EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.7.24.
COM(2020) 605 final

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

A biztonsági unióra vonatkozó uniós stratégia

I. Bevezetés

A Bizottság a politikai iránymutatásában egyértelművé tette, hogy minden követ meg kell mozgatnunk, ha a polgáraink védelméről van szó. A biztonság nem csupán személyes védelmünk alapja, hanem alapvető jogaink záloga is, amely megalapozza a gazdaságunkba, társadalmunkba és demokráciánkba vetett bizalmat, és lehetővé teszi a gazdaság, a társadalom és a demokrácia dinamikus működését. Az európai biztonsági környezet napjainkban folyamatosan változik: befolyásolják a változó fenyegetések, de egyéb tényezők is, mint például az éghajlatváltozás, a demográfiai tendenciák és a határainkon túli politikai instabilitás. Továbbra is jólétünk forrásai közé tartozik a globalizáció, a szabad mozgás és a digitális transzformáció – ezek megkönnyítik életünket, valamint serkentik az innovációt és a növekedést. Előnyeik mellett azonban számos kockázatot is hordoznak, és költségeket emésztenek fel. Kitesznek bennünket a terrorizmus, a szervezett bűnözés, a kábítószer-kereskedelem és az emberkereskedelem manipulációinak, amelyek közvetlen veszélyt jelentenek a polgárokra és az európai életmódunkra nézve. Hozzájárulnak a kibertámadások és a kiberbűncselekmények terjedéséhez. A biztonsági fenyegetések emellett egyre összetettebbé is válnak: ehhez táptalajt nyújt a határokon átnyúló munkavégzés lehetősége, az összekapcsoltság, a fizikai és a digitális világ közötti határok elmosódása, a veszélyeztetett csoportok megléte, valamint a társadalmi és gazdasági különbségek fennállása. Támadás bármely pillanatban előfordulhat, és az elkövetők nem mindig hagynak nyomot maguk után; állami és nem állami szereplők egyaránt különféle hibrid fenyegetések[1] forrásai lehetnek; és az EU belső biztonságát az EU-n kívüli események is döntően befolyásolhatják.

A biztonságról és a biztonsági fenyegetésekről alkotott fogalmaink, valamint a kapcsolódó szakpolitikák a Covid19-válság miatt is átalakulóban vannak. A járvány rávilágított arra, hogy garantálni kell fizikai és digitális környezetünk biztonságát egyaránt. Rámutatott, hogy a nyitott stratégiai autonómia nagy fontossággal bír az ellátási láncaink fenntartása szempontjából, legyen szó akár a kritikus termékekről, akár a szolgáltatásokról, infrastruktúrákról vagy technológiákról. Megerősítette, hogy erőfeszítéseinket valamennyi ágazatra és polgárra ki kell terjesztenünk ahhoz, hogy felkészültebbé és reziliensebbé váljunk, és sikeresebben felvértezzük magunkat a szükséges válaszlépésekhez.

A tagállamok nem képesek arra, hogy önálló fellépéssel egyedül megvédjék polgáraikat. Minden eddiginél fontosabb, hogy erősségeinkre építkezve együttműködjünk, és az EU minden eddiginél jobb helyzetben van ahhoz, hogy változást érjen el. Példát mutatva megerősítheti általános válságkezelési rendszerét, és határain belül és kívül egyaránt munkálkodhat a globális stabilitás megőrzésén. Jóllehet a biztonság elsősorban az egyes tagállamok felelőssége, az elmúlt években egyre világosabbá válik, hogy az egyik tagállam biztonsága az összes uniós tagállam biztonságát jelenti. Az EU lehetővé tudja tenni a multidiszciplináris és integrált válaszlépéseket, és képes a szükséges eszközökkel és információkkal támogatni a tagállamok biztonsági szereplőit[2].

---

[1] Bár a hibrid fenyegetés fogalma többféleképpen is meghatározható, lefedi mindazokat a kényszerítő és felforgató tevékenységeket és hagyományos és nem hagyományos (azaz diplomáciai, katonai, gazdasági, technológiai) módszereket, amelyeket állami vagy nem állami szereplők összehangolt módon felhasználhatnak bizonyos konkrét célok elérésére (úgy, hogy az még ne minősüljön hivatalosan elismert hadviselésnek). Lásd: JOIN(2016) 18 (final).

[2] Például az EU űrprogramjának szolgáltatásaival: a Kopernikusz többek között Föld-megfigyelési adatokat és alkalmazásokat biztosít a határőrizet, a tengeri védelem, a bűnüldözés, a kalóztámadások elleni fellépések, a kábítószer-csempészettől való elrettentés és a veszélyhelyzet-kezelés céljából.

Ezen túlmenően az EU képes biztosítani, hogy a biztonságpolitika továbbra is közös európai értékeinken – a jogállamiság, az egyenlőség[3] és az alapvető jogok tiszteletben tartásán és megőrzésén, valamint az átláthatóság, az elszámoltathatóság és a demokratikus ellenőrzés garantálásán – alapuljon, ami a szakpolitikákba vetett bizalom elengedhetetlen feltétele. Képes olyan hatékony és valódi biztonsági uniót kialakítani, amelyben az egyének jogai és szabadságai megfelelő védelmet élveznek. A biztonság célkitűzése nem ütközik az alapvető jogok tiszteletben tartásának céljával, sőt, összefér azzal és kiegészíti azt. A biztonságpolitikákat mindenképpen az értékeinkre és alapvető jogainkra kell alapoznunk, biztosítva a szükségesség, az arányosság és a jogszerűség elvét, valamint az elszámoltathatóság és a bírósági jogorvoslat megfelelő biztosítékait, lehetővé téve ugyanakkor, hogy az EU hatékony lépéseket tegyen az egyének – különösen a legsérülékenyebbek – védelmében.

Ehhez már most is jelentős jogi, gyakorlati és támogatási eszközök állnak a rendelkezésünkre, amelyeket azonban meg kell erősíteni és hatékonyabban végre kell hajtani. A tagállamokkal folytatott információcsere és hírszerzési együttműködés javítása, valamint a terroristák és bűnözők mozgásterének megszüntetése terén már eddig is jelentős előrelépés történt, a szétaprózódás azonban még nem szűnt meg.

A munkát az EU határain túlra is ki kell terjeszteni. Az Unió és polgárainak védelméhez már nem elég az EU határain belül garantálni a biztonságot – a biztonság külső dimenzióját is kezelni kell. Az EU-n belüli biztonság fokozására irányuló uniós erőfeszítéseknek továbbra is alapvető eleme marad a közös kül- és biztonságpolitika (KKBP) és a közös biztonság- és védelempolitika (KBVP) keretében kialakított, a külső biztonságra vonatkozó uniós megközelítés. A hatékony és átfogó reagálásban központi szerepet játszik a közös kihívások kezelésére irányuló, harmadik országokkal folytatott és globális szintű együttműködés, mivel az EU saját biztonsága szempontjából kritikus fontossággal bír, hogy szomszédságában stabilitás és biztonság uralkodjon.

Ez az új stratégia, amely az Európai Parlament[4], a Tanács[5] és a Bizottság[6] eddigi munkájára épül, bemutatja, hogy a valódi és hatékony biztonsági uniónak szilárd eszközkészletet és politikákat kell tartalmaznia a biztonság gyakorlati megvalósítására, ugyanakkor arra a felismerésre kell épülnie, hogy a biztonság a társadalom és a közrend valamennyi részét érinti. Az EU-nak mindenki számára biztonságos környezetet kell biztosítania, faji vagy etnikai származástól, vallástól, meggyőződéstől, nemtől, kortól vagy szexuális irányultságtól függetlenül.

Ez a stratégia a 2020–2025 közötti időszakra vonatkozik, és elsődleges célja az időtálló biztonsági környezet biztosításához szükséges képességek és kapacitások kiépítése. Olyan, a társadalom egészére kiterjedő biztonsági megközelítést határoz meg, amely képessé tesz bennünket arra, hogy hatékonyan és összehangoltan reagáljunk a gyorsan változó fenyegetettségi helyzetre. Meghatározza azokat a stratégiai prioritásokat és kapcsolódó

[3] Az egyenlőségközpontú Unió: a 2020–2025 közötti időszakra szóló nemi esélyegyenlőségi stratégia, COM(2020)152.

[4] Példa erre az Európai Parlament TERR bizottságának munkája, amely 2018 novemberében terjesztette elő beszámolóját.

[5] Kezdve a megújított belső biztonsági stratégiáról szóló, 2015. júniusi tanácsi következtetésektől a Tanács legutóbbi, 2019. decemberi ülésének eredményeiig.

[6] „Az európai biztonsági stratégia megvalósítása a terrorizmus elleni küzdelem és a hatékony és valódi biztonsági unió előkészítésének érdekében”, COM (2016) 230 final, 2016.4.20. Lásd még a belső biztonsági jogszabályok végrehajtásának közelmúltbeli értékelését: A belső biztonság területére vonatkozó belügyi jogszabályok végrehajtása – 2017–2020 (SWD(2020) 135).

intézkedéseket, amelyek segítenek integrált módon kezelni a digitális és fizikai kockázatokat a biztonsági unió egész ökoszisztémájában, és azokra a területekre összpontosít, amelyeken az EU további értéket tud teremteni. Valódi biztonsági hozadékot kíván teremteni az EU valamennyi polgárának védelméhez.

II. Gyorsan változó európai biztonsági fenyegetettségi helyzet

A polgárok biztonsága, prosperitása és jólléte azon múlik, hogy biztonságban vannak-e. A biztonságukat fenyegető veszélyek összefüggnek azzal, hogy mennyire sebezhető az életük és a megélhetésük. Minél sebezhetőbb, annál könnyebb ezt kihasználni. A sebezhetőségek és a fenyegetések egyaránt folyamatosan változnak, és az EU-nak alkalmazkodnia kell ehhez.

Mindennapi életünkben számos szolgáltatás nélkülözhetetlen, többek között az energetika, a közlekedés, a pénzügy vagy az egészségügy területén. Ezek a szolgáltatások nemcsak fizikai, hanem digitális infrastruktúrákon is alapulnak, ami növeli sebezhetőségünket és a fennakadások lehetőségét. Számos vállalkozás és közszolgáltatás az új technológiáknak köszönheti életben maradását a Covid19-világjárvány során: ezek biztosítják a távmunkázók számára a kapcsolattartást, és tartják fenn az ellátási láncok logisztikáját. Ebben a helyzetben azonban a kártékony támadások száma is rendkívüli módon megnövekedhetett: sokan próbálnak bűncselekmények céljából előnyt kovácsolni a világjárvány okozta zavarból és a digitális otthoni munkavégzés térnyeréséből[7]. Az áruhiány is új lehetőséget teremt a szervezett bűnözés számára. Mindez akár végzetesen is alakulhatott volna, a legnagyobb nyomás idején az alapvető egészségügyi szolgáltatások megbénulását okozva.

Mivel a digitális technológiák egyre több módon szolgálják az életünket, stratégiai jelentőségűvé vált a technológiáink **kiberbiztonsága** is[8]. A kibertámadások súlyosan érintik a háztartásokat, a bankokat, a pénzügyi szolgáltatásokat és a vállalkozásokat (kis- és középvállalkozásokat). A potenciális károkat tovább súlyosbítja, hogy a fizikai és a digitális rendszerek kölcsönösen függnek egymástól: a fizikai behatások szükségszerűen hatással vannak a digitális rendszerekre is, míg az információs rendszerekre és a digitális infrastruktúrákra irányuló kibertámadások akár az alapvető szolgáltatásokat is megbéníthatják[9]. A dolgok internetének terjedése és a mesterséges intelligencia fokozott használata új előnyöket fog nyújtani, de új veszélyeket is teremt.

Világunkat nagy mértékben behálózzák a digitális infrastruktúrák, technológiák és online rendszerek – lehetővé teszik, hogy üzleti vállalkozásokat hozzunk létre, termékeket fogyasszunk és szolgáltatásokat vegyünk igénybe. E rendszerek mindegyike kommunikáción és interakción alapul. A hálózati függőség utat nyit a **kiberbűnözési** hullám

---

[7] Europol: Túl a világjárványon. Hogyan alakítja a Covid19-járvány a súlyos és a szervezett bűnözést az EU-ban? (2020. április).

[8] A Bizottság ajánlása az 5G hálózatok kiberbiztonságáról, C(2019) 2335. Közlemény: Az 5G biztonságos kiépítése az EU-ban – Az uniós eszköztár alkalmazása, COM(2020) 50.

[9] 2020 márciusában Csehországban számítógépes támadás érte a brnói egyetemi kórházat, amely emiatt kénytelen volt a betegeket máshová irányítani és műtéteket halasztani (Europol: Haszonszerzés a pandémiából: Hogyan használják ki a bűnözők a Covid19-válságot?). A mesterséges intelligencia felhasználható digitális, politikai és fizikai támadások végrehajtására és megfigyelések végzésére. A tárgyak internetével kapcsolatos adatgyűjtés (intelligens órák, virtuális asszisztensek stb.) szintén használható az egyének megfigyelésére.

előtt[10]. A „kiberbűnözési szolgáltatásoknak” és a földalatti kiberbűnözési gazdaságnak köszönhetően könnyű hozzáférni az interneten a kiberbűnözési termékekhez és szolgáltatásokhoz. A bűnözők gyorsan alkalmazkodnak a változásokhoz, és saját céljaikra fordítják az új technológiákat. A legális gyógyszerellátási láncba például beszivárognak a hamisított gyógyszerek[11]. Ugrásszerűen szaporodnak a gyermekek szexuális zaklatását ábrázoló internetes anyagok[12], ami arra utal, hogy a változó bűnözési minták társadalmi következményekkel is járnak. Egy közelmúltbeli felmérés szerint az EU lakosságának többsége (55 %) attól tart, hogy a bűnözők és csalók hozzáférhetnek az adataihoz[13].

Ezeket a fenyegetéseket még hangsúlyosabbá teszi a **globális környezet**. A harmadik országok magabiztos iparpolitikája és a kibertechnológiával elkövetett folyamatos szellemitulajdon-lopás együttesen átalakítja az európai érdekek védelmére és előmozdítására alkalmazandó stratégiai paradigmát. Ezt tovább erősíti a kettős felhasználású alkalmazások térnyerése, ami az erős polgári technológiai ágazatot a védelmi és biztonsági képességek erős eszközévé teszi. Az ipari kémkedés jelentősen érinti az uniós gazdaságot, foglalkoztatást és növekedést: az üzleti titkok kibertechnológiával elkövetett lopása a becslések szerint 60 milliárd EUR-val károsítja meg az EU-t[14]. Alaposan át kell tehát gondolnunk, hogy a függőségek és a kiberfenyegetéseknek való fokozott kitettség nyomán mennyire képes az EU megvédeni az egyéneket és a vállalkozásokat.

A Covid19-válság rámutatott arra is, hogy a társadalmi megosztottság és a bizonytalanság biztonsági sebezhetőséget eredményez. Megnövekszik az állami és nem állami szereplők által indítható kifinomultabb és **hibrid támadások** lehetősége, amelyek során a sebezhetőségeket kibertámadásokkal, a kritikus infrastruktúra[15] megrongálásával, félretájékoztatási kampányokkal és a politikai narratívák radikalizálásával használják ki.[16]

Van ugyanakkor több olyan régebbi fenyegetés is, amely továbbra is fejlődik. Jóllehet 2019-ben némileg visszaszorultak a **terrortámadások** az EU-ban, az Iszlám Állam, az al-Kaida és szövetségeseik által indított vagy ihletett dzsihádista támadások továbbra is komoly fenyegetést jelentenek az uniós polgárok számára[17]. Ezzel párhuzamosan erősödik a szélsőjobboldali erőszak veszélye is[18]. A rasszista indíttatású támadásokat nagyon komolyan kell venni: a Hallében elkövetett halálos kimenetelű antiszemita terrortámadások felhívták a

---

[10] Egyes előrejelzések szerint az adatvédelmi incidensek költsége 2024-re eléri az évi 5 billió USD-t, szemben a 2015. évi 3 billió USD-vel (Juniper Research: A kiberbűnözés és a biztonság jövője).

[11] Egy 2016. évi tanulmány (Legiscript) szerint az internetes gyógyszertáraknak világszerte csak 4 %-a működik jogszerűen, míg a 30 000–35 000 illegális online gyógyszertár első számú célpontjai az uniós fogyasztók.

[12] A gyermek szexuális zaklatásával szembeni hatékonyabb küzdelemre vonatkozó uniós stratégia, COM(2020) 607.

[13] Az Európai Unió Alapjogi Ügynöksége (2020), Az Ön jogai fontosak: Biztonsági aggályok és tapasztalatok, alapjogi felmérés, Luxembourg, Kiadóhivatal.

