



Brüsszel, 2022. február 17.
(OR. en)

6316/22

LIMITE

COPS 68	PROCIV 16
POLMIL 33	ESPACE 11
EUMC 50	POLMAR 17
CIVCOM 21	MARE 17
CFSP/PESC 171	COMAR 15
CSDP/PSDC 70	COMPET 97
RELEX 196	IND 41
JAI 202	RECH 89
HYBRID 15	COTER 44
DISINFO 11	POLGEN 21
CYBER 53	

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2022) 61 final
Tárgy:	A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK Ütemterv a biztonsági és védelmi szempontból kritikus technológiákra vonatkozóan

Mellékelten továbbítjuk a delegációknak a COM(2022) 61 final számú dokumentumot.

Melléklet: COM(2022) 61 final



Strasbourg, 2022.2.15.
COM(2022) 61 final

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

Ütemterv a biztonsági és védelmi szempontból kritikus technológiákra vonatkozóan

1. Bevezetés

Európa jólétének, biztonságának és életmódjának biztosításához elengedhetetlen, hogy a kontinens a technológiai fejlődés élvonalában maradjon. Az új technológiák minden eddiginél gyorsabb ütemben alakítják át a biztonsági és a védelmi ágazatot, és elmoszák a polgári és a katonai terület közötti választóvonalat. Különösen a digitális technológiák befolyásolják a globális biztonsági szintéren belül kialakult hatalmi egyensúlyt. Ezért alapvető fontosságú annak biztosítása, hogy Európa biztonsági és védelmi ágazata technológiailag továbbra is megfeleljen a célnak.

Számos, biztonsági és védelmi szempontból kritikus technológia egyre inkább a polgári területről ered, és kettős felhasználású kritikus komponenseket használ. A területek közötti innováció felgyorsítása, valamint a biztonsági és a védelmi ágazat technológiai szuverenitásának előmozdítása érdekében javítani kell a polgári és a védelmi kutatási és innovációs közösségek közötti információcserét. A polgári technológiafejlesztés terén szerzett, régóta fennálló szakértelmére és új védelmi együttműködési eszközeire¹ tekintettel az EU alkalmas arra, hogy vezető szerepet vállaljon. Ehhez azonban arra van szükség, hogy az erőforrásokat hatékonyabban használjuk fel, valamint készen álljunk a kettős felhasználás lehetőségeinek feltárására, egyúttal pedig tiszteletben tartjuk az EU alapvető értékeit. Ez azt is jelenti, hogy csökkenteni kell az e technológiákhoz kapcsolódó érték- és ellátási láncok stratégiai függőségeit és sebezhetőségeit.

Európa biztonsági és védelmi képességeinek széttagoaltsága alacsony gazdasági hatékonysághoz, az operatív kapacitás csökkenéséhez és a stratégiai függőségek növekedéséhez vezetett. A biztonsági és védelmi technológiák napjainkban zajló forradalma és az új uniós védelmi együttműködési eszközök lehetőséget adnak az EU-nak arra, hogy elkerülje a múlt hibáit, meglévő kapacitásaira építsen, valamint megőrizze gazdasági jólétét és biztonságát. **A jövőbeli európai biztonsági és védelmi technológiai és innovációs környezetet a kezdetektől fogva uniós együttműködési keretek között kell kialakítani.**

Ursula von der Leyen elnök az Unió helyzetéről szóló 2021. évi beszédében² elismerte, hogy bár megkezdődött az európai védelmi ökoszisztéma kialakítására irányuló munka, amire igazán szükségünk van, az az európai védelmi unió. Az EU biztonsági és védelmi stratégiai iránytűje (a továbbiakban: a stratégiai iránytű) – amelyet a tagállamok 2022 márciusában fogadnak el – közös stratégiai jövőképet határoz meg a következő évtizedre, valamint felvázolja, hogy az EU miként fogja növelni a különböző válságokra és kihívásokra irányuló cselekvő- és reagálási képességét; hogyan védi meg érdekeit és polgárait; hogyan ruház be és vezet be innovációkat a szükséges képességek és technológiák közös kifejlesztése érdekében; valamint hogyan mélyíti el az uniós értékeken és érdekeken alapuló partnerségeket.

Ez a biztonsági és védelmi szempontból kritikus technológiákra vonatkozó ütemterv az Európai Tanács 2021. február 25–26-i azon kérése³ nyomán született, hogy a Bizottság vázolja fel a

¹ Az Európai Védelmi Alap (EDF), a koordinált éves védelmi szemle (CARD) és az állandó strukturált védelmi együttműködés (PESCO).

² [Ursula von der Leyen, a Bizottság elnökének 2021. évi értékelő beszéde az Unió helyzetéről](#)

³ [Az Európai Tanács tagjainak 2021. február 26-i nyilatkozata](#)

kutatás, a technológiafejlesztés és az innováció (KTF+I) fellendítéséhez, valamint az EU-nak a biztonsági és védelmi szempontból kritikus technológiák és értékláncok területén fennálló stratégiai függőségének csökkentéséhez vezető utat. Az ütemtervet a 2022. március 10–11-én Párizsban tartandó informális csúcstalálkozón terjesztik elő, és az hozzájárulást nyújt a stratégiai iránytűhöz. Az ütemterv javaslatot tesz arra, hogy az EU és a tagállamok közösen érvélik el a fent említett célt, különösen a következők révén:

- az EU biztonsága és védelme szempontjából kritikus technológiák azonosítása, azok fellendítése európai (KTF+I) programokon keresztül,
- annak biztosítása, hogy a védelmi megfontolásokat jobban figyelembe vegyék a polgári KTF+I programokban, valamint adott esetben az ipar- és kereskedelempolitikában, ezzel párhuzamosan pedig a technológiák lehetséges polgári felhasználását is jobban mérlegeljék a védelmi KTF+I programokban,
- a biztonsági és védelmi szempontból kritikus technológiák tekintetében az egész EU-ra kiterjedő stratégiai és összehangolt megközelítés előmozdítása a kezdetektől fogva, hogy a lehető legjobban ki lehessen használni az EU és a tagállamok KTF+I programjait, szinergiákat lehessen kialakítani a polgári és védelmi KTF+I közösségek között, és mérsékelni lehessen a külső forrásokból eredő stratégiai függőségeket, valamint
- a lehető legnagyobb mértékű koordináció más hasonlóan gondolkodó partnerekkel, például az Egyesült Államokkal és az Észak-atlanti Szerződés Szervezetével (NATO), kölcsönösen előnyös feltételek mellett.

2. A biztonsági és védelmi szempontból kritikus technológiák és stratégiai függőségek

„A 2020. évi új iparstratégia frissítése: Erősebb egységes piac kiépítése Európa fellendülése érdekében” című, 2021 májusában közzétett közleményében (a továbbiakban: a frissített iparstratégia)⁴ a Bizottság megerősíti, hogy a technológiai vezető szerep továbbra is az EU versenyképességének és innovációjának alapvető hajtóereje, különösen az úgynevezett „kritikus technológiák” tekintetében⁵. Hangsúlyozza továbbá annak fontosságát, hogy az EU rezilienciájának biztosítása érdekében azonosítsák és mérsékeljék az „érzékeny ökoszisztémák” – többek között a „proximitásalapú gazdaság, szociális gazdaság és polgári biztonság”, valamint az „űripár és védelem” – stratégiai függőségeit.

