EURÓPAI
BIZOTTSÁG

Strasbourg, 2023.4.18.
COM(2023) 207 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

A kiberbiztonsági szakemberhiány megszüntetése az EU versenyképességének, növekedésének és rezilienciájának növelése érdekében („Kiberkészségek Akadémiája”)

A kiberbiztonsági szakemberhiány megszüntetése az EU versenyképességének, növekedésének és rezilienciájának növelése érdekében („Kiberkészségek Akadémiája”)

1. Sürgős szükség van a kockázatok csökkentésére a kiberbiztonsági készségek hiányának és hiányosságainak kezelésével

A kiberbiztonság nemcsak a polgárok, a vállalkozások és a tagállamok biztonságának része. Az EU politikai stabilitásának, a tagállamok demokráciái stabilitásának, valamint társadalmunk és vállalkozásaink jólétének biztosításához is szükséges. A kiberbiztonságot jellemző **fenyegetettségi helyzet** az elmúlt években nagymértékben átalakult, és aggasztó tendencia, hogy egyre több kibertámadás éri az EU katonai és polgári kritikus infrastruktúráit. A fenyegető szereplők növelik képességeiket, és újszerű, hibrid és újonnan megjelenő fenyegetések jelennek meg, mint például a botok és a mesterséges intelligencián alapuló technikák használata[1]. Különösen a zsarolóvírusokkal fenyegető szereplők okoznak rendszeresen jelentős anyagi és hírnévbeli károkat az alanyoknak[2].

Számos kiberbiztonsági esemény a tagállamok közigazgatását és kormányait, valamint az Unió intézményeit, szerveit és hivatalait (EUIBA-k) is célba vette[3]. A pénzügyi[4] és az egészségügyi[5] ágazat, amelyek a társadalom és a gazdaság gerincét képezik, szintén következetesen célkeresztbe kerültek[6]. Az Oroszország Ukrajna elleni agressziós háborújához kapcsolódó geopolitikai feszültségek megnövelték a kiberbiztonsági fenyegetést[7], és potenciálisan destabilizálhatják társadalmunkat. Az EU **biztonsága** nem garantálható **az EU legbecsesebb értéke, az emberek** nélkül. Az EU-nak sürgősen szüksége van olyan szakemberekre, akik rendelkeznek azokkal a készségekkel és kompetenciákkal, amelyekkel megelőzhetik, felderíthetik és elrettenthetik a kibertámadásokat, továbbá megvédhetik ezektől az EU-t – beleértve a legkritikusabb infrastruktúráit is –, és biztosíthatják annak **rezilienciáját**.

A kiberbiztonsági szakemberhiány tovább hátráltatja Európa **versenyképességét** és **növekedését**, amely nagymértékben függ a stratégiai digitális technológiák (pl. mesterséges intelligencia, 5G és felhő) fejlesztésétől és elterjedésétől. Képzett kiberbiztonsági munkaerőre

---

[1] ENISA: Fenyegetettségi helyzetjelentés, 2022 — ENISA (europa.eu).

[2] Europol: Az internetes szervezett bűnözés általi fenyegetettség értékelése, (IOCTA) 2021. Az ilyen szereplők a zsarolóvírus mint szolgáltatás modellre építenek. A vállalkozások éves költségei 2022-ben meghaladták a 18,4 milliárd EUR-t. (Cybereason 2022: Jelentés a zsarolóvírusok valódi költségeiről).

[3] Lásd például: Az ENISA és a CERT-EU közös kiadványa JP-23-01 – *Sustained activity by specific threat actors* [Egyedi fenyegető szereplők folyamatos tevékenysége], TLP:CLEAR, 2023. február 15.

[4] Lásd például Németország esetét, ahol a 2021. június 1. és 2022. május 31. között bejelentett postai csalások 90 %-a pénzügyi adathalászat volt, vagy egy pénzügyi ágazatbeli vállalat elleni támadás esete, amely több mint 20 000 fertőzött eszközt érintett 125 országból, Az IT-biztonság helyzete Németországban 2022-ben, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023. január 1.

[5] Lásd például Franciaország esetét, ahol az állami egészségügyi intézmények, például a Centre Hospitalier Sud Francilien elleni zsarolóvírus-támadások során 11 GB személyes és orvosi adatot, valamint a személyzettel kapcsolatos adatokat veszélyeztetett és tett közzé a támadó, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d’information (ANSSI), janvier 2023.

[6] ENISA: Fenyegetettségi helyzetjelentés, 2022.

[7] Lásd még: CERT-EU – Oroszország háborúja Ukrajna ellen: a kiberműveletek egy éve (europa.eu); Ukrajna ellen irányuló orosz kiberműveletek: A főképviselőnek az Európai Unió nevében tett nyilatkozata, 2022. május 10.; A főképviselőnek az Európai Unió nevében tett nyilatkozata a hekkerek és hekkercsoportok által az Ukrajna elleni orosz agresszióval összefüggésben folytatott rosszindulatú kibertevékenységekről, 2022. július 19.

van szükség ahhoz, hogy az EU továbbra is képes legyen globális szinten kulcsfontosságú, fejlett technológiákat biztosítani.

Az EU kiberbiztonsági politikája az elmúlt években jelentős előrelépést tett a változó fenyegetettségi helyzettel szembeni felkészülés és a vele való szembenézés, valamint az EU versenyképességének előmozdítása érdekében, ami számos kezdeményezés elfogadásához vezetett, mint például az EU kiberbiztonsági stratégiája a digitális évtizedre[8], a hálózati és információs rendszerek biztonságáról szóló felülvizsgált irányelv (a továbbiakban: NIS 2 irányelv)[9], a kiberbiztonságra vonatkozó uniós ágazati jogszabályok[10], az uniós kibervédelmi politika[11], a kiberrezilienciáról szóló jogszabály[12] és a kiberszolidaritásról szóló jogszabály, amelynek javaslatát a Bizottság e közleménnyel együtt terjeszti elő. A végrehajtáshoz szükséges szakképzett emberek nélkül azonban ezek a jogszabályok nem érik el céljaikat. Míg a lakosság kiberbiztonsággal kapcsolatos alapvető ismereteivel a társadalmi részvételhez szükséges általános készségek fejlesztését támogató kezdeményezések részeként foglalkoznak[13], **a kiberbiztonságra vonatkozó jogi és szakpolitikai követelmények teljesítéséhez** mind a köz-, mind a magánszektorban, nemzeti és uniós szinten, beleértve a szabványügyi szervezeteket is, elengedhetetlen a hozzáértő munkaerő.

Az EU biztonsága és versenyképessége ezért attól függ, hogy van-e szakképzett kiberbiztonsági munkaerő. Az EU azonban jelentős hiányt szenved képzett kiberbiztonsági szakemberekből, ami az EU-t, tagállamait, vállalkozásait és polgárait kiberbiztonsági események kockázatának teszi ki. 2022-ben az Európai Unióban a kiberbiztonsági szakemberhiány **260 000**[14] **és 500 000 fő** között mozgott[15], míg az EU kiberbiztonsági munkaerőigényét 883 000 szakemberre[16] becsülték, ami arra utal, hogy a rendelkezésre álló és a munkaerőpiac által igényelt kompetenciák között nincs összhang. A kiberbiztonsági munkaerő továbbra is szenved a műszaki jellegével kapcsolatos tévhitektől, és továbbra sem vonzza a **nőket**, akik a kiberbiztonsági diplomások 20 %-át[17], valamint az információs és kommunikációs technológiai (IKT) szakemberek 19 %-át[18] teszik ki. Ennek megoldására az

[8] Közös közlemény az Európai Parlamentnek és a Tanácsnak, Az EU kiberbiztonsági stratégiája a digitális évtizedre, JOIN(2020) 18 final.