[14] Az ipari kémkedés és az üzleti titkok kibertechnológiával elkövetett lopásának kiterjedése és hatása, 2018.

[15] A kritikus infrastruktúrák elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, és megzavarásuk vagy megsemmisítésük jelentős következményekkel jár (2008/114/EK tanácsi irányelv).

[16] Az uniós polgárok 97 %-a szembesült már álhírrel, 38 %-uk naponta találkozik vele. Lásd: JOIN (2020) 8 final.

[17] 13 uniós tagállam összesen 119 befejezett, sikertelen és meghiúsított terrortámadásról számolt be, melyek összesen tíz halálesettel és 27 sérüléssel jártak (Europol, Európai uniós jelentés a terrorizmus helyzetéről és tendenciáiról, 2020).

[18] 2019-ben hat jobboldali terrortámadás történt (három tagállamban: egy befejezett, egy sikertelen, négy meghiúsított), ezzel szemben 2018-ban mindössze egyetlen eset fordult elő; ezen túlmenően további halálos áldozatot követeltek olyan esetek, amelyeket hivatalosan nem minősítettek terrorizmusnak (Europol, 2020).

figyelmet arra, hogy az ilyen támadások ellen a 2018. évi tanácsi nyilatkozattal összhangban fokozni kell a fellépést[19]. Az EU-ban minden ötödik ember tart attól, hogy a következő 12 hónapban terrortámadás történik[20]. A közelmúltbeli terrortámadások túlnyomó többségéhez nem volt szükség csúcstechnológiai eszközökre – nyilvános helyszíneken magányos elkövetők vettek célba embereket –, viszont a christchurch-i támadások élő közvetítésével az internetes terrorista propaganda új dimenzióba lépett[21]. A radikalizálódott személyek jelentette fenyegetés továbbra is magas, amit potenciálisan tovább erősítenek a visszatérő külföldi terrorista harcosok és a börtönből szabaduló szélsőségesek[22].

A válság rávilágított továbbá, hogy az új körülmények között a már meglévő fenyegetések is más irányt vehetnek. A **szervezett bűnözői** csoportok az áruhiányt kihasználva új illegális piacokat hoztak létre. A legnagyobb bűnözői piac az EU-ban továbbra is a tiltott kábítószerek kereskedelme – kiskereskedelmi értéke a becslések szerint évente legalább 30 milliárd EUR[23]. Változatlanul problémát jelent az emberkereskedelem is: a becslések szerint a kizsákmányolás különböző formáiból származó éves globális nyereség megközelíti a 30 milliárd EUR-t[24]. A hamisított gyógyszerek nemzetközi kereskedelme nagysága elérte a 38,9 milliárd EUR-t[25]. Ugyanakkor az elkobzások alacsony aránya lehetővé teszi, hogy a bűnözők tovább bővítsék bűnözői tevékenységeiket és beszivárogjanak a legális gazdaságba[26]. Lőfegyverhez szintén könnyebb hozzájutni: a bűnözők és a terroristák az online piacokon szerezhetik be ezeket, vagy akár igénybe vehetik az olyan új technológiákat, mint a háromdimenziós nyomtatás[27]. A mesterséges intelligenciával, az új technológiákkal és a robotikával tovább nő annak a kockázata, hogy a bűnözők kártékony célok szolgálatába állítják az innovációt[28].

Ezek a fenyegetések egyszerre több kategóriát is felölelnek, és különbözőképpen érintik a társadalom különböző rétegeit. Mindegyikük komoly fenyegetést jelent az egyénekre és a vállalkozásokra nézve, és átfogó és koherens uniós szintű választ igényel. Amikor az olyan kisebb, összekapcsolt háztartási eszközök is biztonsági sebezhetőséget eredményezhetnek, mint az internetre csatlakoztatott hűtőszekrény vagy kávéfőző, akkor biztonságunk garantálásához már nem elegendőek a hagyományos állami szereplők. A gazdasági szereplőknek nagyobb felelősséget kell vállalniuk az általuk forgalomba hozott termékek és szolgáltatások kiberbiztonságáért, miközben az egyéneknek is legalább alapszintű kiberbiztonsági ismeretekkel kell rendelkezniük ahhoz, hogy képesek legyenek megvédeni magukat.

---

19 Lásd még az antiszemitizmus elleni küzdelemről és az európai zsidó közösségek és intézmények hatékonyabb védelmének közös biztonsági megközelítésének kidolgozásáról szóló tanácsi nyilatkozatot.

20 Az Európai Unió Alapjogi Ügynöksége: Az Ön jogai fontosak: Biztonsági aggályok és tapasztalatok, 2020.

21 2015 júliusától 2019 végéig az Europol 361 platformon talált terrorista tartalmat (Europol, 2020).

22 Europol: A börtönökben zajló radikalizálódás és a terroristák visszaesése elleni küzdelem legjobb transzatlanti gyakorlatainak felülvizsgálata, 2019.

23 Az EMCDDA és az Europol 2019. évi jelentése az EU kábítószerpiacáról.

24 Az Europol emberkereskedelemről szóló jelentése, Financial Business Model (2015).

25 Az Európai Unió Szellemi Tulajdoni Hivatala és az OECD jelentése a hamisított gyógyszerkészítmények kereskedelméről

26 Jelentés – Vagyonvisszaszerzés és elkobzás: Annak biztosítása, hogy a bűnelkövetés ne legyen kifizetődő tevékenység, COM(2020) 217.

27 2017-ben a terrortámadások 41 %-a lőfegyverrel történt (Europol, 2018).

28 2020 júliusában a francia és a holland bűnüldöző és igazságügyi hatóságok, valamint az Europol és az Eurojust közös nyomozásról számoltak be, amely az erőszakos támadásokban, korrupcióban, gyilkossági kísérletekben és nagy volumenű kábítószer-szállításban részt vevő bűnözői hálózatok által használt EncroChat titkosított telefonhálózat felszámolására irányult.

III. Összehangolt uniós válaszlépések a társadalom egésze érdekében

Az EU már megmutatta, hogy képes valódi hozzáadott értéket teremteni. 2015 óta a biztonsági unió új kapcsolatokat alakított ki a biztonsági politikák uniós szintű kezelése terén. Még mindig sok azonban a teendő az egész társadalom bevonása terén, beleértve a különböző szintű kormányzatokat, az összes ágazatban működő vállalkozásokat és valamennyi tagállam polgárait. Ahogy egyre inkább tudatosul bennünk, hogy a függőség kockázatokkal jár[29] és erős európai iparstratégiára van szükségünk[30], egyre világosabbá válik, hogy az EU-ban meg kell teremteni a kritikus mértékű rezilienciát az ipar, a technológiai termelés és az ellátási lánc területén. Az erő azt is jelenti, hogy teljes mértékben tiszteletben kell tartanunk az alapvető jogokat és az uniós értékeket – ezek ugyanis előfeltételei a legitim, hatékony és fenntartható biztonsági politikáknak. Ez a biztonsági unióra vonatkozó stratégia konkrét munkaterületeket határoz meg a további lépések tekintetében. A stratégia a következő közös célkitűzésekre épül:

- ***A válságok korai felismeréséhez, megelőzéséhez és gyors kezeléséhez szükséges képességek és kapacitások kiépítése:*** Európának reziliensebbé kell válnia ahhoz, hogy megelőzze a jövőbeli sokkhatásokat, kivédje azokat és ellenálljon azokkal szemben. A meglévő eszközökből és kezdeményezésekből kiindulva integrált és összehangolt megközelítéssel ki kell építenünk a biztonsági válságok korai felismeréséhez és gyors kezeléséhez szükséges képességeket és kapacitásokat, mind globális szinten, mind az ágazatspecifikus (például a pénzügyi, energetikai, igazságügyi, bűnüldözési, egészségügyi, tengeri és közlekedési ágazatra vonatkozó) kezdeményezések szintjén[31]. A Bizottság emellett javaslatokat fog előterjeszteni egy EU-n belüli széles körű válságkezelési rendszerre, amely szintén mérvadó lehet a biztonság szempontjából.
- ***Eredményközpontúság:*** Annak érdekében, hogy erőfeszítéseinket a lehető leghatékonyabban összpontosítsuk, olyan teljesítményorientált stratégiát kell kialakítanunk, amely a fenyegetések és kockázatok körültekintő értékelésén alapul. A stratégiában megfelelő szabályokat és eszközöket kell meghatározni, és alkalmazni kell azokat. Az uniós biztonságpolitikákat megbízható stratégiai információgyűjtésre kell alapozni. Amennyiben uniós jogalkotásra van szükség, azt a teljes körű végrehajtás érdekében nyomon kell követni, hogy elkerülhető legyen a széttagoltság és a kiskapuk kihasználása. A stratégia végrehajtásának hatékonysága attól is függ majd, hogy a következő, 2021–2027-es programozási időszakban elegendő finanszírozási forrás áll-e rendelkezésre e célokra, többek között a kapcsolódó uniós ügynökségek tekintetében.
- ***Az állami és a magánszektor valamennyi szereplőjének bevonása a közös erőfeszítésbe:*** Az állami és a magánszektor kulcsfontosságú szereplői nemzetbiztonsági vagy versenyképességi okokból nem szívesen adnak közre biztonsággal kapcsolatos információkat.[32] Pedig akkor vagyunk a leghatékonyabbak, ha mindent megteszünk

[29] A külföldtől való függés kockázata fokozottan kitesz bennünket különböző potenciális veszélyeknek, kezdve az informatikai infrastruktúrák sebezhetőségétől – amely veszélyezteti a kritikus (pl. energetikai, közlekedési, banki, egészségügyi) infrastruktúrákat – az ipari vezérlőrendszerek irányíthatóságán át a könnyebb adatlopásig vagy kémkedésig.

[30] A Bizottság közleménye – Új európai iparstratégia, COM(2020) 102.

[31] Ilyen például az uniós politikai szintű integrált válságelhárítási mechanizmus (IPCR), a Veszélyhelyzet-reagálási Koordinációs Központ, a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló bizottsági ajánlás (C(2017) 6100), valamint a hibrid fenyegetések elleni fellépés uniós operatív protokollja (EU Playbook, SWD (2016) 227).

[32] Lásd: Közös közlemény – Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése, JOIN(2017) 450.

egymás támogatására. Ez mindenekelőtt azt jelenti, hogy szorosabbra kell fűzni a tagállamok közötti – például a bűnüldöző, igazságügyi és egyéb hatóságok közötti –, valamint az uniós intézmények és ügynökségek közötti együttműködést annak érdekében, hogy biztosítsuk a közös megoldásokhoz szükséges ismereteket és információcserét. Kulcsfontosságú a magánszektorral való együttműködés is, annál is inkább, mert a bűnözés és a terrorizmus elleni hatékony küzdelemben központi szerepet játszó digitális és nem digitális infrastruktúraik a nagy része az ipar kezében van. A célok eléréséhez a magánszemélyek is hozzájárulhatnak, például azáltal, hogy fejlesztik a számítástechnikai bűnözés és a félretájékoztatás elleni fellépéshez szükséges készségeiket és tudatosságukat. Végezetül e közös erőfeszítésnek túl kell mutatnia határainkon, és szorosabb kapcsolatokat kell kiépíteni más, hasonlóan gondolkodó partnerekkel.

IV. Mindenki védelme az EU-ban: A biztonsági unió stratégiai prioritásai

Az EU kivételesen kedvező helyzetben van ahhoz, hogy ezekre az új globális fenyegetésekre és kihívásokra reagáljon. A fenti fenyegetettség-elemzés négy, egymástól kölcsönösen függő stratégiai prioritásra mutat rá, amelyeket uniós szinten kell megvalósítani, az alapvető jogok teljes körű tiszteletben tartása mellett: 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.

1. Időtálló biztonsági környezet

A kritikus infrastruktúrák védelme és rezilienciája

Az egyének mindennapi életük során különböző kulcsfontosságú infrastruktúrákra támaszkodnak: utaznak, dolgoznak, igénybe veszik az olyan alapvető közszolgáltatásokat, mint a kórházak, a közlekedés, az energiaellátás vagy demokratikus jogaik gyakorlása. Ha ezek az infrastruktúrák nem kellően védettek és reziliensek, a – fizikai vagy digitális – támadások hatalmas fennakadásokat okozhatnak az egyes tagállamokban, sőt potenciálisan az egész EU-ban is.

A létfontosságú infrastruktúrák védelmére és rezilienciájára vonatkozó jelenlegi uniós keret[33] nem tart lépést a változó kockázatokkal. A kölcsönös függőség fokozódása azt jelenti, hogy az egy-egy ágazatban bekövetkező zavarok azonnali hatással lehetnek a többi ágazatban zajló műveletekre: a villamosenergia-termelés elleni támadás ellehetetlenítheti a távközlést, a kórházakat, a bankokat vagy a repülőtereket, míg a digitális infrastruktúra elleni támadás zavarokat okozhat az energia- vagy a finanszírozási hálózatokban. Ahogy gazdaságunk és társadalmunk egyre jobban az internet felé fordul, egyre komolyabbak ezek a kockázatok. Ezt a fokozott összekapcsoltságot és kölcsönös függőséget a jogszabályi keretnek a kritikus infrastruktúrák védelmére és rezilienciájára irányuló erőteljes digitális és fizikai intézkedésekkel kell kezelnie. Az alapvető szolgáltatásokat – beleértve az űrinfrastruktúrán alapulókat is – megfelelően védeni kell a jelenlegi és a várható fenyegetésekkel szemben, miközben azoknak reziliensnek is kell lenniük. Ez azt jelenti, hogy a rendszernek képesnek kell lennie a nemkívánatos eseményekre való felkészülésre,

[33] (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19.); a Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.

azok tervezésére, hatásaik enyhítésére, az azokból való felépülésre és az azokhoz való sikeresebb alkalmazkodásra.

Ugyanakkor a tagállamok mérlegelési jogkörükkel élve különbözőképpen hajtják végre a meglévő jogszabályokat. Az ebből eredő széttöredezettség alááshatja a belső piacot, és megnehezítheti a határokon átnyúló koordinációt – a legnyilvánvalóbb módon a határ menti régiókban. A különböző tagállamokban alapvető szolgáltatásokat nyújtó szereplőknek különböző jelentéstételi rendszereknek kell megfelelniük. A Bizottság jelenleg vizsgálja, hogy **a fizikai és a digitális infrastruktúrákra vonatkozó új keretek** következetesebb és koherensebb megközelítést jelentenének-e az alapvető szolgáltatások megbízható nyújtásához. Ezt a keretet **ágazatspecifikus kezdeményezéseknek** kell kísérniük a kritikus infrastruktúrák – például a közlekedés, az energia, a pénzügyek és az egészségügy – jelentette sajátos kockázatok kezelését illetően[34]. Tekintettel a pénzügyi szektor informatikai szolgáltatásoktól való nagy fokú függőségére és a kibertámadásokkal szembeni nagy fokú sebezhetőségére, az első lépés a pénzügyi szektorok digitális működési reziliencájára vonatkozó kezdeményezés lesz. Az energiarendszer különleges érzékenysége és hatása miatt a Bizottság célzott kezdeményezéssel fogja támogatni a kritikus energiainfrastruktúra fizikai, kiber- és hibrid fenyegetésekkel szembeni rezilienciájának erősítését, egyenlő versenyfeltételeket biztosítva a határokon átnyúló energiaszolgáltatók számára.

A kritikus infrastruktúrákat vagy kritikus technológiákat potenciálisan érintő közvetlen külföldi befektetések biztonsági vonatkozású hatásai szintén értékelésre kerülnek, mégpedig az uniós tagállamok és a Bizottság által a közvetlen külföldi befektetések átvilágítására vonatkozó új európai keretrendszer keretében végzett értékelések részeként[35].

Az EU új eszközöket is kiépíthet a kritikus infrastruktúrák rezilienciájának támogatására. A globális internet eddig nagy fokú rezilienciáról tett tanúbizonyságot, különösen a megnövekedett forgalom támogatására való képesség tekintetében. Fel kell azonban készülnünk arra, hogy a jövőben válságok fenyegethetik az internet biztonságát, stabilitását és rezilienciáját. Ahhoz, hogy az internet továbbra is működjön, szilárdan fel kell lépni a kiberbiztonsági eseményekkel és a kártékony online tevékenységekkel szemben, és korlátozni kell az Európán kívüli infrastruktúráktól és szolgáltatásoktól való függőséget. Ehhez szükség lesz jogalkotásra – többek között felül kell vizsgálni a hatályos szabályokat annak érdekében, hogy az EU-ban egységesen magas szinten biztosítható legyen a hálózati és információs rendszerek biztonsága –; fokozott kutatási és innovációs beruházásokra; valamint az alapvető internetes infrastruktúrák és erőforrások, különösen a domainnév-rendszer kiépítésének vagy szigorításának vizsgálatára[36].