A polgári, a védelmi és az űripár közötti szinergiákról szóló, 2021. februári bizottsági cselekvési terv (a továbbiakban: a szinergiákról szóló cselekvési terv)⁶ elismeri, hogy a polgári területről származó forradalmi és alaptechnológiák egyre nagyobb jelentőséggel bírnak Európa jövőbeli biztonsága és védelme szempontjából, valamint hogy elő kell mozdítani a polgári és védelmi technológiák közötti termékeny kölcsönhatást és szinergiákat. A cselekvési terv számos kulcsfontosságú intézkedést határoz meg a polgári és a védelmi közösségek közötti

⁴ [COM\(2021\) 350 final](#)

⁵ A Bizottság a Kritikus Technológiák Megfigyelőközpontjával kapcsolatos munkája keretében jelenleg folytatja a „kritikusság” mibenlétének meghatározását a világűr, a védelem és a kapcsolódó polgári ágazatok (többek között a biztonság) szempontjából.

⁶ [COM\(2021\) 70 final](#)

információcsere és együttműködés ösztönzésére, amelyhez az uniós KTF+I programok és eszközök alkalmazása szolgál kiindulópontként.

2.1. A biztonsági és a védelmi ágazat sajátos jellemzői

Az EU védelmi iparának szerkezete változatos: nagy multinacionális vállalatok és kis- és közepes méretű szereplők is jelen vannak. A kereslet szinte kizárólag a nemzeti kormányoktól származik, amelyek a védelmi vonatkozású termékek és technológiák beszerzését és kivitelét is ellenőrzik. Az eltérő nemzeti követelmények, valamint a nemzeti közkiadások és beruházások továbbra is széttöredeztették az EU védelmi piacát, és esetenként azzal a kockázattal járhatnak, hogy hátráltatják a tagállamok nemzeti fegyveres erői közötti interoperabilitást. A védelmi ágazat ezért nem követi a tradicionálisabb piacokat szabályozó hagyományos szabályokat és üzleti modelleket, és így korlátozottan tudja befolyásolni a kapcsolódó beruházásokat és piaci döntéseket. Ez megnehezíti az ipar számára, hogy jelentős, önfelfinanszírozott védelmi KTF+I projekteket hajtson végre.

Az EU biztonsági ipara hasonló kihívásokkal néz szembe, mivel a piacok szintén túlnyomórészt nemzeti, de még inkább széttöredeztettek. Ügyfelei különfélék (pl. rendőrségek, belső biztonsági ügynökségek, vámhatóságok, határforgalom-ellenőrzést végző hatóságok, magán biztonsági szolgálatok), a tevékenységek különböző (helyi, regionális, nemzeti) szinteken zajlanak, és felépítésük tagállamonként eltérő. **A Bizottság 2022-ben az uniós biztonsági piacra vonatkozó tanulmányt fog előterjeszteni, amely további betekintést nyújt ebbe az összetett ágazatba.** A Bizottság szolgálatai emellett 2022 első felében összefoglalót készítenek a biztonsági ágazatokban alkalmazandó képességorientált megközelítések elfogadásának előmozdítására irányuló javaslatokból. Ezek a javaslatok megerősítik a biztonsággal és a bűnüldözéssel kapcsolatos igények és megoldások korai és előrettekintő azonosítását.

A világtér és a kibertér stratégiai „támogató tényezők” a biztonsági és a védelmi ágazat számára. Az űrágazat az említett ágazatok számos sajátosságával rendelkezik: piaci volumene kicsi, és a komponensek magánpiacára korlátozott befolyást gyakorol. Az űrprogramok és az űrértékláncok rezilienciája kritikus fontosságú az EU biztonsági és védelmi célkitűzései szempontjából. A kibertér szintén egyre fontosabb szerepet játszik a védelmi képességek terén, valamint odafigyelést és beruházásokat igényel. A polgári és a védelmi eszközöket és hálózatokat egyaránt érintik a gyorsan szaporodó kibertámadások, valamint a polgári ágazat egyre nagyobb szerepet játszik a kiberinnovációban és -szabványosításban, ezért szorosabb kapcsolatra van szükség a kiberbiztonság és a kibervédelem között. „A Bizottság európai védelemhez való hozzájárulása a stratégiai irányítással összefüggésben” című közlemény (a továbbiakban: a védelmi közlemény), amely a védelmi csomag részét képezi, további intézkedéseket vázol fel a két ágazatra vonatkozóan.

2.2. A biztonsági és védelmi szempontból kritikus technológiák és stratégiai függőségek feltérképezése

A frissített ipari stratégia – az érzékeny ökoszisztémákra vonatkozó részletes vizsgálatok első fordulója⁷ alapján – átfogóan feltérképezi és elemzi az EU stratégiai függőségeit és kapacitásait. Bár ez a munka megteremtette az alapot az EU rezilienciájának javítását célzó szakpolitikai intézkedésekhez, azt is elismeri, hogy további kell dolgozni azon, hogy jobban megértsük az EU stratégiai függőségeit, valamint azt, hogy ezek hogyan fejlődhetnek és vezethetnek további sebezhetőségekhez. Ez a munka magában foglalja az érzékeny ökoszisztémákra vonatkozó részletes vizsgálatok második fordulóját, valamint a Kritikus Technológiák Megfigyelőközpontján (a továbbiakban: a megfigyelőközpont) keresztül megvalósuló nyomkövetési rendszert, lásd a 2.3. szakaszt.

A Bizottság szolgálatai a frissített ipari stratégia és a megfigyelőközpont fejlesztésének támogatása érdekében megkezdték a védelmi és biztonsági technológiai területek – többek között a kiberbiztonság – mélyreható felülvizsgálatát. Eddig két előzetes esettanulmány készült az autonóm rendszerek és félvezetők védelmi technológiai területeiről, amelyeket reprezentatív mintának tekintettek, mivel a különböző területeken a katonai képességek szempontjából horizontális jelentőséggel bírnak (lásd: 1. keretes írás). A cél az volt, hogy azonosítsák az e védelmi technológiai területek közötti közös mintákat, különös tekintettel a függőségek és a kapcsolódó kockázatok okaira, valamint ezek enyhítésének kezdeti módjaira.

Az esettanulmányok megerősítik, hogy a védelmi ágazat általában ugyanazokkal a stratégiai függőségekkel és sebezhetőségekkel rendelkezik, mint más érzékeny ökoszisztémák, különösen a technológiai hiányosságok, a (kritikus) nyersanyagok, a készségek, az alacsony KTF+I beruházások, valamint a nem uniós országok területen kívüli szabályozásai tekintetében. Azt is jelzik, hogy az ágazat sebezhetőségeit általában súlyosítja tevékenységeinek stratégiai és érzékeny jellege (pl. az információbiztonság és az ellátásbiztonság magasabb színvonala) és viszonylag marginális piaci mérete.

Az esettanulmányok továbbá azt mutatják, hogy az EU néhány globális versenytársa az EU-hoz képest több offenzív és defenzív intézkedést tesz a kritikus technológiák előmozdítása és a stratégiai függőségek kezelése érdekében. Például szisztematikusabban összekapcsolják a nemzetvédelmi megfontolásokat a polgári technológiafejlesztéssel, jelentős beruházásokat eszközölnék a saját KTF+I és ipari kapacitásukba, külső befektetőket vonzanak be, és időnként agresszív felvásárlási stratégiákat alkalmaznak harmadik országokban. Emellett védik saját ipari szakértelmüket és befolyásukat azáltal, hogy fokozzák a kölcsönös függőségeket, illetve szigorú, területen kívüli szabályozásokat alkalmaznak, hogy korlátozzák a harmadik országok technológiákhoz való hozzáférését.