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

[10] Mint például, a pénzügyi ágazat esetében az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (DORA-rendelet).

[11] Közös közlemény az Európai Parlamentnek és a Tanácsnak az EU kibervédelmi politikájáról, JOIN(2022) 49 final.

[12] 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.

[13] A lakosság általános digitális készségeivel foglalkozó vonatkozó kezdeményezések közül: a lakosság 80 %-a 2030-ra érje el az alapvető digitális készségeket, ahogy ez célként szerepel a szociális jogok európai pillérének megvalósítására szolgáló cselekvési tervben és a digitális iránytűben, a 2021–2027. évi digitális oktatási cselekvési tervben, a digitális készségek kereteszközében vagy a digitális készségek oktatásban és képzésben való elsajátításának javításáról szóló tanácsi ajánlásra irányuló javaslatban.

[14] (ISC)²: A kiberkészségek értékelése az ECSF alapján, ENISA webinárium, 2023. február 16.

[15] Az Európai Kiberbiztonsági Szervezet (ECSO) szerint, amint az a következő dokumentumban is olvasható: Közös közlemény az Európai Parlamentnek és a Tanácsnak az EU kibervédelmi politikájáról, JOIN(2022) 49 final.

[16] (ISC)²: A kiberkészségek értékelése az ECSF alapján, ENISA webinárium, 2023. február 16.

[17] Kiberbiztonsági felsőoktatási adatbázis (CyberHEAD).

[18] Az EU-ban az IKT-szakemberek mindössze 19 %-a nő; A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI) 2022 | Európa digitális jövőjének megtervezése (europa.eu). Az Unió női kiberbiztonsági munkavállalóira vonatkozóan nem áll rendelkezésre számadat.

európai **Digitális évtized 2030 szakpolitikai program**[19] azt a célt tűzte ki, hogy 2030-ig 20 millióval növelje az IKT-szakemberek számát, és egyúttal elérje a nemek közötti konvergenciát. A kialakulóban lévő uniós szakpolitikák végrehajtásához továbbá megfelelően képzett és elegendő munkaerőre van szükség. A pénzügyi szolgáltatási ágazat vezető beosztású informatikai vezetőinek több mint 42 %-a például a kiberbiztonsági készségek és szakértelem hiányát jelölte meg a kiberbiztonsági védelem és eseménykezelés[20] terén a vállalkozásuk előtt álló legfontosabb kihívásként, miközben olyan ágazati kiberbiztonsági jogszabályokat kell végrehajtaniuk, mint a digitális működési rezilienciáról szóló rendelet (DORA).

Tovább szűkíti a munkaerőpiacot a munkaadók vonakodása a humán tőkébe való befektetéstől, mivel már képzett és tapasztalt munkaerőt keresnek[21]. Ez a hiány minden típusú vállalatot érint, beleértve a kis- és középvállalkozásokat (**kkv-kat**) is, amelyek az összes vállalkozás 99 %-át teszik ki az EU-ban[22]. A kihívás a **közigazgatás** számára is nagy, ezeket a leginkább érintett szerveket a kiberbiztonsági események nagymértékben sújtják[23].

Az EU kiberbiztonsági szakemberhiányának megszüntetése ezért sürgős feladat, mivel az EU biztonsága és versenyképessége forog kockán.

2. A kiberbiztonsági készséghiány megszüntetését célzó szinergiák és az összehangolt fellépés hiánya

Nagy számban vannak jelen az állami és magánszervezetek által indított, a kiberbiztonsági munkaerőpiaci hiány kezelésére irányuló európai és nemzeti szintű kezdeményezések. Ezek azonban szétszórtak, és eddig nem érték el a kritikus tömeget ahhoz, hogy valódi változást érjenek el.

Kezdjük azzal, hogy jelenleg csak korlátozottan van egységes kép az uniós kiberbiztonsági munkaerő összetételéről és a kapcsolódó készségekről, miközben a hasonló kiberbiztonsági munkaköri profiloknak ugyanazokat a készségeket kellene magukban foglalniuk. A **kiberbiztonsági szakemberek közös európai referenciakeretének** az érintett szereplők általi alacsony elfogadottsága azt eredményezi, hogy nem áll rendelkezésre kommunikációs eszköz a munkaadók, az oktatók és a politikai döntéshozók között, és képtelenek méréseket végezni, illetve felmérni a kiberbiztonsági munkaerőpiac hiányosságait. Ez akadályozza továbbá az oktatási és képzési tantervek kialakítását, valamint a szakpolitikák és a piac igényeinek megfelelő karrierutak létrehozását a szakmába belépni kívánók számára. A munkaerő **továbbképzése és szakmai átképzése** nagymértékben támaszkodik a kiberbiztonsági képzésekre és tanúsítványokra, amelyeket általában magánszolgáltatók kínálnak. A munkaerőnek azonban nehézséget okoz, hogy áttekintést kapjon a kínált kiberbiztonsági képzések és a kiadott tanúsítványok minőségéről.

Míg az oktatás és képzés, valamint a karrierutak kiépítése a munkaerőpiac kínálati oldalának javításához szükséges, a **keresleti oldal** szerepét a munkaerő képzésében és a munkaerő fejlődéséhez való alkalmazkodásban jelenleg alábecsülik. Az ipari és állami munkáltatóknak

[19] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata (2022. december 14.) a Digitális évtized 2030 szakpolitikai program létrehozásáról, amely nyomonkövetési és együttműködési mechanizmust hoz létre az európai digitális átalakulással kapcsolatos, a 2030-ig szóló digitális iránytűben meghatározott közös célkitűzések és célok elérése érdekében, beleértve a készségek területét is.

[20] S-RM Kiberbiztonsági betekintés jelentés, 2022.

[21] A kiberbiztonsági készségek fejlesztése az EU-ban, ENISA, 2019. december.

[22] Kkv fogalommeghatározás (europa.eu).

[23] ENISA: Fenyegetettségi helyzetjelentés, 2022 — ENISA (europa.eu).

nincsenek közös fórumai és helyei, ahol összegyűjthetnék az ötleteket a munkaerő legjobb képzésével és a **készségek jobb értékelésével** kapcsolatban, különösen a munkaerő-felvételi folyamat során. A legkeresettebb **kemény készségek** a kiberbiztonsághoz[24] kapcsolódhatnak, mint például a szoftverfejlesztés vagy a felhőalapú számítástechnika[25], de a **transzverzális készségeket** még mindig indokolatlanul figyelmen kívül hagyják. A kritikus gondolkodás és elemzés, a problémamegoldás és az önmenedzselés olyan készségcsoportok, amelyekre a munkáltatók nagyobb igényt tartanak[26], és amelyek 2025-ig egyre inkább előtérbe kerülnek[27].

A kiberbiztonsági készségek terén már számos köz- és magánbefektetési kezdeményezés létezik, az EU pedig széles körben **finanszírozza** a projekteket különböző eszközök keretében[28]. A készségek folyamatos hiánya az EU-ban azonban kérdéseket vet fel ezek láthatóságát és hatását illetően, és azt sugallja, hogy ezek nem feltétlenül felelnek meg a piaci igényeknek, amelyeket uniós szinten sürgősen fel kell térképezni. Ezenfelül a többféle finanszírozási forrás párhuzamossághoz vezet, így elmulasztva a kapacitásbővítés és a valódi hatás elérésének lehetőségét. Ráadásul azok, akiknek szükségük van a beruházásra, nem mindig tudják azonosítani az igényeiknek leginkább megfelelő forrásokat.