---

[34] Mivel az egészségügyet különösen súlyosan érinti a Covid19-válság, a Bizottság olyan kezdeményezéseket is fontolóra vesz, amelyek megerősítik az EU egészségbiztonsági keretét és a felelős uniós ügynökségeket annak érdekében, hogy hatékonyabban tudjanak reagálni a határokon átnyúló súlyos egészségügyi veszélyekre.

[35] Miután az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról szóló, 2019. március 19-i (EU) 2019/452 európai parlamenti és tanácsi rendelet 2020. október 11-én teljes körűen alkalmazandóvá válik, ez új együttműködési mechanizmussal fogja felruházni az EU-t a határain kívülről érkező olyan közvetlen befektetésekre vonatkozóan, amelyek valószínűleg hatást gyakorolnak a biztonságra vagy a közrendre. A rendelet értelmében a tagállamok és a Bizottság felmérik az ilyen közvetlen külföldi befektetésekhez kapcsolódó potenciális kockázatokat, és mérséklésükre – amennyiben helyénvaló és egynél több tagállam esetében releváns – megfelelő eszközöket javasolnak.

[36] A domainnévrendszer (DNS) az internethez vagy magánhálózathoz csatlakozó számítógépek, szolgáltatások vagy egyéb erőforrások hierarchikus és decentralizált elnevezési rendszere. A rendszer a doménneveket a számítógépes szolgáltatások és eszközök megtalálásához és azonosításához szükséges IP-címekre fordítja le.

A kulcsfontosságú uniós és nemzeti digitális eszközök védelmének egyik fő eleme a kritikus infrastruktúrák biztonságos kommunikációját lehetővé tevő csatorna biztosítása. A Bizottság együttműködik a tagállamokkal annak érdekében, hogy – az űrprogramról szóló rendeletben[37] meghatározott biztonságos kormányzati műholdas kommunikációs rendszerrel együtt – létrejöjjön egy tanúsított, végponttól végpontig terjedő, földi és űralapú kvantuminfrastruktúra.

Kiberbiztonság

A kibertámadások száma egyre emelkedik[38]. Ezek a támadások kifinomultabbak, mint valaha, számos forrásból származnak az Unión belülről és kívülről egyaránt, és azokat a területeket célozzák meg, ahol a legnagyobb a kiszolgáltatottság. A támadásokban gyakran az állami vagy államilag támogatott szereplők is érintettek, és olyan kulcsfontosságú digitális infrastruktúrák jelentik a célpontot, mint a nagy felhőszolgáltatók[39]. A kiberkockázatok a pénzügyi rendszerre nézve is jelentős fenyegetést jelentenek. A Nemzetközi Valutaalap becslése szerint a kibertámadásoknak betudható éves veszteség a bankok nettó jövedelmének 9 %-a, azaz megközelítőleg 100 milliárd USD[40]. Az összekapcsolt eszközökre való átállás jelentős előnyökkel jár a felhasználók számára: mivel azonban így kevesebb adatot tárolnak és dolgoznak fel az adatközpontokban, és az adatfeldolgozás a felhasználókhoz közelebb, a „peremen”[41] zajlik, már nem lesz elég, ha a kiberbiztonság csak a központi pontok védelmére összpontosít[42].

Az EU 2017-ben olyan kiberbiztonsági megközelítést terjesztett elő, amelynek középpontjában a rezilienciaépítés, a gyors reagálás és a hatékony elrettentés áll[43]. Az EU-nak most gondoskodnia kell arról, hogy kiberbiztonsági képességei megfeleljenek napjaink kívánalmainak, és alkalmasak legyenek arra, hogy biztosítsák a rezilienciát és a reagálást egyaránt. Ehhez egy, ténylegesen a társadalom egészére kiterjedő megközelítésre van szükség, amelynek keretében az uniós intézmények, ügynökségek és szervek, valamint a tagállamok, az ipar, a tudományos élet és az egyének a kiberbiztonság kérdését az azt megillető fontossággal kezelik[44]. Ezt a horizontális megközelítést újfent ágazatspecifikus kiberbiztonsági megközelítésekkel kell kiegészíteni az olyan területeken, mint az energia, a pénzügyi szolgáltatások, a közlekedés vagy az egészségügy. Az uniós munka következő szakaszát egy felülvizsgált európai kiberbiztonsági stratégiában kell összefoglalni.

A hírszerző szolgálatok, az EU INTCEN és a biztonsággal foglalkozó egyéb szervezetek közötti együttműködés új és korszerűbb formáinak feltárását a kiberbiztonság fokozására,

---

37 Rendeletjavaslat az Unió űrprogramjának és Az Európai Unió Űrprogramügynökségének a létrehozásáról, COM(2018) 447.

38 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

39 Az elosztott szolgáltatásmegtagadási támadások továbbra is állandó fenyegetést jelentenek: több jelentős szolgáltatónak is fel kellett már lépnie nagyszabású elosztott szolgáltatásmegtagadási támadás ellen, mint amilyen például az Amazon Web Services elleni 2020. februári támadás is volt.

40 https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

41 A pereminformatika (edge computing) olyan elosztott, nyitott IT-architektúra, amelynek jellemzője a decentrális adatfeldolgozási kapacitás, és amely lehetővé teszi a mobil számítástechnika és a dolgok internete (IoT) technológiákat. A pereminformatika keretében az adatokat maga az eszköz vagy egy helyi személyi számítógép vagy szerver dolgozza fel közvetlenül, anélkül, hogy az adatok átkerülnének egy számítógépközpontba.

42 Közlemény az európai adatstratégiáról, COM(2020) 66 final.

43 Közös közlemény – Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése, JOIN(2017) 450.

44 A Közös Kutatóközpont „Kiberbiztonság – a digitális világunk alapja” című jelentése többdimenziós betekintést nyújt a kiberbiztonság elmúlt 40 évben tapasztalt térnyerésébe.

valamint a terrorizmus, a szélsőségesség, a radikalizmus és a hibrid fenyegetések elleni küzdelemre irányuló erőfeszítések részévé kell tenni.

Tekintettel arra, hogy egész Európában folyamatban van az **5G infrastruktúra** terjeszkedése, és számos kritikus szolgáltatás potenciálisan az 5G hálózatoktól függ, e hálózatok rendszerszintű és széles körű zavarai különösen súlyos következményekkel járhatnak. Az 5G hálózatok kiberbiztonságáról szóló 2019. évi bizottsági ajánlás[45] által bevezetett folyamat eredményeként egyes tagállamok már fellépéseket hajtottak végre az 5G eszköztárban[46] meghatározott kulcsfontosságú intézkedésekkel kapcsolatban.

Az egyik legfontosabb hosszú távú szükséglet a **beépített kiberbiztonság** kultúrájának kialakítása, ami azt jelenti, hogy a biztonságot kezdettől fogva be kell építeni a termékekbe és szolgáltatásokba. Ezt jelentősen elősegíti majd a kiberbiztonsági jogszabály[47] keretében létrehozandó új kiberbiztonsági tanúsítási keretrendszer. A keretrendszer kidolgozása már folyamatban van: két tanúsítási rendszer már előkészítés alatt áll, és a további rendszerek prioritásait még ebben az évben meghatározzák. Ezen a területen kulcsfontosságú az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), az adatvédelmi hatóságok és az Európai Adatvédelmi Testület közötti együttműködés[48].

A Bizottság már megállapította, hogy a strukturált és összehangolt operatív együttműködés biztosítása érdekében szükség van egy **közös kiberbiztonsági egység** létrehozására. Ez magában foglalhatna egy válsághelyzet esetén igénybe vehető uniós szintű kölcsönös segítségnyújtási mechanizmust. A tervezetre vonatkozó ajánlás[49] végrehajtására építve a közös kiberbiztonsági egység kialakíthatná a bizalmat az európai kiberbiztonsági ökoszisztéma különböző szereplői között, és kulcsfontosságú szolgáltatást nyújthatna a tagállamok számára. A Bizottság megbeszéléseket fog kezdeményezni az érdekelt felekkel (kezdve a tagállamokkal), és 2020 végéig egyértelműen meghatározza a folyamatot, a mérföldköveket és az ütemtervet.

Szintén fontos a valamennyi uniós intézmény, szerv és ügynökség által alkalmazandó, az információbiztonságra és a kiberbiztonságra vonatkozó közös szabályok meghatározása. A cél a valamennyi uniós intézményen, szerven és ügynökségen belül alkalmazandó, a biztonságos információcserére és a digitális infrastruktúrák és rendszerek biztonságára vonatkozó kötelező és magas szintű közös normák létrehozása. Ennek az új keretnek elő kell segítenie az uniós intézmények, szervek és ügynökségek közötti erős és hatékony operatív együttműködést a kiberbiztonság terén, amelynek középpontjában a hálózatbiztonsági vészhelyzeteket elhárító csoportnak (CERT-EU) az uniós intézmények, szervek és ügynökségek tekintetében betöltött szerepe áll.

A kibertámadások globális jellege miatt alapvető fontosságú a szilárd **nemzetközi partnerségek** kiépítése és fenntartása a kibertámadások további megelőzése, az ilyen támadásoktól való elrettentés és az azokra való reagálás szempontjából. A rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete

[45] A Bizottság ajánlása az 5G hálózatok kiberbiztonságáról, COM(2019) 2335 final. Az ajánlás felülvizsgálata 2020 utolsó negyedévére várható.

[46] Lásd a Kiberbiztonsági Együttműködési Csoport 2020. július 24-i jelentését az eszköztár végrehajtásáról.

[47] (EU) 2019/881 rendelet az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról (kiberbiztonsági jogszabály).

[48] Közlemény – A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve, COM(2020) 264.

[49] A Bizottság (EU) 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról.

(„kiberdiplomáciai eszköztár”)[50] intézkedéseket határoz meg a közös kül- és biztonságpolitika keretében, beleértve az EU politikai, biztonsági és gazdasági érdekeit sértő tevékenységek elleni fellépést szolgáló korlátozó intézkedéseket (szankciókat). Az EU-nak a fejlesztési és együttműködési alapok révén is el kell mélyítenie kapacitásépítési munkáját annak érdekében, hogy támogassa a partnerállamokat digitális ökoszisztémáik megerősítésében, a nemzeti jogalkotási reformjaik elfogadásában és a nemzetközi normák betartásában. Ez növeli az egész közösség rezilienciáját és a kiberfenyegetések elleni küzdelemre és az azokra történő hatékony reagálásra való képességét. Ide tartozik a szomszédságpolitikában részt vevő partnerországok kiberbiztonságának növelését célzó uniós szabványok és vonatkozó jogszabályok előmozdítására irányuló konkrét munka is[51].

A nyilvános terek védelme

A közelmúltbeli terrortámadások a **nyilvános terekre** – köztük az imahelyekre és a közlekedési csomópontokra – összpontosultak, kiaknázva azok nyitott és hozzáférhető jellegét. A politikai vagy ideológiai indíttatású szélsőségesség szította terrorizmus terjedése miatt ez a fenyegetés még súlyosabbá vált. Szükségessé vált tehát az ilyen helyek hatékonyabb fizikai védelme és a megfelelő felderítési rendszerek alkalmazása, anélkül, hogy a polgárok szabadságait aláásnánk[52]. A Bizottság a finanszírozás, a tapasztalatok és a bevált gyakorlatok cseréje, valamint konkrét iránymutatások[53] és ajánlások[54] révén fokozni fogja a köz- és magánszféra közötti együttműködést a nyilvános terek védelme érdekében. A figyelemfelhívás, a teljesítőképességi követelmények és a felderítő eszközök tesztelése, valamint a belső fenyegetések kezelését célzó háttérellenőrzések fokozása is megközelítés részét képezik majd. A megközelítésnek azt a fontos szempontot is tükröznie kell, hogy a kisebbségek és a kiszolgáltatott személyek – beleértve a vallásuk vagy a nemük miatt veszélyeztetett személyeket – aránytalan mértékben érintettek lehetnek, és ezért különös figyelmet igényelnek. A regionális és helyi hatóságok fontos szerepet játszanak a nyilvános terek biztonságának javításában. A Bizottság emellett támogatja a városoknak a nyilvános terek biztonságával kapcsolatos innovációját is[55]. A városfejlesztési menetrend[56] „nyilvános terek biztonságával” foglalkozó új partnerségének 2018. novemberi elindítása a tagállamok, a Bizottság és a városok azon határozott elkötelezettségét tükrözi, hogy hatékonyabban lépjenek fel a városi területek biztonságát fenyegető veszélyekkel szemben.

---

50 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

51 Lásd a külső kiberkapacitás-építésre vonatkozóan a Tanács 2018. június 26-i következtetéseiben elfogadott uniós iránymutatásokat.

52 A távoli biometrikus azonosító rendszerekről érdemes külön vizsgálatot indítani. A Bizottság kiinduló álláspontját a mesterséges intelligenciáról szóló, 2020. február 19-i bizottsági fehér könyv (COM(2020) 65) ismerteti.

53 Lásd például az „Iránymutatás a nyilvános terek védelmét szolgáló biztonsági akadályok megfelelő megoldásainak kiválasztásához” című dokumentumot (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

54 A bevált gyakorlatokra vonatkozó iránymutatást az SWD(2019) 140 dokumentum tartalmazza, amely egy, a köz- és magánszféra közötti együttműködésről szóló szakaszt is magában foglal. A rendőrségi együttműködést támogató eszköz keretében nyújtott finanszírozás különös hangsúlyt fektet a köz- és magánszféra közötti együttműködés fokozására.

55 Három város (a görögországi Pireusz, a finnországi Tampere és az olaszországi Torinó) új megoldásokat tesztel az Európai Regionális Fejlesztési Alap (ERFA) által társfinanszírozott innovatív városfejlesztési intézkedések keretében.

56 Az uniós városfejlesztési menetrend egy új, többszintű munkamódszer, amely előmozdítja a tagállamok, a városok, az Európai Bizottság és más érdekelt felek közötti együttműködést annak érdekében, hogy az európai városokban ösztönözze a növekedést és az innovációt, illetve javítsa az élhetőséget, valamint azonosítsa és sikeresen kezelje a társadalmi kihívásokat.

A **drónok** piaca továbbra is bővül, és a drónokat immár számos értékes és jogszerű célra használják. Ugyanakkor fennáll a lehetősége, hogy a bűnözők és a terroristák visszaélhetnek azokkal – ebből a szempontból a nyilvános terek különösen veszélyeztetettek. A célpontjaik közé tartozhatnak az egyének, a csoportosulások, a kritikus infrastruktúra, a bűnüldöző hatóságok, a határok vagy a nyilvános terek. A drónok konfliktus során történő alkalmazásával kapcsolatos ismeretekhez a bűnözők és terroristák akár közvetlenül (visszatérő külföldi terrorista harcosoktól), akár online hozzájuthatnak. Az Európai Repülésbiztonsági Ügynökség által már kidolgozott szabályok fontos első lépést jelentenek az olyan területeken, mint például a drónüzemeltetők nyilvántartásba vétele vagy a drónok kötelező távoli azonosítása. Mivel a drónok egyre szélesebb körben érhetők el, megfizethetőbbek és nagyobb teljesítményre képesek, további intézkedésekre van szükség. Ez magában foglalhatja az információk megosztását, a mindenki – ideértve a bűnüldöző hatóságokat is – által használható iránymutatást és bevált gyakorlatokat, valamint a drónokkal kapcsolatos ellenintézkedések fokozottabb tesztelését[57]. Ezen túlmenően a drónok nyilvános teren való használatának a magánélet védelmével és az adatvédelemmel kapcsolatos vonatkozásait illetően további elemzésekre és intézkedésekre van szükség.

