
# I. BEVEZETÉS

Oroszország Ukrajnával szemben provokáció nélkül indított, indokolatlan katonai agressziójával visszatért a háború Európába. Ez arra késztetett mindannyiunkat, hogy megkérdőjelezzük az EU biztonsággal és védelemmel kapcsolatos megközelítését, valamint azt, hogy képes-e megvalósítani jövőképét és megvédeni érdekeit, többek között a kibertérben is. A tekintélyelvű rendszerek megpróbálják a kibertérben megzavarni és aláásni a szabályokon alapuló nemzetközi rendet azzal, hogy a kiberteret, csakúgy mint a szárazföldet, a nyílt tengert, a légteret és a világűrt, egyre vitatottabb területté teszik. Az elmúlt években fokozódott az állami és nem állami szereplők által a kibertérben tanúsított rosszindulatú magatartás, többek között nőtt az EU-ban, valamint az EU-n kívüli missziókkal és műveletekkel kapcsolatban a katonai és polgári kritikus infrastruktúrák ellen irányuló kibertámadások száma.

A kibertér polgári és katonai dimenziói közötti határvonalak nem egyértelműen meghatározhatók, amint azt az energiahálózatok, a közlekedési infrastruktúra és az űrtechnológiai eszközök elleni közelmúltbeli támadások is mutatják. Ezek a támadások jól szemléltetik továbbá a fizikai és a digitális infrastruktúra kölcsönös függőségét, valamint azt, hogy a jelentős kiberbiztonsági események megzavarhatják vagy károsíthatják a kritikus infrastruktúrákat. Nyomatékosan felhívják a figyelmet arra, hogy az EU-nak szoros katonai és polgári együttműködésre van szüksége a kibertérben ahhoz, hogy erősebb biztonságszolgáltatóvá válhasson.

Az EU-nak nagyobb felelősséget kell vállalnia saját biztonságáért. Ehhez modern és interoperábilis európai fegyveres erőkre van szükség. A tagállamoknak ezért sürgősen és prioritásként kötelezettséget kell vállalniuk arra, hogy növelik a teljes spektrumú kibervédelmi képességekbe történő beruházásokat, beleértve az aktív védelmi képességeket is. Az EU-nak – amellett, hogy továbbra is teljes mértékben elkötelezett a kibertérre vonatkozó nemzetközi jog és normák mellett – jeleznie kell, hogy kész ezeket a képességeket összehangolt módon használni egy tagállam elleni kibertámadás esetén.

Ahhoz, hogy ez sikeres legyen, az EU-nak gondoskodnia kell technológiai és digitális szuverenitásáról a kibertérben. Az EU cselekvési képessége attól függ, hogy tudja-e használni és fejleszteni a kiberbiztonság és a kibervédelem élvonalbeli technológiáit az EU-ban. Mivel a kibertechnológiák jelentős potenciált hordoznak magukban a kettős felhasználásra, a kiberbiztonsági és kibervédelmi iparágaknak, a kutatás-fejlesztésnek és az innovációs tevékenységeknek sokkal szinergikusabb módon kell működniük a jobb képességek fejlesztése érdekében.

A közös megelőzés és felderítés az EU védelmi képességeinek fontos része. Az EU-nak a támadások korai szakaszban történő felderítéséhez szükséges kapacitásokkal kell bírnia. A felderítési adatokat hasznosítható információkká kell alakítani, ami a kiberbiztonságot és a kibervédelmet egyaránt szolgálhatja. A védelmi és a polgári kiberközösségek közötti együttműködés képezi az alapot a közös helyzetismeret javításához a kibertérben, mely együttműködés a koordinált válságreagálás terén technikai és műveleti szinten is ugyanilyen fontos.

Az ukrajnai fegyveres konfliktus rávilágított a magánszektorral való szoros együttműködés értékére is, valamint arra, hogy jelentős kibertámadások esetén a reagálás fokozása érdekében szükség lehet – az ilyen esetekben kibertartalékként funkcionáló – megbízható magánszolgáltatókhoz való hozzáférésre. Ezért gondoskodni kell arról, hogy a tagállamok megbízható kiberbiztonsági tartalékokra támaszkodhassanak, és ez biztonságos és összehangolt módon történjen.

Ez a közös közlemény – amellett, hogy a kibervédelmi szakpolitikai keretre[[1]](#footnote-2) épül – ambiciózus stratégiát javasol annak lehetővé tétele érdekében, hogy az EU és tagállamai magabiztosan és asszertíven lépjenek fel a kibertérben. Célja, hogy a tagállamok egyéni vagy együttes fellépése révén növelje a kibervédelmi képességeket, valamint megerősítse az uniós kiberközösségek közötti koordinációt és együttműködést. Emellett előmozdítja az EU stratégiai függőségeinek csökkentését a kritikus kibertechnológiák terén, és megerősíti az európai védelmi technológiai és ipari bázist (EDTIB). A szakpolitika meghatározza az uniós játékszabályokat, és javaslatokat tesz arra, hogy miként lehetne megerősíteni az EU központi értékének számító szolidaritást a kibervédelem területén, valamint a magánszektorral való együttműködést a súlyos kibertámadásokra való reagálás javítása érdekében. Tekintettel a kiberfenyegetések transznacionális jellegére, a szakpolitika keretében kölcsönösen előnyös és testre szabott partnerségeket fogunk kialakítani a kibervédelem területén, beleértve a kibervédelmi kapacitásépítést is, és fokozni fogjuk a partnerországok kiberrezilienciáját.

A Tanács által 2022 márciusában elfogadott, a biztonság és a védelem területére vonatkozó stratégiai iránytűben[[2]](#footnote-3) javasoltaknak megfelelően ez a kibervédelmi politika javítani fogja az EU-t és tagállamait célzó kibertámadások megelőzésére, felderítésére, az azokkal szembeni védekezésre, a helyreállításra és az elrettentésre való képességet valamennyi rendelkezésre álló eszköz felhasználásával. Ez összhangban van a Bizottság digitális prioritásaival, a digitális évtizedre vonatkozó 2020. évi uniós kiberbiztonsági stratégiában[[3]](#footnote-4) meghatározott célkitűzésekkel, Ursula von der Leyen elnöknek az Unió helyzetéről szóló 2021. évi beszédében[[4]](#footnote-5) tett bejelentésével, valamint az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetésekkel[[5]](#footnote-6). A védelmi beruházási hiányokról szóló 2022. évi közös közleményben[[6]](#footnote-7) a Bizottság bátorította az EU-t és tagállamait, hogy kezdjék meg a teljes spektrumú – a kutatástól, a felderítéstől és a védelemtől a reagálásig tartó – kibervédelmi képesség kialakítására irányuló munkát.

# II. UNIÓS KIBERVÉDELEM A KIBERTÁMADÁSOK ELLENI VÉDEKEZÉS, AZOK FELDERÍTÉSE, ELHÁRÍTÁSA ÉS AZ AZOKTÓL VALÓ ELRETTENTÉS ÉRDEKÉBEN

**1. Együttes fellépés az erősebb kibervédelem érdekében**

A kibertámadások gyakran határokon átnyúló jellegűek, és fizikai hatással lehetnek az EU kritikus infrastruktúrájára. A jelentős kiberbiztonsági események olyan súlyos zavarokat okozhatnak, amelyeket az érintett tagállam vagy tagállamok egyedül nem tudnak elhárítani. Ezek az incidensek a harmadik országok által végrehajtott olyan nagyobb hibrid támadásoknak is részét képezhetik, amelyek célja a gazdaság és a társadalom destabilizálása, az EU biztonságának garantálásához szükséges kritikus infrastruktúra gyengítése, illetve a demokráciák működésének aláásása és károsítása, többek között a választási infrastruktúrák elleni támadások révén.

2018-ban az EU megállapította, hogy a kibertér a katonai műveletek egyik területe. A 2021-ben elfogadott „Kibertérrel mint műveleti területtel kapcsolatos katonai koncepció és stratégia” című dokumentum[[7]](#footnote-8) meghatározza a keretfeltételeket, és leírja az ahhoz szükséges célokat, módszereket és eszközöket, amelyekkel a kibertér az EU közös biztonság- és védelempolitikai (KBVP) műveleteit támogató műveleti területként hasznosítható. A kibervédelem és a kapcsolódó képességeknek a katonai kibertér-műveletek teljes spektrumában történő alkalmazása a tagállamok nemzeti előjoga, a kibervédelem azonban szélesebb ökoszisztémára támaszkodik, beleértve az uniós szintű képességfejlesztés által támogatott erős ipari bázist is.

A tagállamok védelmi hatóságaiból álló és az uniós intézmények, szervek és hivatalok által támogatott uniós kibervédelmi közösség a többi kiberközösséghez[[8]](#footnote-9) képest egyedi jellegű, és eltérő irányítási modellt követ. Az uniós katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok (milCERT-ek) közötti – többek között a katonai KBVP-missziókat és -műveleteket támogató – információcsere és együttműködés kialakított keretének hiánya problémát jelent, tekintettel az állami és nem állami szereplők által jelentett kiberfenyegetések megnövekedett szintjére.

A polgári, diplomáciai és bűnüldözési kiberközösségek és azok védelmi partnerei közötti együttműködés valamennyi érintett szereplő számára magas hozzáadott értéket képvisel majd. Ennélfogva elengedhetetlen, hogy lehetővé váljon ez az együttműködés: biztosítani kell az információcsere megfelelő és biztonságos eszközeit, valamint a bizalmat és közös értelmezést kialakító gyakorlatokban és egyéb tevékenységekben való részvételt.

Emellett jelenleg csak korlátozott mértékű kölcsönös operatív segítségnyújtás áll rendelkezésre a tagállamok között. Meg kell vizsgálni a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok koncepciójának további kiterjesztését az egész EU-ra, a kapcsolódó állandó strukturált együttműködési (PESCO) projektre – kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén (CRRT)[[9]](#footnote-10) – építve, többek között az Európai Unióról szóló szerződés (EUSZ) 42. cikkének (7) bekezdésével[[10]](#footnote-11) („kölcsönös segítségnyújtási záradék”) és az Európai Unió működéséről szóló szerződés (EUMSZ) 222. cikkével[[11]](#footnote-12) („szolidaritási záradék”) összefüggésben is. Hasonlóképpen, az Oroszország agresszív háborújával összefüggésben a sikeres ukrán kibervédelemből levont egyik tanulság a magánszektor meghatározó szerepe. Ezért meg kell vizsgálni, hogy a magánszektor milyen mértékben járulhat hozzá a kiberbiztonsági eseményekre való reagálás fokozásához.

### 1.1. A közös helyzetismeret és koordináció erősítése a védelmi közösségen belül

Tekintettel a kibertámadásokhoz kapcsolódó kockázat mértékére, a tagállamoknak a lehető legteljesebb kollektív helyzetismerettel kell rendelkezniük, beleértve a korai észlelési kapacitást, valamint a megfelelő reagáláshoz és a szolidáris és összehangolt módon történő helyreállításhoz szükséges erőforrásokat.