Bár az EU-nak megvannak a saját eszközei ahhoz, hogy az uniós szabályoknak megfelelően megerősítse ipari kapacitását, azt hátráltatja az uniós védelmi piaci kereslet még mindig nagymértékű szétterjedettsége, a polgári és a védelmi KTF+I régóta tartó szigorú uniós szintű szétválasztása, valamint az európai védelmi technológiai és ipari bázisba (EDTIB) irányuló tagállami beruházások viszonylag alacsony szintje. A tagállamok védelmi innovációra fordított

⁷ [SWD\(2021\) 352 final](#)

együttes kiadásai (2,5 milliárd EUR, azaz a védelmi kiadások 1,2 %-a) továbbra is elmaradnak az Európai Védelmi Ügynökség (EDA) 15 évvel ezelőtti 2 %-os célkitűzésétől.

Noha a piaci erők olyan helyzetbe vezettek, amelyben egyetlen ország sem képes teljes technológiai szuverenitást elérni egy adott technológiai területen, globális verseny folyik a technológiai vezető szerepért és a kapcsolódó gazdasági és katonai előnyökért. Ez súlyosbíthatja az EU meglévő stratégiai függőségeit, és újakat teremthet, ha az EU nem tesz lépéseket. Strukturált megközelítésre van szükség ahhoz, hogy az EU továbbra is a kritikus technológiák élvonalában maradjon, valamint hogy azonosítsa és enyhítse a biztonság és a védelem területén fennálló stratégiai függőségeket. Az ütemterv célja egy ilyen megközelítés biztosítása, amelyet bele kell foglalni az uniós stratégiai iránytűbe.

1. keretes írás: Esettanulmányok – autonóm védelmi rendszerek és félvezetők

A Bizottság autonóm védelmi rendszerekkel kapcsolatos elemző munkája – amely különös figyelmet szentelt a mesterséges intelligenciának (MI) és a gépi tanulásnak – azonosította a releváns kritikus technológiákat és négy olyan fő területet, ahol az EU lemaradásban van, nevezetesen: készségek, adatok, hardver és tesztelés. A kezelésükre irányuló lehetséges intézkedések a meglévő uniós MI-stratégiára⁸ és a kapcsolódó szakpolitikai kezdeményezésekre, valamint a tagállamok MI-re vonatkozó nemzeti stratégiáira épülnének. Ide tartoznak a KTF+I tevékenységek (pl. az adatok és az MI-vel kapcsolatos képzés fokozott elérhetősége, kapcsolat az „Európai processzor” kezdeményezéssel), az infrastruktúra (pl. a felhőalapú számítástechnikai kapacitás védelmi célokra, belföldi tesztelési létesítmények) és a meglévő kritikus eszközök védelme (pl. a közvetlen külföldi befektetések átvilágítása).

A védelmi célú félvezetőkkel kapcsolatos elemző munka rávilágított arra, hogy a félvezetők mindenütt jelen vannak a védelmi felszerelésekben, valamint kiemelte a meglévő és jövőbeli függőségeket, amelyeket különösen a legfejlettebb csomópontok tekintetében fennálló saját uniós kapacitás (öntödék) hiánya okoz. A Bizottság enyhítő intézkedéseket foglalt bele a csipekről szóló, 2022. február 8-án elfogadott európai jogszabályjavaslatba⁹, amelynek célja a legkorszerűbb európai csip-ökoszisztéma létrehozása az uniós képességek javítása érdekében ezen a területen, és ezáltal a védelmi szükségletek kielégítése.

2.3. A Kritikus Technológiák Megfigyelőközpontja

Az EU harmadik országoktól való egyes meglévő stratégiai függőségeinek (pl. távirányítású rendszerek, félvezetők) részben az az oka, hogy nem látták előre a technológiák jövőbeli jelentőségét. Az EU-nak strukturáltabb előrejelzésre és stratégiai gondolkodásra van szüksége a biztonsági és védelmi szempontból kritikus technológiákkal kapcsolatban annak érdekében, hogy kiemelt területeket azonosítson a kutatás és innováció fellendítése, a meglévő stratégiai függőségek csökkentése és az újak kialakulásának elkerülése érdekében.

Ezt a gondolkodást fogja elősegíteni a Kritikus Technológiák Uniós Megfigyelőközpontja, amelyet a Bizottság jelenleg hoz létre a szinergiákról szóló cselekvési tervvel (4. intézkedés)

⁸ [COM\(2018\) 237 final](#)

⁹ [COM\(2022\) 45 final](#)

összhangban. A megfigyelőközpont munkamódszerei a párhuzamosságok elkerülése érdekében más hasonló kezdeményezéseket¹⁰ is figyelembe fognak venni. Ez lehetővé teszi a szinergiákról szóló cselekvési tervben szereplő kritikus technológiák listájának finomhangolását, hogy az tükrözze a változó technológiai környezetet és képességeket.

A megfigyelőközpont azonosítja, nyomon követi és értékeli az új-, a védelmi és a kapcsolódó polgári ágazatok számára kritikus technológiákat, azok potenciális alkalmazását, valamint a kapcsolódó érték- és ellátási láncokat. Emellett azonosítja, nyomon követi és elemzi a meglévő és kiszámítható technológiai hiányosságokat, a stratégiai függőségek és sebezhetőségek kiváltó okait.

Alapvető fontosságú, hogy a tagállamokkal érdemi részletességű megállapodás jöjjön létre e kérdések uniós szintű megvitatása érdekében, valamint arról, hogy a releváns adatokat meg kell osztani a tagállamokkal és a Bizottsággal. A megfigyelőközponton belül külön szakértői csoport formájában mechanizmust hoznak létre a tagállamokkal minősített környezetben folytatott eszmecsere és vitára. Ennek keretében többek között megvitatják majd az új és forradalmi technológiák megjelenését, hogy el lehessen kerülni a biztonsági, védelmi és úripartól való új függőségek kialakulását. A főképviselő és szolgálatai részt vesznek majd ebben a folyamatban.

A Bizottság a megfigyelőközpont adatai alapján 2022 végéig, majd azt követően két évente minősített jelentést nyújt be a tagállamoknak a kritikus technológiákról, valamint a biztonságot, a világúrt és a védelmet érintő stratégiai függőségekkel kapcsolatos kockázatokról. A Bizottság e jelentések alapján technológiai ütemterveket fog készíteni, amelyek magukban foglalják a KTF+I fellendítését, valamint a biztonságot és a védelmet érintő stratégiai függőségek csökkentését célzó enyhítő intézkedéseket.

Amint a megfigyelőközpont megfelelően működik, munkája kiterjeszhető más iparágakra is, amint azt a frissített ipari stratégia is jelzi.

A következő lépések:

- 2022-ben a Bizottság szakértői csoportot hoz létre, hogy megkönnyítse a kritikus technológiákról, az érték- és ellátási láncokról a tagállamokkal folytatott információcserét. Ez a szakértői csoport a védelem, az úrkutatás és a kapcsolódó polgári iparágak kritikus technológiáival foglalkozó megfigyelőközpont része lesz. A cél a következő lenne:
 - rendszeres konzultáció folytatása a tagállamok hatóságaival a minősített jelentés elkészítése érdekében,
 - a Kritikus Technológiák Megfigyelőközpontja keretében kicserélhető érzékeny és minősített adatok, valamint a kapcsolódó jelentések és ütemtervek megfelelő kezelésének biztosítása.
- 2022 közepéig a Bizottság tanulmányt terjeszt elő az EU biztonsági piacáról, amelynek célja a polgári biztonsági piac sajátosságainak jobb megértése, a kritikus technológiák és a stratégiai függőségek azonosításának támogatása, valamint a biztonságra és más KTF+I

¹⁰ Például a fejlett ipari technológiák (ATI) támogatása és eszközei, az úrkutatás szempontjából kritikus technológiák nyomon követése, az Európai Védelmi Ügynökség (EDA) átfogó stratégiai kutatási menetrendje (OSRA), technológiai építőelemei (TBB) és kiemelt stratégiai tevékenységei (KSA).

tevékenységekre vonatkozó új képességorientált megközelítés alátámasztása.