Kulcsfontosságú intézkedések
• A kritikus infrastruktúra védelmére és rezilienciájára vonatkozó jogszabályok • A hálózati és információs rendszerek biztonságáról szóló irányelv felülvizsgálata • Kezdeményezés a pénzügyi ágazat működési rezilienciájának fokozására • A kritikus energetikai infrastruktúra védelme és kiberbiztonsága, valamint a határokon átnyúló villamosenergia-áramlásokra vonatkozó kiberbiztonsági üzemi és kereskedelmi szabályzat • Európai kiberbiztonsági stratégia • A közös kiberbiztonsági egység létrehozása felé vezető következő lépések • Az uniós intézmények, szervek és ügynökségek által alkalmazandó, az információbiztonságra és a kiberbiztonságra vonatkozó közös szabályok • Fokozott együttműködés a nyilvános terek – köztük az imahelyek – védelme érdekében • A drónnal való visszaélések problémájának kezelésével kapcsolatos bevált gyakorlatok megosztása

2. A változó fenyegetések kezelése

Kiberbűnözés

A technológia új lehetőségeket teremt a társadalom számára. Új eszközöket is kínál az igazságszolgáltatásnak és a bűnüldözésnek. Ugyanakkor utakat nyit a bűnözők számára is. Egyre gyakoribbak a rosszindulatú szoftverek, a személyes vagy üzleti adatok hekkelés révén történő ellopása, valamint a digitális tevékenység anyagi kárral vagy a jó hírnév sérelmével járó megbénítása. Az erős kiberbiztonság által megteremtett ellenállóképes környezet alkotja a védelem első vonalát. A bűnüldöző hatóságoknak képesnek kell lenniük digitális nyomozásokat végezni, és ennek részeként egyértelmű szabályokat alkalmazni a bűncselekmények kivizsgálására és büntetőeljárás alá vonására, valamint biztosítani az áldozatok számára a szükséges védelmet. Ennek a munkának az Europolon belül működő, a számítástechnikai bűnözéssel foglalkozó közös akciócsoportra, valamint a nagyszabású

[57] A közelmúltban többéves tesztelési program indult, amely támogatja a tagállamokat az e területre vonatkozó közös módszertan és tesztelési platform kidolgozásában.

kibertámadásokra való reagálás koordinálása céljából létrehozott bűnüldözési vészhelyzet-elhárítási protokollra kell épülnie. A köz- és magánszféra közötti partnerségeket és együttműködést lehetővé tevő hatékony mechanizmusok szintén kulcsfontosságúak.

Ezzel párhuzamosan a kiberbűnözés elleni küzdelemnek EU-szerte stratégiai kommunikációs prioritássá kell válnia, hogy felhívjuk az európaiak figyelmét a kockázatokra és a saját maguk által megtehető megelőző intézkedésekre. Ennek egy proaktív megközelítés részét kell képeznie. Elengedhetetlen a jelenlegi jogi keret teljes körű végrehajtása is[58]: a Bizottság készen áll arra, hogy adott esetben a kötelezettségszegési eljárásokhoz folyamodjon, és folyamatosan felülvizsgálja ezt a keretet annak biztosítása érdekében, hogy az továbbra is megfeleljen a célnak. A Bizottság az Europollal és az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) együtt meg fogja vizsgálni egy olyan, a számítástechnikai bűnözéssel kapcsolatos uniós sürgősségi riasztórendszer kivitelezhetőségét is, amely biztosítaná az információáramlást és a számítástechnikai bűncselekményekre való gyors reagálást.

A számítástechnikai bűnözés olyan globális kihívás, amely hatékony nemzetközi együttműködést tesz szükségessé. Az EU támogatja az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményét, amely egy hatékony, jól megalapozott keret, és lehetővé teszi valamennyi ország számára annak megállapítását, hogy milyen rendszereket és kommunikációs csatornákat kell bevezetniük ahhoz, hogy hatékonyan tudjanak együttműködni egymással.

Az uniós polgárok közel fele aggódik az adatokkal való visszaélés[59] és a **személyazonosság-lopás** miatt.[60] A személyazonosság pénzügyi haszonszerzés céljából történő csalárd felhasználása az egyik kérdés, de jelentős személyes és pszichológiai hatások is jelentkezhetnek, mivel a személyazonosság-tolvajok által illegálisan közzétett tartalmak képesek évekig megmaradni az interneten. A Bizottság meg fogja vizsgálni a lehetséges gyakorlati intézkedéseket annak érdekében, hogy megvédje az áldozatokat a személyazonosság-lopás valamennyi formájával szemben, figyelembe véve a küszöbön álló európai digitális személyazonosító kezdeményezést[61].

A számítástechnikai bűnözés elleni küzdelem azt jelenti, hogy előre kell tekinteni. Hasonlóképpen ahhoz, ahogy a társadalom az új technológiai fejlesztéseket a gazdaság és a társadalom megerősítésére használja fel, a bűnözők is megpróbálhatják ezeket az eszközöket negatív célokra felhasználni. A bűnözők például használhatnak mesterséges intelligenciát jelszavak felderítésére és azonosítására, rosszindulatú szoftverek létrehozásának egyszerűsítésére, vagy olyan képek és hanganyagok felhasználására, amelyek személyazonosság-lopásra vagy személyazonossággal való visszaélésre használhatók fel.

Korszerű bűnüldözés

A bűnüldöző és igazságügyi szakembereknek alkalmazkodniuk kell az új technológiákhoz. A technológiai fejlődés és az újonnan megjelenő fenyegetések szükségessé teszik, hogy a bűnüldöző hatóságok hozzáférjenek az új eszközökhöz, új készségeket szerezzenek és

[58] 2013/40/EU irányelv az információs rendszerek elleni támadásokról.

[59] 46 % (Eurobarométer az európaiak kiberbiztonsággal kapcsolatos attitűdjeiről, 2020. január).

[60] Az „Európaiak hozzáállása a kiberbiztonsághoz” című 2018. évi Eurobarométer felmérés válaszadóinak túlnyomó többsége (95 %) szerint a személyazonosság-lopás súlyos, tízből hét szerint pedig nagyon súlyos bűncselekmény. A 2020 januárjában közzétett Eurobarométer felmérés megerősítette a számítástechnikai bűnözéssel, az online csalással és a személyazonosság-lopással kapcsolatos aggályok létezését: a válaszadók kétharmada aggódik a banki csalás (67 %) vagy személyazonosság-lopás (66 %) miatt.

[61] Közlemény – Európa digitális jövőjének megtervezése, 2020. február 19., COM(2020) 67.

alternatív nyomozási technikákat fejlesszenek ki. A nyomozások során az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférés javítását célzó jogalkotási intézkedések kiegészítéseként az EU segítheti a bűnüldöző hatóságokat abban, hogy kialakítsák a bűncselekmények kivizsgálásához szükséges adatok azonosításához, biztosításához és olvasásához szükséges kapacitást, és hogy ezeket az adatokat bizonyítékként használják fel a bíróságon. A Bizottság meg fogja vizsgálni **a bűnüldözési kapacitások digitális nyomozások terén való növelésére** irányuló intézkedéseket, és meg fogja határozni, hogy a kutatás és fejlesztés hogyan segíthetne a legtöbbet a bűnüldözés új eszközeinek létrehozásában; valamint hogy a képzés hogyan kínálhatja a megfelelő készségeket a bűnüldözés és az igazságszolgáltatás számára. Ez magában foglalja szigorú tudományos értékelések és vizsgálati módszerek biztosítását is a Bizottság Közös Kutatóközpontjának közreműködésével.

A közös megközelítések azt is biztosíthatják, hogy **a mesterséges intelligencia, az űrképességek, a nagy adathalmazok és a nagy teljesítményű számítástechnika** a bűncselekmények elleni küzdelem és az alapvető jogok biztosítása szempontjából egyaránt hatékony módon **épüljenek be** a biztonságpolitikába. A mesterséges intelligencia hatékony eszközként szolgálhat a bűnözés elleni küzdelemben, hatalmas nyomozati képességeket teremtve a nagy mennyiségű információ elemzése, valamint a minták és anomáliák azonosítása révén.[62] Konkrét eszközöket is kínálhat, például segítheti az online terrorista tartalmak azonosítását, a veszélyes termékek értékesítése terén felfedhet gyanús tranzakciókat, vagy vészhelyzetben segítséget nyújthat a polgároknak. E potenciál kiaknázása azt jelenti, hogy a kutatást, az innovációt és a mesterséges intelligencia felhasználóit össze kell hozni a megfelelő irányítással és technikai infrastruktúrával, aktívan bevonva a magánszektort és a tudományos köröket. Ez azt is jelenti, hogy biztosítani kell az alapvető jogok tiszteletben tartásának legmagasabb szintű normáit, ugyanakkor biztosítani kell a polgárok hatékony védelmét. Az egyéneket érintő határozatokat emberi felülvizsgálatnak kell alávetni, és meg kell felelniük a vonatkozó alkalmazandó uniós jognak.[63]

A súlyos bűncselekményekkel kapcsolatos nyomozások mintegy 85 %-ában elektronikus információkra és bizonyítékokra van szükség, míg az összes megkeresés 65 %-a más joghatóság alá tartozó szolgáltatókhoz érkezik[64]. Az a tény, hogy a hagyományos fizikai nyomok helyett az interneten találhatóak a nyomok, tovább növeli a bűnüldözés és a bűnözők képességei közötti szakadékot. Alapvető fontosságú az elektronikus bizonyítékokhoz való, a nyomozások során történő határokon átnyúló hozzáférés egyértelmű szabályozása. Ezért az elektronikus bizonyítékokra vonatkozó javaslatoknak az Európai Parlament és a Tanács általi gyors elfogadása kulcsfontosságú ahhoz, hogy a szakemberek hatékony eszközt kapjanak a kezükbe. Az e-bizonyítékokhoz való határokon átnyúló hozzáférés többoldalú és kétoldalú nemzetközi tárgyalások révén történő megvalósítása

[62] Például pénzügyi bűncselekmények esetében.

[63] Ez a hatályos jogszabályoknak való megfelelést jelenti, ideértve az (EU) 2016/679 általános adatvédelmi rendeletet, valamint a személyes adatoknak a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelését szabályozó (EU) 2016/680, a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet

[64] Európai Bizottság, SWD(2018) 118 final.

szintén kulcsfontosságú ahhoz, hogy nemzetközi szinten kompatibilis szabályok jöjjenek létre[65].

A digitális bizonyítékokhoz való hozzáférés az információk rendelkezésre állásától is függ. Ha az adatokat túl gyorsan törlik, fontos bizonyítékok tűnhetnek el, és emiatt nem lesz lehetséges a gyanúsítottak és a bűnözői hálózatok (valamint az áldozatok) azonosítása és megtalálása. Másrészt az adatmegőrzési rendszerek kérdéseket vetnek fel a magánélet védelmével kapcsolatban. Az Európai Bíróság előtt folyamatban lévő ügyek kimenetelétől függően a Bizottság értékelni fogja az adatmegőrzéssel kapcsolatos további lépéseket.

Az internetes doménnév-nyilvántartási információkhoz (WHOIS-adatok)[66] való hozzáférés fontos a nyomozások, a kiberbiztonság és a fogyasztóvédelem szempontjából. Az ezekhez az információkhoz való hozzáférés azonban egyre nehezebbé válik, amíg a Bejegyzett Nevek és Számok Internetszervezete (ICANN) el nem fogadja a WHOIS új politikáját. A Bizottság továbbra is együttműködik az ICANN-nal és a több érdekelt felet tömörítő közösséggel annak biztosítása érdekében, hogy a jogosan hozzáférést kérők – többek között a bűnüldöző szervek – az uniós és a nemzetközi adatvédelmi szabályozással összhangban hatékony hozzáférést kaphassanak a WHOIS-adatokhoz. Ez magában foglalja a lehetséges megoldások értékelését, beleértve azt is, hogy szükség lehet-e jogalkotási lépésekre az ilyen információkhoz való hozzáférésre vonatkozó szabályok tisztázása érdekében.

A bűnüldöző és igazságügyi hatóságoknak az **5G-s mobiltávközlési architektúra** EU-ban történő teljes körű bevezetése után képesnek kell lenniük a szükséges adatok és bizonyítékok beszerzésére oly módon, ami tiszteletben tartja a kommunikáció titkosságát. A Bizottság támogatni fogja a megerősített és összehangolt megközelítést a nemzetközi szabványok kialakítása, a bevált gyakorlatok, a folyamatok és a műszaki interoperabilitás meghatározása során az olyan kulcsfontosságú technológiai területeken, mint a mesterséges intelligencia, a dolgok internete vagy a blokklánc-technológiák.

Manapság a bűnözés és a terrorizmus valamennyi formája ellen folyó nyomozások jelentős részében játszanak **titkosított információk** szerepet. A titkosítás alapvető fontosságú a digitális világ számára, mivel biztosítja a digitális rendszerek és tranzakciók biztonságát, valamint számos alapvető jog védelmét, ideértve a véleménynyilvánítás szabadságát, a magánélet védelmét és az adatvédelmet. Ha azonban bűncselekmény céljára használják, elfedheti a bűnözők személyazonosságát is, és titokban tarthatja a kommunikációjuk tartalmát. A Bizottság megvizsgálja és támogatja a kihívások kiegyensúlyozott technikai, operatív és jogi megoldásait, és olyan megközelítést mozdít elő, amely megőrzi a titkosítás hatékonyságát a magánélet védelme és a kommunikáció biztonsága terén, ugyanakkor hatékony választ ad a bűnözésre és a terrorizmusra.

A jogellenes online tartalmak elleni küzdelem

Az online és a fizikai környezet biztonságának összehangolásához folyamatos lépésekre van szükség a **jogellenes online tartalmak elleni küzdelem terén**. A polgárokat fenyegető olyan alapvető veszélyek, mint a terrorizmus, a szélsőségesség vagy a gyermekek szexuális bántalmazása egyre inkább a digitális környezetre támaszkodnak: emiatt konkrét fellépésre és az alapvető jogok tiszteletben tartását biztosító keretre van szükség. Az első alapvető lépés az online terrorista tartalomról szóló jogszabályjavaslattal kapcsolatos tárgyalások

[65] Különösen az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményének második kiegészítő jegyzőkönyve, valamint az EU és az Egyesült Államok közötti, az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférésről szóló megállapodás.

[66] Szerte a világon 2 500 regiszter- és regisztrátor által működtetett adatbázisokban tárolják.

gyors lezárása[67] és a jogszabály végrehajtásának biztosítása. A bűnüldöző szervek és a magánszektor közötti önkéntes, az **uniós internetfórum** keretében zajló együttműködés megerősítése szintén kulcsfontosságú az internet terroristák, erőszakos szélsőségesek és bűnözők általi helytelen használata elleni küzdelemben. Az Europol szélsőséges internetes tartalmakkal foglalkozó uniós egysége továbbra is kulcsfontosságú szerepet fog játszani a terrorista csoportok online tevékenységének és a platformok fellépéseinek nyomon követésében[68], valamint az **uniós válsághelyzeti protokoll**[69] továbbfejlesztésében. Ezen túlmenően a Bizottság továbbra is együtt fog működni a nemzetközi partnerekkel, többek között azáltal, hogy részt vesz **a terrorizmus elleni küzdelemmel foglalkozó globális internetes fórumon** e kihívások globális szintű kezelése érdekében. A civil társadalom szerepvállalását előmozdító program keretében folytatódik az alternatív és ellenpropaganda fejlesztésének támogatása[70].

A Bizottság a jogellenes online gyűlöletbeszéd megelőzése és megakadályozása érdekében 2016-ban kiadott egy, a jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódexet, amelyben az online platformok önkéntesen kötelezettséget vállaltak a gyűlöletbeszéd-tartalmak eltávolítására. A legutóbbi értékelés azt mutatja, hogy a vállalatok 24 órán belül megvizsgálják a megjelölt tartalmak 90 %-át, és a jogellenes gyűlöletbeszédnek minősített tartalmak 71 %-át eltávolítják. A platformoknak azonban tovább kell növelniük az átláthatóságot és javítaniuk a felhasználóknak szóló visszajelzéseket, valamint biztosítaniuk kell a megjelölt tartalmak következetes megvizsgálását[71].

Az uniós internetfórum a gyermekek online szexuális bántalmazásával kapcsolatos kihívások kezelése érdekében elősegíti a meglévő és a fejlődő technológiák cseréjét is. A gyermekek online szexuális bántalmazásának kezelése a **gyermekek szexuális bántalmazása elleni küzdelem** [72]fokozására irányuló új stratégia központi eleme, amely arra törekszik, hogy a lehető legnagyobb mértékben kihasználja az uniós szinten rendelkezésre álló eszközöket az ilyen bűncselekmények elleni küzdelemben. A vállalatok számára lehetővé kell tenni, hogy folytassák a gyermekpornográfiát ábrázoló anyagok online felderítésére és eltávolítására irányuló munkájukat, és az ezen anyagok által okozott károk miatt olyan szabályozásra van szükség, amely egyértelmű és állandó kötelezettségeket határoz meg a probléma kezelésére. A stratégia azt is be fogja jelenteni, hogy a Bizottság ágazatspecifikus jogszabályok előkészítését is meg fogja kezdeni a gyermekek online szexuális bántalmazásának hatékonyabb kezelése érdekében, az alapvető jogok teljes körű tiszteletben tartása mellett.

Általánosabban fogalmazva a digitális szolgáltatásokról szóló, küszöbön álló jogszabály egyértelművé teszi és továbbfejleszti a digitális szolgáltatásokra vonatkozó felelősségi és biztonsági szabályokat, és megszünteti azokat az akadályokat, amelyek gátolják a jogellenes tartalmak, áruk vagy szolgáltatások elleni fellépést.