Ami a katonai helyzetismeretet illeti, létre kell hozni az **EU kibervédelmi koordinációs központját (EUCDCC)**, amely támogatja a fokozott helyzetismeretet a védelmi közösségen belül, beleértve az összes uniós katonai KBVP-parancsnokot. A főképviselő – a PESCO-nak a Kiber- és az Információs Terület Koordinációs Központjára (CIDCC) vonatkozó projektjére[[12]](#footnote-13) építve – a tagállamoknak megfontolás céljából elő fogja terjeszteni az EUCDCC-re vonatkozó javaslatot. A kibervédelmi koordinációs központ célja, hogy holisztikus elemzést nyújtson a kibertérről, az elektromágneses környezetről és a kognitív területről azáltal, hogy a különböző információforrásokat becsatornázza a katonai stratégiai és műveleti szintekre. Az egységes információelemzési kapacitás keretében megfelelő kapcsolatokat kell kialakítani az EUCDCC és az Európai Unió Helyzetelemző Központja (EU INTCEN), valamint az EU Katonai Törzsének hírszerzése között. A külső információforrások mellett az EUCDCC-nek létre kell hoznia és integrálnia kell egy független, aktív információtechnológiai érzékelőrendszert, hogy megerősítse az EU saját, katonai KBVP-missziókat és -műveleteket támogató csomópontjainak monitoringját. Ennek eredményeképpen javul a felderítési képesség és az információk egy új rétege jön létre a kiberkockázat-értékelés és a helyzetismeret információs alapjának további javítása érdekében.

E célból olyan képességekre van szükség, amelyek lehetővé teszik és biztosítják a kibertérről a hét minden napján, napi 24 órában működő és lehetőség szerint elismert kép kialakítását és fenntartását, többek között az ellenfelek és a baráti erők folyamatban lévő és küszöbön álló kiberműveleteiről is. Ez a kép hozzájárulna az uniós katonai KBVP-missziók és -műveletek tervezéséhez és végrehajtásához. Ez lesz tehát a katonai hozzájárulás ahhoz, hogy az EU többet tudjon a kibertérben folyó rosszindulatú fellépésekről, és hatékonyabban reagáljon azokra.

A bizalom javítása, valamint a jelentős kiberbiztonsági eseményekkel kapcsolatos megbízható és kellő idejű stratégiai információk cseréje érdekében tovább fejlesztik és erősítik **az uniós kibervédelmi parancsnokok konferenciáját**[[13]](#footnote-14). A konferencia titkárságaként az Európai Védelmi Ügynökség (EDA) jár el. A konferencia az Európai Unió Katonai Törzsének részvételével évente legalább kétszer ülésezik, hogy megvitassa az operatív kérdéseket és egyéb releváns témákat.

Az EDA támogatásával létrejön a **milCERT-ek** operatív hálózata **(MICNET)**. Minden tagállam felkérést kap a MICNET-ben való részvételre, amely várhatóan 2023 januárjában kezdi meg működését.

A milCERT-ek közötti információcsere megkönnyítésével a MICNET elő fogja mozdítani az EU-n belüli védelmi rendszereket – többek között a katonai KBVP-missziókban és -műveletekben alkalmazott rendszereket – érintő kiberbiztonsági fenyegetésekre való erőteljesebb és összehangoltabb reagálást. A MICNET lehetővé teszi továbbá a képzési folyamatok fenntartását és a milCERT-ek közösségét illető új, hosszabb távon érvényben tartandó követelmények folyamatos azonosítását. Az elkövetkező négy évben az EDA a tagállamokkal közösen információmegosztási infrastruktúrát, valamint kapcsolódó eszközöket és eljárásokat fog kifejleszteni a milCERT-ek közötti információmegosztás támogatása érdekében. A MICNET az új követelmények és megoldások tesztelésére, validálására és azonosítására szolgáló éves gyakorlat keretét is biztosítja majd.

### 1.2. A civil közösségekkel folytatott koordináció javítása

A MICNET-nek keretet és infrastruktúrát kell biztosítania a kibervédelmi közösség különböző szintjei és a külső érdekelt felek közötti információmegosztáshoz.

Amint a MICNET kiforrottabb szintet ér el, az EDA támogatni fogja a tagállamokat a nemzeti **számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT-ek)** és az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportját (CERT-EU) tömörítő CSIRT hálózatával való együttműködés lehetőségeinek feltárásában. Ez az együttműködés közös üléseket és gyakorlatokat is magában foglalhat. Meg kell vizsgálni továbbá a magánszektor bevonását a releváns információmegosztásra és a biztonsági eseményekre való reagálásra irányuló erőfeszítésekbe.

Az uniós kibervédelmi parancsnokok konferenciájának a hatékonyabb kiberválság-kezelés lehetővé tétele céljából együttműködést kell kezdenie az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatával (CyCLONe). Ez a hálózat a tagállamokat és a Bizottságot fogja össze az EU-n belüli nagyszabású kiberbiztonsági események koordinációjának és kezelésének elősegítése érdekében. Az említett együttműködés során stratégiai és műveleti szinten ötvözik a katonai tapasztalatokat és a polgári helyzetismeretet.

Az EUCDCC-nek a kibervédelemmel kapcsolatos információk gyűjtését, elemzését, értékelését, majd végül – különösen a katonai KBVP-missziók és -műveletek számára történő – terjesztését végző központi csomópont szerepét kellene betöltenie, ugyanakkor kapcsolatot tarthatna a kiberválsággal foglalkozó intézményközi munkacsoporttal[[14]](#footnote-15) is, amelyet azért hoztak létre, hogy nagyszabású kiberválságok esetén stratégiai és műveleti szinten biztosítsa a megalapozott döntéshozatalt és az Európai Unió intézményeinek, szerveinek és hivatalainak összehangolt válaszlépéseit.

Az EUCDCC releváns információkat cserélhet a kiberbiztonsági helyzetfeltáró és elemző központtal is, amely az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) és a CERT-EU támogatásával a Bizottságon belül kerül felállításra, hogy elemzéseket és hatékonyabb válságkezelési támogatást nyújtson.

Emellett továbbra is jelentős akadályt jelent a tagállamok és az érintett uniós intézmények, szervek és hivatalok közötti, közösen megosztott vagy interoperábilis biztonságos kommunikációs eszközök és platformok hiánya. A Bizottságnál és az érintett intézményeknél jelenleg zajlik a kibertérben folytatott biztonságos kommunikáció meglévő eszközeinek feltérképezése. A meglévő eszközök feltérképezését követően a Bizottság 2022 végén benyújtja ajánlásait a Tanácsnak az elfogadandó további intézkedésekről.

**Uniós kiberbiztonsági szolidaritás a közös felderítés és helyzetismeret javítása érdekében**

A polgári támogató fellépések tovább javíthatják a közös helyzetismeretet. A kibervédelmi közösség az EU kritikus infrastruktúrájának védelme érdekében kifejlesztett, erősebb polgári felderítési és helyzetismereti képességek előnyeit élvezheti majd. E célból a Bizottság a biztonsági műveleti központok (SOC-k) uniós infrastruktúrája kiépítésének előmozdítását célzó kezdeményezés előkészítésén dolgozik, melynek első szakasza az elkövetkező hetekben indul, majd a későbbiekben bővítésre és szélesebb körű alkalmazásra kerül[[15]](#footnote-16). Ez az infrastruktúra végső soron számos, több országot összefogó SOC-platformból állna majd, amelyek mindegyike a nemzeti SOC-k egy csoportját tömöríti, a kapcsolódó nemzeti finanszírozás pedig a Digitális Európa program (DEP)[[16]](#footnote-17) támogatásával egészülne ki. A Digitális Európa program jogszabályi módosításai hosszabb távú pénzügyi támogatást tennének lehetővé az új generációs rendkívül biztonságos eszközök és infrastruktúra közös beszerzéséhez. Ez lehetővé tenné, hogy a tervezett uniós SOC-infrastruktúra a legújabb mesterséges intelligencia (MI) és adatelemzések alkalmazásával javítsa a kollektív felderítési képességeket, a civil kommunikációs hálózatokra is kiterjedően. A hasznosítható kiberfenyegetettségi információk e generációja lehetővé tenné a hatóságok és az érintett szervezetek időben történő figyelmeztetését, hogy azok felderíthessék a jelentős kiberbiztonsági eseményeket és hatékonyan reagálhassanak ezekre. Az infrastruktúra nagyságrendje és hatóköre attól függ, hogy mekkora a nemzeti szinten igénybe vehető és a többéves pénzügyi keretben rendelkezésre álló költségvetés alapján az Unió által mozgósítható teljes finanszírozás.

Az ilyen, több országra kiterjedő SOC-k az irányítás és a megosztott információk típusa tekintetében egy „védelmi pillér” létrehozásával is lehetővé tehetik a védelmi szervezetek részvételét. Ezt a „védelmi pillért” a főképviselővel közösen dolgoznák ki, és magában foglalhatna egy kifejezetten a katonai szereplőkkel – többek között az EUCDCC-vel – való információcserére szolgáló mechanizmust, amelyre vonatkozóan védelmi szintű biztonsági előírásokat lehetne kidolgozni.

**Uniós kiberbiztonsági szolidaritás a felkészültség, a reagálás és a helyreállítás terén**

A jelentős kiberbiztonsági események gyakran olyan súlyos zavarokat okoznak, amelyeket az érintett tagállam vagy tagállamok egyedül nem tudnak elhárítani. Ilyen esetekben a tagállamok számára lehetővé kell tenni, hogy kölcsönös segítségnyújtásra és szolidaritásra támaszkodhassanak, többek között az EUSZ 42. cikkének (7) bekezdésével és az EUMSZ 222. cikkével összefüggésben. A főképviselő a Bizottsággal és a tagállamokkal együttműködve – a kapcsolódó PESCO CRRT projektre építve – meg fogja vizsgálni **a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok (CRRT) koncepciója kiterjesztésének** lehetőségeit annak érdekében, hogy az jobban támogassa az uniós tagállamokat, valamint a KBVP-missziókat és -műveleteket. Az ilyen csoportok feladata az lenne, hogy kérésre és az egyes esetekben felmerülő konkrét igényektől függően testre szabott és célzott rövid távú segítséget nyújtsanak. A hatékony válasz- és helyreállítási intézkedések biztosítása érdekében adott esetben lehetőség lenne a megbízható magánpartnerek által nyújtott támogatásra is.

Az EU kiberbiztonsági szolidaritási kezdeményezésének részeként a Bizottság intézkedéseket dolgoz ki a felkészültségi és reagálási intézkedések Unió-szerte történő megerősítésére. Mindez kiterjedne **a kritikus infrastruktúrát működtető alapvető szervezetek potenciális sérülékenységeinek uniós kockázatértékeléseken alapuló tesztelésére** – a Bizottság és az ENISA által közösen már megkezdett fellépések alapján –,valamint azokra az eseményreagálási intézkedésekre, amelyek a súlyos biztonsági események hatásának enyhítésére, az azonnali helyreállítás támogatására és/vagy az alapvető szolgáltatások működésének helyreállítására irányulnak[[17]](#footnote-18).

Az uniós kiberbiztonsági szolidaritási kezdeményezés támogathatná **a megbízható magánszolgáltatók szolgáltatásaiból származó uniós szintű kiberbiztonsági tartalék fokozatos kiépítését,** amely készen állna arra, hogy a tagállamok kérésére beavatkozzon jelentős, határokon átnyúló kiberbiztonsági események esetén. Egyértelműen meg kell határozni a szerepeket és felelősségi köröket, és azokat teljes mértékben össze kell hangolni a meglévő szervek szerepével és felelősségével annak érdekében, hogy az uniós szintű kiberbiztonsági tartalékból származó támogatás ott álljon rendelkezésre, ahol arra szükség van, és kiegészítse az egyéb lehetséges segítségnyújtási formákat. Bár a konkrét beavatkozások hatóköre és költségeinek elosztása a rendelkezésre álló uniós finanszírozástól függene, az EU azáltal is többletértéket teremtene, hogy biztosítja egy ilyen uniós szintű tartalék rendelkezésre állását és készenlétét. A magas szintű bizalom biztosítása érdekében a Bizottság azt is fontolóra fogja venni, hogy miképpen támogathatná kiberbiztonsági tanúsítási rendszerek kidolgozását a szóban forgó kiberbiztonsági magánvállalatok számára.