- 2022 közepéig a Bizottság szolgálatai összefoglalót készítenek a biztonsági ágazatokban alkalmazandó képességorientált megközelítések elfogadásának előmozdítására irányuló javaslatokból.

3. A biztonsági és védelmi szempontból kritikus technológiákkal kapcsolatos KTF+I fellendítése

A Bizottság által a megfigyelőközpont értékelései alapján elkészítendő technológiai ütemtervek a kritikus technológiákkal kapcsolatos KTF+I programozásától a nagyobb kiemelt kezdeményezések kidolgozásáig terjedő tevékenységek alapjául szolgálnak majd, amelyek hozzájárulnak az EU versenyképességének és rezilienciájának megerősítéséhez a biztonsági és a védelmi ágazatban. E célkitűzések megvalósítása érdekében a meglévő uniós és nemzeti KTF+I programok és eszközök jobb összehangolása révén hatékonyabban kell felhasználni a rendelkezésre álló pénzügyi forrásokat.

3.1. Az uniós polgári és védelmi KTF+I szétválasztásának megszüntetése

A Bizottság a szinergiákról szóló cselekvési terve (2. intézkedés) értelmében kötelezettséget vállalt arra, hogy 2022-ig fokozza az uniós programok és eszközök közötti belső koordinációt (lásd: 2. keretes írás) annak érdekében, hogy felszabadítsa a polgári és a védelmi KTF+I közötti szinergiákat, amelyek hatalmas előnyöket rejtenek a gazdasági növekedés, az egységes piac és az európai polgárok biztonsága szempontjából.

Bár e célkitűzés megvalósítása 2023-ban is folytatható (pl. jobb tervezés és szinkronizálás, a tagállamok irányító hatóságainak nyújtott iránymutatás stb. révén), egyes akadályok rövid és középtávon nehezebben kezelhetők, és más érdekelt felek bevonását tehetik szükségessé. Ez a helyzet különösen akkor, ha az uniós programok és eszközök alap-jogiaktusainak jogi rendelkezései gyakorlati korlátokat szabnak. Például míg a kettős felhasználású tevékenységek finanszírozhatók az Európai Hálózatfinanszírozási Eszköz (CEF) és az európai strukturális és beruházási alapok (esb-alapok) keretében, a Horizont Európa¹¹ keretében végzett tevékenységek a polgári alkalmazásokra összpontosítanak; a KTF+I programoknál és eszközöknél nincs keret az ilyen tevékenységek közvetlen támogatására. Ehhez hasonlóan az Európai Beruházási Bank hitelezési politikája továbbra is korlátozza a védelmi ágazatot.

A polgári és a védelmi közösségek közötti cserék megkönnyítése érdekében – különösen a kritikus technológiák területén – a Bizottság 2023-ban kidolgozza a kettős felhasználású KTF+I uniós szintű ösztönzésére vonatkozó megközelítést, amelyet közép- és hosszú távon teljes mértékben végre kell hajtani az uniós programokban és eszközökben. Ez a munka a releváns ágazati programok – például a közös rendelkezésekről szóló rendelet szerinti alapok, többek

¹¹ Ebben a dokumentumban a „Horizont Európa” kifejezés a Horizont Európa kutatási és innovációs keretprogram végrehajtását szolgáló egyedi programra és az Európai Innovációs és Technológiai Intézetre utal; az ezek keretében végzett tevékenységek kizárólag a polgári alkalmazásokra összpontosítanak.

között az egészségügyi szükséghelyzet-felkészültségre szánt alapok – félidős értékeléséhez is hozzájárulást nyújt.

2. keretes írás: A biztonság és védelem szempontjából releváns kritikus technológiákkal kapcsolatos KTF+I-t, valamint ezek infrastruktúrájának kiépítését támogató uniós programok és eszközök a többéves pénzügyi keretben (2021–2027)

- Az EDF 8 milliárd EUR-t fordít a védelmi kutatásra és fejlesztésre. Az EDF kutatási-fejlesztési költségvetésének 4–8 %-át – azaz évente akár 100 millió EUR-t – a forradalmi technológiákra fordítják.
- A Horizont Európa a „Globális kihívások és európai ipari versenyképesség” elnevezésű II. pillér keretében 1,6 milliárd EUR-t allokál a polgári biztonsági kutatásra és innovációra „A társadalmat szolgáló polgári biztonság” klaszteren belül, míg a kritikus technológiákat a „Digitális gazdaság, ipar és világűr”, az „Éghajlat, energiaügy és mobilitás”, valamint az „Élelmiszerek, biogazdaság, természeti erőforrások, mezőgazdaság és környezet” klaszter keretében támogatja. A kiegészítő tevékenységeket a „Kiváló tudomány” elnevezésű I. pillér, az „Innovatív Európa” elnevezésű III. pillér – az Európai Innovációs Tanács (EIC) és az Európai Innovációs és Technológiai Intézet (EIT) –, valamint az európai partnerségek keretében finanszírozzák, amelyek egyesítik és mozgósítják az erőforrásokat annak érdekében, hogy a kritikus területeken biztosítsák az EU technológiai vezető szerepét és nyitott stratégiai autonómiáját.
- A Digitális Európa program (DEP) elő fogja mozdítani a kritikus technológiákhoz kapcsolódó kiépítési tevékenységeket a kiberbiztonság, az MI és a szuper-számítástechnika kiemelt területein.
- A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a koordinációs központok hálózata 2022-ben a kiberbiztonsági beruházásokra vonatkozó stratégiai menetrendet fog elfogadni, amely hozzájárulást nyújt a Horizont Európához és a Digitális Európa programhoz. A polgári és a védelmi technológiák, valamint a kettős felhasználású alkalmazások közötti szinergiákat fel lehet tárni az EDF-hez való kapcsolódás révén, az alkalmazandó szabályokkal összhangban.
- Az esb-alapok (különösen az Európai Regionális Fejlesztési Alap és az Európai Szociális Alap+ esetében) felhasználhatók az EDTIB támogatására.
- Az egyéb releváns uniós programok, alapok és eszközök közé tartozik az újprogram, az Európai Hálózatfinanszírozási Eszköz, az InvestEU program, a Helyreállítási és Rezilienciaépítési Eszköz, a LIFE program, a köz- és magánszféra közötti partnerségek, valamint a vegyes finanszírozási eszközök.

3.2. A biztonsági és védelmi szempontból kritikus technológiákkal kapcsolatos KTF+I-t támogató uniós és nemzeti programok és eszközök összekapcsolása

Az uniós programok és eszközök jelentős finanszírozást nyújtanak az uniós biztonsági és védelmi KTF+I tevékenységekhez, azonban az ilyen tevékenységek többségét továbbra is a tagállamok finanszírozzák, és a biztonsági és védelmi piacok széttöredezettsége továbbra is komoly problémát jelent. Ebből következően egyes kritikus technológiai területeken a technológiai szuverenitás eléréséhez, más területeken pedig a stratégiai függőségek enyhítéséhez uniós szintű koordinációra lesz szükség.

A Bizottság felkéri a tagállamokat, hogy a stratégiai iránytűben vállaljanak kötelezettséget arra, hogy a Bizottsággal együtt a kezdetektől fogva uniós szintű, összehangolt stratégiai megközelítést dolgozzanak ki a biztonság és a védelem szempontjából releváns kritikus technológiákra vonatkozóan, teljes mértékben tiszteletben tartva az uniós és nemzeti programok és eszközök irányításának sokféleségét és összetettségét. Ez a megközelítés más koordinációs struktúrákat is figyelembe venne, például a Belső Biztonságra Vonatkozó Operatív Együtműködéssel Foglalkozó Állandó Bizottság (COSI) által elnökölt, a belső biztonság új uniós innovációs központját, valamint az EDA által létrehozandó új uniós védelmi innovációs központot.

