

Az **EU ukrajnai tanácsadó missziója** 2014 óta támogatja az ország bűnüldöző hatóságainak és jogállamisági intézményeinek reformját. 2022 márciusában módosították a misszió megbízatását, lehetővé téve a Lengyelországgal, Romániával és Szlovákiával közös ukrán határátkelőhelyeken nyújtott támogatást, hozzájárulva a helyzetismeret kialakításához a határokon átnyúló bűnözői tevékenységekkel, többek között az emberkereskedelemmel, valamint a segélyszállítmányok Ukrajnába történő beáramlásával kapcsolatban.

IV. FEGYVEREK, VESZÉLYES ANYAGOK ÉS KRITIKUS ESEMÉNYEK

A háború jelentősen megnövelte a tűzfegyverek és más fegyverek forgalmát Ukrajnán belül, ami új kockázatokat jelent az EU és az Ukrajnával szomszédos más államok számára.

Éberség és koordináció

A márciusban kiadott operatív iránymutatás tanácsot adott a tagállamoknak arra vonatkozóan, hogy miként kezeljék a tűzfegyverek fokozott forgalmából eredő kihívást, miközben emberek tömegei érkeznek az EU külső határához[36]. Az iránymutatás hangsúlyozza, hogy a tűzfegyverek jelenlétét folyamatosan ellenőrizni kell, és engedély nélkül senki sem léphet be tűzfegyverrel az EU-ba. Amennyiben az ukrán hatóságok e tűzfegyverek bármelyikét eltűntként jelentik be, a tagállamoknak jelenteniük kell azokat a Schengeni Információs Rendszerben.

[34] COM(2020) 796.
[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.
[36] A bizottság közleménye – Operatív iránymutatás a külső határok igazgatására vonatkozóan az EU és Ukrajna közötti határátlépések megkönnyítése érdekében (2022/C 104 I/01).

Alapvető fontosságú, hogy az Ukrajnába irányuló összes tűzfegyverszállítmányt megfelelően nyilvántartásba vegyék minden lényeges adattal együtt (úgymint típus, a gyártás országa és éve, márka, gyártmány, kaliber, sorozatszám) annak érdekében, hogy mind Ukrajnában, mind az EU-ban könnyebb legyen e tűzfegyverek nyomon követhetősége.

Az EU nyilvánosan elítélte az Oroszország által az Ukrajnában lévő polgári, nukleáris, biológiai és vegyi létesítményeknél és azok közvetlen közelében végrehajtott meggondolatlan katonai támadásokat, továbbá minden olyan cselekményt, amely veszélyezteti e létesítmények biztonságát. A Bizottság figyelemmel kíséri az ukrajnai helyzetet, különös tekintettel a radiológiai fenyegetésre, ami az EU belső biztonsága szempontjából a legnagyobb problémát jelenti[37]. A Bizottság figyelemmel kíséri a potenciális vegyi fenyegetést is, és belső koordinációs mechanizmust hozott létre arra az esetre, ha gyors kockázatértékelésre lenne szükség.

Felkészültség

Ukrajna már egyike azoknak az országoknak, amelyeket a tűzfegyverek tiltott kereskedelmére vonatkozó 2020–2025-ös uniós cselekvési tervben a külügyi szintű egyedi intézkedések szempontjából kulcsfontosságúként határoztak meg. Meghatározott műveleti fellépésre is sor kerül a régióban – így Ukrajnában is –, az EMPACT Tűzfegyverek keretében. Tekintettel azonban a tűzfegyverek illetéktelen kezekbe jutásának kockázatára, szükség lesz uniós finanszírozású egyedi projektekre, valamint az Europollal, a Frontexszel és az EMPACT Tűzfegyverekkel foglalkozó ágával való operatív együttműködésre. A Bizottság hamarosan javaslatot fog előterjeszteni a tűzfegyverekről szóló rendeletnek[38] a polgári célú lőfegyverek kivitele, behozatala és tranzitja tekintetében történő felülvizsgálatára vonatkozóan, a tűzfegyverek tiltott kereskedelmének megelőzését, felderítését, kivizsgálását és büntetőeljárás alá vonását szolgáló átfogó jogi és működési keret részeként.