A gyakorlatok a felkészültség kiépítésének kulcsfontosságú elemei. Előmozdítják a kibervédelem közös tudásalapjának és közös értelmezésének kialakítását, ez pedig javítja a műveleti felkészültséget. A közös kibervédelmi gyakorlatok az érdekelt felek közötti interoperabilitást és bizalmat is kiépítik, többek között a katonai KBVP-missziók és -műveletek támogatása érdekében. A CYBER PHALANX kiadványsorozatra[[18]](#footnote-19) és a milCERT-gyakorlatokra építve **az EDA az összes tagállamot összefogó új CyDef-X projektet fog létrehozni, amely keretként szolgál majd az uniós kibervédelmi gyakorlatokhoz**. Ez a projekt az EUSZ 42. cikkének (7) bekezdése szerinti kölcsönös segítségnyújtást szolgálhatná. Meg kell vizsgálni továbbá a célzott kibervédelmi tesztelési, képzési és gyakorlati környezetek (pl. az összevont virtuális gyakorlóterek – CRF) alkalmazását, többek között a PESCO összevont virtuális gyakorlóterekkel kapcsolatos projektjének[[19]](#footnote-20) igénybevételével.

A gyakorlatok fontos szerepet játszhatnak a polgári és katonai szervezetek közötti együttműködés javításában is. A gyakorlatok szervezésekor ezért az ENISA-nak, az EDA-nak és más érintett szervezeteknek szisztematikusan mérlegelniük kell más kiberközösségek résztvevőinek bevonását.

A kibertámadások megelőzésére, megakadályozására és az azokra való reagálásra irányuló uniós kapacitás megerősítésének részeként, valamint a 2020. évi uniós kiberbiztonsági stratégiával és a stratégiai iránytűvel összhangban a főképviselő 2023-ban alternatívákat fog javasolni az Unió kiberdiplomáciai eszköztárának[[20]](#footnote-21) további erősítésére az uniós kiberbiztonsági helyzet elemei és az eszköztár eddigi végrehajtásából levont tanulságok alapján.

|  |
| --- |
| ***Kibervédelmi intézkedések**** Az EU kibervédelmi koordinációs központjának létrehozása a közös katonai helyzetismeret központjaként, valamint a Bizottság helyzetelemző központjával való együttműködés módozatainak feltárása.
* Az uniós kibervédelmi parancsnokok konferenciájának további fejlesztése és megerősítése.
* A tagállamok ösztönzése arra, hogy aktívan vegyenek részt a MICNET-ben – a katonai CERT-ek hálózatában, és törekedjenek a polgári CSIRT-hálózattal való együttműködés kialakítására.
* Az uniós kibervédelmi gyakorlatokat támogató új, CyDef-X elnevezésű keretprojekt kidolgozása.
* A PESCO CRRT-projektjére építve a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok koncepciójának továbbfejlesztésére vonatkozó lehetőségek vizsgálata.
* Az összevont virtuális gyakorlóterekkel kapcsolatos projektek továbbfejlesztésére vonatkozó lehetőségek feltárása.

***Polgári támogató fellépések*** * Az uniós kiberbiztonsági szolidaritási kezdeményezés előkészítése – beleértve a Digitális Európa program jogalkotási módosításaira irányuló esetleges jogi aktust is –az alábbiak céljából:
	+ a közös uniós felderítési, helyzetismereti és reagálási képességek megerősítése,
	+ a megbízható magánszolgáltatók által biztosított uniós szintű kiberbiztonsági tartalék fokozatos kiépítése,
	+ a kritikus fontosságú szervezetek uniós kockázatértékeléseken alapuló tesztelésének támogatása az esetleges sebezhetőségek tekintetében.
* A kiberbiztonsági ipar és a magánvállalkozások tekintetében uniós szintű kiberbiztonsági tanúsítási rendszerek kialakítási lehetőségeinek a feltárása.
* A kibervédelem és más kiberközösségek közötti stratégiai, operatív és technikai szintű együttműködés fokozása.
 |

**2. Az uniós védelmi ökoszisztéma biztonságának garantálása**

Az elmúlt években drámaian megnőtt a kibertámadások száma, köztük az ellátási láncot célzó támadásoké is, amelyek célja a kiberkémkedés, a zsarolóvírusok alkalmazása vagy a zavarkeltés. 2020-ban a SolarWinds ellátási láncára irányuló támadás[[21]](#footnote-22) világszerte több mint 18 000 szervezetet érintett, köztük kormányzati ügynökségeket, nagyobb vállalkozásokat és védelmi vállalatokat. Az Apache log4j szoftvere sebezhetőségének[[22]](#footnote-23) kihasználása rávilágított arra, hogy még a nem magas kockázatúnak vagy nem kritikusnak minősülő szoftverösszetevők is fegyverként használhatók ahhoz, hogy sikeres támadásokat hajtsanak végre az EU-ban nagy vállalatok vagy kormányok ellen, többek között a védelem területén is. Ez azt mutatja, hogy egyértelműen meg kell erősíteni az uniós védelmi ökoszisztémában aktív szervezetek – köztük a katonai szervezetek, a védelmi ipar és a magánszereplők – kiberrezilienciáját.

A fegyveres erők nagymértékben függenek a polgári kritikus infrastruktúráktól, legyen szó akár a mobilitásról, a kommunikációról vagy az energiáról. Jó példa erre a kölcsönös függésre a KA-SAT műholdas hálózat[[23]](#footnote-24) elleni orosz támadás, amely megzavarta több hatóság és az ukrán fegyveres erők kommunikációját. Ez jól mutatja, mennyire fontos az ilyen kritikus infrastruktúra biztonságáról gondoskodni.

A kommunikációs és információs rendszereik biztonságával kapcsolatos kérdések kezelése érdekében a tagállamok saját biztonsági szabványokat és követelményeket dolgoznak ki a katonai rendszerekre vonatkozóan, amelyek nem mindig veszik figyelembe az interoperabilitás szükségességét, sem pedig a kettős felhasználású termékekre vonatkozó polgári szabványok meglétét. Ez negatív hatást gyakorol a tagállamok azon képességére, hogy együtt lépjenek fel a kibertérben, a katonai KBVP-missziók és -műveletek összefüggésében is, és akadályokat gördít a kölcsönös segítségnyújtás elé. Emellett elő kell mozdítani a katonai és polgári szabványosítási irányvonalak közötti erősebb szinergiákat is, mivel a polgári és katonai ügyfelekre vonatkozó, hasonló, de nem azonos szabványok betartása növeli a kettős felhasználású termékek ipari fejlesztésének termelési költségeit.

***2.1. A védelmi ökoszisztéma kiberrezilienciájának javítása***

A védelmi ökoszisztéma kiberrezilienciájának javításához célzott intézkedésekre és beruházásokra van szükség a szervezetek széles körében, a tagállamok katonai infrastruktúrájától és KBVP-misszióitól és -műveleteitől kezdve a kritikus infrastruktúrákig, a védelmi iparig és az érintett kutatási szervezetekig.

A sikeres KBVP-missziókhoz és -műveletekhez szükség van a megalapozott döntéshozatalhoz szükséges információk védelmére. Az EU-nak és tagállamainak tovább kell erősíteniük katonai vezetési és irányítási struktúráikat az infrastruktúrájuk fejlesztése és biztonságossá tétele mellett. Ez a műveleti parancsnokság – többek között a Katonai Tervezési és Végrehajtási Szolgálat (MPCC) – hatékony alkalmazása érdekében a válságkezelés korai szakaszában folytatott politikai-katonai konzultációra is igaz. Ezt különösen az uniós műveleti nagytávolságú hálózat továbbfejlesztése révén fogják kezelni.

A katonai missziókkal és műveletekkel összefüggésben a kibervédelmi szereplők különböző formátumú információkat és osztályozásokat használnak, amelyek különböző forrásokból származnak. Ez rendkívül fontossá teszi a biztonságos, legkorszerűbb technológiák, például a mesterséges intelligencia alkalmazását az ipar támogatásával.

A kommunikációs és információs rendszerek infrastruktúrájának biztonságát kölcsönösen elfogadott irányítási eljárások alkalmazásával kell javítani, ezáltal erősítve az érdekelt felek körében elérhető információk integritásába vetett bizalmat. Emellett a főképviselő – többek között az EDA vezetőjeként – a Bizottság támogatásával segíteni fogja a tagállamokat **a védelmi közösség számára jogilag nem kötelező erejű ajánlások kidolgozásában – az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvből (NIS 2) merítve**[[24]](#footnote-25), mivel a védelem nem tartozik az irányelv hatálya alá. Ez hozzá fog járulni a kibervédelem általános érettségi szintjének javulásához.

A digitális elemeket tartalmazó termékekre vonatkozóan kiberbiztonsági követelmények megállapítását célzó kiberrezilienciáról szóló jogszabályra irányuló bizottsági javaslat[[25]](#footnote-26) tovább fogja csökkenteni a támadási felületet a kettős felhasználású termékek esetében – például a védelmi ipar és a kormányzati védelmi szereplők által használt kommunikációs és információs rendszerek terén. A javaslat szerint a gyártóknak 24 órán belül jelentést kellene tenniük az aktívan kihasznált sebezhetőségekről az ENISA-nak, amely ezt követően tájékoztatja az érintett nemzeti CSIRT-eket. E tekintetben fontos lenne annak biztosítása is, hogy a védelmi közösség gyorsan tájékoztatást kapjon a digitális elemeket tartalmazó termékek sebezhetőségeiről, valamint a rendelkezésre álló és/vagy alkalmazott javításokról és kockázatcsökkentő intézkedésekről.

Figyelembe véve a katonaság függését a polgári kritikus infrastruktúráktól, még inkább fontos, hogy **tovább javuljon a kritikus infrastruktúrák védelme a nagyszabású kibertámadásokkal szemben.** A Tanács kérésére[[26]](#footnote-27) a Bizottság, a főképviselő és a Kiberbiztonsági Együttműködési Csoport[[27]](#footnote-28) a digitális infrastruktúra biztonságára vonatkozó kockázati forgatókönyveket dolgoz ki. A hangsúly első körben az energia-, a távközlési és a közlekedési ágazat, valamint az űripar kiberbiztonságán lesz. Emellett célzott kiberbiztonsági kockázatértékelések készülnek az uniós kommunikációs infrastruktúrára és hálózatokra (többek között a helyhez kötött és mobil infrastruktúrára, a műholdakra, a tenger alatti kábelekre és az internetes útvonal-meghatározásra [routing]) vonatkozóan is[[28]](#footnote-29). A kritikus infrastruktúrák ember okozta – többek között hibrid – fenyegetésekkel szembeni védelmét illetően a kritikus infrastruktúrák rezilienciájának megerősítésére irányuló összehangolt uniós megközelítésről szóló tanácsi ajánlásra vonatkozó javaslat[[29]](#footnote-30) felszólítja a tagállamokat, hogy biztosítsák többek között a megfelelő stressztesztelést és válságkoordinációt. Az EU tengeri védelmi stratégiájának és a kapcsolódó cselekvési tervnek a közelgő felülvizsgálata tovább foglalkozik majd a kritikus tengeri infrastruktúrával, ideértve a tenger alatti adatkábelek védelmét. Az energiarendszer kritikus infrastruktúrája kiberbiztonságának megerősítésére irányuló további intézkedéseket az energiarendszer digitalizációjára vonatkozó uniós cselekvési terv határozza meg[[30]](#footnote-31).