A megközelítés a kritikus technológiákról szóló minősített jelentéseket és a Bizottság által készített technológiai ütemterveket használná kiindulópontként a tagállami hatóságok és a Bizottság közötti megbeszélésekhez. A cél az lenne, hogy a technológiai ütemtervek alapján azonosítsák a legsürgetőbb fellépést igénylő területeket, és mozgósítsák az EU és a tagállamok programjait, eszközeit és politikáit annak érdekében, hogy azokat az állami támogatásokra vonatkozó uniós szabályokkal összhangban, összehangolt módon kezeljék. Ez biztosítaná, hogy a beruházások azokra a területekre összpontosuljanak, amelyek a leginkább fontosak az uniós polgárok biztonsága szempontjából. A prioritásokat rendszeresen frissítenék annak biztosítása érdekében, hogy azok továbbra is relevánsak maradjanak, és a kiadások hatékonyak legyenek.

A Bizottság együtt fog működni a tagállamokkal annak érdekében, hogy meghatározza a koordinációs munka elősegítésére szolgáló legjobb mechanizmust (pl. a megfigyelőközpont szakértői csoportja).

3.3. A biztonsági és védelmi innováció és vállalkozói készség támogatása – Az uniós védelmi innovációs program létrehozása

Az EU-nak a biztonság és a védelem támogatása érdekében jobban ki kell használnia az innovációs közösségében rejlő lehetőségeket. Ehhez az szükséges, hogy a két ágazatban a nem hagyományos szereplők és a meglévő innovatív induló vállalkozások és kis- és középvállalkozások (kkv-k) segítséget kapjanak ahhoz, hogy leküzdjék a jelentős technológiai, igazgatási, szabályozási és a piacra lépést nehezítő akadályokat, valamint megfeleljenek a magas szintű biztonsági szabványoknak és hozzáférjenek a finanszírozási eszközökhöz. A védelmi piac gyakran néhány nagy szereplő köré szerveződik, amelyeket olyan szakosodott kkv-k támogatnak, melyek csak korlátozottan férnek hozzá közvetlenül ehhez a piachoz. Ennek következtében az innovatív védelmi kkv-k nehezen juthatnak finanszírozáshoz, ami növelheti annak valószínűségét, hogy külföldi befektetőkhez fordulnak, vagy azok célpontjaivá válnak. Hasonló a helyzet az innovatív biztonsági kkv-k esetében is, amelyek hasonló kihívásokkal szembesülnek a potenciális ügyfelek megkeresése vagy a testreszabott finanszírozáshoz való hozzáférés terén¹².

A Bizottság az induló innovatív biztonsági vállalkozásokat és kkv-ket a Horizont 2020 keretében támogatta, ahol a 7. társadalmi kihívás („A társadalmat szolgáló polgári biztonság”) keretében allokált finanszírozás és általános sikerességi arány a kis innovátorok esetében átlag feletti volt.

¹² [Kihívások és lehetőségek a kkv-k és az induló innovatív vállalkozások számára az uniós biztonsági kutatásban és innovációban](#), CERIS SSRI virtuális rendezvény, 2021. április 30.

Ez a támogatás a Horizont Európa keretében is folytatódik, az induló biztonsági vállalkozásoknak és kkv-knek azonban további testreszabott támogatásra lesz szükségük ahhoz, hogy felgyorsítsák a piacra jutásukat. A kettős felhasználású innováció új eszközeinek feltárása fokozhatja termelési kapacitásukat, versenyképességüket és fenntarthatóságukat.

A Bizottság hasonló tevékenységeket kezdett az EDF keretében a védelem és a kettős felhasználású innováció 1–9. technológiai készenléti szintre (TRL-ek)¹³ kiterjedő eszközkészletének kidolgozása érdekében. Folyamatban van a védelem, az új technológiák és a kettős felhasználás területére vonatkozó alábbi eszközökkel kapcsolatos munka:

- a) *Védelmi innováció az EDF-en keresztül*: jelenleg folyik konkrét intézkedések feltérképezése a forradalmi technológiákkal, valamint az innovatív és jövőorientált védelmi megoldásokkal kapcsolatos projektek jobb támogatása érdekében, ösztönözve különösen az innovatív kkv-k, az innovatív laboratóriumok, valamint a kutatási és technológiai szervezetek (ktsz-ek) részvételét. Ezek az intézkedések különböző formákat ölthetnek, például üzleti coaching (2021. évi munkaprogram); technológiai kihívások (WP2022. évi munkaprogram), hackathonok vagy pénzdíjak (2023. évi vagy későbbi munkaprogram). Emellett az EIC releváns tapasztalataira is támaszkodni fognak, és kapcsolódhatnak az új védelmi „Cassini” ürvállalkozási kezdeményezéshez.
- b) *A védelmi beruházások vegyes finanszírozási eszköze az InvestEU keretében*: egy ilyen eszköz létrehozása lehetővé tenné a Bizottság számára, hogy Unió-szerte garantálja a pénzügyi közvetítők által az innovatív vagy stratégiai védelmi kkv-kbe eszközölt beruházásokat. Ez enyhítené azokat a problémákat, amelyekkel az európai védelem szempontjából ígéretes technológiákat fejlesztő kkv-k a finanszírozási eszközökhöz való korlátozott hozzáférés miatt szembesülnek, ugyanakkor megbízható tőkét biztosítana, és elkerülhetővé tenné a harmadik országbeli jogalanyok általi ellenséges felvásárlásokat. Annak lehetővé tétele, hogy az innovatív védelmi kkv-k és közepes piaci tőkeértékű vállalatok jobban hozzáférjenek a sajáttőke-finanszírozáshoz, támogatná növekedésüket, és végső soron elősegítené az EDTIB innovatív jellegét. A Bizottság továbbá meg fogja vizsgálni, hogy szükség van-e további eszközökre az értéklánc kulcsfontosságú piaci szereplőinek támogatására.
- c) *Védelmi Cassini*: ezt a kezdeményezést a meglévő „Cassini” kezdeményezés inspirálná, amely az úriparban működő kkv-k és induló innovatív vállalkozások támogatására irányul. A következő szolgáltatásokat nyújtaná számukra: vállalkozásfejlesztés és hálózatok (pl. kapcsolatteremtés, vállalkozás-akcelátor), pénzdíjak és versenyek (beleértve a hackathonokat, mentorálást stb.), amelyek kiegészítik a védelmi beruházások fent említett vegyes finanszírozási eszközét.

¹³ Az EU 2014 óta széles körben elfogadta a technológiai készenléti szint (TRL) alkalmazását a KTF+I programjai és eszközei keretében. A skála kilenc technológiai érettségi szintet különböztet meg, az 1. TRL alatti alapkutatástól a 9. TRL alatti piacra lépésre kész végtermékig. Mivel egy technológia alkalmazása és így a kettős felhasználású potenciál jellemzően az 5–6. TRL-en derül ki, úgy tekinthető, hogy az adott technológia a TRL 1–4. szintjén „semleges”.