Az **érdekeltek** megpróbálták kezelni a kiberbiztonsági készségek hiányának összetett és sokrétű problémáját. Az EU Kiberbiztonsági Ügynöksége (a továbbiakban: ENISA) a szerepkörökhöz vagy a felsőoktatáshoz kapcsolódó eszközöket fejlesztett ki[29], az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC)[30] egy külön munkacsoportban foglalkozik a kiberbiztonsági készségekkel, az Európai Biztonsági és Védelmi Főiskola (a továbbiakban: EBVF) a közös biztonság- és védelempolitika keretében a polgári és katonai munkaerő kiberbiztonsági készségeivel foglalkozik[31], magánszervezetek próbálják kezelni a kérdést[32], a kiberbiztonsági tanúsítási ágazat pedig a készséghiányt célzó ütemtervet és képzéseket dolgoz ki[33]. A tagállamok is különböző kezdeményezésekkel próbálják kezelni a kérdést, a szabályozástól[34] kezdve a kiberkészségek akadémiái[35] vagy kiberkampuszok[36], kiberbűnözéssel foglalkozó kiválósági központok[37] létrehozásáig, illetve a köz- és magánszféra közötti partnerségek[38] révén. Mindezen érdekeltek munkája azonban gyakran nem eléggé összehangolt és szinergiamentes, és nem érte el a potenciális hatását, ami jelentős változást hozhatott volna a munkaerőpiacon,

[24] LinkedIn: A legkeresettebb készségek: Sajátítsa el a vállalatoknak leginkább szükséges készségeket, 2023.

[25] ISACA: A kiberbiztonság helyzete, 2022 infografika.

[26] Mint például a CEDEFOP eszköze: Online álláshely-elemző eszköz Európa számára CEDEFOP (europa.eu).

[27] A munkahelyek jövője jelentés, 2020. október, Világgazdasági Fórum.

[28] Például: Kiberbiztonsági készségek szövetsége – Új jövőkép Európa számára – REWIRE projekt (az Erasmus+ program finanszírozásával); a Kiberbiztonsági Kompetencia Központot támogató projektek (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (a Horizont 2020 program finanszírozásával), Cybersecpro project (a Digitális Európa program támogatásával).

[29] Nevezetesen: az Európai kiberbiztonsági készségkeret (ECSF); a CYBERHEAD – Kiberbiztonsági felsőoktatási adatbázis; a Kibergyakorlat Platform (CEP); az Európai kiberbiztonsági kihívás; az Európai kiberbiztonsági hónap.

[30] Az Európai Parlament és a Tanács (EU) 2021/887 rendelete (2021. május 20.) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetencia Központ és a Nemzeti Koordinációs Központok Hálózatának létrehozásáról.

[31] Nevezetesen a Kibervédelmi oktatási, képzési, gyakorlási és értékelési platform (ETEE).

[32] Például az Európai Kiberbiztonsági Szervezet (ECSO) 5. munkacsoportja: „Oktatás, képzés, tudatosság, kiberbiztonsági gyakorlóterek, emberi tényezők”; A DIGITALEUROPE szervezet.

[33] Például a SANS Intézet, (ISC)², ISACA.

[34] Például az oktatásra vagy a kiberbiztonságra vonatkozó nemzeti stratégiákban.

[35] Például a C-Academy Portugáliában.

[36] Például a Kiberkampuszok Franciaországban.

[37] Például a Litvániai kiberbűnözés elleni kiválósági központ a képzés, kutatás és oktatás területén Litvániában (L3CE).

[38] Például a Microsoft kiberbiztonsági szakképzési kezdeményezése.

amint azt a kiberbiztonsági munkaerő növekvő hiánya mutatja az EU-ban. A kiberközösségek közötti szinergiák fokozására is szükség van, mivel a kiberbiztonság fenntartásához, a **számítógépes bűnözés** elleni küzdelemhez vagy a **kibervédelmi** válaszok kialakításához szükséges készségek gyakran hasonló jellegűek.

Végezetül, az EU-nak ma korlátozott eszközei vannak a **kiberbiztonsági munkaerőpiac** és a munkaerő készségei **állapotának és fejlődésének értékelésére**. A tagállamok és az Unió intézményei, szervei és hivatalai vagy a magánszervezetek által gyűjtött adatokra, vagy az EU által gyűjtött szélesebb körű adatokra támaszkodnak, amelyeket az Eurostat[39] és az Európai Szakképzésfejlesztési Központ (CEDEFOP)[40] gyűjt az IKT-szakemberekről. Más szóval az EU részleges és széttagolt képpel rendelkezik a szükségletekről, ami megakadályozza, hogy a kiberbiztonsági munkaerőpiac helyzetéről egységes képet alkosson.

3. Az egész EU-ra kiterjedő összehangolt válasz: a Kiberkészségek Akadémiája

3.1.A célkitűzés

A kiberbiztonsági készségek kezelésével és a munkaerőpiaci szakadék megszüntetésével kapcsolatos kihívás megoldása érdekében a Bizottság javaslatot tesz a **Kiberkészségek Akadémiájára**, amint azt a Bizottság elnöke az Unió helyzetét értékelő 2022. évi szándéknyilatkozatában[41, , 42], és a készségek európai éve keretében bejelentette.

A Kiberkészségek Akadémiája (röviden: az Akadémia) célja, hogy egy **egyablakos ügyintézési pontot és szinergiákat** hozzon létre a kiberbiztonsági oktatási és képzési ajánlatok, valamint a finanszírozási lehetőségek és a kiberbiztonsági készségek fejlesztését támogató különleges intézkedések számára. Az Akadémia az érdekelt felek kezdeményezéseit fogja bővíteni, hogy elérje azt a kritikus tömeget, amely változást hoz a munkaerőpiacon, többek között a védelmi ágazatban is. Ezek a tevékenységek közös célok és kulcsfontosságú teljesítménymutatók mentén igazodnának egymáshoz a nagyobb hatás elérése érdekében.

Az Akadémia középpontjában a **kiberbiztonsági szakemberek** képzése áll majd. Az Akadémia tevékenységei a kiberbiztonsággal kapcsolatos uniós szakpolitikákba, valamint az oktatásba és az egész életen át tartó tanulásba is beépülnek. Az Akadémia kiegészíti a digitális oktatással és készségekkel kapcsolatos két tanácsi ajánlást, amelyeket a Bizottság e közleménnyel egy időben javasolt[43].

Az Akadémia négy pillérre fog támaszkodni: 1. az **oktatás és képzés révén történő tudásgenerálás** elősegítése a kiberbiztonsági szerepkörök és a kapcsolódó készségek közös keretrendszerének kidolgozásával, az európai oktatási és képzési kínálat igényeknek megfelelő bővítése, a karrierútvonalak kiépítése, valamint a kiberbiztonsági képzések és tanúsítványok láthatóságának és egyértelműségének biztosítása a munkaerő-kínálat javítása érdekében, 2. a készségekkel kapcsolatos tevékenységekre rendelkezésre álló **finanszírozási lehetőségek** jobb csatornázásának és láthatóságának biztosítása a hatásuk maximalizálása érdekében, 3. az érdekeltek **cselekvésre** való felhívása, valamint 4. mutatók meghatározása **a**

[39] IKT-szakemberek foglalkoztatása – Statisztikák magyarázata (europa.eu).

[40] Mint például a CEDEFOP eszköze: Online álláshely-elemző eszköz Európa számára CEDEFOP (europa.eu).