Ezen túlmenően a Bizottság – többek között a független tanácsadó bizottságon keresztül – továbbra is együtt fog működni a nemzetközi partnerekkel, többek között azáltal, hogy részt vesz a **terrorizmus elleni küzdelemmel foglalkozó globális internetes fórumon** e kihívások globális szintű kezelésének megvitatása érdekében, az uniós értékek és alapvető

[67] Javaslat az online terrorista tartalom terjesztésének megelőzéséről, COM(2018) 640, 2018. szeptember 12.
[68] Europol, 2019. november.
[69] A Europe that protects - EU Crisis Protocol: responding to terrorist content online. (2019. október).
[70] A radikalizálódástudatossági program munkájával kapcsolatban lásd az alábbi IV.3. szakaszt.
[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf
[72] A gyermekek szexuális bántalmazása elleni hatékonyabb küzdelmet célzó uniós stratégia, COM(2020) 607.

jogok megőrzése mellett. Olyan új kérdésekkel is foglalkozni kell, mint például az algoritmusok vagy az online játékok[73].

Hibrid fenyegetések

A hibrid fenyegetések nagyságrendje és sokfélesége napjainkban példa nélküli. A Covid19-válság több bizonyítékkal is szolgált erre: számos állami és nem állami szereplő próbálta kihasználni a világjárványt – különösen az információs környezet manipulálása és az alapvető infrastruktúrák ellen intézett kihívások révén. Ez gyengítheti a társadalmi kohéziót, és aláásható az uniós intézményekbe és a tagállamok kormányaiba vetett bizalmat.

A hibrid fenyegetésekkel kapcsolatos uniós megközelítést a 2016. évi közös keret[74] és a hibrid fenyegetésekkel szembeni reziliencia megerősítéséről szóló 2018. évi közös közlemény[75] tartalmazza. Az uniós szintű fellépést a belső-külső kapcsolatot lefedő jelentős eszköztár segíti, amely a társadalom egészére kiterjedő megközelítésen és a stratégiai partnerekkel, nevezetesen a NATO-val és a G7-csoporttal folytatott szoros együttműködésen alapul. A hibrid fenyegetésekkel kapcsolatos uniós megközelítés végrehajtásáról szóló jelentést e stratégiával együtt teszik közzé[76]. Az e stratégiával párhuzamosan bemutatott feltérképezés[77] alapján a Bizottság szolgálatai és az Európai Külügyi Szolgálat **korlátozott hozzáférésű online platformot** hoznak létre, amely lehetővé teszi a tagállamok számára, hogy uniós szinten hivatkozzanak a hibrid elleneszközökre és intézkedésekre.

Noha a hibrid fenyegetésekkel szembeni fellépés – a nemzeti biztonsági és védelmi politikákkal való szoros kapcsolat miatt – elsősorban a tagállamok felelőssége, egyes sebezhetőségek közösek valamennyi tagállamban, egyes fenyegetések pedig határokon átnyúlóak, például a határokon átnyúló hálózatokat vagy infrastruktúrákat céloznak meg. A Bizottság és a főképviselő olyan uniós megközelítést alakít ki a hibrid fenyegetésekkel kapcsolatban, amely a külső és a belső dimenziót egy zökkenőmentes szemléletbe integrálja, és összekapcsolja a nemzeti és az uniós szintű megfontolásokat. Ennek a tevékenységek teljes skáláját le kell fednie, a korai észleléstől az elemzésen, a tudatosság növelésén, az ellenálló képesség kiépítésén és a megelőzésen át a válságelhárításig és a következmények kezeléséig.

A megerősített végrehajtás mellett a hibrid fenyegetések folyamatos fejlődése miatt különös figyelmet fog kapni a **hibrid fenyegetésekkel kapcsolatos megfontolásoknak a szakpolitikai döntéshozatalba való beépítése** a dinamikus fejleményekkel való összhang fenntartása és annak biztosítása érdekében, hogy egyetlen potenciálisan releváns kezdeményezést se maradjon figyelmen kívül. Az új kezdeményezések hatásait a hibrid fenyegetések szempontjából is értékelni fogják, ideértve az olyan területekre vonatkozó kezdeményezéseket is, amelyek eddig nem tartoztak az antihibrid keretrendszerbe, mint például az oktatás, a technológia és a kutatás. Ehhez a megközelítéshez hasznos lenne a hibrid fenyegetések koncepciójának kidolgozása terén végzett munka, amely átfogó képet

[73] A terroristák egyre gyakrabban használják a szerencsejáték-platformok üzenetküldő rendszerét üzenetváltásokra, a fiatal terroristák pedig erőszakos támadásokat is újrajátszanak a videojátékokban.

[74] A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz, JOIN (2016) 18.

[75] A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése, JOIN (2018) 16.

[76] SWD(2020(153) hibrid fenyegetésekkel szembeni fellépésre vonatkozó 2016. évi közös keret, valamint a reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítéséről szóló 2018-as közös közlemény végrehajtásáról szóló jelentés

[77] SWD(2020) 152 Az ellenálló képesség fokozásával és a hibrid fenyegetésekkel szembeni fellépéssel kapcsolatos intézkedések feltérképezése.

nyújt az ellenérdekű felek által használható különböző eszközökről[78]. A cél annak biztosítása, hogy a döntéshozatali folyamat a hibrid fenyegetések alakulásáról szóló rendszeres, átfogó, hírszerzési információkon alapuló jelentésekre támaszkodjon. Ez a munka nagymértékben a tagállamok hírszerzési információira, valamint a tagállamok illetékes szolgálataival az EU INTCEN-en keresztül folytatott hírszerzési együttműködés tovább erősítésére fog támaszkodni.

A **helyzetismeret** fejlesztése érdekében a Bizottság szolgálatai és az Európai Külügyi Szolgálat fel fogják tárni a különböző forrásokból – többek között a tagállamoktól, valamint az uniós ügynökségektől, például az ENISA-tól, az Europoltól és a Frontextől – érkező információáramlás racionalizálásának lehetőségeit. A hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport továbbra is a hibrid fenyegetések értékelésének uniós fókuszpontja marad. A **rezilienciaépítés** központi szerepet játszik a hibrid fenyegetések megelőzésében és az ellenük való védekezésben. Ezért alapvető fontosságú az e területen elért eredmények szisztematikus nyomon követése és objektív mérése. Az első lépés az ágazati hibrid reziliencia alapértékeinek meghatározása mind a tagállamok, mind az uniós intézmények és szervek számára. Végezetül a **hibrid válsághelyzetekre való felkészültség** fokozása érdekében a jelenlegi protokollt felül kell vizsgálni a 2016. évi EU Playbookban[79] meghatározottak szerint, tükrözve a jelenleg átgondolás alatt álló uniós válságreagálási rendszer szélesebb körű felülvizsgálatát és megerősítését[80]. A cél az uniós fellépés hatásának maximalizálása az ágazati válaszok gyors összehangolása és a partnereinkkel, elsősorban a NATO-val való zökkenőmentes együttműködés biztosítása révén.

Kulcsfontosságú intézkedések
• A számítástechnikai bűnözésre vonatkozó jogszabályok végrehajtásának és a célra való alkalmasságának biztosítása • A gyermekek szexuális bántalmazása elleni hatékonyabb küzdelmet célzó uniós stratégia • Javaslatok a gyermekpornográfiát ábrázoló anyagok felderítésére és eltávolítására • A hibrid fenyegetésekkel szembeni fellépés uniós megközelítése • A hibrid fenyegetésekkel szembeni fellépés uniós operatív protokolljának (EU Playbook) felülvizsgálata • A digitális nyomozásokat érintő bűnüldözési kapacitások növelése lehetőségeinek vizsgálata

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

Terrorizmus és radikalizálódás

A terrorfenyegetés szintje továbbra is magas az EU-ban. Noha összességében csökkent a támadások száma, hatásuk még mindig pusztító lehet. A radikalizálódás tágabb értelemben is polarizálhatja és destabilizálhatja a társadalmi kohéziót. A terrorizmus és a radikalizálódás

[78] The Landscape of Hybrid Threats: A conceptual Model (Átfogó kép a hibrid fenyegetésekről: egy koncepcionális modell, JRC117280), amelyet a Közös Kutatóközpont és a hibrid fenyegetések elleni küzdelem európai kiválósági központja közösen fejlesztett ki.

[79] EU operational protocol for countering hybrid threats 'EU Playbook' (A hibrid fenyegetésekkel szembeni fellépés uniós operatív protokollja – (EU Playbook)), SWD(2016) 227.

[80] A 2020. március 26-i videokonferenciát követően az Európai Tanács tagjai nyilatkozatot fogadtak el a Covid19-világjárvány kitörésére válaszul hozott uniós intézkedésekről, amelyben felkérték a Bizottságot, hogy tegyen javaslatokat egy ambiciózusabb és szélesebb körű uniós válságkezelési rendszerre.

elleni küzdelemért való elsődleges felelősség továbbra is a tagállamoké. A fenyegetés egyre növekvő, határokon/ágazatokon átnyúló dimenziója azonban további lépéseket tesz szükségessé az uniós együttműködés és koordináció terén. Prioritás a terrorizmus elleni uniós jogszabályok hatékony végrehajtása, beleértve a korlátozó intézkedéseket[81] is. Célkitűzés marad az Európai Ügyészség hatáskörének a határon átnyúló terrorista bűncselekményekre való kiterjesztése.

A terrorizmus elleni küzdelem a kiváltó okok kezelésével kezdődik. A társadalom polarizálódása, a valós vagy vélt megkülönböztetés és más pszichológiai és szociológiai tényezők erősíthetik az emberek radikális diskurzusnak való kiszolgáltatottságát. Ebben az összefüggésben a **radikalizálódás** elleni küzdelem együtt jár a helyi, nemzeti és európai szintű társadalmi kohézió előmozdításával. Az elmúlt évtizedben számos hatékony kezdeményezést és szakpolitikát dolgoztak ki, különösen az uniós radikalizálódástudatossági hálózat és „Az Unió városai a radikalizálódással szemben kezdeményezés révén.[82] Eljött az ideje annak, hogy fontolóra vegyük a radikalizálódás elleni küzdelmet szolgáló uniós szakpolitikák, kezdeményezések és alapok összhangba hozását. Ezek az intézkedések támogathatják a képességek és készségek fejlesztését, fokozhatják az együttműködést, megerősíthetik a tényalapot és segíthetik az előrehaladás értékelését, bevonva az összes érdekelt felet, köztük az első vonalban dolgozó szakembereket, a politikai döntéshozókat és a tudományos köröket[83]. Az olyan puha politikák, mint az oktatás, a kultúra, az ifjúság és a sport hozzájárulhatnak a radikalizálódás megelőzéséhez, lehetőségeket kínálva a veszélyeztetett fiataloknak és az Unión belüli kohézióra[84]. A kiemelt területek közé tartozik a korai felismeréssel és kockázatkezeléssel, a rezilienciaépítéssel és a kivonással, valamint a rehabilitációval és a társadalomba való visszailleszkedéssel kapcsolatos munka.

A terroristák **vegyi, biológiai, radiológiai és nukleáris** (CBRN)[85] anyagok megszerzésére és fegyverré alakítására, valamint a felhasználásukhoz szükséges ismeretek és kapacitások fejlesztésére törekedtek[86]. A CBRN-támadások lehetősége kitüntetett helyet foglal el a terrorista propagandában. A lehetséges károk miatt erre különös figyelmet kell fordítani. A robbanóanyag-prekurzorokhoz való hozzáférés szabályozása során alkalmazott megközelítésre építve a Bizottság meg fogja vizsgálni, hogy szükséges-e korlátozni bizonyos olyan veszélyes vegyi anyagokhoz való hozzáférést, amelyeket támadások végrehajtására lehetne használni. Kulcsfontosságú lesz továbbá a rescEU-képességek fejlesztése a CBRN területén. A harmadik országokkal folytatott, az EU globális CBRN kiválósági központjait kiaknázó együttműködés szintén fontos a CBRN-biztonság és -védelem közös kultúrájának megerősítéséhez. Ez az együttműködés kiterjed a nemzeti hiány- és kockázatértékelésekre, a nemzeti és regionális CBRN cselekvési tervek támogatására, a bevált gyakorlatok cseréjére és a CBRN kapacitásépítési tevékenységekre.

---

81 A Tanács a terrorizmus elleni küzdelem érdekében az ISIL-re (Dáisra) és az al-Kaidára terkintettel korlátozó intézkedéseket, valamint egyes személyekkel és szervezetekkel szemben egyedi korlátozó intézkedéseket fogadott el. Lásd az EU szankciótérképén (https://www (https://www.sanctionsmap.eu/#/main) az összes korlátozó intézkedés áttekintését.

82 „Az Unió városai a radikalizálódás ellen” elnevezésű kísérleti kezdeményezés kettős célja, hogy előmozdítsa a szakértelem cseréjét az uniós városok között, és visszajelzéseket gyűjtsön arról, hogy miként lehet uniós szinten a legjobban támogatni a helyi közösségeket.

83 Például az Európai Biztonsági Alapból és a befektetői állampolgársági programból nyújtott finanszírozás.

84 Olyan uniós intézkedések, mint az Erasmus+ virtuális csereprogramok és az e-twinning.

85 Az elmúlt két évben például Európában (Franciaország, Németország, Olaszország) és máshol (Tunézia, Indonézia) is előfordultak biológiai anyagokkal (általában növényi eredetű toxinokkal) kapcsolatos esetek.

86 A Tanács a vegyi fegyverek elterjedésének és használatának visszaszorítását célzó korlátozó intézkedéseket fogadott el.

Az EU a világ legelőremutatóbb jogszabályait dolgozta ki a **robbanóanyag-prekurzorokhoz**[87] való hozzáférés korlátozására és a rögtönzött robbanószerkezetek gyártását célzó gyanús tranzakciók felderítésére. A házi készítésű robbanóanyagok jelentette fenyegetés szintje azonban továbbra is magas, ezeket Unió-szerte számos támadásban használják fel.[88] Az első lépés a szabályok végrehajtása, valamint annak biztosítása, hogy az online környezet ne tegye lehetővé az ellenőrzések megkerülését.

A terrorista bűncselekmények elkövetői – köztük a jelenleg Szíriában és Irakban tartózkodó **külföldi terrorista harcosok** — tényleges felelősségre vonása szintén fontos eleme a terrorizmusellenes politikának. Bár ezekkel a kérdésekkel elsősorban a tagállamok foglalkoznak, az uniós koordináció és támogatás segítheti a tagállamokat a közös kihívások kezelésében. Fontos lépés lesz a határbiztonsági jogszabályok[89] teljes körű végrehajtása és az összes releváns uniós adatbázis teljes körű kiaknázása az ismert gyanúsítottakra vonatkozó információk megosztása érdekében. A magas kockázatú személyek azonosítása mellett reintegrációs és rehabilitációs politikára is szükség van. A – többek között a börtönőrök és a pártfogó felügyelőkkel folytatott – szakmaközi együttműködés segíteni fogja az erőszakos szélsőségességhez vezető radikalizálódási folyamatok igazságügyi megítélését, valamint az igazságügyi ágazatnak az ítéletkiszabással és a fogva tartás alternatíváival kapcsolatos megközelítését.

A külföldi terrorista harcosok jelentette kihívás jól illusztrálja a belső és a **külső biztonság** közötti kapcsolatot. Az Unión belüli biztonság szempontjából központi jelentőségű a terrorizmus elleni küzdelem, valamint a radikalizálódás és az erőszakos szélsőségesség megelőzése és leküzdése terén folytatott együttműködés[90]. Az EU terrorizmusellenes/biztonsági szakértői hálózatának szakértelmére építve további lépésekre van szükség a terrorizmus elleni partnerségek és a szomszédságbeli és azon kívüli országokkal való együttműködés fejlesztése érdekében. A Nyugat-Balkánra vonatkozó, terrorizmus elleni küzdelemről szóló közös cselekvési terv jó hivatkozási alap az ilyen célzott együttműködéshez. Különösen a partnerországok külföldi terrorista harcosok azonosítására és megtalálásra való képességeinek támogatására kell törekedni. Az EU továbbra is elő fogja mozdítani a többoldalú együttműködést, az e területen tevékenykedő vezető globális szereplőkkel, például az Egyesült Nemzetek Szervezetével, a NATO-val, az Európa Tanáccsal, az Interpollal és az EBESZ-szel együttműködve. Együttműködik továbbá a terrorizmus elleni küzdelem világfórumával és a Dáis elleni nemzetközi koalícióval, valamint az érintett civil társadalmi szereplőkkel. Az Unió külpolitikai eszközei – a fejlesztést és az együttműködést is beleértve – szintén fontos szerepet játszanak a terrorizmus és a kalózkodás megelőzése érdekében harmadik országokkal folytatott együttműködés során. A nemzetközi együttműködés szintén alapvető fontosságú a **terrorizmusfinanszírozás** valamennyi forrásának — például a Pénzügyi Akció Munkacsoporton keresztül történő – felszámolásához.