A népegészségügyi kockázatokra – például a CBRN-fenyegetésekre – való uniós felkészültség és reagálás javítása érdekében a Bizottság az uniós polgári védelmi mechanizmuson (UCPM) keresztül kiépíti a reagálási képességek stratégiai tartalékát, amit az Egészségügyi Szükséghelyzet-felkészültségi és -reagálási Hatóság (HERA) finanszíroz[39]. A Bizottság szolgálatai közösen dolgoznak egy 540,5 millió EUR összegű rescEU stratégiai készlet létrehozásán. Ez a készlet a vegyi, biológiai, radiológiai és nukleáris vészhelyzetekből származó anyagoknak kitett betegek kezelésére szolgáló felszerelésekből és gyógyszerekből, oltóanyagokból és egyéb terápiás készítményekből fog állni, valamint fertőtlenítő-mentesítő létesítményeket és szakértőkből álló reagáló csoportokat biztosító, mentesítési célú rescEU-képességeket foglal majd magában. Azonnali első lépésként az EU mobilizálta rescEU orvosi tartalékát kálium-jodid tabletták beszerzése érdekében, amelyek használata megvédi az embereket a sugárzás káros hatásaival szemben, valamint más, olyan termékek beszerzése

[37] A Bizottság az egyesült államokbeli partnereivel együttműködve munkaértekezletet szervez a szabályozói ellenőrzés alól kikerülő kórházakban található radiológiai anyagokkal kapcsolatos kockázatokról.

[38] Az Európai Parlament és a Tanács 258/2012/EU rendelete (2012. március 14.) az Egyesült Nemzeteknek a nemzetközi szervezett bűnözés elleni egyezményét kiegészítő, a tűzfegyverek, részeik, alkotóelemeik és a lőszerek tiltott gyártásáról és kereskedelméről szóló jegyzőkönyve (az ENSZ tűzfegyverekről szóló jegyzőkönyve) 10. cikkének végrehajtásáról, valamint a tűzfegyverek, tűzfegyverdarabok, alkotóelemeik és lőszereik kiviteli engedélyezési, behozatali és tranzit szabályainak létrehozásáról.

[39] A HERA 2022. évi munkaterve (europa.eu).

érdekében, amelyekre sürgősen szükség van Ukrajnában. Az UCPM-en keresztül már csaknem 3 millió kálium-jodid tablettát szállítottak Ukrajnába Franciaország és Spanyolország segítségével.

V. ÖSSZEHANGOLT FELLÉPÉS AZ OROSZ AGRESSZIÓ ELSZÁMOLTATÁSA ÉRDEKÉBEN

Az EU döntő szerepet játszik a nemzetközi közösség arra irányuló intézkedéseiben, hogy nyomásgyakorolással elérje, hogy Oroszország véget vessen az ukrán állam és a konfliktusban érintett civilek elleni elfogadhatatlan és a nemzetközi joggal ellentétes agressziónak. Ez a nyomásgyakorlás az elkövetőket érintő következményekkel járó intézkedéseket, például súlyos szankciókat foglal magában, valamint a háborús bűncselekmények azonosítására és az azokkal kapcsolatos büntetőeljárások lefolytatásának megkönnyítésére irányuló intézkedéseket.

Korlátozó intézkedések és elkobzás

Azóta, hogy Oroszország 2022. február 21-én elismerte Ukrajna Donyeck és Luhanszk régiójának nem kormányzati ellenőrzés alatt álló területeit, és 2022. február 24-én megszállta Ukrajnát, az EU minden eddiginél jelentősebb szankciók sorát vezette be Oroszországgal szemben. Eddig öt szankciócsomagot fogadtak el. Ezek az intézkedések a kulcsfontosságú ágazatokra, köztük a pénzügyi ágazatra, a kereskedelemre, a közlekedésre, a védelemre és a médiára összpontosulnak, továbbá a politikai és katonai elitet, valamint a prominens orosz és fehérorosz oligarchákat veszik célba. A jegyzéken már több mint 1 000 személy és 80 szervezet szerepel. A Tanács jelenleg tárgyalja a hatodik szankciócsomagot.