[41] Az Unió helyzetét értékelő, Roberta Metsola elnökhöz és Petr Fiala miniszterelnökhöz intézett 2022. évi szándéknyilatkozat.

[42] Közös közlemény az Európai Parlamentnek és a Tanácsnak az EU kibervédelmi politikájáról, JOIN(2022) 49 final.

[43] Javaslatok a sikeres digitális oktatás és képzés kulcsfontosságú tényezőiről, valamint a digitális készségek oktatásban és képzésben való elsajátításának javításáról szóló tanácsi ajánlásokra.

piac alakulásának nyomon követése érdekében, és hogy képesek legyenek felmérni intézkedéseik hatékonyságát.

Az Akadémia megvalósítását a Digitális Európa program 10 millió EUR-s finanszírozása támogatja[44].

3.2.Az Akadémia irányítása

Végső soron az Akadémia egy **európai digitális infrastruktúra-konzorcium (EDIC)**[45] formáját ölthetné annak érdekében, hogy olyan infrastruktúrát biztosítson, amely **egyetlen belépési pontként** szolgál az akadémiai szféra, a képzési szolgáltatók és az ipar közötti együttműködés előmozdítására, ahol az uniós kiberbiztonsági ökoszisztéma keresleti és kínálati oldala találkozhatna és képzést kaphatna. Ez az eszköz lehetővé tenné a tagállamok számára, hogy közösen dolgozzanak a kiberbiztonsági készséghiány megszüntetésén, valamint hogy megbízatásukkal és hatáskörükkel összhangban szorosan együttműködjenek a Bizottsággal, az ENISA-val és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközponttal (ECCC), és hogy valamennyi érintett érdekelt felet bevonják, de az európai, nemzeti és magánbefektetéseket is egy közös cél felé irányítsák. E célból az érdekelt tagállamokat arra ösztönzik, hogy 2023. május 30-ig nyújtsanak be előzetes bejelentést a Bizottságnak egy ilyen EDIC létrehozására irányuló jövőbeli kérelmükről. Ez az önkéntes előzetes bejelentés lehetővé tenné a Bizottság számára, hogy korai észrevételeket tegyen az EDIC-kérelem tervezetével kapcsolatban, lehetővé téve ezáltal annak gyorsabb továbbfejlesztését és hivatalos benyújtását. A teljes folyamat során és a tagállamok által kért mértékben a Bizottság, több országot érintő projektgyorsítóként eljárva, megkönnyíti az EDIC-kérelem elkészítését. Ezután a Bizottság a kérelem Bizottság általi pozitív elbírálását és a Digitális Évtized Programbizottság általi jóváhagyását követően határozatot hoz az EDIC létrehozásáról, és ezt követően segít koordinálni az EDIC megvalósítását[46].

Addig is, amíg az EDIC hivatalos felállítása folyamatban van, a Bizottság az európai kiberbiztonsági közösségi támogatási projekt (ECCO) támogatásával a Bizottság **digitális készségekkel és munkahelyekkel foglalkozó platformjának**[47] fejlesztésével virtuális egyablakos ügyintézési pontot hoz létre[48].

Az **ENISA** az ügynökség célkitűzéseivel[49] összhangban hozzájárul az Akadémia megvalósításához, különösen a kiberbiztonsági oktatás és képzés terén nyújtott segítség tekintetében, és figyelembe véve a NIS 2 irányelv[50] szerinti jelentéstételi kötelezettségeit. Az **ECCC** a stratégiai menetrendjével összhangban fog dolgozni a Kiberkészségek Akadémiája

---

[44] Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről.

[45] Az EDIC-eket a Digitális évtized 2030 szakpolitikai program létrehozásáról szóló 2022. december 14-i európai parlament és a tanácsi (EU) 2022/2481 határozat 13. és azt követő cikkei hozták létre.

[46] Uo., 12. cikk.

[47] Nyitólap | Digitális készségekkel és munkahelyekkel foglalkozó platform (europa.eu).

[48] Lásd Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont: új, uniós finanszírozású projekt a kiberközösség támogatására (europa.eu). 2022 decemberében az Európai Bizottság 3 millió EUR-s szerződést írt alá az EU kiberközösségének támogatására az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont keretében. Ez a projekt hozzájárul az EU közösség- és kapacitásépítési céljaihoz a kiberbiztonsági kutatás, az innováció, az elterjedés és az ipari bázis tekintetében.

[49] „Az ENISA támogatja a kapacitásépítést és a felkészültséget az egész Unióban azáltal, hogy segítséget nyújt az Unió intézményei, szervei és hivatalai valamint a tagállamok és a köz- és magánszféra érdekelt felei számára […] a kiberbiztonság területén a készségek és kompetenciák fejlesztéséhez.” A kiberbiztonsági jogszabály 4. cikkének (3) bekezdése.

[50] A NIS 2 irányelv 18. cikke.

megvalósításának támogatása érdekében. Az ECCC különösen a Digitális Európa program 3. stratégiai célkitűzését (Kiberbiztonság) fogja végrehajtani. A **nemzeti koordinációs központokon (a továbbiakban: NCC-k)** keresztül a Bizottság és a tagállamok támogatását fogja élvezni. Adott esetben a NIS 2 irányelv[51] alapján létrehozott **együttműködési csoportot** is megkeresik. Végezetül pedig az **iparral** és a **tudományos körökkel** való összefogásra lesz szükség ahhoz, hogy az Akadémia elérje a kiberbiztonsági készségekben mutatkozó hiány megszüntetésére irányuló célját.

4. Tudásgenerálás és képzés: közös uniós megközelítés kialakítása a kiberbiztonsági képzésre vonatkozóan

A Kiberkészségek Akadémiája tudásgenerálási és képzési pillérének keretében strukturált megközelítést dolgoznak ki azzal az egyértelmű céllal, hogy növeljék a kiberbiztonsági készségekkel rendelkezők **számát** az EU-ban, a képzéseket jobban a **piaci igényekhez** igazítsák, és átláthatóbbá tegyék a **karrierutakat**.

4.1. Egy nyelvet beszélünk: közös megközelítés a kiberbiztonsági szerepkörök és a kapcsolódó készségek tekintetében

Az ENISA már megkezdte a munkát a kiberbiztonsági szakemberek szerepprofiljainak meghatározására az európai kiberkészség-kompetenciakeret **(a továbbiakban: ECSF)**[52] keretében. Ennek kell alapul szolgálnia az Akadémia számára a vonatkozó készségek meghatározásához és értékeléséhez, a készséghiányok alakulásának nyomon követéséhez és az új igényekre vonatkozó jelzésekhez. Az ECSF egyes kiberbiztonsági szerepköreihez egy sor alkalmazandó európai e-kompetencia keretrendszer[53] beépül a profilleírás elemeként[54].

Az ENISA ezért felül fogja vizsgálni az ECSF-et, és **azonosítani fogja** a kiberbiztonsági munkaerővel kapcsolatos **változó készségigényeket és hiányosságokat**, többek között fejlett eszközök (pl. mesterséges intelligencia, big data[55], adatbányászat) révén. E célból az ENISA feladatait a létrehozandó EDIC irányítása alatt fogja ellátni, az ECCC-vel, a nemzeti együttműködési központokkal, a Bizottsággal, az ECCO-projekttel és a piaci szereplőkkel együtt[56]. A kibervédelmi munkaerő tekintetében az ENISA kellően figyelembe veszi az EBVF által végzett munkát. Hasonlóképpen, a számítógépes bűnözés elleni küzdelem területén az ENISA figyelembe fogja venni az Európai Unió Bűnüldözési Képzési Ügynöksége (a továbbiakban: CEPOL) és az Europol által végzett tevékenységeket a kibertámadásokkal kapcsolatos operatív képzési szükségletelemzés[57] kidolgozása során.