- d) *Innovációs inkubátor*: a Bizottság 2022-ben innovációs inkubátort hoz létre az új technológiák fejlesztésének támogatása és a kettős felhasználású innovációnak a szinergiákról szóló cselekvési tervvel összhangban történő alakítása érdekében (6. intézkedés), amely fontos szerepet játszhat a polgári és a védelmi vonatkozású KTF+I programok közötti szakadék áthidalásában. A korai szakaszban történő technológiafejlesztés eredményeinek szisztematikus elemzését követően az inkubátor azokat a projekteket és/vagy technológiákat jelölné meg a Bizottság és a tagállamok érintett szolgálatainak számára, amelyek általuk is bevezethető, potenciális biztonsági, ür- vagy védelmi alkalmazások kifejlesztéséhez vezethetnek. A Bizottság értékelné, hogy ezeket a megjelölt projekteket adott esetben hogyan lehetne további finanszírozási lehetőségekhez – például az EIC vagy az EDF átmeneti finanszírozási rendszeréhez – juttatni.
- e) *Az innovációs hálózatok támogatása*: a határokon átnyúló védelmi innovációs hálózatok innovációs közvetítői szerepet tölthetnek be, és ösztönözhetik az együttműködésen alapuló projekteket az innovatív megoldások integrálása érdekében. A technológiai kutatás feltárná és azonosítaná azokat az új innovatív megoldásokat és technológiákat, amelyek potenciálisan előnyösek lehetnek a védelmi alkalmazások tekintetében. A kutatóközpontok és a műszaki vizsgálólétesítmények ezt követően tesztelnék a polgári területről származó ilyen technológiák relevanciáját, és megosztanák egymással a bevált gyakorlatokat. Az EDA a Bizottság központi partnere lenne a szinergiákról szóló cselekvési terv 6. intézkedése egy tovább részének végrehajtásában.

A Bizottság meg fogja határozni, hogy miként kapcsolható össze az eszköztár az innovációt támogató eszközökkel a biztonság (pl. a Horizont Európa) vagy a kiberbiztonság területén (pl. a nemzeti kiberbiztonsági koordinációs központok hálózata az európai digitális innovációs központokkal együttműködésben).

A Bizottság és az EDA egymást kiegészítő erősségeit egy „**uniós védelmi innovációs program**” keretében kell összefogni. A program keretében a Bizottság – az uniós költségvetésnek a védelmi, a polgári és kettős felhasználású KTF+I támogatása céljából történő végrehajtása terén szerzett tapasztalatai alapján – központi szerepet játszik majd abban, hogy az EDTIB számára ösztönözze az innovációt. Tekintettel védelmi szakértelmére – többek között a kialakulóban lévő és forradalmi technológiák, valamint a katonai képességre vonatkozó követelmények összekapcsolása terén –, az EDA a védelmi innovációs központján keresztül továbbra is összekapcsolja és támogatja a tagállamok erőfeszítéseit. A szoros együttműködés révén a Bizottság és az EDA egymással szinergiában felgyorsítja az EU és tagállamai biztonsági és védelmi innovációját.

3.4. Készségek

A készségek és a munkaerő hiánya – különösen a természettudományok, a technológia, a műszaki tudományok és a matematika terén tapasztalattal rendelkező szakképzett munkavállalók esetében – jelentős kihívást támaszt a védelmi és biztonsági ipar számára, amely sok más csúcstechnológiai iparághoz hasonlóan nagymértékben támaszkodik rájuk. Mivel a technológia és a fenyegetettség helyzete gyorsan változik, fontos, hogy az ágazat jobban bevonja az új és fiatal kutatókat és vállalkozókat, köztük a nőket is, valamint inkluzív és hozzáférhető

megközelítést alkalmazzon valamennyi tehetség, készség és a rendelkezésre álló munkaerő tekintetében.

2020 novemberében a Bizottság elindította a készségfejlesztési paktumot, és ezzel a készségfejlesztési partnerségek első hullámát a mikroelektronika, a gépjárműipar, valamint az űr- és védelmi ipar három kulcsfontosságú ipari ökoszisztémájában. A paktum tagjai (iparágak, egyetemek és képzési szervezetek, szociális partnerek) elkötelezettek amellett, hogy azokon a területeken, ahol azokra a legnagyobb szükség van, folyamatos és fenntartható készségkínálatot biztosítanak 200 000 munkavállaló továbbképzése és 300 000 ember átképzése révén, és 2030-ig 1 milliárd EUR összegű köz- és magánberuházást hajtanak végre.

A következő lépések:

- A Bizottság felkéri a tagállamokat, hogy a stratégiai iránytűben vállaljanak kötelezettséget arra, hogy a biztonság és a védelem szempontjából releváns kritikus technológiák tekintetében már a kezdetektől fogva uniós szintű, összehangolt stratégiai megközelítést dolgoznak ki.
- 2023-ban a Bizottság felül fogja vizsgálni a meglévő uniós eszközöket, és további megoldásokat fog javasolni a kettős felhasználású KTF+I uniós szintű ösztönzésére.
- A Bizottság a következő eszközök alapján támogatja a biztonsági és védelmi szempontból kritikus technológiákkal kapcsolatos innovációt és vállalkozói készséget: a) célzott EDF-fellépések; b) az InvestEU keretében létrehozott új védelmi beruházások vegyes finanszírozási eszköze; c) egy új védelmi Cassini; d) az új technológiák és a kettős felhasználású innováció új innovációs inkubátora 2022-ben; valamint e) az innovációs hálózatok fokozott támogatása.
- A Bizottság az EDA-val és annak védelmi innovációs központjával együtt uniós védelmi innovációs programot hoz létre annak érdekében, hogy felgyorsítsa az EU és tagállamainak biztonsági és védelmi innovációját.

4. A biztonsági és védelmi szempontból kritikus technológiák és értékláncok stratégiai függőségeinek csökkentése

Az EU a KTF+I programjain és eszközein kívül számos olyan szakpolitikai eszközzel rendelkezik, amelyek segítségével csökkenthetők a kritikus technológiáktól és értékláncoktól való stratégiai függőségei a biztonsági és a védelmi ágazatban. Mindezek hozzájárulnak az EU ipari kapacitásának, versenyképességének, technológiai szuverenitásának és rezilienciájának megerősítéséhez, valamint a jelenlegi és jövőbeli technológiai fejlesztések és képességek védelméhez.

A Bizottság – a Kritikus Technológiák Megfigyelőközpontja által végzett munka alapján és a frissített ipari stratégia keretében – adott esetben szisztematikusan értékelné fogja a biztonsági és védelmi megfontolásokat a meglévő uniós ipari és kereskedelmi eszközök végrehajtása és felülvizsgálata, illetve újak kidolgozása során annak biztosítása érdekében, hogy azok megfeleljenek a célnak.

- *Ipari szövetségek:* az ipari szövetségek a partnerek széles körét (pl. állami és magánszereplők, civil társadalom) vonják be a kulcsfontosságú uniós szakpolitikai célkitűzésekre irányuló közös fellépésekbe az egyes iparágakban vagy értékláncokban. A szövetségek a nyilvánosság, az átláthatóság, a sokféleség és az inkluzivitás elvén alapulnak, és a versenyszabályokkal teljes összhangban működnek. Az ipari szövetségek adott esetben konkrét munkaterületekre is kiterjedhetnek a biztonsági és védelmi ágazat stratégiai függőségeinek csökkentése érdekében. Ennek mérlegelése jelenleg folyik az Európai Ipariadat- és Számításifelhő-szövetség, valamint a processzorokkal és félvezető technológiákkal foglalkozó ipari szövetség keretében.
- *Közös európai érdeket szolgáló fontos projektek:* a közös európai érdeket szolgáló fontos projekteket a tagállamok kezdeményezik, és azokra az uniós állami támogatási szabályok vonatkoznak. E projekteket úgy alakítják ki, hogy azok Uniós-szerte összefogják a tudást, a szakértelmet, a pénzügyi erőforrásokat és a gazdasági szereplőket azzal a céllal, hogy leküzdjék azokat a piaci vagy rendszerszintű hiányosságokat és társadalmi kihívásokat, amelyeket a magánszereplők egyedül nem tudnának kezelni, különösen az áttörést hozó innováció és a kulcsfontosságú infrastruktúrák területén. A közös európai érdeket szolgáló fontos projektek figyelembe tudják venni a biztonsági és védelmi szempontokat. Ez igaz lehet a mikroelektronikára vonatkozóan a közös európai érdeket szolgáló második fontos projekt esetében is, amelyet a csipekről szóló jogszabályban jelentettek be.
- *Uniós finanszírozási programok:* az EU mindig is nyitott kutatási és innovációs politikával rendelkezett, amelyet a nyitott stratégiai autonómia elve vezérel, és célja az egyenlő versenyfeltételek és a kölcsönösség biztosítása. Az EU kutatással és innovációval kapcsolatos globális megközelítése ösztönzi a hasonlóan gondolkodó partnerekkel való, és az EU nemzetközi kötelezettségeivel (pl. NATO, Egyesült Államok, Kanada, Japán, Dél-Korea stb.) összhangban álló stratégiai partnerségeket¹⁴.