Az orosz és fehérorosz személyekkel és vállalatokkal szembeni jelenlegi és korábbi korlátozó intézkedéseknek az ereje azok érvényesítésén múlik. Az uniós koordináció jelentős mértékben hozzájárulhat az esetleges joghézagok megszüntetéséhez, és a Bizottság írásbeli iránymutatás, az érdekelt felek találkozói és egy erre a célra létrehozott szakértői csoport révén széles körű támogatást nyújt az érdekelt feleknek, valamint számos erőforrást biztosít a megfelelés megkönnyítése érdekében.

Emellett a Bizottság létrehozott egy befagyasztásokkal és lefoglalásokkal foglalkozó munkacsoportot (‘Freeze and Seize’ Task Force), amelyben a Bizottság szolgálatai, a tagállamok, az Eurojust és az Europol vesznek részt. Mindezidáig a tagállamok 9,89 milliárd EUR értékű vagyon befagyasztásáról számoltak be[40]. Április 11-én az Europol a tagállamokkal, az Eurojusttal és a Frontexszel közösen elindította az Oscar-műveletet, amelynek célja az Ukrajna elleni orosz agresszióval kapcsolatban uniós szankciók hatálya alá vont személyek és jogalanyok tulajdonában lévő, bűncselekményekből származó vagyonra irányuló pénzügyi és bűnügyi nyomozások támogatása. Az EU befagyasztásokkal és lefoglalásokkal foglalkozó munkacsoportja szorosan együttműködik a G7-ek (Kanada, Franciaország, Németország, Olaszország, Japán, Egyesült Királyság, Egyesült Államok) által létrehozott, az orosz elittel, szövetségesekkel és oligarchákkal foglalkozó munkacsoporttal („Russian Elites, Proxies, and Oligarchs” – REPO – Task Force), valamint hasonlóan gondolkodó partnerekkel, például Ausztráliával, az USA KleptoCapture munkacsoportjával és az ukrán munkacsoporttal.

[40] Az Oroszországi Központi Bank mintegy 23 milliárd EUR összegű eszközét is zárolták.

A befagyasztásokkal és lefoglalásokkal foglalkozó munkacsoport platformként szolgál arra, hogy koordinálják és előmozdítsák a tagállamok közötti információ- és tapasztalatcserét, iránymutatást nyújtsanak a szankciók végrehajtásához, és kicseréljék a nyomozásokkal és az elkobzással kapcsolatos bevált gyakorlatokat. Különösen fontos, hogy a bűnüldöző hatóságok éberek és proaktívak legyenek a szankcionált személyek és szervezetek által elkövetett potenciális bűncselekményekkel kapcsolatban. A munkacsoport célja továbbá, hogy megbeszéléseket kezdeményezzen az elkobzott pénzeszközök lehetséges felhasználásáról, például Ukrajna újjáépítéséhez.

A Bizottság a mai napon **a vagyoni eszközök visszaszerzéséről és elkobzásáról** szóló csomagot[41] fogad el, amely figyelembe veszi az orosz és fehérorosz személyekkel és szervezetekkel szembeni uniós korlátozó intézkedések végrehajtásából levont tanulságokat. Ez elősegíti majd az uniós korlátozó intézkedések Unió-szerte történő hatékony végrehajtását azáltal, hogy lehetővé teszi az ilyen intézkedések hatálya alá tartozó személyek vagy szervezetek tulajdonában vagy ellenőrzése alatt álló vagyon gyors felkutatását és azonosítását. A vagyoni eszközök visszaszerzésére és elkobzására vonatkozó megerősített keret a korlátozó intézkedések megsértése esetén is alkalmazandó lesz, és így biztosítani fogja a korlátozó intézkedések megsértéséből származó jövedelmek hatékony felkutatását, befagyasztását, kezelését és elkobzását. Annak biztosítása érdekében, hogy a korlátozó intézkedéseket megsértő személyek és szervezetek vagyona ténylegesen elkobozható legyen, a Bizottság a mai napon tanácsi határozatra irányuló javaslatot fogad el a szankciók megsértésének az EUMSZ 83. cikke (1) bekezdésében felsorolt uniós bűncselekményi területekhez való hozzáadására vonatkozóan[42], amelyet egy közlemény[43] kísér, azzal a céllal, hogy a bűncselekményi tényállások meghatározása, valamint a korlátozó intézkedések megsértése esetén kiszabható büntetések közelítéséről szóló irányelvjavaslatot terjesszen elő.