---

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

[52] Európai kiberbiztonsági készségkeret (ECSF) – ENISA (europa.eu). Az ECSF támogatja az európai kiberbiztonsági szakemberek szerepéhez kapcsolódó feladatok, kompetenciák, készségek és ismeretek meghatározását és artikulálását. Az összes kiberbiztonsággal kapcsolatos szerepkört profilokba foglalja össze, amelyeket külön-külön elemez a megfelelő felelősségi körök, készségek, szinergiák és kölcsönös függőségek részleteire kitérve.

[53] Európai e-kompetencia keretrendszer (e-CF) | Esco (europa.eu). Az e-CF következetes kapcsolatokat biztosít az IKT-képesítések és más, az ágazat szempontjából releváns keretrendszerek, így a DigComp között.

[54] Lásd e tekintetben: Felhasználói kézikönyv – Európai kiberbiztonsági készségkeret (ECSF) – 2022. szeptember.

[55] Lásd például a Cedefop által létrehozott Online álláshely-elemző eszközt Európa számára.

[56] Az ügynökség tovább fogja hasznosítani az egyéb uniós finanszírozású projektek eredményeit (pl. REWIRE, közös európai készségadattér (DS4S), CyberSecPro, Concordia) és a hasonló kezdeményezésekből származó módszertanokat (pl. „Képzett kiberbiztonsági munkaerő kiépítése öt országban: Meglátások Ausztráliából, Kanadából, Új-Zélandról, az Egyesült Királyságból és az Egyesült Államokból”, OECD-jelentés, amelyet 2023. március 21-én mutattak be), hogy a jövőben naprakész képet kapjunk a szükségletekről egy olyan környezetben, ahol a kereslet folyamatosan változik.

[57] CEPOL: Az operatív képzési szükségletek felmérése (OTNA).

Az ECSF-et az Akadémia keretében kétéves időközönként rendszeresen kiegészítik és felülvizsgálják. Ezen túlmenően a Bizottság és az Európai Külügyi Szolgálat – az uniós ügynökségek és szervek, például az EBVF[58], az Europol és a CEPOL[59] támogatásával – szükség szerint hozzájárul az egyes ágazatokra vonatkozó speciális profilok és kapcsolódó készségek meghatározásához.

Az ECSF és az EU foglalkoztatáspolitikájának vonatkozó eszközei között is kapcsolatokat fognak teremteni[60]. Különösen az ECSF munkaköri profiljait és a kapcsolódó készségeket fogják integrálni az **ESCO osztályozásba**. Ez javítani fogja a kiberbiztonság területén a foglalkozások és készségek osztályozását és a köztük lévő kapcsolatokat, megkönnyítve az egyének számára a tovább- és átképzést, valamint támogatva a készségalapú munkaközvetítést és a határokon átnyúló mobilitást.

4.2.Együttműködés elősegítése a kiberbiztonsági oktatás és képzés tanterveinek kialakítása érdekében

Az EDIC létrehozatalát követően az Akadémiának támogatást kell kapnia a tagállamoktól, hogy Európában a legkeresettebb készségekkel foglalkozó **kiberbiztonsági képzések megtervezésének és megvalósításának referenciahelyévé** váljon, és munkahelyi képzéseket és gyakornoki lehetőségeket biztosítson az induló vállalkozások és kkv-k, valamint a közigazgatás számára a kiberbiztonság és a kiberbiztonsági kompetenciaközpontok területén működő innovatív vállalatokban. Az EDIC-nek együtt kell működnie az összes érintett érdekelt féllel, beleértve az ipart is, az ilyen képzések megtervezése érdekében, és olyan projektekre kell építenie, mint például a Digitális Európa program által finanszírozott **CyberSecPro**[61], amely 16 tagállam 17 felsőoktatási intézményét és 13 biztonsági vállalatot tömörít annak érdekében, hogy az összes kiberbiztonsági képzési program legjobb gyakorlatává váljon.

Az Akadémia együttműködik az összes érdekelt féllel annak érdekében, hogy a **fiatal generációkat a kiberbiztonsági pályára vonzza**. A digitális készségek oktatásban és képzésben való elsajátításának javításáról szóló tanácsi ajánlásra irányuló javaslattal összhangban a tagállamoknak intézkedéseket kell létrehozniuk és megerősíteniük a szakosodott tanárok és oktatók felvételére és képzésére, valamint a kiberbiztonsági készségek megszerzésének megkönnyítésére, többek között szakmai gyakorlatok révén. Ösztönözni kell a kiberbiztonság integrálását az oktatási és képzési programokba, biztosítva ugyanakkor azok hozzáférhetőségét, a **tanulószerződéses gyakorlati képzések** és a szakmai gyakorlatok kínálatának fejlesztését, az innovatív megközelítések, köztük például a komoly játékok és a közös szimulációs platformok támogatását, a kiberbiztonsági pozíciókba való elmélyülést biztosító hetek szervezését, a nem műszaki jellegű szerepprofilok ismertetését. Támogatni kell a nehezen elérhető csoportok, például a fogyatékkal élő, a távoli vagy vidéki területeken

[58] Lásd e tekintetben: Közös közlemény az Európai Parlamentnek és a Tanácsnak az EU kibervédelmi politikájáról, JOIN(2022) 49 final.

[59] E tekintetben figyelmet kell fordítani a jelenleg kidolgozás alatt álló, a számítógépes bűnözés elleni képzési kompetenciakeretre (TCF) irányuló munkára.

[60] Mint például a készségek, kompetenciák, képesítések és foglalkozások európai osztályozása (ESCO), az Europass, a foglalkoztatási szolgálatok európai hálózata (EURES).

[61] A CyberSecPro például elemezni fogja az egyetemeken kínált kiberbiztonsági programokat, kurzusokat és nyári egyetemeket, valamint az alkalmazott európai kreditátviteli és -gyűjtési rendszer (ECTS) besorolási táblázatait, biztosítani fogja a 3 éves időszak alatt megcélzott több mint 530 gyakornok bevonását, külsősöket fog képezni különböző iparágakból és ágazatokból.

élő, illetve más kisebbségi csoportokhoz tartozó fiatalok részvételét ezekben a kiberbiztonsági tanulási lehetőségekben.

A Bizottság továbbra is támogatja a mikrotanúsítványok, a szakképzési programok fejlesztését. Az Erasmus+ keretében továbbra is finanszírozni fogják különösen a **közös alap- és mesterképzési programokat, a mikrotanúsítványokhoz vezető közös kurzusokat vagy modulokat**, valamint az összes témában – többek között **a kiberbiztonság területén – a vegyes intenzív programokat**[62]. Az **„Európai Egyetemek" kezdeményezés**[63] és a **szakképzési kiválósági központok**[64] további elterjedését is támogatni fogják, hogy Európa-szerte ösztönözzék a felsőoktatás és az érintett szakoktatási és szakképzési intézmények közötti szorosabb együttműködést. Az uniós finanszírozási programok, köztük az Erasmus+ és a Digitális Európa program, támogatni fogják ezt a mélyebb együttműködésre irányuló célt, csakúgy, mint az **egyéni tanulási számlák**[65] fejlesztésére szánt uniós források.