---

[87] Olyan vegyi anyagok, amelyekkel házilag készített robbanóanyagok gyártása céljából vissza lehet élni. Ezeket a robbanóanyag-prekurzorok forgalmazásáról és felhasználásáról szóló, 2019. évi (EU) 2019/1148 rendelet szabályozza.

[88] Az ilyen pusztító támadások közé tartoznak például az oslói (2011), a párizsi (2015), a brüsszeli (2016), és a manchesteri (2017) támadás. Egy házilag készített robbanóanyaggal elkövetett támadás Lyonban 2019-ben 13 embert sebesített meg.

[89] Ideértve az Európai Határ- és Partvédelmi Ügynökség (Frontex) új megbízatását.

[90] A Tanács a 2020. június 16-i következtetéseiben hangsúlyozta, hogy meg kell védeni az uniós polgárokat a terrorizmus és az erőszakos szélsőségesség minden formájától függetlenül azok eredetétől, valamint hogy bizonyos kiemelt földrajzi és tematikus területeken tovább kell erősíteni az EU terrorizmus elleni külső szerepvállalását és fellépését.

Szervezett bűnözés

A szervezett bűnözés óriási gazdasági költséggel és személyes veszteséggel jár. A szervezett bűnözés és a korrupció okozta gazdasági veszteség a becslések szerint évi 218–282 milliárd EUR között van[91]. 2017-ben több mint 5 000 szervezett bűnözői csoport ellen folyt nyomozás Európában, ami 50 %-os növekedést jelent 2013-hoz képest[92]. A szervezett bűnözés egyre inkább határokon átnyúló dimenziót ölt, többek között az EU közvetlen szomszédságából kiindulva, ami fokozott operatív együttműködést és információcserét tesz szükségessé a szomszédságon belüli partnerekkel.

Az újonnan felmerülő kihívásokkal egyre nagyobb teret nyer az internetes bűnözés: a Covid19-világjárvány idején jelentősen megnövekedett a veszélyeztetett csoportokat célba vevő online csalások, valamint az egészségügyi és higiéniai termékekre irányuló lopások és betörések száma[93]. Az EU-nak meg kell erősítenie a szervezett bűnözés elleni – többek között nemzetközi szintű – fellépését, és több eszközt kell rendelkezésre bocsátania a szervezett bűnözés üzleti modelljének felszámolására. A szervezett bűnözés elleni küzdelem szoros együttműködést tesz szükségessé a helyi és regionális közigazgatási szervekkel és a civil társadalommal – amelyek kulcsfontosságú partnerek a bűnmegelőzés, valamint az áldozatoknak nyújtott segítség és támogatás terén –, különös figyelmet fordítva a határ menti régiók közigazgatásai közötti együttműködésre. Az ezzel kapcsolatos munkát egy, **a szervezett bűnözés elleni küzdelemre vonatkozó program** fogja összefogni.

Az EU-ban aktív szervezett bűnözői csoportok több mint egyharmada részt vesz a kábítószerek előállításában, kereskedelmében vagy terjesztésében. A kábítószer-függőség több mint nyolcezer túladagolásos halálhoz vezetett az EU-ban 2019-ben. A **kábítószer-kereskedelem** jelentős része határokon átnyúló jellegű, és a nyereség nagy része beszivárog a legális gazdaságba[94]. A kábítószer elleni új uniós program[95] meg fogja erősíteni az EU és a tagállamok által a kábítószer-kereslet és -kínálat csökkentése terén tett erőfeszítéseket, együttes fellépéseket létrehozva a közös probléma kezelése, valamint az EU és a külső partnerek között a kábítószerekkel kapcsolatban folytatott párbeszéd és együttműködés megerősítése érdekében. A Kábítószer és a Kábítószerfüggőség Európai Megfigyelőközpontjára (EMCDDA) irányuló értékelés alapján a Bizottság értékelni fogja, hogy szükség van-e a Megfigyelőközpont megbízatásának az új kihívásokkal összefüggésben történő aktualizálására.

A szervezett bűnözői csoportok és a terroristák kulcsfontosságú szerepet játszanak az **illegális tűzfegyverekkel** való kereskedelemben is. 2009 és 2018 között 23 tömegmészárlás volt Európában, amelyek során több mint 340 ember vesztette életét[96]. A tűzfegyverek gyakran a közvetlen szomszédságon keresztül kerülnek az EU-ba[97]. Emiatt meg kell erősíteni a koordinációt és az együttműködést mind az EU-n belül, mind a nemzetközi partnerekkel, különösen az Interpollal annak érdekében, hogy össze lehessen hangolni a

[91] Bruttó hazai termékben (GDP) kifejezve; Europol jelentés: „Does crime still pay?" – Criminal asset recovery in the EU (Még mindig jól fizető üzlet a bűnözés? Vagyonvisszaszerzés az EU-ban), 2016.

[92] Europol, A súlyos és szervezett bűnözés általi fenyegetettség értékelése, 2013 és 2017.

[93] Europol, 2020.

[94] EMCDDA és Europol, Jelentés az uniós kábítószerpiacokról, 2019. (2019. november).

[95] Kábítószer elleni uniós program és cselekvési terv (2021–2025), COM(2020) 606.

[96] Flamand Békeintézet (Flemish Peace Institute), Armed to kill (Fegyverkezés a gyilkolásért). (2019. október).

[97] Az EU 2002 óta finanszírozza a kézi- és könnyűfegyverek elterjedése és kereskedelme elleni küzdelmet a régióban; elsősorban a délkelet-európai tűzfegyver-szakértői hálózat (SEEFEN) részesült finanszírozásban. A nyugat-balkáni partnerek 2019 óta teljeskörűen részt vesznek az Európai Multidiszciplináris Platform a Bűnügyi Fenyegetettség Ellen (EMPACT) tűzfegyverekre vonatkozó prioritásában.

tűzfegyverek lefoglalásával kapcsolatos információgyűjtést és bejelentéseket. Alapvető fontosságú továbbá a fegyverek – többek között az interneten keresztül történő – nyomonkövethetőségének javítása, valamint az engedélyező és bűnüldöző hatóságok közötti információcsere biztosítása. A Bizottság **új uniós cselekvési tervet terjeszt elő a tűzfegyverek tiltott kereskedelme ellen**[98], és megvizsgálja, hogy a tűzfegyverek kiviteli engedélyezési, behozatali és tranzit szabályai továbbra is megfelelőek-e[99].

A bűnszervezetek árucikként kezelik a migránsokat és a nemzetközi védelemre szoruló személyeket. Az EU-ba érkező irreguláris migránsok 90 %-át szervezett bűnözői hálózatok csempészik be[100]. A migránscsempészés gyakran a szervezett bűnözés más formáival, így különösen az emberkereskedelemmel is összefonódik[101]. Az emberkereskedelem – amellett, hogy óriási emberi áldozatokat követel – az Europol becslései szerint a különböző kizsákmányolási formákból évi 29,4 milliárd EUR nyereségre tesz szert világszinten. Transznacionális bűncselekményről van szó, amelyet EU-n belüli és azon kívüli illegális kereslet táplál, és amely az EU összes tagállamára hatással van. Az e bűncselekmények azonosítása, büntetőeljárás alá vonása és elítélése terén tapasztalt hiányosságok új megközelítést tesznek szükségessé a területre irányuló fellépés fokozása érdekében. Egy, az **emberkereskedelemre vonatkozó új átfogó megközelítés** össze fogja fogni a fellépés különböző irányvonalait. Emellett a Bizottság **új, migránscsempészés elleni uniós cselekvési tervet** is előterjeszt majd a 2021–2025-ös időszakra. Mindkét munkaterület a szervezett bűnözői hálózatok elleni küzdelemre, az együttműködés fokozására és a bűnüldözés támogatására fog összpontosítani.

A szervezett bűnözői csoportok – ahogy a terroristák is – más területeken is lehetőségeket keresnek, különösen olyanokon, ahol alacsony felderítési kockázat mellett nagy nyereségre tehetnek szert, ilyen például a **környezeti bűnözés**. Az illegális vadászat, a vadon élő állatok és növények jogellenes kereskedelme, az illegális bányászat és fakitermelés, valamint az illegális hulladéklerakás és -szállítás a világ negyedik legjelentősebb bűnözői ágazatává vált[102]. A kibocsátáskereskedelmi rendszerek és az energetikai tanúsítványok rendszerei területén is voltak bűnözői visszaélések, továbbá a környezeti rezilienciára és a fenntartható fejlődésre elkülönített források esetében is fény derült hűtlen kezelésre. Amellett, hogy előmozdítja az EU, a tagállamok és a nemzetközi közösség fellépését a környezeti bűnözés elleni küzdelem fokozása terén[103], a Bizottság jelenleg értékeli, hogy a környezet büntetőjog általi védelméről szóló irányelv[104] továbbra is megfelelő-e. **A kulturális javakkal folytatott illegális kereskedelem** – amely egyre nagyobb mértéket ölt – szintén a legjövedelmezőbb bűncselekmények egyikévé vált, finanszírozási forrást biztosítva a terroristák és a szervezett bűnözés számára. Meg kell vizsgálni, hogy milyen intézkedésekre van szükség a kulturális javak belső piaci online és offline nyomonkövethetőségének javítása, a kulturális javak fosztogatásának helyszínéül szolgáló harmadik országokkal folytatott együttműködés megerősítése, illetve a bűnüldözést és a tudományos közösségeket célzó aktív támogatás biztosítása érdekében.

---

98 COM(2020) 608.

99 258/2012/EU rendelet az Egyesült Nemzeteknek a tűzfegyverek tiltott gyártásáról és kereskedelméről szóló jegyzőkönyve 10. cikkének végrehajtásáról.

100 Forrás: Europol.

101 Europol, a Migránscsempészés Elleni Küzdelem Európai Központja, 4. éves jelentés.

102 Az UNEP-INTERPOL gyorsreagálási értékelése: The Rise of Environmental Crime (A környezeti bűnözés megerősödése), 2016. június

103 Lásd: Az európai zöld megállapodás, COM(2019) 640 final.

104 2008/99/EK irányelv a környezet büntetőjog általi védelméről.

A **gazdasági és pénzügyi bűnözés** rendkívül összetett, mégis évente polgárok millióit és vállalkozások ezreit érinti az EU-ban. A csalás elleni küzdelem alapvető fontosságú, és uniós szintű fellépést tesz szükségessé. Az Europol az Eurojusttal, az Európai Ügyészséggel és az Európai Csalás Elleni Hivatallal együtt támogatja a tagállamokat és az EU-t a gazdasági és pénzügyi piacok, valamint az uniós adófizetők pénzének védelmében. Az Európai Ügyészség 2020 végén kezdi meg teljes körű működését, és hatáskörrel rendelkezik majd az uniós költségvetés elleni bűncselekmények – például csalás, korrupció és pénzmosás – esetén a nyomozás, a vádhatósági eljárás lefolytatása és a bíróság elé állítás terén. Emellett fellép a határokon átnyúló héacsalással szemben is, amely évente legalább 50 milliárd EUR-ba kerül az adófizetőknek.

A Bizottság támogatni fogja továbbá az újonnan felmerülő kockázatokkal – például a kriptoeszközökkel és az új fizetési rendszerekkel – kapcsolatos szakértelem és jogszabályi keret kialakítását. Mindenekelőtt megvizsgálja, milyen intézkedéseket célszerű hozni válaszképpen a kriptoeszközök (például a bitcoin) megjelenésére. Ezek az új technológiák hatással lesznek a pénzügyi eszközök kibocsátására, cseréjére, megosztására és az azokhoz való hozzáférésre.

Az Európai Unióban zéró toleranciát kell tanúsítani az illegális pénzáramlásokkal szemben. Az EU az elmúlt harminc évben szilárd szabályozási keretet hozott létre a **pénzmosás** és a terrorizmusfinanszírozás megelőzésére és az ellenük folytatott küzdelemre, teljes mértékben tiszteletben tartva a személyes adatok védelmének szükségességét. Mindazonáltal egyre nagyobb az egyetértés azzal kapcsolatban, hogy a jelenlegi keret végrehajtása jelentős javításra szorul. Megoldást kell találni a keret alkalmazásának módjában mutatkozó jelentős eltérésekre és a szabályok végrehajtásának súlyos hiányosságaira. Amint azt a 2020. májusi cselekvési terv[105] is kifejti: folyamatban van a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem uniós keretének javítására irányuló lehetőségek értékelése. A megvizsgálandó területek közé tartozik a nemzeti központi bankszámla-nyilvántartások összekapcsolása, ami jelentősen felgyorsíthatja a pénzügyi információs egységek és az illetékes hatóságok pénzügyi információkhoz való hozzáférését.

A **szervezett bűnözői csoportok** nyeresége a becslések szerint évente 110 milliárd EUR-t tesz ki az EU-ban. A jelenlegi válaszintézkedés az elkobzásra és a vagyonvisszaszerzésre vonatkozó jogszabályok harmonizálását[106] foglalja magában, amelynek célja a bűncselekményekből származó vagyon befagyasztásának és elkobzásának javítása az EU-ban, valamint a tagállamok közötti kölcsönös bizalom és hatékony, határokon átnyúló együttműködés elősegítése. Azonban e nyereség mindössze 1 %-át kobozzák el[107], aminek eredményeként a szervezett bűnözői csoportok befektethetnek bűnözői tevékenységeik további bővítésébe, illetve beépülhetnek a legális gazdaságba és különösen a hitelhez jutás terén nehézségekkel küzdő, a pénzmosás fontos célpontjának számító kis- és középvállalkozásokba. A Bizottság elemezni fogja a jogszabályok[108] végrehajtását és a további közös szabályok esetleges szükségességét, ideértve az elítélés nélküli elkobzásra

[105] A pénzmosás és a terrorizmusfinanszírozás megelőzését szolgáló cselekvési terv, C(2020) 2800.

[106] Az uniós jog szerint valamennyi tagállamban vagyonvisszaszerzési hivatalokat kell létrehozni.

[107] Jelentés – Vagyonvisszaszerzés és elkobzás: Annak biztosítása, hogy a bűnelkövetés ne legyen kifizetődő tevékenység, COM(2020) 217.

[108] 2014/42/EU irányelv a bűncselekmény elkövetési eszközeinek és az abból származó jövedelemnek a befagyasztásáról és elkobzásáról.

vonatkozó szabályokat is. A vagyonvisszaszerzési hivatalok[109] – a vagyonvisszaszerzési eljárás kulcsfontosságú szereplői – számára jobb eszközöket lehetne biztosítani a vagyoni eszközök felkutatásának és azonosításának EU-szerte történő felgyorsításához, ezáltal növelve az elkobzások arányát.

A szervezett bűnözés és a **korrupció** szoros kapcsolatban áll egymással. A becslések szerint a korrupció önmagában évi 120 milliárd EUR-ba kerül az uniós gazdaságnak[110]. A korrupció megelőzésére és a korrupció elleni küzdelemre továbbra is rendszeres nyomon követés fog vonatkozni a jogállamisági mechanizmus és az európai szemeszter keretében. Az európai szemeszter keretében értékelés tárgyát képezik a korrupció elleni küzdelem terén fennálló kihívások, így például a közbeszerzés, a közigazgatás, az üzleti környezet vagy az egészségügy. A Bizottság új éves jogállamisági jelentése kitér majd a korrupció elleni küzdelemre is, és megelőzési célú párbeszédet tesz lehetővé uniós és nemzeti szinten a nemzeti hatóságokkal és az érdekelt felekkel. A civil társadalmi szervezetek is kulcsszerepet játszhatnak a szervezett bűnözés és a korrupció megelőzésével, illetve az ellenük folytatott küzdelemmel kapcsolatos hatósági fellépés ösztönzése terén, és ezeket a csoportokat hasznos lenne egy közös fórum keretében összefogni. A határokon átnyúló jelleg miatt további fontos dimenziót jelent a szervezett bűnözés és a korrupció kapcsán az EU-val szomszédos régiókkal folytatott együttműködés és segítségnyújtás.