Általánosabb értelemben ez a csomag kulcsfontosságú lépést jelent a szervezett bűnözés elleni küzdelemben. Követi a Bizottság által a biztonsági unióra vonatkozó stratégiában és a 2020–2025 közötti időszakra vonatkozó, szervezett bűnözés elleni küzdelemre irányuló stratégiában[44] tett kötelezettségvállalásokat. Felülvizsgálja a vagyonelkobzásról szóló 2014. évi irányelvet, a vagyonvisszaszerzési hivatalokról szóló 2007. évi tanácsi határozatot, valamint a bűncselekményből származó jövedelmek, vagyon és az elkövetéshez használt eszközök elkobzásáról szóló 2005. évi kerethatározatot annak érdekében, hogy megerősítse a képességeket a felkutatás, az azonosítás, végső soron pedig az illegális jövedelmek elkobzása terén, javítva az EU-ban tapasztalható rendkívül alacsony elkobzási arányokat[45]. A csomag bővíti a hatálya alá tartozó bűncselekmények körét, és kiterjeszti az elkobzásra vonatkozó szabályokat olyan esetekre, amikor egy adott bűncselekmény vonatkozásában nem lehet bűnösséget megállapító ítéletet hozni, de a vagyon egyértelműen bűnözői tevékenységből származik. A felülvizsgálat megerősíti továbbá a befagyasztott és elkobzott vagyoni eszközök hatékony kezelését, valamint megerősíti a vagyonvisszaszerzési hivatalok azon képességét, hogy felkutassák és azonosítsák a jogellenesen szerzett javakat. Az új uniós vagyonvisszaszerzési keret célja, hogy kezelje a gyakran határokon átnyúlóan működő

[41] COM(2022) 245.
[42] COM(2022) 247.
[43] COM(2022) 249.
[44] COM(2021) 170.
[45] Az Europol becslése szerint a bűncselekményből származó vagyoni eszközök csupán 2 %-a került zár alá vételre (2,4 milliárd EUR) és 1 %-a elkobzásra (1,2 milliárd EUR), miközben az EU fő bűnözői piacain a bűncselekményből származó bevételek 2019-ben 139 milliárd EUR-t tettek ki (az uniós GDP 1 %-a).

bűnszervezetek összetett működését, amelyek vagyonuk eltitkolása érdekében különböző módszereket, például kriptoeszközöket alkalmaznak.

Összehangolt igazságszolgáltatási reagálás

Uniós szinten folyik a munka azon is, hogy biztosítsák az Ukrajnában feltételezetten elkövetett **nemzetközi bűncselekményekre** való összehangolt igazságszolgáltatási reagálást, hogy az elkövetőket felelősségre lehessen vonni.

Két tagállam és Ukrajna közös nyomozócsoportot hozott létre az Ukrajna területén feltételezetten elkövetett háborús bűncselekmények, emberiesség elleni bűncselekmények és más nemzetközi bűncselekmények kivizsgálására. Az Eurojust jogi, elemzési, pénzügyi és logisztikai támogatást nyújt ennek a közös nyomozócsoportnak. 2022. április 25-én a Nemzetközi Büntetőbíróság ügyészi hivatala résztvevőként[46] csatlakozott a közös nyomozócsoporthoz, és várhatóan hamarosan további résztvevők is csatlakoznak hozzá.

A Bizottság 2022. április 25-én javaslatot terjesztett elő az Eurojustról szóló rendelet módosítására[47] annak érdekében, hogy az Eurojust megőrizze, elemezze és tárolja az alapvető nemzetközi bűncselekményekkel kapcsolatos bizonyítékokat. Az Eurojust és az Europol folytatják szoros együttműködésüket e folyamat során. Az igazságszolgáltatási reagálás összehangolásában döntő szerepet játszik a népirtás elleni hálózat is, amely titkárságának az Eurojust ad otthont. A népirtás elleni hálózat titkársága elkészítette az Ukrajnában jelenleg tevékenykedő nem kormányzati szervezetek atlaszát, és támogatja a tagállamok és Ukrajna azon nemzeti szakértőit, akik a háborúval kapcsolatban folyamatban lévő ügyeket kezelnek.