A nemzeti szintű együttműködés megkönnyítése érdekében a tudományos körök és a kiberbiztonsági készségekkel kapcsolatos képzések szolgáltatói, valamint a magán- és közszektor munkaadói között, továbbá a köz- és magánszektor közötti szinergiák előmozdítása érdekében a nemzeti együttműködési központok felkérést kapnak arra, hogy vizsgálják meg a **kiberkampuszok** létrehozásának lehetőségét a tagállamokban. A kiberkampuszok célja az lenne, hogy nemzeti szinten kiválósági központokat biztosítsanak a kiberbiztonsági közösség számára, az Akadémia pedig segítené a hálózatépítést és tevékenységeik további összehangolását.

Az ENISA emellett továbbfejleszti kiberbiztonsági képzési kínálatát, összehangolva **tanfolyami katalógusát**[66] az ECSF profiljaival, és képzési modulokat dolgoz ki profilonként, ami javíthatja a tagállamok képzési kínálatát. Az ENISA bővíteni fogja az **„oktatók képzésére" irányuló programját**[67] is, amely az Unió intézményei, szervei és hivatalai, valamint a tagállamok hatóságainak és a NIS 2 irányelv hatálya alá tartozó **legfontosabb köz- és magánvállalkozások** szakmai igényeit célozza meg.

Emellett más uniós ügynökségek és szervek is megerősítik a kiberbiztonsági képzési kínálatukat. Az EU kibervédelmi politikájának végrehajtása során például az **EBVF** új kiberbiztonsági tanfolyamokat fog kidolgozni, és a jelenlegi tanfolyamai közül néhányat összehangol az ECSF-fel. Ezek a tanfolyamok a tanulási eredmények tanúsításához vezetnek majd[68]. Az EBVF a Bizottsággal együttműködve meg fogja vizsgálni annak lehetőségét, hogy a tanúsítványokat beépítsék az EUeID-tárcába. Az EBVF tovább vizsgálja a készségértékelési mechanizmusok lehetőségeit, amelyek alapján a tanúsítványokat ki fogják állítani. Hasonlóképpen, a számítógépes bűnözés elleni küzdelem területén a **CEPOL Kiberbűnözés elleni akadémiájával**[69] való szoros kapcsolatra törekszenek a szinergiák és a

[62] A kevert intenzív programok az online oktatást rövid ideig tartó fizikai mobilitással kombinálják.

[63] „Európai Egyetemek" kezdeményezés | Európai oktatási térség (europa.eu).

[64] Szakképzési kiválósági központok | Erasmus+ (europa.eu).

[65] Összhangban az egyéni tanulási számlákról szóló 2022. június 16-i tanácsi ajánlással.

[66] Képzési tanfolyamok – ENISA (europa.eu).

[67] Az oktatók képzése program – ENISA (europa.eu).

[68] Összhangban az Európai Biztonsági és Védelmi Főiskola létrehozásáról, valamint a (KKBP) 2016/2382 határozat hatályon kívül helyezéséről szóló 2020. október 19-i (KKBP) 2020/1515 tanácsi határozat 20. cikkének (4) bekezdésével.

[69] A CEPOL Kiberbűnözés elleni Akadémiáját 2019-ben hozták létre azzal a céllal, hogy korszerű platformot biztosítson a kiberbűnözéssel kapcsolatos ismeretek és az európai kiberkapacitások fejlesztéséhez.

kiegészítő jelleg előmozdítása érdekében a képzési tantervek kialakítása és végrehajtása során.

4.3.Szinergiák létrehozása és a kiberbiztonsági képzések és tanúsítások láthatóságának biztosítása a tagállamokban

Az Akadémiának foglalkoznia kell a képzések és tanúsítások láthatóságának és szinergiáinak kérdésével. Ez előnyös lenne a polgári, a védelmi, a bűnüldözési és a diplomáciai kiberközösségek számára, mivel valamennyi ágazatnak sok esetben ugyanarra a szakértelemre van szüksége, amely hasonló tanterveken és tanulási eredményeken alapul.

Az Akadémia **egyablakos ügyintézési pontot** biztosítana a kiberbiztonsági karrier iránt érdeklődők számára. Rövid távon ez a Bizottság **digitális készségekkel és munkahelyekkel foglalkozó platformjának** az ECCO-projekt támogatásával történő továbbfejlesztésével valósul meg. A kiberbiztonsági pályáknak szentelt külön rész összekapcsolódik a meglévő eszközökkel, a felsőoktatási programoktól a képzési lehetőségeken át – beleértve a mikrotanúsítványokhoz vezető tanfolyamokat és a szakképzési programokat – az állásajánlatokig. Ezt úgy érik el, hogy hivatkoznak a folyamatban lévő olyan munkákra és kezdeményezésekre – illetve integrálják azokat a platformba –, mint például az ENISA, amely az akadémiai szférával együttműködve létrehozta a kiberbiztonsági programokat nyújtó **oktatási intézmények térképét**. Ezt az NCC-k támogatásával továbbfejlesztik. Ezenkívül az ENISA a nemzeti együttműködési központok, a Bizottság és az ECCO-projekt támogatásával, valamint a tanúsítványokat kiállító szervezetekkel együttműködve és más vonatkozó kezdeményezésekre támaszkodva két, **az állami és a magánszektorban már létező képzések és kiberbiztonsági tanúsítványok gyűjteményét** fogja kialakítani és konszolidálni[70]. Ezeket a digitális készségek és munkahelyek platformjának egyablakos ügyintézési pontjába is integrálják. Ez a munka az NCC-knek is hasznára válik, amelyek feladata különösen a kiberbiztonsági oktatási programok népszerűsítése és terjesztése[71].

Biztosítékokat kell nyújtani a szakemberek számára arra vonatkozóan is, hogy az általuk elvégzett képzések megfelelő minőségűek legyenek. E tekintetben az ENISA egy **kísérleti projektet** fog kidolgozni, amely a kiberbiztonsági készségek európai tanúsítási rendszerének létrehozását vizsgálja.

Ezen túlmenően a készségek és képzések azonosítása és a munkaköri profilhoz való társítása alapvető fontosságú, de fontos annak biztosítása is, hogy a kiberbiztonsági szolgáltatásokat a szükséges kompetenciával, szakértelemmel és tapasztalattal nyújtsák. Ez különösen igaz az olyan területeken működő irányított biztonsági szolgáltatókra, mint a kiberbiztonsági eseményekre való reagálás, a behatolástesztelés, a biztonsági auditok és a tanácsadás. A NIS 2 irányelv és a kiberszolidaritásról szóló jogszabály javaslata konkrét feladatokat határoz meg az ilyen irányított biztonsági szolgáltatók számára. A Bizottság ezért a **kiberbiztonsági jogszabály**[72] **célzott módosítását** is javasolja, hogy uniós szinten lehetővé tegye az irányított biztonsági szolgáltatások tanúsítási rendszereit. Az ilyen tanúsítási rendszerek célja többek

[70] Például a W4C Akadémia – Women4Cyber vagy a Globális kiberbűnözés elleni tanúsítási projekt a bűnüldözési és igazságügyi hatóságok számára.

[71] „1. A nemzeti koordinációs központok az alábbi feladatokat látják el: […] g) a tagállamok oktatási hatáskörének sérelme nélkül és az ENISA vonatkozó feladatainak figyelembevételével a nemzeti hatóságokkal való együttműködés a kiberbiztonsági oktatási programok előmozdításához és terjesztéséhez való lehetséges hozzájárulás tekintetében”, az ECCC-rendelet 7. cikke (1) bekezdésének g) pontja. Lásd még a kapcsolódó (28) preambulumbekezdést.