Kulcsfontosságú intézkedések
• Terrorizmus elleni uniós program, ideértve a radikalizálódás elleni intézkedések megújítását az EU-ban • Új terrorizmus elleni együttműködés a kulcsfontosságú harmadik országokkal és a nemzetközi szervezetekkel • A szervezett bűnözés elleni küzdelemre vonatkozó program, az emberkereskedelmet is ideértve • Kábítószer elleni uniós program és cselekvési terv (2021–2025) • A Kábítószer és a Kábítószerfüggőség Európai Megfigyelőközpontjára irányuló értékelés • A tűzfegyverek tiltott kereskedelmére vonatkozó uniós cselekvési terv (2020–2025) • A befagyasztásra és elkobzásra, valamint a vagyonvisszaszerzési hivatalokra vonatkozó jogszabályok felülvizsgálata • A környezet büntetőjog általi védelméről szóló irányelv értékelése • Migránscsempészés elleni uniós cselekvési terv (2021–2025)

4. Erős biztonsági ökoszisztéma

A valódi és hatékony biztonsági uniót olyan közös erőfeszítés eredményeként kell létrehozni, amelyben a társadalom minden rétege részt vesz. A kormányokat, a bűnüldöző szerveket, a magánszektort, az oktatást és magukat a polgárokat is be kell vonni a megvalósításba, fel kell őket ruházni a szükséges képességekkel, és meg kell közöttük

[109] A Tanács 2007/845/IB határozata a tagállamok vagyonvisszaszerzési hivatalai közötti, a bűncselekményből származó jövedelmek és a bűncselekményekhez kapcsolódó egyéb tulajdon felkutatása és azonosítása terén való együttműködésről.

[110] Nehéz megbecsülni a korrupció teljes gazdasági költségét, bár erre történtek erőfeszítések többek között olyan szervek által, mint a Nemzetközi Kereskedelmi Kamara, a Transparency International, az ENSZ Globális Megállapodás és a Világgazdasági Fórum. E szervek becslései szerint a korrupció a globális GDP 5 %-át teszi ki.

teremteni a megfelelő kapcsolatokat a mindenkire és különösen a legkiszolgáltatottabb csoportokra, az áldozatokra és a tanúkra kiterjedő felkészültség és reziliencia kialakítása érdekében.

Minden szakpolitikának ki kell alakítani a biztonsági dimenzióját, és az EU minden szinten hozzájárulhat ehhez. Az otthonokban a kapcsolati erőszak az egyik legsúlyosabb biztonsági kockázat. Az EU-ban a nők 22 %-át bántalmazta már partnere[111]. Az EU csatlakozása a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről és azok megelőzéséről szóló Isztambuli Egyezményhez továbbra is kulcsfontosságú prioritás marad. Amennyiben az egyezménnyel kapcsolatos tárgyalások továbbra sem haladnak előre, a Bizottság egyéb intézkedéseket fog hozni az egyezmény célkitűzéseinek elérése érdekében, többek között javaslatot tesz arra, hogy a nők elleni erőszakot vegyék fel a Szerződésben meghatározott uniós bűncselekmények listájára.

Együttműködés és információcsere

Az EU többek között azáltal tud a leginkább hozzájárulni a polgárok védelméhez, hogy elősegíti a biztonságért felelős személyek és szervezetek jó együttműködését. A bűnözés és a terrorizmus elleni küzdelem, valamint az igazságszolgáltatás leghatékonyabb eszköze az együttműködés és az információmegosztás. Ahhoz, hogy ezek hatékonyan működhessenek, célzottnak és időszerűnek kell lenniük. Ahhoz, hogy bizalommal forduljanak feléjük, mindkettőt közös biztosítékok és kontrollmechanizmusok kíséretében kell alkalmazni.

Számos uniós eszköz és ágazatspecifikus stratégia[112] került kialakításra a tagállamok közötti **operatív bűnüldözési együttműködés** továbbfejlesztése érdekében. A tagállamok közötti bűnüldözési együttműködést támogató egyik fő uniós eszköz a Schengeni Információs Rendszer, amely a körözött és eltűnt személyekre és tárgyakra vonatkozó adatok valós idejű cseréjét szolgálja. Az eredmények a bűnözők kézre kerítésében, a kábítószerek lefoglalásában és a potenciális áldozatok megmentésében érhetők tetten.[113] Az együttműködés szintje azonban még javítható a rendelkezésre álló eszközök észszerűsítése és korszerűsítése révén. Az operatív bűnüldözési együttműködést alátámasztó uniós jogi keret nagy részét 30 évvel ezelőtt alakították ki. A tagállamok közötti kétoldalú, sok esetben idejétmúlt vagy alig használt megállapodások összetett hálózata a szétaprózottság kockázatát rejti magában. A kisebb vagy tengerparttal nem rendelkező országokban a határokon átnyúlóan tevékenykedő bűnüldözési tisztviselőknek úgy kell operatív intézkedéseket végrehajtaniuk, hogy közben bizonyos esetekben hét különböző szabályrendszert követnek. Ennek eredményeként egyes műveletek, például a gyanúsítottak belső határokon átnyúló üldözése egyszerűen nem valósulnak meg. A jelenlegi uniós keret nem terjed ki egyes új technológiákkal, például a drónokkal kapcsolatos operatív együttműködésre sem.

Az operatív hatékonyságot konkrét bűnüldözési együttműködéssel lehet támogatni, amely kulcsfontosságú támogatást nyújthat más szakpolitikai célok, például a közvetlen külföldi befektetések új értékeléséhez nyújtott biztonsági hozzájárulás eléréséhez is. A Bizottság meg fogja vizsgálni, hogyan támogathatná ezt a törekvést egy rendőrségi együttműködési kódex kidolgozása. A tagállamok bűnüldöző hatóságai egyre inkább igénybe veszik az uniós szintű támogatást és szakértelmet, míg az Európai Unió Helyzetelemző Központja (EU INTCEN)

[111] Az egyenlőség Uniója: a 2020–2025 közötti időszakra szóló, nemi esélyegyenlőségi stratégia, COM(2020) 152 final.

[112] Ilyen például az EU tengerhajózási biztonsági stratégiájára vonatkozó cselekvési terv, amely fontos eredményekhez vezetett az érintett uniós ügynökségek között a parti őrségi feladatok terén folytatott együttműködés terén.

[113] A szervezett bűnözés elleni uniós küzdelem 2019-ben (Tanács, 2020).

döntő módon mozdította elő a stratégiai hírszerzési információk cseréjét a tagállamok hírszerzési és biztonsági szolgálatai között, hírszerzési helyzetismeretet biztosítva ezáltal az uniós intézmények számára[114]. Az **Europol** ugyancsak kulcsszerepet játszhat a harmadik országokkal a bűnözés és a terrorizmus elleni küzdelem terén folytatott együttműködés kiterjesztésében, az EU egyéb külső politikáival és eszközeivel összhangban. Az Europol azonban ma számos komoly akadállyal szembesül – különösen a személyes adatok magánfelekkel való közvetlen cseréje tekintetében –, ami akadályozza abban, hogy hatékonyan támogassa a tagállamokat a terrorizmus és a bűnözés elleni küzdelemben. Jelenleg folyik az Europol megbízatásának értékelése annak megállapítása érdekében, hogy az hogyan javítható úgy, hogy az ügynökség teljes mértékben el tudja látni feladatait. Ezzel összefüggésben az érintett uniós szintű hatóságoknak (például az OLAF-nak, az Europolnak, az Eurojustnak és az Európai Ügyészségnek) szorosabban együtt kell működniük, és javítaniuk kell az információcserét.

Egy másik kulcsfontosságú kapcsolódási pont az **Eurojust** továbbfejlesztése, amelynek célja a bűnüldözési együttműködés és az igazságügyi együttműködés közötti szinergiák maximalizálása. Az EU számára a stratégiai koherencia erősítése is előnyöket tartogat: az **EMPACT**[115] — a súlyos és nemzetközi szervezett bűnözésre vonatkozó uniós szakpolitikai ciklus – bűnüldözési információkon alapuló módszertant biztosít a hatóságok számára az EU-t érintő legfontosabb bűnügyi fenyegetések közös kezeléséhez. Segítségével az elmúlt évtizedben jelentős operatív eredményeket[116] sikerült elérni. A gyakorló szakemberek tapasztalatai alapján a 2022–2025-ös új szakpolitikai ciklus keretében a jelenlegi mechanizmust észszerűsíteni és egyszerűsíteni kell a legsürgetőbb és a változó bűnügyi fenyegetések eredményesebb kezelése érdekében.

Az időszerű és releváns **információk** kulcsfontosságúak a bűncselekmények üldözésével kapcsolatos napi munka szempontjából. Annak ellenére, hogy új uniós szintű biztonsági és határigazgatási adatbázisok kerültek kifejlesztésre, a tagállami hatóságok még mindig sok információt tárolnak a nemzeti adatbázisokban, vagy cserélnek ki egymással az uniós eszközökön kívül. Ez jelentős többletmunkát és késedelmet eredményez, és a kulcsfontosságú információk figyelmen kívül hagyásának fokozott kockázatával jár. A jobb, gyorsabb és egyszerűbb, az egész biztonsági közösséget bevonó folyamatok jobb eredményeket hoznának. A megfelelő eszközök elengedhetetlenek ahhoz, hogy ki lehessen aknázni azokat a lehetőségeket, amelyeket az információcsere tartogat a bűncselekmények hatékony üldözésében, szem előtt tartva egyúttal azokat a szükséges biztosítékokat, amelyek lehetővé teszik hogy az adatmegosztás tiszteletben tartsa az adatvédelmi jogszabályokat és az alapvető jogokat. A technológiai, kriminológiai és adatvédelmi fejlemények, valamint a megváltozott operatív igények fényében az EU mérlegelheti, hogy szükség van-e a DNS-adatok, az ujjnyomat-adatok és a gépjármű-nyilvántartási adatok automatizált cseréjét létrehozó eszközök, például a **2008. évi prümi határozatok** korszerűsítésére annak érdekében, hogy lehetővé váljon a tagállamok bűnügyi vagy egyéb adatbázisaiban bűnügyi nyomozások céljából már rendelkezésre álló további adatkategóriák automatizált cseréje. Ezen túlmenően a Bizottság meg fogja vizsgálni egyes rendőrségi nyilvántartások cseréjének lehetőségét annak beazonosítása érdekében, hogy létezik-e rendőrségi nyilvántartás egy adott személyről más tagállamban, és hogy megkönnyítse az ezekhez a nyilvántartásokhoz való hozzáférést, minden szükséges biztosíték mellett.

[114] Az EU INTCEN az egyetlen olyan kapu a tagállamok hírszerzési és biztonsági szolgálatai számára, amelyen keresztül hírszerzési helyzetismeretet biztosíthatnak az EU számára.

[115] Európai Multidiszciplináris Platform a Bűnügyi Fenyegetettség Ellen.

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

Az **utazókra vonatkozó információk** hozzájárultak a határellenőrzés javításához, az irreguláris migráció csökkentéséhez és a biztonsági kockázatot jelentő személyek azonosításához. Az előzetes utasinformációs adatok az egyes utasokra vonatkozóan a légitársaságok által az utasfelvétel során gyűjtött és az utazási célország szerinti határellenőrző hatóságoknak előzetesen megküldött személyazonosító adatok. A jogi keret felülvizsgálata[117] lehetővé tenné az információk hatékonyabb felhasználását, miközben biztosítaná az adatvédelmi jogszabályoknak való megfelelést, és megkönnyítené az utasforgalmat. Az utasnyilvántartási adatállomány (PNR) az utasok által a repülőjáratok foglalásakor szolgáltatott adatokat tartalmazza. A PNR-irányelv[118] végrehajtása kulcsfontosságú, és az irányelvet Bizottság továbbra is támogatja és érvényesíti. Ezen túlmenően a Bizottság félidős intézkedésként megkezdi a **PNR-adatok harmadik országokba történő továbbítására** vonatkozó jelenlegi megközelítés felülvizsgálatát.

Az **igazságügyi együttműködés** a határokon átnyúló bűnözés elleni rendőrségi fellépés szükséges kiegészítője. Az igazságügyi együttműködés az elmúlt 20 évben mélyreható változásokon ment keresztül. Az olyan szerveknek, mint az **Európai Ügyészség** és az **Eurojust**, rendelkezniük kell a teljes körű működésükhöz szükséges eszközökkel, vagy meg kell erősíteni őket. Fokozni lehetne az igazságügyi szakemberek közötti együttműködést is, például a bírósági határozatok kölcsönös elismerése tekintetében eszközölt további lépések, igazságügyi képzések és az információcserére irányuló további lépések révén. A cél a bírák és ügyészek közötti kölcsönös bizalom növelése, ami központi szerepet játszik a határokon átnyúló eljárások zökkenőmentes lebonyolításában. Igazságszolgáltatási rendszereink hatékonyságát a **digitális technológiák** alkalmazása is javíthatja. Az Eurojust támogatásával folyamatban van egy új digitális információcsere-rendszer létrehozása az európai nyomozási határozatok, a kölcsönös jogsegély iránti megkeresések és a tagállamok közötti kapcsolódó közlemények továbbítására. A Bizottság együtt fog működni a tagállamokkal, hogy előmozdítsa a szükséges informatikai rendszerek nemzeti szintű bevezetésének felgyorsítását.

A nemzetközi együttműködés a hatékony bűnüldözés és igazságügyi együttműködés szempontjából is kulcsfontosságú. A kulcsfontosságú partnerekkel kötött kétoldalú megállapodások kulcsszerepet játszanak az EU-n kívülről származó információk és bizonyítékok beszerzésében. Fontos szerepe van az **Interpolnak** mint az egyik legnagyobb kormányközi bűnügyi rendőrségi szervezetnek. A Bizottság megvizsgálja az Interpollal való együttműködés megerősítésének lehetséges módjait, beleértve az Interpol adatbázisaihoz való esetleges hozzáférést, valamint az operatív és stratégiai együttműködés megerősítésének lehetőségét. Az uniós bűnüldöző hatóságok részben a kulcsfontosságú partnerországokra támaszkodnak a bűnözők és terroristák felderítése és nyomozása során. Meg lehetne erősíteni az **EU és harmadik országok közötti biztonsági partnerségeket** az olyan közös fenyegetésekkel szembeni együttműködés fokozása érdekében, mint a terrorizmus, a szervezett bűnözés, a kiberbűnözés, a gyermekek szexuális bántalmazása és az emberkereskedelem. Ez a megközelítés a közös biztonsági érdekeken alapulna, és a kialakult együttműködésen és biztonsági párbeszédeken alapulna.

Az információcsere mellett a szakértelem cseréje is különösen fontos lehet a bűnüldözés **nem hagyományos fenyegetésekre** való felkészültségének növelése szempontjából. A

[117] A 2004/82/EK tanácsi irányelv a fuvarozóknak az utasokkal kapcsolatos adatok közlésére vonatkozó kötelezettségéről.

[118] Az (EU) 2016/681 irányelv az utas-nyilvántartási adatállománynak (PNR) a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében történő felhasználásáról.

bevált gyakorlatok cseréjének ösztönzése mellett a Bizottság meg fogja vizsgálni egy vis maior események, például járványok esetén alkalmazható **uniós szintű rendőrségi koordinációs mechanizmus** lehetőségét. A világjárvány azt is bizonyította, hogy a digitális közösség rendjének fenntartása, valamint az online rendfenntartást elősegítő jogi keretek alapvető fontosságúak lesznek a bűnözés és a terrorizmus elleni küzdelemben. A rendőrség és a helyi közösségek közötti – offline és online – partnerségek segíthetik a bűnmegelőzést, és enyhíthetik a szervezett bűnözés, a radikalizálódás és a terrorista tevékenységek hatását. A helyi és regionális szintű rendőrségi megoldások összekapcsolása a nemzeti és uniós szintű rendőrségi megoldásokkal az EU biztonsági uniója egészének sikere szempontjából kulcsfontosságú tényező.

Az erős külső határok nyújtotta hozzájárulás

A külső határok modern és hatékony igazgatása kettős előnnyel jár: egyrészt fenntartja a schengeni térség integritását, másrészt biztonságot nyújt polgárainknak. Az összes releváns szereplő bevonása annak érdekében, hogy a lehető legnagyobb biztonságról gondoskodjunk a határokon, valódi hatást gyakorolhat a határokon átnyúló bűnözés és terrorizmus megelőzésére. A közelmúltban megerősített Európai Határ- és Parti Őrség közös műveleti tevékenységei[119] hozzájárulnak a **külső határokon** és az Unión kívül a határokon átnyúló bűnözés megelőzéséhez és felderítéséhez. Azok a vámügyi intézkedések, amelyek valamennyi áru biztonsági és védelmi kockázatának felderítésére irányulnak, mielőtt azok az EU-ba érkeznek, valamint amelyek megérkezésükkor az áruk ellenőrzését célozzák, kulcsfontosságúak a határokon átnyúló bűnözés és terrorizmus elleni küzdelemben. A vámunióra vonatkozó, hamarosan elkészülő cselekvési terv olyan intézkedéseket fog bejelenteni, amelyek a kockázatkezelés megerősítésére és a belső biztonság fokozására is irányulnak, többek között a biztonsági kockázatelemzés szempontjából releváns információs rendszerek közötti kapcsolat megvalósíthatóságának értékelése révén.