2022 áprilisában a Tanács ismét módosította az **EU ukrajnai tanácsadó missziójának** megbízatását, lehetővé téve ezzel a misszió számára, hogy támogatást nyújtson az ukrán hatóságoknak az orosz katonai agresszióval összefüggésben elkövetett nemzetközi bűncselekmények kivizsgálása és büntetőeljárás alá vonása terén. A misszió stratégiai tanácsadást nyújt az ukrán hatóságoknak a nemzetközi bűncselekmények kivizsgálásával és büntetőeljárás alá vonásával, az ukrán jogszabályok szükséges módosításaival, a kommunikációs stratégiával, valamint a kapcsolódó ügyeket érintő képzéssel kapcsolatban. A misszió egyike az ebben a témában indított számos koordinációs kezdeményezésnek, és az Unió küldöttségével közösen részt vesz az Egyesült Államok és az EU Ukrajnában elkövetett atrocitás-bűncselekményekkel foglalkozó tanácsadó csoportjának.

VI. KÜLFÖLDI INFORMÁCIÓMANIPULÁCIÓ ÉS BEAVATKOZÁS

A jelenlegi geopolitikai fejlemények rávilágítottak a külföldi beavatkozás kockázataira. Az Ukrajna elleni orosz katonai agressziót **információmanipulációs és beavatkozási** tevékenységek kísérik. Az ukrán kormány ellen irányuló, „nácizmust” és „népirtást” emlegető alaptalan állításokat, megtévesztő műveleteket, valamint a NATO-val és a Nyugattal szemben felhozott megalapozatlan vádakat vetettek be az Ukrajna elleni brutális támadások igazolására, miközben Oroszországon belül elnyomják a szólásszabadságot és a független tudósításokat. Állandó kockázatot jelentenek a manipulált audiovizuális anyagok és a félrevezető információk, amelyeket Oroszország esetleg ürügyként használhat fel további katonai támadásokra, hogy meggyengítse az ukrán ellenállás elszántságát, megossza a

[46] https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine
[47] COM(2022) 187 final.

nemzetközi közösséget a háborúval szembeni kiállása terén, vagy kételyeket ébresszen a nemzetközi jog Oroszország általi megsértéseivel kapcsolatban. „A biztonság és a védelem területére vonatkozó stratégiai iránytű” című dokumentumban az EU kötelezettséget vállalt arra, hogy határozottan reagál a külföldi információmanipulációra és beavatkozásra, valamint fokozza az ilyen fenyegetésekkel szembeni rezilienciáját és képességét.[48] Az EU-n belüli demokratikus vita manipulálása a tárgya az európai demokráciáról szóló cselekvési tervnek, ami a Bizottság összehangolt terve a dezinformáció kezelésére és a demokratikus reziliencia megerősítésére[49].

Éberség és koordináció

Az Európai Unió határozott és összehangolt fellépéssel reagált Oroszország dezinformációs kampányára az Ukrajna elleni katonai agresszióval összefüggésben. Az EU a riasztási rendszeren keresztül szorosan együttműködik tagállamaival, valamint nemzetközi partnereivel, köztük a NATO-val, az USA-val, Kanadával és a G7-ek riasztási mechanizmusával, hogy megossza a Kreml által alkalmazott manipulációs tendenciákkal és taktikákkal kapcsolatos ismereteket. Intenzívebbé vált a Kreml manipulációinak leleplezésére irányuló munka, különösen az angol, orosz, ukrán és más nyelveken közvetítő EUvsDisinfo weboldalon keresztül, hogy tényszerű információkkal szolgáljanak az EU-ban, Ukrajnában és a régióban, valamint Oroszországon belül is. Március 2-án az EU által elfogadott korlátozó intézkedések következtében felfüggesztették az orosz állami média RT és Sputnik nevű csatornáinak közvetítését és sugárzását az EU-ban, illetve az EU felé. Az online platformok, a vezető közösségi hálózatok, a hirdetők és a reklámipar – a dezinformáció visszaszorítását célzó gyakorlati kódex[50] aláírói – sürgős lépéseket tesznek az Ukrajna elleni orosz agresszióval kapcsolatos dezinformáció visszaszorítása érdekében. A Bizottság és az EKSZ ellenőrzi ezeket az erőfeszítéseket. A rendelkezésre bocsátott információk azt mutatják, hogy a platformok megerősítették ellenőrzési és beavatkozási eszközeiket a háborúval kapcsolatban.