Európának ugyanakkor biztosítania kell stratégiai érdekeinek megóvását. A 2021 és 2027 közötti időszakra vonatkozóan a Bizottság az uniós programok és eszközök tekintetében egyértelműsítette és összehangolta a nem uniós országok részvételi szabályait, valamint a szervezetek támogathatóságát. Bizonyos programok (Horizont Európa, DEP, EDF, Űrprogram, CEF) esetében konkrét támogathatósági feltételeket határozott meg a biztonsági szempontból érzékeny tevékenységekre vonatkozóan, és az EU alapvető biztonsági érdekeinek védelme érdekében azokat tovább pontosította a vonatkozó munkaprogramokban. A költségvetési rendelet folyamatban lévő, Bizottság általi felülvizsgálata azt is tisztázni fogja, hogy miként lehet fenntartani az EU nyitott stratégiai autonómiára vonatkozó megközelítését, azaz teljes mértékben megóvni az EU alapvető biztonsági érdekeit, egyúttal pedig tiszteletben tartani nemzetközi kötelezettségeit.

- *Szabványok:* a szinergiákról szóló cselekvési terv keretében a Bizottság előmozdítja a meglévő polgári/védelmi hibrid szabványok alkalmazását és újak 2022 végéig történő kidolgozását (5. intézkedés), valamint a védelem figyelembevételét a Bizottság

¹⁴ Meg kell azonban jegyezni, hogy legtöbb partnerünk védelmi vonatkozású kutatási és fejlesztési programjai nem állnak nyitva az uniós vállalatok előtt.

szabványosítási politikájában és intézkedéseiben. Bár az EU szabványosítási stratégiájának¹⁵ célja, hogy biztosítsa az EU vezető szerepét a polgári szabványok meghatározásában, a védelmi ágazat számára is rendkívül fontos lesz, mivel a védelmi ágazatban alkalmazott szabványok közel 80 %-a polgári ágazatokból származik. A Bizottság az érdekelt felekkel (pl. az EDA-val) együtt megvizsgálja annak lehetőségét, hogy a védelmi követelményeket beépítsék az általa támogatott jövőbeli szabványosítási erőfeszítésekbe annak érdekében, hogy azok jobban megfeleljenek a védelmi szükségleteknek.

- *A közvetlen külföldi befektetések átvilágítása:* az EU a világ egyik legnyitottabb környezete a külföldi befektetések számára, és világszerte a közvetlen külföldi befektetések egyik fő célpontja. Egyes beruházások azonban az EU alapvető biztonsági érdekeit is veszélyeztethetik. Az ilyen kockázatok megelőzése érdekében az EU létrehozta a közvetlen külföldi befektetések átvilágításának keretét, amely 2020 októbere óta működik. A közvetlen külföldi befektetések átvilágításáról szóló első éves jelentés megerősíti, hogy mennyire fontos a közvetlen külföldi befektetések hatékony tagállami szintű átvilágítása és az uniós szintű szoros együttműködés, amely a potenciális biztonsági és közrendi kockázatokra összpontosít. A Bizottság arra ösztönzi a tagállamokat, hogy hozzanak létre a közvetlen külföldi befektetések átvilágítására szolgáló nemzeti mechanizmusokat; 18 tagállam már rendelkezik ilyennel, további hat tagállam pedig jelenleg dolgozik saját mechanizmusának kialakításán. A Bizottság 2023 októberéig értékeli a rendeletet és erről jelentést nyújt be az Európai Parlamentnek és a Tanácsnak.
- *Kritikus infrastruktúrák:* az új és forradalmi technológiák egyre gyorsabb megjelenése jelentős hatást gyakorolt a stratégiai ágazatok – köztük a biztonsági és a védelmi ágazat – berendezéseinek, infrastruktúrájának, szolgáltatásainak, valamint érték- és ellátási láncainak biztonságára. Az EU-nak és a tagállamoknak átfogóbb módon kell figyelembe venniük ezeket a sebezhetőségeket a vonatkozó kockázatértékelésekben és nyomon követésben, valamint a biztonsági fenyegetésekkel – például hibrid vagy kiberfenyegetésekkel – szembeni rezilienciát javító intézkedések végrehajtása során. Uniós koordinációra lesz szükség annak biztosításához, hogy a tagállamok a sebezhetőségek elkerülése érdekében időtálló rezilienciaszintet és következetes uniós szintű biztonsági normákat tartsanak fenn.
- *Intelligens és körforgásos anyagfelhasználás:* a körforgásos gazdaságra vonatkozó, 2020. márciusi új cselekvési terv az európai zöld megállapodás – a fenntartható növekedés új európai menetrendje – egyik fő építőeleme. A fokozott erőforrás-hatékonyságon, az új anyagok kifejlesztésén, a másodlagos nyersanyagok népszerűsítésén és a fenntarthatóbb közbeszerzésen alapuló innováció és új üzleti modellek nemcsak a környezetet védik, hanem az ipar számára is biztosítják az anyagokhoz való hozzáférést. Az additív gyártási technikák, a zöld közbeszerzés és az anyagok újrafeldolgozása – amennyiben azokat megfelelően hajtják végre – szintén hozzájárulhatnak az uniós biztonsági és védelmi ipar versenyképességének és az EU rezilienciájának megerősítéséhez.

¹⁵ [COM\(2022\) 31 final](#)

- *Adatbiztonság*: az európai adatstratégia intézkedéseket határoz meg annak biztosítására, hogy az egyének és a vállalkozások továbbra is ellenőrizni tudják adataikat. Ezzel az adatmegosztási jogszabály foglalkozik majd, amelyet a Bizottság 2022 elején fog elfogadni.
A közös adatinfrastruktúrákra és -szolgáltatásokra irányuló, több országra kiterjedő (az európai felhőszövetséget és a közös európai adattereket összefogó) projekt részeként a Bizottság elősegíti a biztonságos, reziliens, energiahatékony és valós időben hozzáférhető, valamint Európa-szerte minőségi szolgáltatást nyújtó felhő–perem (cloud-to-edge) kapacitásokba történő beruházásokat (pl. DEP, CEF, Next Generation EU alap). A felhő- és peremtechnológiák terén a polgári (különösen a biztonsági), a védelmi és az úripar közötti technológiaátadás fokozná a technológiai szuverenitást. Az Európai Ipariadat- és Számításifelhő-szövetség lehetséges platformot biztosít az ilyen szinergiák előmozdításához.
- *Kereskedelempolitika*: a globális ellátási láncok összetettsége és sebezhetősége nem csak az EU számára jelent problémát. Más országok az EU-tól („fordított függőségek”) függnek, és a kereskedelem („kölcsonös függőség”) hozzájárulhat a globális értékláncok stabilitásához. Az EU arra is készen áll, hogy határozottan fellépjen és megvédje magát a tisztességtelen nemzetközi kereskedelmi gyakorlatokkal – például a torzító hatású külföldi támogatásokkal – szemben, tiszteletben tartva ugyanakkor nemzetközi kötelezettségvállalásait is. Az EU továbbra is maximálisan ki fogja használni a kereskedelmi és versenyszabályainak eszköztárát, egyúttal gondoskodik arról, hogy az uniós eszközök hatékonyak és naprakészek legyenek. A Bizottság ezért olyan új eszközöket javasolt, mint például a külföldi támogatásokról szóló rendelet¹⁶, amely a belső piacon a külföldi támogatások által okozott torzulásokat kezeli.