[72] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály).

között annak biztosítása, hogy ezeket a szolgáltatásokat az érintett területeken igen magas szintű műszaki ismeretekkel és szakértelemmel rendelkező személyzet nyújtsa.

A mikrotanúsítványok minőségbiztosítási és elismerési mechanizmusai[73] megkönnyítik a tanulási eredmények átláthatóságát, összehasonlíthatóságát és hordozhatóságát. A mikrotanúsítványok európai megközelítéséről szóló tanácsi ajánlással összhangban[74] a tagállamokat arra ösztönzik, hogy a kiberbiztonsági mikrotanúsítványokat is foglalják bele nemzeti képesítési keretrendszerükbe. Ez lehetővé tenné számukra, hogy a kiberbiztonsági mikrotanúsítványokat az európai képesítési keretrendszerhez kapcsolják[75]. Az Európai Digitális Tanulási Oklevelek infrastruktúrája rendelkezésre áll a digitálisan aláírt kiberbiztonsági képesítések és az egyének mikrotanúsítványainak kiadásához. Ezek számos adatot tartalmaznak többek között a kiberbiztonsági tanulási eredményekről, és a jövőbeni **EUeID digitális tárcában**[76] tárolhatók.

Az Akadémia keretében végzett tevékenységek

A Tagállamok és az ágazat

- A kiberbiztonsági tanulási **mikrotanúsítványok** fejlesztése és elismerése támogatásának biztosítása, a mikrotanúsítványok európai megközelítéséről szóló tanácsi ajánlással összhangban.
- A kiberbiztonsági képesítések, köztük a mikrotanúsítványok felvétele a **nemzeti képesítési keretrendszerekbe.**
- **Munkahelyi tanulási lehetőségek** biztosítása a kiberbiztonsági készségfejlesztési kezdeményezésekben részt vevő személyek számára tanulószerződéses gyakorlati képzésen keresztül.

Bizottság

- Rövid távon, 2023 végéig a **digitális készségek és munkahelyek platformján** keresztül hozzon létre **egy egyablakos ügyintézési pontot** a kiberbiztonsági programok, a meglévő képzések és a kiberbiztonsági tanúsítványok számára.
- Tegyen javaslatot a **kiberbiztonsági jogszabály** módosítására, hogy 2023. április 18-án lehetővé váljon az irányított biztonsági szolgáltatók tanúsítása.

Uniós szervek és ügynökségek

- A kiberbiztonsági szerepkörök és a kapcsolódó készségek közös megközelítéseként 2023 végéig hozzák létre az **ECSF**-et.
- Az ENISA kezdeményezi egy kísérleti projekt kidolgozását, amely 2023 második negyedévében létrehozza a kiberbiztonsági készségek **európai tanúsítási rendszerét**.
- Az ENISA felülvizsgálja **kurzuskatalógusát**, és 2023 végéig megnyitja a **„képzők képzése" programot** az alapvető fontosságú állami és magánszereplők számára.

[73] Például a kisebb képzések után megszerzett tanulási eredményekről szóló nyilvántartás vagy tanúsítványok.

[74] A Tanács ajánlása az egész életen át tartó tanulást és a foglalkoztathatóságot célzó mikrotanúsítványok európai megközelítéséről.

[75] A Tanács 2017. május 22-i ajánlása az egész életen át tartó tanulás európai képesítési keretrendszeréről, valamint az egész életen át tartó tanulás európai képesítési keretrendszerének létrehozásáról szóló, 2008. április 23-i európai parlamenti és tanácsi ajánlás hatályon kívül helyezéséről.

[76] A 910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat.

- Fejezze be az **EBVF tantervei ECSF-hez való igazítását** 2023 közepéig.

5. Az érdekelt felek bevonása: kötelezettségvállalás a kiberbiztonsági készséghiány megszüntetésére

Az Akadémia keretében összehangolt megközelítést dolgoznak ki az érdekelt felek bevonására a kiberbiztonsági készséghiány megszüntetése érdekében. A cél az lesz, hogy maximalizálják a különböző érdekelt felek kiberbiztonsági készséghiány csökkentésére irányuló kötelezettségvállalásainak láthatóságát és hatását.

A Bizottság felszólítja az érdekelt feleket, hogy tegyenek olyan konkrét kötelezettségvállalásokat, amelyek a munkavállalók képzettségének célzott fellépések révén történő növelésére és átképzésére irányulnak, a lehető legnagyobb mértékben építve az azonosított kiberbiztonsági készséghiányra. Az **érdekelt felek ilyen kiberbiztonsági kötelezettségvállalásait** a **digitális készségek és munkahelyek platformján** kell jelenteni, hasonlóan a platformon már látható egyéb digitális kötelezettségvállalásokhoz. A Bizottság továbbá arra ösztönzi a platformon kiberbiztonsági kötelezettségvállalást tevő érdekelt feleket, hogy csatlakozzanak **digitális széles körű partnerséghez a készségfejlesztési paktum keretében**[77]. A digitális széles körű partnerség keretében tett kiberbiztonsági kötelezettségvállalásokat a digitális készségek és munkahelyek platformján javasolt benyújtani. Hasonlóképpen, a digitális készségek és munkahelyek platform keretében tett kötelezettségvállalásokat a készségfejlesztési paktum digitális széles körű partnerségének keretében is javasolt bejelenteni.

A Bizottság továbbá felszólítja a tagállamokat, hogy **folytassák a „Nők a digitális világban” nyilatkozat**[78] **végrehajtására irányuló erőfeszítéseket**, hogy ösztönözzék a nőket arra, hogy aktív és kiemelkedő szerepet játsszanak a digitális technológiai ágazatban, és érjék el a nemek közötti konvergenciát a kiberbiztonsági pozíciókban. A Bizottság arra is ösztönzi a tagállamokat, hogy alakítsanak ki szinergiákat az **Európai Szociális Alap+** (ESZA+) programjaikkal, hogy tovább támogassák a nemek közötti egyenlőség célkitűzését a munkaerőpiaci részvétel terén[79], például a **lányok és nők számára mentorprogramok** létrehozásával. Ezek elősegíthetik a példaképek kialakítását, hogy a lányok számára vonzóvá váljanak a kiberbiztonsági szakmák, küzdve egyúttal a nemekkel kapcsolatos sztereotípiák ellen. Emellett ösztönzi a nők tovább- és átképzését, és elősegíti egy olyan közösség kialakulását, amely támogathatja a nőket a kiberbiztonsági munkaerőpiacra való belépésükben vagy előmenetelükben.

A tagállamoknak **nemzeti kiberbiztonsági stratégiáik részeként konkrét intézkedéseket kell elfogadniuk a kiberbiztonsági készséghiány enyhítése**[80], a készséghiány megszüntetésére irányuló erőfeszítések azonosítása és jobb irányítása, valamint végső soron a NIS 2 irányelv szerinti kötelezettségeik megfelelő végrehajtásának biztosítása érdekében.

---

[77] Új európai partnerségek indultak az EU digitális évtizedre vonatkozó célkitűzéseinek megvalósítása érdekében | Európa digitális jövőjének megtervezése (europa.eu), a készségfejlesztési paktum keretében jött létre az információs és kommunikációs technológiák (IKT) hiányának kezelésére.

[78] Az uniós országok vállalják, hogy növelik a nők részvételét a digitális világban | Európa digitális jövőjének alakítása (europa.eu).

[79] Az Európai Parlament és a Tanács (EU) 2021/1057 rendelete (2021. június 24.) az Európai Szociális Alap Plusz (ESZA+) létrehozásáról és az 1296/2013/EU rendelet hatályon kívül helyezéséről, 4. cikk (1) bekezdés c) pont.