Emellett rohamléptekben zajlik intézkedések bevezetése a közép-ázsiai és a nyugat-balkáni országok támogatására az információs reziliencia megerősítése, valamint a külföldi információmanipuláció és dezinformáció elleni küzdelem érdekében.

Felkészültség

A külföldi információmanipuláció és beavatkozás – ennek során pedig a dezinformáció mint a hibrid fenyegetések egyik eszköze – leplezetlen alkalmazása miatt különösen sürgőssé vált az európai demokráciáról szóló cselekvési terv nyomon követése. Az elmúlt hónapokban az uniós intézmények támogatást nyújtottak a tagállamoknak – különösen a riasztási rendszer keretében – a külföldi információmanipuláció és beavatkozás elleni küzdelem terén azzal, hogy megosztották a külföldi információmanipulációt és beavatkozást végző szereplők által alkalmazott taktikákkal és a reagálási stratégiákkal kapcsolatos ismereteiket. Folyamatban vannak a külföldi információmanipulációra és beavatkozásra adott átfogó uniós válasz további megerősítését célzó megbeszélések az EKSZ által előterjesztett, az e fenyegetés kezelésére szolgáló **eszköztár** kidolgozásáról szóló stratégiai feljegyzés alapján. Ez az eszköztár tömöríti a meglévő belső intézkedéseket és az új uniós eszközöket a közös kül- és

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/hu/pdf

[49] COM(2020) 790.

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

biztonságpolitika keretében. Emellett lehetőség nyílik az Európai Külügyi Szolgálat stratégiai kommunikációval foglalkozó részlege[51] és a Bizottság általi intenzívebb fellépés előnyeinek kihasználására is.

A Digitális Média Európai Megfigyelőközpontja (EDMO) dezinformációval foglalkozó munkacsoportot hozott létre az ukrajnai háború kitörése után, és hálózatában koordinálja a tényellenőrzők és a kutatók tevékenységeit. Azt vizsgálja, hogy a Covid19-cel kapcsolatos összeesküvés-elméletek gyártói miként váltottak át szempillantás alatt oroszbarát álhírek terjesztésére, ami számos tagállamban megfigyelhető elmozdulás[52].

A digitális szolgáltatásokról szóló jogszabályjavaslat célja a gyorsan fejlődő digitális technológiákhoz való igazodás, valamint mindahhoz, amit ez jelent az olyan technológiai és demokratikus kihívások tekintetében, mint például a gyűlöletbeszéd, az online dezinformáció és a destabilizációs stratégiák. Az Európai Parlament és a Tanács által folytatott tárgyalások során elért jelentős eredményeknek lehetővé kell tenniük a csomag gyors elfogadását.

VII. ÁTFOGÓBB FELKÉSZÜLTSÉG

Egy olyan időszakban, amikor Európában ismét háború dúl, és amikor jelentős geopolitikai változások következnek be, intenzívebbé vált az Unión belüli biztonsági koordináció, olyan kezdeményezésekre támaszkodva, amelyek folyamatban voltak már Oroszország Ukrajna elleni agresszív háborúja előtt is. Az elsősorban az EU külső biztonságát célzó kezdeményezések erőteljes hatást gyakorolnak a biztonsági unió belső menetrendjére.