A világűrbe telepített szolgáltatások egyre nagyobb jelentőséggel bírnak a védelem szempontjából, legyen szó megfigyelésről, helyzetismeretről, pontos helymeghatározásról vagy ultrabiztonságos kommunikációról. Ezért ezek kulcsfontosságú stratégiai eszközök a technológiai szuverenitás szempontjából. A világűrbe telepített szolgáltatások megzavarása jelentős hatást gyakorolhat a védelmi rendszerekre, de a társadalom és a gazdaság egészére is. Rezilienciájuk központi fontosságú az általános kibervédelmi reziliencia szempontjából, mivel rosszindulatú támadások célpontjai lehetnek. Amint azt a KA-SAT hálózatok elleni támadások is mutatják, az űrrendszerek egyre nagyobb kiberfenyegetéseknek vannak kitéve, amelyek befolyásolhatják a világűrbe telepített szolgáltatások rendelkezésre állását vagy folytonosságát. Ez kockázatot jelent az EU világűrrel kapcsolatos stratégiai és biztonsági érdekeire, valamint a kibervédelmet lehetővé tevő és támogató űrbeli képességekre nézve. A stratégiai iránytűben[[31]](#footnote-32) bejelentett uniós biztonsági és védelmi űrstratégia intézkedéseket fog felvázolni az űrinfrastruktúrák és a kapcsolódó szolgáltatások megbízhatóságának és kiberrezilienciájának javítása, valamint az érzékeny uniós űrrendszereket és -szolgáltatásokat veszélyeztető fenyegetésektől való elrettentés és az azokra való reagálás céljából, különös tekintettel a kiberfenyegetésekre.

A Bizottság felszólítja továbbá a tagállamokat, hogy sürgősen hajtsák végre az 5G kiberbiztonsággal kapcsolatos uniós eszköztárban ajánlott intézkedéseket[[32]](#footnote-33). Azoknak a tagállamoknak, amelyek még nem vezettek be korlátozásokat a magas kockázatú beszállítókra vonatkozóan, ezt haladéktalanul meg kell tenniük, figyelembe véve, hogy az elvesztegetett idő növelheti a hálózatok sebezhetőségét az EU-ban. Ezek a kockázatok relevánsak lehetnek a katonai eszközök szempontjából, és hatással lehetnek a tagállamok általános védelmi környezetére.

Ami **az európai védelmi ipar, valamint a védelmi kutatás-fejlesztési szervezetek kiberrezilienciáját** illeti, az ilyen szervezetek a NIS 2 irányelv hatálya alá tartoznak, kivéve, ha a tagállamok kifejezetten kizárják ezt. Ez megkövetelné, hogy az ilyen szervezetek kiberbiztonsági kockázatkezelési programmal rendelkezzenek, amely kiterjed az ellátási lánc biztonságára és a biztonsági események bejelentésére is. Mivel a magánszektor jelentős szerepet játszik a védelmi ökoszisztémán belüli kiberbiztonsági szolgáltatások nyújtásában, a tagállamoknak emellett kiberbiztonsági tanúsítási rendszereket is alkalmazniuk kell. Az ENISA tapasztalataira építve fel lehetne tárni egy, **a védelmi ipar számára szolgáltatásokat nyújtó vállalatokra vonatkozó uniós kiberbiztonsági tanúsítási rendszer** létrehozásának lehetőségét, amely lehetővé tenné a piacba vetett bizalom szintjének harmonizálását.

## 2.2. Az uniós kibervédelem interoperabilitásának és a szabványok koherenciájának biztosítása

Az interoperabilitás és a hasonlóság fontos követelmények, amelyeket a kibervédelmi képességek tervezési szakaszától kezdve szem előtt kell tartani, figyelembe véve a folyamatban lévő missziókból és műveletekből levont, az Európai Unió Katonai Törzsének vezetésével – az EDA támogatásával – megállapított tanulságokat is. Az interoperabilitás biztosítása érdekében a szövetséges műveleti hálózat[[33]](#footnote-34) keretében elfogadott elveknek, folyamatoknak és szabványoknak kell vezérelniük a nemzeti kibervédelmi képességek fejlesztését.

Az együttműködési erőfeszítéseket megkönnyítheti az új generációs kibervédelmi képességekre vonatkozó követelmények harmonizálása, ami potenciálisan közös fejlesztési és közbeszerzési kezdeményezésekhez és integrált életciklus-támogatáshoz vezethet. Ezért az EDA és az Európai Unió Katonai Törzse **ajánlásokat fog kidolgozni az uniós kibervédelmi interoperabilitási követelményekre vonatkozóan**. Ezeket a követelményeket minden tervezési időtávon figyelembe kell venni annak érdekében, hogy garantálják a szabványosításnak mint az interoperabilitás stratégiai eszközének valamennyi aspektusát. A tesztelésre, értékelésre és tanúsításra vonatkozó követelmények szintén kulcsfontosságúak.

A kiberrezilienciáról szóló jogszabályjavaslat[[34]](#footnote-35) keretében harmonizált kiberbiztonsági szabványokat fognak kidolgozni a hardver- és szoftvertermékekre és -összetevőkre vonatkozóan. Ezek a szabványok minden digitális elemet tartalmazó polgári és kettős felhasználású termékre vonatkoznak majd, amelyek a védelmi ágazatban használt termékek nagy részét teszik ki. A Bizottság lehetőség szerint ösztönözni fogja a digitális termékekre vonatkozó, védelemmel kapcsolatos kiberbiztonsági szabványokkal való koherenciát. A polgári, a védelmi és az űripar közötti szinergiákról szóló cselekvési tervben[[35]](#footnote-36) (a továbbiakban: a szinergiákról szóló cselekvési terv) foglaltaknak megfelelően a Bizottság a kulcsfontosságú érdekelt felekkel szoros együttműködésben tervet fog előterjeszteni a meglévő polgári/védelmi hibrid szabványok alkalmazásának és újak kidolgozásának előmozdítására. Tovább kell fejleszteni az együttműködést az összes érdekelt fél – köztük az európai szabványügyi szervezetek, az Észak-atlanti Szerződés Szervezete (NATO) és más partnerek – között, e célból a lehető legjobban kiaknázva az Európai Védelmi Szabványügyi Bizottság munkáját. Hasonlóképpen, amikor a katonai szabványügyi testületek új kiberbiztonsági szabványokat dolgoznak ki a védelmi célú digitális elemeket tartalmazó termékekre vonatkozóan, a kiberrezilienciáról szóló jogszabály alapján kidolgozott harmonizált szabványokat kell alapul venniük[[36]](#footnote-37).

***Kibervédelmi intézkedések***

* A tagállamok támogatása a NIS 2 által inspirált, jogilag nem kötelező erejű ajánlások kidolgozásában a védelmi közösség számára annak érdekében, hogy nemzeti szinten hozzájáruljanak a kibervédelem általános érettségi szintjének javításához.
* Ajánlások kidolgozása az uniós kibervédelmi interoperabilitási követelmények vonatkozásában.
* Az összes érintett szereplővel való együttműködés fokozása a védelemmel kapcsolatos szabványok terén az Európai Védelmi Szabványügyi Bizottság keretében.

***Polgári támogató fellépések***

* A katonai kommunikáció és mobilitás szempontjából fontos kritikus infrastruktúrára vonatkozó kockázati forgatókönyvek kidolgozása a felkészültségi intézkedések célzottá tétele érdekében, többek között behatolás-tesztelés révén.
* A polgári és katonai szabványügyi szervezetek közötti együttműködés előmozdítása a kettős felhasználású termékekre vonatkozó harmonizált szabványok kidolgozása érdekében.

**3. Beruházás a kibervédelmi képességekbe**

Az elmúlt években növekedtek a kibervédelmi beruházások az EU-ban, miközben állami és nem állami szereplők egyre több rosszindulatú kibertevékenységet folytatnak. Döntő fontosságú, hogy az EU megerősítse kibervédelmi képességeit. Oroszország Ukrajna elleni agresszív háborúja tovább erősíti a beruházások növelésének szükségességét annak biztosítása érdekében, hogy a tagállamok korszerű helyhez kötött és telepíthető kibervédelmi képességekkel rendelkezzenek.

A technológiai fejlesztések elengedhetetlenek a versenytársakkal és ellenfelekkel szembeni előny fenntartásához, akik szintén jelentős beruházásokat hajtanak végre az új technológiákba. Ezért az EU-nak és a tagállamoknak a közös képességfejlesztés, valamint a kutatás-fejlesztésbe történő beruházások növelése révén kell fokozniuk a kibervédelemmel kapcsolatos együttműködésüket és interoperabilitásukat.

Emellett foglalkozni kell a stratégiai függőségekből és az EDTIB széttagoltságából[[37]](#footnote-38) eredő sebezhetőségekkel is. A készségek és kompetenciák különösen elengedhetetlenek a kiberbiztonságtól és a kibervédelemtől való stratégiai függőségek leküzdéséhez Európában. Az európai védelmi iparnak a meglévő kulcsfontosságú készségek megőrzése mellett új készségeket kell szereznie ahhoz, hogy globális környezetben is képes legyen csúcstechnológiai megoldásokat kínálni[[38]](#footnote-39). A készségek hiánya negatív hatással van a védelmi ágazatra, mivel minden területen akadályozza a képességfejlesztést. Az összes intézkedés teljes mértékben összhangban áll majd a szinergiákról szóló cselekvési tervben, a biztonsági és védelmi szempontból kritikus technológiákra vonatkozó ütemtervben (a továbbiakban: az ütemterv)[[39]](#footnote-40) és a hiányelemzésben[[40]](#footnote-41) bejelentett megközelítésekkel.

## 3.1. A legkorszerűbb kibervédelmi képességek teljes spektrumának kialakítása

A tagállamok felelősek és illetékesek a kibervédelmi képességek használatáért, az EU pedig fontos szerepet játszik a konkrét katonai képességek további fejlesztésének támogatásában, lefedve a doktrína, a szervezés, a kiképzés, az eszközök, a személyzet, a vezetés, a létesítmények és az interoperabilitás (DOTMLPF-I) teljes spektrumát, a kibertérben való cselekvési szabadság megteremtése érdekében. Valamennyi képességi területen tovább kell egységesíteni a kibervédelem megközelítését, és azt hozzá kell igazítani a változó geopolitikai környezethez. Ezért azonosítani kell a meglévő képességek hiányzó elemeit, és összehangolt és mérhető módon támogatni kell az új képességek fejlesztését.