A védelmi közlemény további releváns szakpolitikai intézkedéseket sorol fel (pl. a hozzáadottérték-adó [héta] alóli esetleges mentesség bevezetése, az uniós finanszírozású védelmi termékek transzferének megkönnyítése).

A következő lépések:

- A Bizottság jelenleg vizsgálja annak lehetőségét, hogy védelmi munkaterületekkel egészítse ki az olyan kezdeményezéseket, mint az Európai Ipariadat- és Számításifelhő-szövetség, valamint a processzorokkal és félvezető technológiákkal foglalkozó szövetség.
- A Bizottság a tagállamokkal együtt 2023-ban meghatározza majd, hogy az EU biztonsági és védelmi érdekeinek jobb védelme érdekében szükség van-e a kritikus infrastruktúrák ellátási láncainak kockázatértékelésére, különösen a digitális területen.
- A Bizottság arra ösztönzi azokat a tagállamokat, amelyek ezt még nem tették meg, hogy hozzanak létre a közvetlen külföldi befektetések átvilágítására szolgáló nemzeti mechanizmust.

¹⁶ [COM\(2021\) 223 final](#)

5. Külső dimenzió

A hasonlóan gondolkodó partnerekkel világszerte folytatott együttműködés elengedhetetlen az EU rezilienciájának és ellátásbiztonságának fokozásához, egyúttal csökkenti a stratégiai függőségeket és fokozza a kölcsönös előnyöket. A viszonyosság elve fontos szerepet játszik ebben az összefüggésben. A technológia, a biztonság és a védelem területén az EU hagyományos partnerei közé tartoznak az Európai Gazdasági Térség tagjai (különösen Norvégia), a tagjelölt országok, a szomszédos országok és más harmadik országok (pl. az Egyesült Államok, Kanada, Japán, Dél-Korea), valamint a nemzetközi szervezetek (pl. a NATO). A közelmúltban különösen a következő eszmecserékre került sor:

5.1. *EU–USA Kereskedelmi és Technológiai Tanács*

Az EU–USA Kereskedelmi és Technológiai Tanács első ülésére 2021. szeptember 29-én került sor. A közös nyilatkozatban az EU és az USA megerősítették elkötelezettségüket az iránt, hogy „a zöld és digitális átállás, valamint polgáraink védelmének biztosítása szempontjából kulcsfontosságú ágazatokban az ellátási láncok rezilienciájának és az ellátás biztonságának előmozdítására összpontosítson”, valamint megerősítették, hogy céljuk „a kínálat és a kereslet átláthatóságának növelése; a meglévő ágazati képességek feltérképezése; a szakpolitikai intézkedésekről, valamint a kutatási és fejlesztési prioritásokról szóló információcsere; továbbá az ellátási lánc rezilienciájának és diverzifikációjának előmozdítását célzó stratégiák kidolgozásában való együttműködés”. A jelenlegi ütemterv szempontjából a biztonságos ellátási láncokkal (ideértve a félvezetőket egy külön eljárás keretében), az információs és kommunikációs technológiák biztonságával, az exportellenőrzéssel és a befektetésátvilágítással foglalkozó munkacsoportokban folyó munka a legrelevánsabb. A közelmúltban elindított EU–USA biztonsági és védelmi párbeszéd is fórumként szolgálhat az e kérdésekről folytatott megbeszélésekhez.

5.2. *Partnerség a NATO-val*

A 2021. évi brüsszeli csúcstalálkozón a NATO vezetői ambiciózus menetrendet határoztak meg a technológiákra, különösen a kialakulóban lévő és a forradalmi technológiára vonatkozóan¹⁷. Ez további iránymutatást nyújtott a NATO védelmi miniszterei által 2021 februárjában jóváhagyott, a NATO-nak az említett technológiákra vonatkozó végrehajtási stratégiájával összhangban végzett munkához,

A Bizottság és a főképviselelő a NATO-val való rendszeres munkakapcsolat révén figyelemmel kíséri a releváns NATO-kezdeményezések előrehaladását ezen a területen annak érdekében, hogy lehetséges, kölcsönösen elfogadható és előnyös kölcsönhatás alakuljon ki a kapcsolódó uniós kezdeményezésekkel, a tagállamok számára teljes átláthatóság mellett, elkerülve ugyanakkor az új technológiai vagy képességbeli függőségek kialakulását vagy a meglévők növelését.

¹⁷ amely magában foglalta az Atlanti-óceán északi részére vonatkozó védelmi innovációs akcelerátor (DIANA) és a NATO innovációs alapjának elindításáról szóló határozatot.

A következő lépések:

- A Bizottság és a főképvisele az EU–USA Kereskedelmi és Technológiai Tanács, valamint a közelmúltban elindított, a biztonságról és védelemről szóló EU–USA párbeszéd keretében meg fogja vizsgálni, hogy miként lehetne előmozdítani az ellátási lánc rezilienciáját és biztosítani polgáraink védelmét.
- A Bizottság és a főképvisele – az EU–NATO együttműködésről szóló együttes nyilatkozatok keretében és a tagállamok számára biztosított teljes átláthatóság mellett – a NATO-val közösen meg fogja vizsgálni, hogy miként lehetne előmozdítani a vonatkozó kezdeményezések közötti kölcsönösen elfogadható és előnyös kölcsönhatást.

6. Következtetések

Mivel a globális geopolitikai helyzet továbbra is összetett, és folytatódik a verseny a biztonság és a védelem szempontjából releváns új technológiákért, az EU-nak és tagállamainak meg kell erősíteniük együttműködésüket az Európa hosszú távú biztonsága és védelme szempontjából kritikus fontosságú technológiák, valamint a kapcsolódó stratégiai függőségek csökkentésére irányuló erőfeszítések tekintetében.

Az ütemterv a tagállamokkal való szoros együttműködést javasol a biztonság és a védelem szempontjából kritikus technológiák és értékláncok – valamint a Kritikus Technológiák Megfigyelőközpontjának keretében a kapcsolódó stratégiai függőségek kiváltó okainak – azonosításában. Ennek az a célja, hogy alátámassza a biztonság és a védelem szempontjából releváns kritikus technológiákra vonatkozó uniós szintű, összehangolt stratégiai megközelítést, amely maximálisan ki fogja használni az uniós és nemzeti KTF+I programokat és eszközöket.

A biztonsági és a védelmi ágazat versenyképességének és rezilienciájának fokozása érdekében a megfigyelőközpont megállapításai és a frissített ipari stratégia keretében végzett kapcsolódó munka hozzá fog járulni annak biztosításához is, hogy a biztonsági és védelmi megfontolásokat – adott esetben, valamint az uniós versenyszabályokkal és az EU nemzetközi kötelezettségeivel összhangban – jobban figyelembe vegyék az uniós ipar- és kereskedelempolitikában.

Az ezen ütemtervben szereplő javaslatok célja, hogy hozzájáruljanak a hamarosan elkészülő uniós stratégiai iránytű KTF+I dimenziójához, amelynek segítségével a tagállamok ambiciózus, hosszú távú célokat tűznek ki Európa biztonságának és védelmének jelentős fokozása érdekében.