2022. február 15-én a Bizottság előterjesztette a **védelmi csomagot**[53], amely számos, az EU-n belüli védelem és biztonság szempontjából kritikus területekre irányuló kezdeményezést tartalmaz. A Bizottság e hozzájárulása az európai védelemhez és biztonsághoz a kihívások teljes körét lefedi. Konkrét lépéseket javasol egy integráltabb és versenyképesebb európai védelmi piac felé, különösen az EU-n belüli együttműködés fokozása és a méretgazdaságosság megteremtése révén. Tartalmaz továbbá egy ütemtervet a biztonság és a védelem szempontjából kritikus technológiákkal kapcsolatban a kutatás, a technológiai fejlesztés és az innováció ezen ágazatokban történő fellendítése, valamint a kritikus technológiáktól és értékláncoktól való függőség csökkentése érdekében. A csomag célja továbbá a világűrkutatás védelmi vetületének uniós szintű megerősítése. Emellett megvizsgálja, hogy a Bizottság miként tudná fokozni a hibrid fenyegetésekkel – többek között a kiberterületen – szembeni fellépését, valamint a katonai mobilitást Európán belül és kívül, és hogy milyen egyéb módon kezelhetők a védelemmel kapcsolatos éghajlatváltozási kihívások. E munka kiegészítéseként **„A védelmi beruházási hiányok elemzéséről és a következő lépésekről”**[54] szóló május 18-i közös közlemény figyelembe veszi azokat a

[51] Az Európai Külügyi Szolgálat stratégiai kommunikációval, munkacsoportokkal és információelemzéssel foglalkozó részlege stratégiai kommunikációs támogatást nyújt az uniós kül- és biztonságpolitika végrehajtása terén a kapcsolódó kiemelt régiókban (déli és keleti szomszédság, Nyugat-Balkán), az uniós szakpolitikák, értékek, célkitűzések és érdekek előmozdítására összpontosító egyedi stratégiai kommunikációs intézkedések kidolgozása és végrehajtása révén.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/

[53] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en

[54] JOIN(2022) 24.

képességbeli és ipari hiányosságokat, amelyeket kezelni kell a leginkább veszélyeztetett uniós tagállamok támogatása és a feltárt hiányosságok enyhítését célzó intézkedések meghatározása érdekében.

Az EU e fenyegetésekkel szembeni rezilienciája a biztonsági ágazatra kiterjedő képességorientált megközelítést is magában foglalja, amint azt a polgári, a védelmi és az űripar közötti szinergiákról szóló bizottsági cselekvési terv[55] is szorgalmazza. Folyamatban van a képességorientált megközelítés előmozdítására irányuló munka a belső biztonság és a bűnüldözés terén.

2022. március 21-én a Tanács elfogadta **A biztonság és a védelem területére vonatkozó stratégiai iránytű**[56] című dokumentumot, amit röviddel ezt követően jóváhagyott az Európai Tanács. A stratégiai iránytű ambiciózus cselekvési tervet vázol fel az EU biztonság- és védelempolitikájának 2030-ig történő megerősítéséhez. A cél az, hogy az EU erősebb és cselekvőképesebb biztonságszolgáltatóvá váljon, amely megvédi polgárait, és hozzájárul a nemzetközi békéhez és biztonsághoz. Konkrét javaslatokat tartalmaz a végrehajtásra vonatkozó nagyon pontos ütemtervvel együtt annak érdekében, hogy az EU válság esetén gyorsabban és határozottabban léphessen fel.

A stratégiai iránytű egyik eredménye egy olyan **uniós hibrid eszköztár** kidolgozása, amely keretet biztosít az EU-t és tagállamait érintő hibrid hadjáratokra való összehangolt reagáláshoz, beleértve a belső és külső intézkedéseket is. Az ágazati reziliencia alapértékeinek 2022 elején történő meghatározását[57] követően sor kerül a hiányosságok és az igények elemzésére. Az EU ebben a keretben folytatja az Oroszország agressziójából, valamint a demokráciák és a szabályokon alapuló multilaterális rend destabilizálására irányuló kísérletekből eredő fenyegetésekre való felkészültség, reziliencia és reagálás megteremtését.

VIII. ELŐRETEKINTÉS

Ami a jövőt illeti, az EU-nak továbbra is rendkívül éberen kell figyelnie a folyamatosan változó fenyegetéseket, és **minden eshetőséggel számolva meg kell teremtenie a felkészültséget és a rezilienciát**. A háború hatásai különböző formákban jelenhetnek meg, és még nem értékelhető e hatások mindegyike.