A tagállamok együttműködésen alapuló kibervédelmi fejlesztési projektekben való részvételének mértéke azonban egyelőre nem elegendő, és azt az uniós szintű hatás maximalizálása érdekében fokozni kell. Minden tagállamnak növelnie kell a teljes spektrumú kibervédelmi képességek fejlesztésére irányuló beruházásait, és ezeket a többiekkel együttműködve kell fejlesztenie. A tagállamoknak fontolóra kell venniük **önkéntes kötelezettségvállalások kidolgozását a nemzeti kibervédelmi képességek**, valamint a meglévő PESCO keretében zajló kibervédelmi projekteken[[41]](#footnote-42) túlmutató multinacionális képességek fejlesztésére vonatkozóan. A koordinált éves védelmi szemle (CARD) folyamatát fel lehetne használni arra, hogy párbeszéd kezdődjön a tagállamokkal a kibervédelmi követelményekről és a kibervédelmi képességek fejlesztésére vonatkozó nemzeti célkitűzésekről, valamint hogy értékelésre kerüljön a kötelezettségvállalások végrehajtása. A Bizottság az Európai Védelmi Alapon (EDF) keresztül támogatja és társfinanszírozza a teljes spektrumú kibervédelmi képességfejlesztést és kutatást, az aktív védelmi képességeket is ideértve. A Bizottság már növelte az EDF-en keresztül megvalósított kibervédelmi beruházásokat, amelyek közös és/vagy interoperábilis európai eszközök kifejlesztését célozzák a kibertér-műveletekhez és az incidensek kezeléséhez, az informatikai hadviselési védelmi műveletekhez és a megelőző intézkedésekhez, valamint a kommunikációs és információs rendszerek rezilienciájának javításához. Ezek a beruházások olyan területeket céloznak meg, mint a kiberbiztonsággal kapcsolatos helyzetismeret, a fenyegetettségek valós idejű proaktív felderítése és a reagálási műveleti képességek, a kiberműveleti képességek, valamint a kiberképzések és -gyakorlatok[[42]](#footnote-43). Annak biztosítása érdekében, hogy a tagállamok képesek legyenek közös kiberműveleteket lebonyolítani, az elkövetkező években az EDF a reagálási műveletekhez és a kiberműveleti képességekhez fog támogatást nyújtani. Végezetül a Bizottság arra ösztönzi a tagállamokat, hogy aktívan vegyenek részt a különböző együttműködési keretekben, és használják ki az uniós szinten létrehozott valamennyi eszközt, köztük az EDA kibervédelmi projektcsoportját[[43]](#footnote-44) is.

A 2018. évi uniós képességfejlesztési prioritások[[44]](#footnote-45) folyamatban lévő felülvizsgálata időszerű lehetőséget kínál az együttműködésen alapuló és kollaboratív fejlesztés prioritásainak aktualizálására, ami lehetővé teszi az együttműködésen alapuló képességfejlesztés ilyen mértékű növelését. A kibervédelmre vonatkozó konkrét prioritás felülvizsgálata során figyelembe kell venni a 2022. évi koordinált éves védelmi szemle eredményét, valamint a tagállamoknak 2022 májusában benyújtott hiányelemzés megállapításait. Ezt követően a koordinált éves védelmi szemle rendszeres keretet biztosít majd az aktualizált prioritás nemzeti szintű végrehajtása terén elért eredmények áttekintéséhez, valamint a kibervédelmi képességek tagállamokkal való együttműködésen alapuló fejlesztése tekintetében újonnan felmerülő lehetőségek feltérképezéséhez. Az aktualizált uniós képességfejlesztési prioritások kulcsfontosságú referenciaként szolgálnak majd a kibervédelemmel kapcsolatos PESCO-projektek számára.

E tekintetben az Európai Unió Katonai Bizottságának megbízása alapján az EU Katonai Törzse a tagállamokkal szoros együttműködésben fogja kidolgozni a kibertérre vonatkozó műveletek végrehajtási tervét, hogy áttekintést nyújtson a kibervédelmi képességek megvalósításának jelenlegi állásáról, valamint támogassa a tagállamokat erőfeszítéseik és tevékenységeik jobb összehangolásában. Ezek az erőfeszítések az EU által vezetett katonai műveletekre és missziókra vonatkozó kibervédelmi uniós koncepción alapulnak, amely tükrözi a képességfejlesztési terv (CDP) prioritásait.

**A kibervédelem szempontjából kulcsfontosságú technológiákra irányuló kutatási erőfeszítések fokozása**

A legkorszerűbb kibervédelmi képességek fenntartásához lépést kell tartani a technológia fejlődésével és annak a védelmi vonatkozású rendszerekben való alkalmazásával, különös tekintettel a kialakulóban lévő és forradalmi technológiákra (EDT-k, pl. mesterséges intelligencia, titkosítás és kvantum-számítástechnika)[[45]](#footnote-46). Az EU-nak különösen a posztkvantum-kriptográfiába kell beruháznia annak biztosítása érdekében, hogy védelmi rendszerei biztonságosak maradjanak. Tekintettel a technológiai fejlődés gyors ütemére, az együttműködésen alapuló kutatási és technológiafejlesztési erőfeszítéseket úgy kell kialakítani, hogy azok technológiailag kellően kiforrottak legyenek, és így az eredményeik gyorsabban beépülhessenek a meglévő és jövőbeli képességekbe.

A Bizottság az EDF keretében finanszírozza a védelmi célú technológiai innovációt, valamint támogatja a kialakulóban lévő, forradalmi és élvonalbeli technológiák fejlesztését, többek között a kibervédelem terén is. Az EDF költségvetésének legfeljebb 8 %-át a védelmi vonatkozású forradalmi technológiákkal foglalkozó témákra különítik el, ideértve néhány, a kibervédelemmel kapcsolatos témát is. Az elkövetkező években az EDF keretében különös figyelmet fognak fordítani azokra a kutatási tevékenységekre és projektekre, amelyek a kialakulóban lévő és változó fenyegetésekkel szemben fejlesztett új technológiákkal, valamint a reziliencia növelésével, a kiberbiztonság fokozásával és ezeknek a védelmi képességekbe való integrálásával foglalkoznak.

Az EDA a kialakulóban lévő és forradalmi technológiákra vonatkozó cselekvési tervvel[[46]](#footnote-47) összhangban évente tájékoztatja a tagállamokat a kialakulóban lévő technológiák helyzetéről, beleértve a kibervédelem terén alkalmazható technológiákat is. Ezen túlmenően az EDA kidolgozza a kialakulóban lévő és forradalmi technológiák európai stratégiai értékelését annak érdekében, hogy támogassa a tagállamokat a hosszú távú stratégiai irányvonalak meghatározásában, valamint a szinergiák és az együttműködési lehetőségek azonosításában. Az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont (ECCC) stratégiai beruházási menetrendet fogad el a kulcsfontosságú kiberbiztonsági területeken, amely irányt mutat majd a Digitális Európa program és a Horizont Európa kutatási és innovációs keretprogram kiberbiztonsággal kapcsolatos jövőbeli munkaprogramjainak elkészítéséhez, támogatva a kutatást, az innovációt és a piaci elterjedést. A szinergiák előmozdítása érdekében az ECCC és az EDA munkamegállapodást dolgoznak ki azzal a céllal, hogy megkönnyítsék a két szervezet személyzete közötti információmegosztást a polgári, a kettős felhasználású és a védelmi technológiai prioritásokkal kapcsolatban.

**A kibervédelem technológiai igényeire való reagálás**

További intézkedésekre és koordinációra van szükség annak biztosítása érdekében, hogy a védelmi ágazat gyorsan reagálhasson a kibertér gyors technológiai fejlődésére. Ez magában foglalja a kibervédelem és a kiberbiztonság szempontjából kritikus technológiák azonosítására irányuló erőfeszítések fokozását, ami prioritásnak számít az EU technológiai függőségeinek csökkentése érdekében, valamint annak értékelését, hogy a jelenleg meghatározott prioritások és finanszírozási eszközök megfelelően kezelik-e ezeket a függőségeket.

Ennek érdekében a Bizottság az EDA-val és a tagállamokkal együtt 2023-ban **technológiai ütemtervre tesz majd javaslatot a kritikus kibertechnológiákra vonatkozóan**, adott esetben többek között az iparral folytatott releváns konzultációk alapján. A technológiai ütemterv azonosítja majd az EU technológiai szuverenitása szempontjából fontos kibertechnológiákat, kiterjed mind a kibervédelemre, mind a kiberbiztonságra, feltérképezi a technológiai fejlesztéseket és a stratégiai függőségeket, és fellép ez utóbbiak csökkentése érdekében. A kibertechnológiai ütemterv információkkal szolgál majd az uniós finanszírozási eszközök stratégiai prioritásaihoz, és javasolni fogja a polgári és védelmi kutatás-fejlesztési és képességfejlesztési programok, valamint a finanszírozási eszközök teljes körű kiaknázását azok irányítási szabályaival összhangban. Emellett további módokat fog javasolni a kiberbiztonsággal és a kibervédelemmel kapcsolatos kettős felhasználású kutatás, technológiafejlesztés és innováció uniós és tagállami szintű fejlesztésének ösztönzésére.

Ezzel összefüggésben a Bizottság[[47]](#footnote-48) az ECCC-vel és az EDA-val együttműködve 2023-ban értékelni fogja a kibervédelem szempontjából már kritikusnak minősített technológiákat, és – lehetőség szerint a Kritikus Technológiák Uniós Megfigyelőközpontjának támogatásával – folytatja a meglévő függőségek feltérképezését és azonosítását[[48]](#footnote-49). Ez figyelembe veszi az EDA éves nyomonkövetési dokumentumával[[49]](#footnote-50) és a kialakulóban lévő és forradalmi technológiák stratégiai európai értékelésével[[50]](#footnote-51) összefüggésben végzett munkát. Ezenkívül az ECCC célzott szakpolitikai támogatási projektet indíthatna, amely beépülhetne a technológiai ütemtervek folyamatába, és összehozhatná a polgári és katonai szféra érdekelt feleit, és együttműködhetne velük.

A szinergiákra vonatkozó cselekvési tervben, az ütemtervben és a hiányelemzésében felvázolt tevékenységek részeként már számos intézkedés van folyamatban a szinergiák megerősítésére a kettős felhasználású technológiákban rejlő lehetőségek jobb kiaknázása érdekében, többek között a kibertér tekintetében is.

Emellett a Bizottság arra ösztönzi a tagállamokat, hogy teljes mértékben használják ki a kutatást és a technológiafejlesztést támogató meglévő kezdeményezéseket, nevezetesen a védelem tekintetében az EDA védelmi képességekkel foglalkozó technológiai csoportjait[[51]](#footnote-52) és az OSRA kapcsolódó technológiai építőelemeit[[52]](#footnote-53), az EDA ad hoc keretét[[53]](#footnote-54), az EDF-et és a PESCO-t. A polgári és a kettős felhasználású technológiák esetében az ECCC és a hálózat a jogalapjában[[54]](#footnote-55) mind védelmi, mind polgári dimenzióval rendelkezőként meghatározott projekteket irányíthat. A szinergiákról szóló cselekvési tervben és az ütemtervben foglaltaknak megfelelően a Bizottság törekedni fog az ECCC és az EDF kiberbiztonsági és kibervédelmi tevékenységei közötti szinergiák megerősítésére is, az EDF irányítási szabályaival összhangban.

## 3.2. Agilis, versenyképes és innovatív európai védelmi ipar

Az EU-nak erős, agilis, versenyképes és innovatív európai védelmi iparra van szüksége, amely képes biztosítani a legkorszerűbb védelmi képességek teljes spektrumát, beleértve a kibervédelmi képességeket is. Ami azonban a kibervédelmet illeti, az EU védelmi ipara jelenleg jelentős mértékben támaszkodik a polgári megoldásokra és a külső piacokra a legkorszerűbb megoldások biztosításához. Bár a polgári területen gyors a technológiai fejlődés, és a polgári információs és a kiberbiztonsági termékek piaca gyorsan növekszik, vannak olyan konkrét katonai követelmények, amelyeket a kész polgári termékek nem elégítenek ki. A kibervédelemhez jelenleg használt hardverek és szoftverek fontos alkotórészei nem az EU-ban készülnek, ami ipari és technológiai függőségeket teremthet. Az EU jelenléte nem meghatározó a globális kiberbiztonsági és kibervédelmi iparban sem. A rendkívül széttagolt **európai védelmi technológiai és ipari bázis (EDTIB)** jelentősen csökkenti az EU versenyképességének javítására irányuló képességét[[55]](#footnote-56), mivel az Unió kiberbiztonsági vállalatainak többsége kis- és középvállalkozás (kkv)[[56]](#footnote-57). A technológiailag szuverén ipari kapacitás az EU cselekvőképességének sarokköve.