A bel- és igazságügy területén működő **uniós információs rendszerek közötti interoperabilitás** kereteit 2019 májusában fogadták el. Ez az új felépítés az új vagy korszerűsített információs rendszerek[120] hatékonyságának és eredményességének javítását célozza. Ennek eredményeképpen a bűnüldöző szervek tagjai, a határőrök és a migrációs tisztviselők gyorsabb és rendszeresebb információhoz fognak jutni. Elősegíti a személyazonosság helyes megállapítását és hozzájárul a személyazonossággal való visszaélés elleni küzdelemhez. Ennek érdekében az interoperabilitás megvalósítása politikai és technikai szinten egyaránt prioritás kell, hogy legyen. Az uniós ügynökségek és az összes tagállam közötti szoros együttműködés rendkívül fontos ahhoz, hogy 2023-ra megvalósuljon a teljes interoperabilitásra vonatkozó cél.

Az úti okmányokkal való visszaélés az egyik leggyakrabban elkövetett bűncselekmény. Megkönnyíti a bűnözők és terroristák illegális mozgását, és kulcsszerepet játszik az emberkereskedelemben és a kábítószer-kereskedelemben.[121] A Bizottság meg fogja vizsgálni, hogy miként lehetne bővíteni az uniós tartózkodási és úti okmányok biztonsági

[119] Tagjai az Európai Határ- és Partvédelmi Ügynökség (Frontex), valamint a tagállamok határőrizeti és partvédelmi hatóságai.

[120] A határregisztrációs rendszer (EES), az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS), a kibővített Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS-TCN rendszer), a Schengeni Információs Rendszer, a Vízuminformációs Rendszer és a jövőbeni, naprakésszé tett Eurodac.

[121] Az okmányokkal való visszaélés és az emberkereskedelem közti összefüggést az emberkereskedelem elleni küzdelem terén elért eredményekről szóló második jelentés (COM(2018) 777 és az azt kísérő SWD(2018) 473), valamint az Europol „Emberkereskedelem az Európai Unióban” című, 2016. évi helyzetjelentése határozza meg.

előírásaival kapcsolatos eddigi munkát, többek között a digitalizáció révén. 2021 augusztusától a tagállamok megkezdik a személyazonosító igazolványok és tartózkodási okmányok harmonizált biztonsági előírások szerinti kiállítását, ideértve az összes uniós határforgalom-ellenőrzést végző hatóság által ellenőrizhető, biometrikus azonosítókat tartalmazó chipet is. A Bizottság nyomon fogja követni ezen új szabályok végrehajtását, többek között a jelenleg forgalomban lévő okmányok fokozatos lecserélését is.

A biztonsági kutatás és innováció megerősítése

A kiberbiztonság biztosítására, valamint a szervezett bűnözés, a kiberbűnözés és a terrorizmus elleni küzdelemre irányuló munka nagyban támaszkodik az e jövőt szolgáló eszközök kifejlesztésére: a biztonságosabb és védettebb új technológiák létrehozásának elősegítése, a technológiák jelentette kihívások kezelése, valamint a bűnüldözési munka támogatása érdekében. Ez viszont a magánszektorbeli partnerekre és iparágakra támaszkodik.

Az innovációt stratégiai eszköznek kellene tekinteni a jelenlegi fenyegetések elleni küzdelemben, valamint a jövőbeli kockázatok és lehetőségek előrejelzésében. Az innovatív technológiák új eszközökkel segíthetik a bűnüldözést és más biztonsági szereplőket. A mesterséges intelligencia és a nagy adathalmazok (big data) elemzése kihasználhatná a nagy teljesítményű számítástechnikát, hogy hatékonyabb észlelést és gyors, átfogó elemzést kínálhasson[122]. A megbízható technológiák kifejlesztésének kulcsfontosságú előfeltételei az algoritmusok tanításához, teszteléséhez és validálásához az illetékes hatóságok számára rendelkezésre álló kiváló minőségű adatkészletek[123]. Általánosabban fogalmazva, napjainkban erős a technológiai függőség kockázata – az EU például a kiberbiztonsági termékek és szolgáltatások nettó importőre, annak a gazdaságra és a kritikus infrastruktúrákra vonatkozó minden hatásával. A fejlett technológiai tudás megszerzése és az ellátás folyamatosságának biztosítása érdekében – nemkívánatos események és válságok esetén is – Európának jelenlétre és kapacitásra van szüksége az érintett értékláncok kritikus részein.

Az uniós **kutatás, innováció és technológiafejlesztés** lehetőséget kínál arra, hogy e technológiák kifejlesztése és alkalmazása során figyelembe vegyék a biztonsági dimenziót. Az uniós finanszírozási javaslatok következő generációja jelentős ösztönző erővel bírhat[124]. Az európai adatterekkel és felhőalapú infrastruktúrákkal kapcsolatos kezdeményezések már a kezdetektől fogva figyelembe vették a biztonságot. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózata[125] arra törekszik, hogy hatékony és eredményes struktúrát hozzon létre a kiberbiztonsági kutatási kapacitások és eredmények összevonásához és megosztásához. Az Európai Unió űrprogramja az Unió, a tagállamai és az egyének biztonságát támogató szolgáltatásokat nyújt[126].

---

[122] Ennek a mesterséges intelligenciára vonatkozó bizottsági stratégiára kell épülnie.

[123] Európai adatstratégia (COM(2020 66 final).

[124] Az Európai horizont kutatási és innovációs keretprogramra, a Belső Biztonsági Alapra, az Integrált Határigazgatási Alapra, az EUInvest programra, az Európai Regionális Fejlesztési Alapra és a Digitális Európa programra vonatkozó bizottsági javaslatok mindegyike támogatni fogja az innovatív biztonsági technológiák és megoldások kifejlesztését és alkalmazását a biztonsági értéklánc mentén.

[125] A 2018. szeptember 12-i COM(2018) 630 javaslat az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról.

[126] A Kopernikusz program például olyan szolgáltatásokat nyújt, amelyek lehetővé teszik az EU külső határainak felügyeletét és a tengerfelügyeletet, ami segíti a kalóztevékenység és a csempészés elleni

A 2007 óta indított, összesen közel 3 milliárd EUR értékű, több mint 600 projekttel az uniós finanszírozású biztonsági kutatás kulcsfontosságú eszköz a biztonsági megoldásokat támogató technológia és tudás ösztönzésében. Az Europol megbízatásának felülvizsgálata keretében a Bizottság meg fogja vizsgálni a **belső biztonság európai innovációs központja**[127] létrehozásának lehetőségét, amelynek célja, hogy közös megoldásokat kínáljon a közös biztonsági kihívásokra és lehetőségekre, amelyeket a tagállamok önmagukban esetleg nem tudnának kihasználni. Az együttműködés alapvető fontosságú ahhoz, hogy a beruházások a lehető leghatékonyabbak legyenek, és olyan innovatív technológiákat fejlesszenek ki, amelyek biztonsági és gazdasági előnyökkel egyaránt járnak.

Készségek és figyelemfelkeltés

A biztonsági kérdések tudatosítása és a potenciális fenyegetések kezeléséhez szükséges készségek elsajátítása elengedhetetlen ahhoz, hogy reziliensebb társadalmat építsünk, felkészültebb vállalkozásokkal, közigazgatási szervekkel és magánszemélyekkel. Az informatikai infrastruktúrával és az elektronikus rendszerekkel kapcsolatos kihívások rámutattak, hogy fejlesztenünk kell humán kapacitásainkat a kiberbiztonsági felkészültséggel és reagálással kapcsolatban. A világjárvány rávilágított a digitalizáció fontosságára is az EU gazdaságának és társadalmának valamennyi területén.

Még a **biztonsági fenyegetésekre** és az ellenük való küzdelem módjára **vonatkozó alapszintű ismeretek** is valós hatást gyakorolhatnak a társadalom rezilienciájára. A kiberbűnözés kockázataival kapcsolatos tudatosság és az azzal szembeni önvédelem szükségessége jól kiegészíti a szolgáltatók által a kibertámadások leküzdéséhez biztosított védelmet. A kábítószer-kereskedelem veszélyeire és kockázataira vonatkozó tájékoztatás megnehezítheti a bűnözők sikerét. Az EU ösztönözheti a bevált gyakorlatok terjesztését, például a Biztonságosabb Internet Központok[128] hálózatán keresztül, és biztosíthatja, hogy ezek a célok megjelenjenek saját programjaiban.

A jövőbeni digitális oktatási cselekvési tervnek célzott intézkedéseket kell tartalmaznia annak érdekében, hogy a teljes népességet biztonsági informatikai készségekhez juttassa. A nemrégiben elfogadott készségfejlesztési program[129] az egész életen át tartó készségfejlesztést támogatja. Ez célzott intézkedéseket tartalmaz, amelyek célja a természettudomány, a technológia, a műszaki tudományok, a bölcsészet és a matematika területén végzettek számának növelése a korszerű ágazatokban, mint például a kiberbiztonság területén jelentkező szükségletek kielégítésére. A Digitális Európa program által finanszírozott további intézkedések lehetővé teszik a szakemberek számára, hogy lépést tartsanak a biztonsági fenyegetettségi helyzet alakulásával, ugyanakkor betöltsék az uniós munkaerőpiac e téren jelentkező hiányosságait. Ennek általános hatása az lesz, hogy lehetővé teszi az egyének számára a biztonsági fenyegetések kezeléséhez szükséges készségek elsajátítását, a vállalkozások számára pedig azt, hogy megtalálják az e területen számukra szükséges szakembereket. A küszöbön álló Európai Kutatási Térség és európai

---

fellépést, valamint támogatja a kritikus infrastruktúrákat. Amint teljes mértékben működőképessé válik, kulcsfontosságú támogató eszköz lesz a polgári és katonai missziók és műveletek számára.

[127] Ez a központ együttműködne az Európai Határ- és Parti Őrséggel/Frontex-szel, a CEPOL-lal, az eu-LISA-val és a Közös Kutatóközponttal is.

[128] Lásd a www.betterinternetforkids.eu oldalt: a központi portál és a nemzeti Biztonságosabb Internet Központok finanszírozása jelenleg az Európai Hálózatfinanszírozási Eszköz/Távközlés keretében történik, a jövőbeli finanszírozásra pedig a Digitális Európa program keretében tettek javaslatot.

[129] A fenntartható versenyképességre, a társadalmi méltányosságra és a rezilienciára vonatkozó európai készségfejlesztési program, COM(2020) 274 final.

oktatási térség a természettudományok, a technológia, a műszaki tudományok, a bölcsészet és a matematika területén is elő fogja mozdítani a karrierlehetőségeket.

Fontos továbbá, hogy a **bűncselekmények áldoztai** élhessenek jogaikkal; egyedi körülményeik miatt meg kell kapniuk a szükséges segítséget és támogatást. Különös erőfeszítésekre van szükség a kisebbségek és a legveszélyeztetettebb sértettek, például a szexuális kizsákmányolás céljából emberkereskedelem áldozatává vált vagy családon belüli erőszaknak kitett gyermekek vagy nők esetében.[130]

Különös szerepe van a megerősített **készségeknek a bűnüldözésben**. A jelenlegi és az új technológiai fenyegetések miatt több beruházásra van szükség a bűnüldöző szervek személyzetének a lehető legkorábbi szakaszban és egész pályafutásuk ideje alatt történő továbbképzése terén. A CEPOL nélkülözhetetlen partner, amely segítséget nyújt a tagállamoknak e feladat ellátásában. A rasszizmussal és idegengyűlölettel, valamint általánosabban a polgárok jogaival kapcsolatos bűnüldözési képzésnek az uniós biztonsági kultúra alapvető elemét kell képeznie. A nemzeti igazságszolgáltatási rendszereket és igazságügyi szakembereket is fel kell vértezni az alkalmazkodásra és a példa nélküli kihívásokra való reagálásra. A képzés rendkívül lényeges ahhoz, hogy a helyszínen eljáró hatóságok operatív helyzetben kihasználják ezeket az eszközöket. Emellett minden erőfeszítést meg kell tenni a nemek közötti egyenlőség általános érvényesítésének és a nők bűnüldözésben való részvételének megerősítése érdekében.

Kulcsfontosságú intézkedések
• Az Europol mandátumának megerősítése • Egy uniós „rendőrségi együttműködési szabályzat” és a válsághelyzeti rendőrségi koordináció lehetőségének vizsgálata • Az Eurojust megerősítése az igazságügyi és bűnüldöző hatóságok összekapcsolása érdekében • Az előzetes utasinformációs irányelv felülvizsgálata • Az utasnyilvántartási adatállomány külső dimenziójáról szóló közlemény • Az EU és az Interpol közötti együttműködés megerősítése • A kulcsfontosságú harmadik országokkal az információmegosztásról folytatott tárgyalások kerete • Az úti okmányokra vonatkozó biztonsági előírások javítása • Egy belső biztonságra vonatkozó európai innovációs központ létrehozási lehetőségének vizsgálata

V. Következtetések

Az egyre turbulensebb világban az Európai Uniót még mindig széles körben az egyik legbiztonságosabb és legvédettebb helynek tekintik. Ezt azonban nem vehetjük készpénznek.

A biztonsági unióra vonatkozó új uniós stratégia egy olyan biztonsági ökoszisztéma alapjait fekteti le, amely az európai társadalom egészére kiterjed. Azon az ismereten alapul, hogy a biztonság közös felelősség. A biztonság egy mindenkit érintő kérdés. Társadalmaink

[130] Lásd a nemi esélyegyenlőségi stratégiát, COM(2020) 152; az áldozatok jogaira vonatkozó stratégiát, COM(2020) 258; és a gyermekbarát internet európai stratégiáját, COM(2012) 196.

biztonságosabbá tétele érdekében valamennyi kormányzati szervnek, vállalkozásnak, társadalmi szervezetnek, intézménynek és polgárnak teljesítenie kell saját kötelezettségeit.

A biztonsági kérdéseket most sokkal szélesebb perspektívából kell nézni, mint a múltban. Túl kell lépni azon, hogy hibásan különbséget akarunk tenni a fizikai és a digitális kérdések között. Az EU biztonsági unióra vonatkozó stratégiája összegyűjti a biztonsági szükségletek teljes körét, és azokra a területekre összpontosít, amelyek az elkövetkező években a legkritikusabbak az EU biztonsága szempontjából. Elismeri továbbá, hogy a biztonsági fenyegetések nem tartják tiszteletben a földrajzi határokat, valamint azt, hogy egyre szorosabb a kapcsolat a belső és a külső biztonság között[131]. Ebben az összefüggésben fontos lesz, hogy az EU együttműködjön nemzetközi partnereivel valamennyi uniós polgár védelme érdekében, és e stratégia végrehajtása uniós külső tevékenységgel szoros összhangban történjen.

Biztonságunk alapvető értékeinkhez kapcsolódik. Az e stratégiában javasolt valamennyi intézkedés és kezdeményezés teljes mértékben tiszteletben fogja tartani az alapvető jogokat és európai értékeinket. Ezek képezik európai életmódunk alapját, és minden munkánk során a középpontban kell, hogy maradjanak.

Végül a Bizottság továbbra is teljes mértékben tudatában van annak, hogy minden szakpolitika vagy intézkedés csak akkor jó, ha a végrehajtása is az. Ezért állandó hangsúlyt kell fektetni a meglévő és jövőbeli jogszabályok megfelelő végrehajtására és érvényesítésére. Ezt a biztonsági unióról szóló rendszeres jelentések útján nyomon fogjuk követni, és a Bizottság teljeskörűen tájékoztatni fogja az Európai Parlamentet, a Tanácsot és az érdekelt feleket, és bevonja őket valamennyi vonatkozó fellépésbe. Emellett a Bizottság készen áll arra, hogy részt vegyen a biztonsági unióra vonatkozó stratégiáról szóló, az intézményekkel folytatott közös vitákban és megszervezze azokat annak érdekében, hogy az előttünk álló kihívások közös vizsgálata mellett együtt vegyék számba az elért eredményeket.

A Bizottság felkéri az Európai Parlamentet és a Tanácsot, hogy hagyják jóvá a biztonsági unióra vonatkozó stratégiát mint a következő öt évben a biztonságra irányuló együttműködés és együttes fellépés alapját.

[131] Lásd az EU globális stratégiáját.