Egyelőre nem ismert, hogy az ukrán bűnözői hálózatok milyen mértékben kényszerültek helyváltoztatásra. Az Eurojust korábbi konkrét ügyei olyan tendenciát jeleznek, hogy a heroin Afganisztánból az EU-ba irányuló tiltott kereskedelme Ukrajnán keresztül zajlik, és ezt a Kábítószer és a Kábítószerfüggőség Európai Megfigyelőközpontja (EMCDDA) is megerősítette[58]. Az instabilitás megnehezítheti az ezen az útvonalon zajló

[55] COM(2021) 70.

[56] A biztonság és a védelem területére vonatkozó stratégiai iránytű – Egy, a polgárait, az értékeit és az érdekeit megvédő Európai Unióért, amely hozzájárul a nemzetközi béke és biztonság megvalósításához: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/hu/pdf

[57] SWD(2022) 21 final.

[58] Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data), OEDT, Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery (2020. évi jelentés az ukrajnai kábítószer- és alkoholhelyzetről [a 2019. évi adatok

heroinkereskedelem elleni fellépést, ami magában hordozza annak a veszélyét, hogy fokozódhat a kábítószerek EU-ba történő beáramlása.

Az EU-t érő bizonyos kockázatok nagy valószínűséggel fokozódni fognak, amikor véget érnek a harcok, vagy a tűzszünetekben. Különös figyelmet kell fordítani a tűzfegyverek forgalmára, aminek a veszélye fokozódni fog, amint az Ukrajnában dúló harcok alábbhagynak. A múltbeli tapasztalatok arra a kockázatra is rámutatnak, hogy a visszatérő külföldi harcosok, akik tapasztalatot szereztek a harcban, és esetleg kapcsolatba kerültek szélsőséges csoportokkal, később esetleg terrorcselekményeket szervezhetnek az EU-ban. Ezt a potenciális jelenséget körültekintően figyelemmel kell kísérni, és a Bizottság már most arra ösztönzi a tagállamokat, hogy folytassanak megbeszéléseket az erőszakos szélsőséges háttérrel rendelkező visszatérő külföldi önkéntesek által jelentett kihívásokkal kapcsolatban.

E lehetséges fenyegetésekre tekintettel fontos, hogy folytatódjon a biztonsági unióra vonatkozó stratégia végrehajtása, többek között az olyan kulcsfontosságú stratégiák végrehajtásával, mint a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégia, a szervezett bűnözés leküzdésére irányuló stratégia (2020–2025), az EU terrorizmus elleni programja (2020–2025), a tűzfegyverek tiltott kereskedelmére vonatkozó uniós cselekvési terv (2020–2025), az emberkereskedelem elleni küzdelemre irányuló stratégia (2021–2025) és az EU 2021–2025-re szóló drogstratégiája.

Folytatódnak az erőfeszítések a szükséges uniós jogszabályi keret megteremtése érdekében. Például a Bizottság jelenleg a magas kockázatú vegyi anyagok forgalomba hozatalának és felhasználásának a szabályozására irányuló javaslat hatásvizsgálatának előkészítésén dolgozik.

IX. KÖVETKEZTETÉS

A biztonsági unió továbbra is betölti szerepét, és segít az EU-t és tagállamait felkészíteni a meglévő és potenciális fenyegetések kezelésére. Oroszország Ukrajna elleni agresszív háborúja rámutatott arra, hogy az elméleti fenyegetések milyen gyorsan valósággá válhatnak, és rámutat az éberség, a koordináció és a felkészültség fontosságára.

A biztonsági unióra vonatkozó stratégia végrehajtásáról szóló negyedik eredményjelentés azt mutatja, hogy az EU képes az alkalmazkodásra még olyan kivételes és váratlan fenyegetésekkel szembesülve is, mint amilyen Oroszország Ukrajna elleni agresszív háborúja. A biztonsági unióra vonatkozó stratégia határozott végrehajtása fontosabb, mint valaha.

alapján], OEDT, Egy heroint helyettesítő kábítószer illegális kereskedelmének megállítása Franciaországban, Lengyelországban és Ukrajnában, beleértve az ellenőrzött szállítás megtervezését és végrehajtását), 2021/00446, Eurojust, 2020. május.