Az EU számos programon és kezdeményezésen keresztül támogatja az erős európai védelmi technológiai és ipari bázis kialakítását. Míg az EDF finanszírozza a védelmi célú technológiai innovációt és támogatja az olyan technológiák fejlesztését, amelyek végül közösen kifejlesztett élvonalbeli katonai képességekhez vezetnek és hozzájárulnak az uniós védelmi ipar versenyképességéhez, a Horizont Európa és a Digitális Európa program a kiberbiztonsági kutatást és a kettős felhasználású technológiák – többek között a kvantum, a titkosítás, a biztonságos felhő és a mesterséges intelligencia – fejlesztését támogatja[[57]](#footnote-58).

További intézkedésekre van szükség a kibervédelem szempontjából kritikus technológiákkal, valamint **a kritikus kibertechnológiákra vonatkozó technológiai ütemtervben** azonosított ipari szükségletekkel kapcsolatban. Meg kell határozni a megfelelő támogatási csatornákat, például a közös közbeszerzési erőfeszítések ösztönzése érdekében, többek között a jövőbeli európai védelmi beruházási program révén, vagy meg kell könnyíteni a tőkéhez és hitelekhez való hozzáférést az Európai Beruházási Alapon és az Európai Beruházási Bankon keresztül.

Az erős európai védelmi technológiai és ipari bázis (EDTIB) létrehozása érdekében biztosítani kell a polgári és védelmi vállalatok közötti szinergiák kiaknázását. Az uniós védelmi innovációs program (EUDIS) keretében javasolt innovációs intézkedések – többek között a kkv-k elérése és a technológia felkutatása – pozitív hatást gyakorolhatnak az EU védelmi iparára és az EDTIB-re.

A Bizottság ágazati párbeszédet is kezdeményez az EU kibervédelmi iparának fejlesztése céljából, adott esetben az EDA bevonásával.

A Bizottság és a főképviselő számos intézkedés bevezetését javasolja annak érdekében, hogy az ipar megfelelően fel legyen vértezve a rövid és hosszú távú eredmények eléréséhez. Ez rövid távon magában foglalja az EU védelmi ipari gyártási képességeinek mélyreható feltérképezését annak érdekében, hogy pontosan meg lehessen határozni a hiányosságokat és azokat a területeket, ahol fejlesztésre van szükség.

Az Ursula von der Leyen elnöknek az Unió helyzetéről szóló 2022. szeptemberi beszédében bejelentett új Európai Szuverenitási Alap is foglalkozhatna a kiberkérdések terén fennálló kritikus függőségek csökkentésével, amelyeket a technológiai ütemtervekben is azonosíthatnak.

A közvetlen külföldi befektetések átvilágítására szolgáló uniós keretet továbbra is használni fogják a védelmi és biztonsági kockázatok tekintetében kockázatot jelentő európai technológiák vagy megoldások felvásárlásával kapcsolatos kockázatok csökkentésére. Azoknak a tagállamoknak, amelyek még nem hoztak létre nemzeti átvilágítási mechanizmusokat, ezt haladéktalanul meg kell tenniük.

## 3.3. Uniós kibervédelmi munkaerő

Európa valós és riasztó kiberbiztonsági készséghiánnyal néz szembe: az Európai Kiberbiztonsági Szervezet (ECSO) becslése szerint már 2022-ben összesen 500 000 szakemberre lenne szükség. Ez a készséghiány akadályozza az EU azon képességét, hogy új technológiákat fejlesszen ki és megvédje kritikus infrastruktúránkat. Az olyan kormányzati szervek esetében, mint például a védelmi minisztériumok és a katonaság, a készségekért folytatott kiélezett verseny és a magánszektor által kínált vonzó fizetések tovább súlyosbítják a kibertehetségek vonzásával és megtartásával kapcsolatos nehézségeket.

A készségek 2023-as európai éve keretében a Bizottság **kezdeményezni fogja a Kiberkészségek Akadémiájának létrehozását**. Az akadémia ernyőkezdeményezésként fog működni, amely a kiberbiztonsági képzettséggel rendelkező szakemberek számát hivatott növelni. Számos, különböző kiberkészségekkel kapcsolatos kezdeményezést fog majd össze és biztosítja az azokkal kapcsolatos koordinációt, integrációt és közös kommunikációt. A Kiberkészségek Akadémiája – amely olyan cselekvési pillérek köré szerveződik, mint a finanszírozás, a közösségi támogatás, a képzés és tanúsítás, az érdekeltek bevonása és a tudásgenerálás – a kibervédelmi munkaerő számára is hasznos lesz. Az Európai Biztonsági és Védelmi Főiskola (EBVF) meg fogja vizsgálni, hogy miként lehetne elősegíteni a bevált gyakorlatok cseréjét és a katonai és polgári területek közötti további szinergiákat a képzés és a kibertér-specifikus katonai készségek fejlesztése tekintetében.

Az EBVF, az EDA és a tagállamok a képzési követelmények és a képzési igények elemzése alapján továbbfejlesztik és megszervezik a kibervédelmi képzési tevékenységeket és gyakorlatokat az uniós intézmények, a KBVP-műveletek és -missziók, valamint a tagállami tisztviselők számára. A képzési kapacitások bővítése érdekében meg fogják vizsgálni **az EBVF kiberoktatással, -képzéssel, -értékeléssel és -gyakorlattal kapcsolatos platformjának (ETEE) továbbfejlesztését** is. Ennek magában kell foglalnia a konkrét műveleti területre és a több területre kiterjedő műveletekre vonatkozó képzéseket is. Szinergiákra kell törekedni különösen az Uniós Kiberakadémia és Innovációs Központ (EU CAIH) PESCO-projekttel[[58]](#footnote-59).

A Bizottság arra ösztönzi a tagállamokat, hogy a (polgári és katonai) felsőoktatási intézmények bevonásával dolgozzanak ki speciális oktatási programokat a kibervédelem területén a közös kibervédelmi tantervek kidolgozása és létrehozása, a bevált gyakorlatok megosztása, a partnerségek és közös projektek megvalósítása, valamint az oktatók és gyakornokok cseréjének megkönnyítése érdekében. Az interoperabilitás és az EU-n belüli közös kultúra biztosítása érdekében az EBVF az ETEE-n keresztül elő fogja mozdítani a tagállamok közötti információcserét.

A tagállamoknak fokozniuk kell a képzés és az oktatás szereplői közötti szélesebb körű együttműködést, ötvözve mind a polgári, mind a katonai szempontokat a technikai, a műveleti, a stratégiai és a jogi területeken, megteremtve az alapot a polgári, a bűnüldözési, a diplomáciai és a kibervédelmi közösségek közös és szabványosított képzési programjainak létrehozásához különböző szinteken. Emellett a tagállamoknak együtt kell működniük az európai magánszektor képzési szolgáltatóival és a tudományos intézményekkel a katonai KBVP-missziókban és -műveletekben részt vevő személyzet kompetenciáinak és készségeinek javítása érdekében.

Emellett elő kell mozdítani a kibervédelmi képzési szabványokkal és tanúsítással kapcsolatos együttműködést a tagállamok, az uniós intézmények, szervek és ügynökségek, a nemzetközi partnerek és más szereplők, többek között a magánszektor és a tudományos élet szereplői között. Az EBVF a meglévő polgári kezdeményezésekre, például az ENISA által kidolgozott Európai Kiberbiztonsági Készségek Keretére (ECSF) építve kidolgozza a kibervédelmi készségek tanúsítási keretrendszerét. A Bizottság mérlegelné a piacon és a tudományos körökben rendelkezésre álló kiberkészségek tanúsításának különböző megközelítéseit is, miközben a Kiberkészségek Akadémiáján keresztül arra törekszik, hogy ösztönözze az e megközelítések közötti szinergiákat és pótolja a hiányosságokat, különösen célzott uniós finanszírozás révén.

***Kibervédelmi intézkedések***

* A kialakulóban lévő és forradalmi technológiák stratégiai értékelésének kidolgozása a hosszú távú stratégiai beruházási döntések támogatása érdekében.
* Technológiai ütemterv kidolgozása az EU számára a kritikus kibertechnológiákra vonatkozóan, amely kiterjed a kibervédelem és a kiberbiztonság szempontjából kritikus technológiákra a függőségek szintjének értékelése érdekében.
* Javaslatok tétele az összes uniós eszköz – köztük a Digitális Európa program, a Horizont Európa és az Európai Védelmi Alap – felhasználásával a függőségek csökkentésére, valamint a technológiai fejlődés irányának előrejelzése a technológiai szuverenitás növelése és a cselekvőképesség biztosítása érdekében.
* Támogatás a kibervédelmi készségek tanúsítási keretrendszerének kidolgozásához.
* Uniós kibervédelmi gyakorlatok kidolgozása, valamint annak feltárása, hogy miként lehetne továbbfejleszteni az EBVF kiberoktatással, -képzéssel, -értékeléssel és -gyakorlattal kapcsolatos platformját (ETEE) a képzési kapacitások növelése érdekében.

***Polgári támogató fellépések***

* A Kiberkészségek Európai Uniós Akadémiájának létrehozása a különböző szakmai profilok és tevékenységi ágazatok – így a védelmi munkaerő – különleges szakismereti igényeinek mérlegelésével.
* A kiberkészségek tanúsítására vonatkozó megközelítések elemzése, eközben törekvés a szinergiák előmozdítására és a hiányosságok pótlására, többek között uniós finanszírozás révén.

**4. Összefogás a közös kihívások kezelése érdekében**

A partnerek számára előnyös lesz, ha az EU képességekkel és rezilienciával rendelkezik a kibertérben, valamint a vonatkozó uniós eszközök révén nyújtott uniós kibervédelmi segítségnyújtásból és kapacitásépítésből is profitálnak. Az EU arra fog törekedni, hogy testre szabott partnerségeket hozzon létre a kibervédelem területén, amennyiben ezek kölcsönösen előnyösek. A kibervédelmi partnerségek a partnerországok katonai KBVP-missziókban és -műveletekben való részvételével összefüggésben is napirendre kerülnek.

Ez a munka adott esetben a meglévő kiberdialógusokra, valamint a biztonsági és védelmi párbeszédekre fog épülni. A főképviselő fel fogja tárni **az informális uniós kiberdiplomáciai hálózat és az uniós küldöttségek védelmi attaséinak hálózata** közötti szinergiákat is.

***4.1. Együttműködés a NATO-val***

Az EU és a NATO közötti stratégiai partnerség továbbra is alapvető fontosságú az euroatlanti biztonság szempontjából, amint azt a stratégiai iránytű és a NATO 2022. évi stratégiai koncepciója[[59]](#footnote-60) is hangsúlyozza. Az EU továbbra is teljes mértékben elkötelezett e kulcsfontosságú partnerség erősítése mellett, többek között a kibervédelem területén is, és további lépések megtételét sürgeti a közös fenyegetésekre és kihívásokra vonatkozó közös megoldások kidolgozása érdekében. Az EU és a NATO közötti együttműködésről szóló varsói és brüsszeli együttes nyilatkozatokkal[[60]](#footnote-61) összhangban, valamint az átláthatóság, a kölcsönösség és az inkluzivitás, a nyitottság és mindkét szervezet döntéshozatali autonómiájának elve alapján a kiberbiztonság és a kibervédelem az egyik kiemelt együttműködési terület az EU számára.

A kölcsönösség elve alapján az EU továbbra is eszmecserét folytat a NATO-val a kibervédelmi szempontoknak a katonai KBVP-missziók és -műveletek tervezésébe és végrehajtásába történő integrálására vonatkozó katonai koncepcionális keretről. Az EU a lehető legnagyobb mértékben törekedni fog az összeegyeztethetőségre a NATO kibervédelmi koncepcióival és doktrínájával.

Tekintettel a kibervédelmi képességek iránti nagy keresletre, az EU ösztönözni fogja a szervezeti és nemzeti határokon átnyúló szinergiák és komplementaritás kiaknázását a NATO-val. Az EU partnerként fog együttműködni a NATO-val a kibervédelmi képességek technikai és eljárási interoperabilitásának megerősítése érdekében, ideértve a képességeknek a szövetséges műveleti hálózat (FMN) kezdeményezéssel összhangban történő fejlesztését is. Ez megnyitja az utat a kibervédelmi képességek potenciálisan egymást kölcsönösen támogató fejlesztése és alkalmazása előtt. Különös figyelmet kell fordítani a szabványok interoperabilitására, hozzájárulva a kiberrezilienciához és a katonai kommunikációs és információs rendszerek interoperabilitásához, adott esetben az ipar bevonásával.

Annak érdekében, hogy koherens képzést biztosítson az érintett kibervédelmi személyzet számára, az EU adott esetben meg fogja erősíteni a NATO-val a képzési igények és a követelmények elemzésének összehangolása terén folytatott együttműködést, közös tanterveket, tanfolyamokat és gyakorlatokat dolgozva ki. A kölcsönösség és a megkülönböztetésmentesség elve alapján az EBVF megnyitja kibervédelmi képzéseit a NATO személyzete előtt, és platformot hoz létre a közös tanfolyamok meghirdetésére. Az EU emellett ösztönözni fogja a NATO személyzetének részvételét a kibergyakorlatokban és a kiberelemeket tartalmazó válságkezelési gyakorlatokban.

Az EU és a NATO emellett együttműködik a kölcsönös helyzetismeret további javítása érdekében, és fel fogja térképezni a koordináció lehetőségeit, többek között az NCIRC és a CERT-EU közötti együttműködés megerősítése révén. A válságkezelés és -reagálás kiberszempontú vonatkozásaival és következményeivel kapcsolatos együttműködés előmozdítása érdekében az EU hozzá fog járulni a katonai, polgári és közös kezdeményezésekkel foglalkozó személyzet közötti eszmecseréhez, valamint adott esetben a vonatkozó válságkezelési keretek és kezdeményezések potenciális szinergiáinak kialakításához, többek között a nagyszabású kiberbiztonsági események esetében is. A kölcsönös kiegészítő jelleg biztosítása és a szükségtelen párhuzamos erőfeszítések elkerülése érdekében az EU szorosabb együttműködésre és információcserére fog törekedni a NATO-val a partnerországok kibervédelmi kapacitásépítési erőfeszítéseiről.

***4.2. Együttműködés a hasonlóan gondolkodó partnerekkel***

A főképviselő szisztematikusabban fel fogja venni a kibervédelmi kérdéseket a partnerekkel folytatott meglévő és jövőbeli kiber-, valamint biztonsági és védelmi dialógusok napirendjére. Ahogy a kibervédelmi szempontok egyre nagyobb hangsúlyt kapnak a kétoldalú párbeszédek során, egyre nagyobb lehetőség nyílik arra, hogy a kibervédelmi kérdéseket az uniós partnerekkel folytatott együttműködés más formáiba is bevezessék.

Az EU és az **Egyesült Államok** közötti stratégiai partnerség keretében folytatódik a biztonság és a védelem terén folytatott együttműködés kölcsönösen előnyös elmélyítése, többek között a helyzetismerettel kapcsolatos strukturált információcsere révén. A rendszeres EU–USA kiberpárbeszédek és az EU–USA biztonsági és védelmi párbeszédek állandósítják az erős transzatlanti partnerséget. A főképviselő adott esetben be fogja építeni e párbeszédekbe a kibervédelem releváns szempontjait.

Az EU nemzetközi partnereivel együtt továbbra is támogatni fogja **Ukrajnát**, többek között kiberpárbeszéd révén. Tekintettel Ukrajnának a kiberreziliencia és a kibervédelmi képességek kiépítése terén szerzett tapasztalataira, a kibervédelemmel kapcsolatos bevált gyakorlatok – többek között a fenyegetettségi helyzetre és a helyzetismeretre vonatkozó információk – cseréje, valamint a releváns szakpolitikai fejlemények továbbra is közös érdeklődésre tartanak számot, és egyre inkább ki fognak terjedni.

A hasonlóan gondolkodó partnerek fontos szerepet játszanak a globális, nyitott, stabil és biztonságos kibertér fenntartásában, és kiegészíthetik az EU azon képességét, hogy megelőzze, visszatartsa és eltántorítsa a kibertérben tanúsított rosszindulatú magatartást, illetve reagáljon arra. Az EU továbbra is nyitott a széles körű, ambiciózus és kölcsönösen előnyös biztonsági és védelmi szerepvállalásra, többek között a kibervédelem terén, valamennyi hasonlóan gondolkodó partner bevonásával.

***4.3. Kibervédelmi kapacitásépítési támogatás a partnerországok számára***

A globális és regionális kihívások növelték az EU és partnerei kölcsönös egymásrautaltságát, és rávilágítottak arra, hogy szorosabb partnerségeket kell kialakítani a biztonság és a védelem területén. Ez különösen fontos az uniós tagjelölt országok tekintetében. A közelmúltbeli nagyszabású kibertámadások azt jelzik, hogy a meglévő programokra építve fokozott uniós szerepvállalásra és partnerségre van szükség a kiberbiztonság és a kibervédelem terén. A kiberfenyegetések transznacionális jellege miatt a partnerországok – különösen az alacsonyabb szintű kiberérettséggel rendelkező országok – kiberrezilienciájának fokozása hozzá fog járulni kibertér biztonságának növeléséhez. Az EU képességei ezzel javulnának a kibertámadások megelőzése, felderítése, az ellenük való védekezés és az azoktól való elrettentés terén.Az EU – többek között a meglévő párbeszédek révén – meg fogja erősíteni a partnerországokkal folytatott biztonsági és védelmi együttműködést annak érdekében, hogy megerősítse kiberrezilienciájukat. Amennyiben az megvalósítható és kölcsönösen előnyös, az EU hozzá fog járulni partnerei kibervédelmi kapacitásépítési erőfeszítéseihez, különösen azon uniós tagjelölt országok esetében, amelyek joganyagukat már harmonizálták az EU közös kül- és biztonságpolitikájával és közös biztonság- és védelempolitikájával. Ez kiterjedhet szakpolitikai és jogalkotási keretek támogatására, a partnerek fegyveres erőinek és biztonsági erőinek kiképzésére, mentorálására és felszerelésére, valamint az ezek részére való tanácsadásra. A tagállamok dönthetnek úgy, hogy kibervédelmi operatív segítséget nyújtanak a partnereknek. Emellett az EU segíteni fogja partnereit abban, hogy megerősítsék a katonai KBVP-missziókhoz és -műveletekhez való hozzájárulásra irányuló kapacitásukat, mivel ez értékes hozzájárulást jelent a béke és a biztonság előmozdítására irányuló kölcsönös erőfeszítésekhez.

Az Európai Békekeret továbbra is támogatni fogja azokat az uniós erőfeszítéseket, amelyek célja a védelmi kapacitások – többek között a kibervédelem – kiépítésének elősegítése a partnerországokban, különösen az EU szomszédságában, kiegészítve a KBVP keretében folytatott válságkezelési erőfeszítéseket. E tekintetben az EU szükség esetén jobban összekapcsolja a kibervédelmi segítségnyújtást a polgári kiberbiztonsági kapacitásépítéssel, különösen az uniós kiberkapacitás-építési testületen keresztül. A kibervédelmi és kiberbiztonsági kapacitásépítési intézkedések sikeréhez hatékony koordinációra lesz szükség a vonatkozó uniós programok és eszközök – köztük az Európai Békekeret – és a tagállamok között.

Amellett, hogy támogatást nyújt a partnerországoknak a kibervédelmi kapacitásépítési erőfeszítéseikhez, az EU szorosan együtt fog működni más donorokkal a helyzetismereti és koordinációs platformok kialakítása érdekében azzal a céllal, hogy a lehető legjobb, testre szabott támogatást lehessen nyújtani, valamint biztosítani lehessen az erőfeszítések koherenciáját és a felesleges duplikációk elkerülését.

***Kibervédelmi intézkedések***

* Az EU és a NATO közötti együttműködés megerősítése a kibervédelmi kiképzés, oktatás, helyzetismeret és gyakorlatok terén.
* A kibervédelmi témák felvétele az EU által vezetett kiberdialógusok, valamint a partnerországokkal folytatott biztonsági és védelmi párbeszédek napirendjére.
* Együttműködés a hasonlóan gondolkodó országokkal, többek között a kibervédelmi képességek fejlesztésével és a kiberrezilienciával összefüggésben.
* A partnereknek nyújtott támogatás növelése – többek között az Európai Békekereten (EPF) keresztül – a kibervédelmi képességek fejlesztése terén, különösen az EU szomszédságában és az uniós tagjelölt országok támogatása céljából.

***Polgári támogató fellépések***

* Az EU és a NATO közötti együttműködés megerősítése a kiberbiztonság területén a helyzetismeret, a válságreagálás, a kritikus infrastruktúrák védelme, valamint a szabványosítás és a tanúsítás tekintetében.

# III. KÖVETKEZTETÉS

A főképviselő – aki egyben az EDA vezetője is –, valamint a Bizottság felszólítja a tagállamokat, hogy dolgozzák ki a kibervédelmi politika releváns szempontjait. Előbbiek kapcsolatot fognak tartani a tagállamokkal a gyakorlati végrehajtási intézkedések azonosítása érdekében. A tagállamokkal együttműködve végrehajtási tervet lehetne kidolgozni. Az uniós kibervédelmi politika végrehajtásának eredményei elősegítik majd az uniós kiberbiztonsági stratégia és a stratégiai iránytű átfogó célkitűzéseinek megvalósítását.

A kibervédelmi politika végrehajtásának nyomon követése és értékelése céljából éves jelentés kerül benyújtásra a Tanácshoz. A Bizottság arra ösztönzi a tagállamokat, hogy segítsék a jelentés elkészítését a nemzeti vagy együttműködési formában megvalósuló végrehajtási intézkedések haladásával kapcsolatos információkkal.

1. Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat), 2018. november 19., http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf [↑](#footnote-ref-2)
2. [A biztonság és a védelem területére vonatkozó stratégiai iránytű – Egy, a polgárait, az értékeit és az érdekeit megvédő Európai Unióért, amely hozzájárul a nemzetközi béke és biztonság megvalósításához](https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/hu/pdf) [↑](#footnote-ref-3)
3. Az EU kiberbiztonsági stratégiája a digitális évtizedre, [JOIN/2020/18 final](https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=JOIN:2020:18:FIN). [↑](#footnote-ref-4)
4. https://ec.europa.eu/commission/presscorner/detail/hu/SPEECH\_21\_4701 [↑](#footnote-ref-5)
5. [9364/22](https://www.consilium.europa.eu/media/56358/st09364-en22.pdf) [↑](#footnote-ref-6)
6. [JOIN(2022) 24 final](https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52022JC0024&qid=1667903048025). [↑](#footnote-ref-7)
7. EEAS(2021) 706 REV4. [↑](#footnote-ref-8)
8. Polgári, diplomáciai és bűnüldözési kiberközösségek. [↑](#footnote-ref-9)
9. Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén [↑](#footnote-ref-10)
10. Az Európai Unióról szóló szerződés, egységes szerkezetbe foglalt változat: Hivatalos Lap C 326., 2012.10.26., 1. o. [↑](#footnote-ref-11)
11. Az Európai Unió működéséről szóló szerződés, egységes szerkezetbe foglalt változat: Hivatalos Lap C 326., 2012.10.26., 1. o. [↑](#footnote-ref-12)
12. A projekt célja a Kiber- és az Információs Terület (CID) multinacionális Koordinációs Központjának (CIDCC) kifejlesztése, létrehozása és működtetése állandó multinacionális katonai elemként. [↑](#footnote-ref-13)
13. Az európai kibervédelmi parancsnokok 2022. januári és júniusi első két stratégiai konferenciájára (CyberCo) építve az uniós kibervédelmi parancsnokok úgy határoztak, hogy saját szintjükön állandóbb jellegű fórumot hoznak létre. [↑](#footnote-ref-14)
14. A Bizottság és a főképviselő közös elnökletével működő, az érintett bizottsági szolgálatokat, az EKSZ-t, az Európai Uniós Kiberbiztonsági Ügynökséget (ENISA), a CERT-EU-t és az Europolt magában foglaló informális csoport. [↑](#footnote-ref-15)
15. Az EU kiberbiztonsági stratégiája a digitális évtizedre, (JOIN/2020/18 final) és a biztonsági unióra vonatkozó uniós stratégia (COM(2020) 605) [↑](#footnote-ref-16)
16. A Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről szóló, 2021. április 29-i (EU) 2021/694 európai parlamenti és tanácsi rendelettel (HL L 166., 2021.5.11., 1. o.) összhangban, annak esetleges módosítására figyelemmel. [↑](#footnote-ref-17)
17. [Az EU kiberbiztonsági képességeinek megerősítésére irányuló nevers-i felhívás.](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/) [↑](#footnote-ref-18)
18. https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx [↑](#footnote-ref-19)
19. https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/ [↑](#footnote-ref-20)
20. A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”). [↑](#footnote-ref-21)
21. https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/ [↑](#footnote-ref-22)
22. https://english.ncsc.nl/topics/log4j-vulnerability [↑](#footnote-ref-23)
23. A főképviselőnek az Európai Unió nevében tett nyilatkozata a hekkerek és hekkercsoportok által Oroszország Ukrajna elleni agressziójával összefüggésben végzett rossz szándékú kibertevékenységekről: https://www.consilium.europa.eu/hu/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/ [↑](#footnote-ref-24)
24. Az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló irányelv, amelyről a társjogalkotók a közelmúltban állapodtak meg, és amelynek hivatalos elfogadására várhatóan ez év végéig sor kerül. [↑](#footnote-ref-25)
25. Javaslat – Az Európai Parlament és a Tanács rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról, [COM/2022/454 final](https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=celex%3A52022PC0454). [↑](#footnote-ref-26)
26. A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról; ST09364/22, 2022. május 23. [↑](#footnote-ref-27)
27. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group [↑](#footnote-ref-28)
28. [Az EU kiberbiztonsági képességeinek megerősítésére irányuló nevers-i felhívás.](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/) [↑](#footnote-ref-29)
29. Javaslat – A TANÁCS AJÁNLÁSA a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről, [COM/2022/551 final.](https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270) [↑](#footnote-ref-30)
30. Az energiarendszer digitalizációja – Uniós cselekvési terv, COM/2022/552 final. [↑](#footnote-ref-31)
31. A biztonság és a védelem területére vonatkozó stratégiai iránytű, 2022. március 21. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/hu/pdf [↑](#footnote-ref-32)
32. [Az 5G-hálózatok kiberbiztonsága: a kockázatcsökkentő intézkedések uniós eszköztáraEurópa digitális jövőjének megtervezése (europa.eu).](https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures) [↑](#footnote-ref-33)
33. https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx [↑](#footnote-ref-34)
34. COM/2022/454 final. [↑](#footnote-ref-35)
35. COM(2021) 70 final. [↑](#footnote-ref-36)
36. Az (EU) 2022/30 felhatalmazáson alapuló rendelet alapján folyamatban van a rádióberendezésekre vonatkozó kiberbiztonsági követelményekkel kapcsolatos szabványosítási munka. Amennyiben a Bizottság hatályon kívül helyezi vagy módosítja ezt a felhatalmazáson alapuló rendeletet oly módon, hogy az a kiberrezilienciáról szóló jogszabály hatálya alá tartozó bizonyos termékekre már nem alkalmazandó, a kiberrezilienciáról szóló jogszabály végrehajtásának megkönnyítése érdekében a Bizottságnak és az európai szabványügyi szervezeteknek figyelembe kell venniük a C(2022)5637 bizottsági végrehajtási határozat keretében a fent említett felhatalmazáson alapuló rendeletre irányuló szabványosítási kérelemmel kapcsolatban elvégzett szabványosítási munkát a harmonizált szabványok kidolgozása és továbbfejlesztése során. [↑](#footnote-ref-37)
37. Pl. a védelmi beruházási hiányok elemzésében meghatározottak szerint. [↑](#footnote-ref-38)
38. Számos kezdeményezés indult, például a védelmi készségekkel foglalkozó európai partnerség. [↑](#footnote-ref-39)
39. A Bizottság a kritikus technológiákra vonatkozó ütemtervben felszólított az Európa hosszú távú biztonsága és védelme szempontjából kritikus technológiák terén folytatott együttműködés és a kapcsolódó stratégiai függőségek csökkentésére irányuló erőfeszítések megerősítésére. [↑](#footnote-ref-40)
40. A védelmi beruházási hiányok elemzéséről és a következő lépésekről szóló közös közlemény, amelyben a Bizottság és a főképviselő számos intézkedést javasolt annak biztosítása érdekében, hogy az uniós ipar képes legyen rövid és hosszú távon is eredményeket felmutatni. [↑](#footnote-ref-41)
41. Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén (CRRT), A Kiber- és az Információs Terület Koordinációs Központja (CIDCC), a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform (CTIRISP), az Összevont virtuális gyakorlóterek (CRF), Uniós Kiberakadémia és Innovációs Központ (EU CAIH). [↑](#footnote-ref-42)
42. Az európai védelmi ipari fejlesztési program (EDIDP) keretében 6 projektet (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET és HERMES) finanszíroztak 39 millió EUR költségvetéssel. A 2021. évi EDF keretében csaknem 40 millió EUR-t különítenek el 3 együttműködésen alapuló kibervédelmi K+F projektre, amelyeket finanszírozásra kiválasztottak (ACTING, AInception, EU-GUARDIAN). [↑](#footnote-ref-43)
43. A kibervédelmi projektcsoport fórumot biztosít a tagállamok számára a katonai vonatkozású kibervédelmi kérdések megvitatására. [↑](#footnote-ref-44)
44. Az EDA képességfejlesztési prioritásokról szóló tájékoztatója (2018. június 28.): [Tájékoztató a képességfejlesztési tervről](https://eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0fInsert%20). [↑](#footnote-ref-45)
45. A kibervédelmi stratégiai kutatási tervben és az átfogó stratégiai kutatási menetrendben (OSRA) meghatározottak szerint. [↑](#footnote-ref-46)
46. A „Kialakulóban lévő és forradalmi technológiák (EDT): képességvezérelt cselekvési terv” című dokumentumot 2021. december 16-án fogadta el az EDA kutatás-fejlesztési igazgatók összetételben ülésező irányítóbizottsága. [↑](#footnote-ref-47)
47. A Közös Kutatóközponttal együtt. [↑](#footnote-ref-48)
48. A Kritikus Technológiák Uniós Megfigyelőközpontja, amelyet a polgári, a védelmi és az űripar közötti szinergiákról szóló cselekvési tervben jelentettek be. [↑](#footnote-ref-49)
49. Az EDA kialakulóban lévő és forradalmi technológiákra vonatkozó 2021. évi cselekvési tervének első szakasza. [↑](#footnote-ref-50)
50. Az EDA 2021. évi cselekvési tervének második szakasza. [↑](#footnote-ref-51)
51. A CapTechs hálózatépítési fórumokat kínál a tagállami szakértők számára, és rugalmas keretet biztosít az együttműködésen alapuló projektekhez. A CapTechs-re vonatkozó, kibertérhez kapcsolódó további információk (kiber, információ, komponensek) a következő internetcímen érhetők el: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs). [↑](#footnote-ref-52)
52. Az OSRA feltérképezi a releváns védelmi kutatási és technológiai területeket, és részletezi a konkrét együttműködési lehetőségeket. Jelenleg 17 technológiai építőelem és a hozzájuk tartozó kibertechnológiai ütemtervek foglalkoznak a kibervédelmi helyzetismerettel, a katonai kommunikációs rendszerek védelmével, a heterogén forrásokból származó információk feldolgozásával, a modellezéssel és szimulációval, a kvantuminformatikával és a kriptográfiával, valamint a kiberműveletek és az elektronikus hadviselés közötti szinergiák feltárásával. A mesterséges intelligencia és a nagy adathalmazok kulcsszerepet játszanak az információfeldolgozásban. [↑](#footnote-ref-53)
53. Az EDA ad hoc keretét a (KKBP) 2015/1835 tanácsi határozat határozza meg. Jelenleg 6 kibertechnológiai elemet tartalmazó projekt (ANQUOR, CERERE, EDA SOC 2, MASFAD II, PASEI II, ASSAI) végrehajtása van folyamatban ebben a keretben, mintegy 20 millió EUR költségvetéssel. [↑](#footnote-ref-54)
54. Az Európai Parlament és a Tanács (EU) 2021/887 rendelete (2021. május 20.) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról. [↑](#footnote-ref-55)
55. A védelmi beruházási hiányok elemzéséről és a következő lépésekről szóló közös közleményben meghatározottak szerint. [↑](#footnote-ref-56)
56. A becslések szerint összesen mintegy 2 500 kkv működik az EU-n belüli többrétegű és gyakran határokon átnyúló védelmi ellátási láncokban. Ezek védelmi területen tevékenykedő ügyfeleket szolgálnak ki, miközben üzleti tevékenységük 7,8 %-a kapcsolódik a kibertevékenységhez. [↑](#footnote-ref-57)
57. A Horizont Európa előirányozza, hogy az EDF-fel való szinergiák a polgári és védelmi kutatás számára is előnyösek, ugyanakkor a keretprogram tevékenységei kizárólag a polgári alkalmazásokra fognak összpontosítani. [↑](#footnote-ref-58)
58. https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/ [↑](#footnote-ref-59)
59. https://www.nato.int/strategic-concept/ [↑](#footnote-ref-60)
60. Az együtes nyilatkozatot 2016-ban, illetve 2018-ban írták alá. [↑](#footnote-ref-61)