[80] NIS 2 irányelv, 7. cikk (2) bekezdés f) pont.

Egyes tagállamok kihasználják **a polgári, védelmi és bűnüldözési kezdeményezések közötti szinergiákat**. Például a nemzeti kötelező katonai szolgálat bevonásával történő munkaerő-bővítés vagy a kibervédelmi tartalékosok, azaz a fegyveres erőknél kiberbiztonsági pozíciókat betöltő, katonai kiképzésben részesült állampolgárok közreműködése[81] lehetővé teszi a lakosság, és különösen a fiatal felnőttek számára, hogy elmélyítsék kiberbiztonsági és kibervédelmi készségeiket. Ugyanez vonatkozik a **kiberbűnözés elleni küzdelem** területére is, mivel sok hasonlóság van az általános kiberbiztonsági erőfeszítések és a bűnüldözési tevékenységek között a kiberbiztonsági eseményekre való reagálás során. A Bizottság ösztönzi a tagállamok közötti megbeszéléseket az ilyen kezdeményezésekről, és felkéri őket annak felmérésére, hogy a képzett munkaerő hogyan szolgálhatja legjobban mind a védelmi, mind a polgári kiberbiztonsági közösségeket.

A Bizottság javaslatokat fog kidolgozni arra vonatkozóan, hogy miként lehetne pótolni az uniós intézmények, szervek és ügynökségek szükségleteinek felülvizsgálata során azonosított jelenlegi és várható hiányosságokat. A Bizottság különösen arra fogja ösztönözni a személyzetet, hogy használják ki az EU–USA párbeszéd keretében létrejövő **EU–Egyesült Államok (USA) kiberbiztonsági ösztöndíjat**.

Az Akadémia keretében végzett tevékenységek

A nemzetgazdasági ágazat

- 2023. április 18-tól konkrét **kiberbiztonsági kötelezettségvállalásokat** javasol a digitális készségek és munkahelyek platformján.

Tagállamok

- A **nemzeti kiberbiztonsági stratégiákba** konkrét intézkedéseket építenek be a kiberbiztonsági készséghiány kezelésére.

A Tagállamok és az ágazat

- A „Nők a digitális világban” nyilatkozat végrehajtása és a **nemek közötti egyenlőség elérése a kiberbiztonsági pozíciókban** 2030-ig.

6. Finanszírozás: szinergiák kiépítése a kiberbiztonsági készségek fejlesztésére fordított kiadások hatásának maximalizálása érdekében

Az Akadémia keretében a kiberbiztonsági készségekbe történő beruházások hatása maximalizálható lesz azáltal, hogy közös belépési pontot biztosít, megkönnyíti a pénzeszközök piaci igényeknek jobban megfelelő csatornázását és a finanszírozás felhasználásának általános érvényesítését, elősegítve a különböző eszközök közötti szinergiákat, ugyanakkor elkerülve a párhuzamos erőfeszítéseket[82].

6.1. A pénzeszközök és az igények összehangolása

[81] Jelentés – Kiberbesorozás: A kiválasztott országok tapasztalatai és legjobb gyakorlatai, Martin Hurt és Tiia Sõmer, Nemzetközi Védelmi és Biztonsági Központ, 2021 február.

[82] Finanszírozási lehetőségek (europa.eu). A készségfejlesztési paktum szolgáltatásai egyablakos ügyintézési pontot biztosítanak a készségek finanszírozására vonatkozó információkhoz, beleértve a digitális ökoszisztémára vonatkozó információkat is. A paktum támogatási szolgáltatásai általános információkat nyújtanak olyan finanszírozási eszközökről, amelyek nem kifejezetten a kiberbiztonsági készségekre irányulnak, ennek ellenére az Akadémiának figyelembe kell vennie munkájukat a párhuzamosságok elkerülése érdekében.

Az Akadémia keretében az ECCC a Bizottság, az ECCO-projekt és a nemzeti együttműködési központok támogatásával **információkat gyűjt arról, hogy az uniós forrásokat hogyan használják fel a kiberbiztonsági készségek finanszírozására**, és értékeli, hogy az uniós források hogyan támogatják a kiberbiztonsági készségekben mutatkozó hiány csökkentését. Ezen összesített információk figyelembevételével az ECCC arra fog törekedni, hogy az uniós forrásokat jobban a feltárt igényekre irányítsa. Olyan intézkedéseket fog finanszírozni, amelyek a kiberbiztonsági munkaerőben mutatkozó legsürgetőbb hiányosságokat orvosolnák, beleértve a kiberbiztonsági szakpolitikai igények végrehajtásához kapcsolódó hiányosságokat is.

6.2. A kiberbiztonsági készségekre rendelkezésre álló források és partnerségi kezdeményezések láthatóvá tétele

Rövid távon a **digitális készségek és munkahelyek platformja** lesz az érdekeltek számára az az egyablakos ügyintézési pont, ahol a kiberbiztonsági készségekkel kapcsolatos finanszírozási lehetőségekkel kapcsolatos valamennyi információ elérhető lesz.

Az EU befektet az emberekbe és készségeikbe, és különösen az ágazattal kötött partnerségek segítségével, az **európai készségfejlesztési programban**[83] meghatározott számos eszköz, így a **készségfejlesztési paktum**[84] és a **digitális oktatási cselekvési terv**[85] révén mobilizálja a továbbképzésre és átképzésre irányuló intézkedéseket. A **Digitális Európa program** a kiberbiztonsági készségekkel kapcsolatos lehetőségeket finanszírozza, különösen a több országot érintő projektkezdeményezéseken keresztül, egyértelműen kiegészítve a Horizont Európa által a kiberbiztonság területén a kutatás és az innovatív technológiai megoldások számára nyújtott támogatást. Az **Európai Védelmi Alap**[86] finanszírozza a hatékony kiberműveletek végrehajtásához szükséges kutatást és technológiafejlesztést, beleértve a képzéseket és gyakorlatokat is[87]. Az **Erasmus+** továbbra is támogatja az ilyen kezdeményezéseket, többek között a vegyes intenzív programok és együttműködési projektek révén.

A tagállamokat arra ösztönzik, hogy az általuk közvetlenül kezelt uniós forrásokat mozgósítsák a kiberbiztonsági készségek és munkahelyek támogatására. A kohéziós politikai alapok, például az **Európai Regionális Fejlesztési Alap (ERFA)** és az **ESZA+** jelentős szinergiapotenciállal bírnak e tekintetben[88]. A **Helyreállítási és Rezilienciaépítési Eszköz** (RRF)[89] és az **InvestEU**[90] keretében megvalósuló intézkedések további kulcsfontosságú kiegészítő elemeket tartalmaznak az Akadémia célkitűzéseinek megvalósítása szempontjából.

---

[83] Európai készségfejlesztési program – Foglalkoztatás, szociális ügyek és társadalmi befogadás – Európai Bizottság (europa.eu).

[84] A továbbképzés és átképzés uniós finanszírozási eszközei – Foglalkoztatás, szociális ügyek és társadalmi befogadás – Európai Bizottság (europa.eu).

[85] 2021 és 2027 közötti időszakra szóló digitális oktatási cselekvési terv.

[86] Az Európai Parlament és a Tanács (EU) 2021/697 rendelete (2021. április 29.) az Európai Védelmi Alap létrehozásáról és az (EU) 2018/1092 rendelet hatályon kívül helyezéséről.

[87] A tagállamok elkötelezték magukat a közös képzések és gyakorlatok mellett, például az állandó strukturált együttműködés (PESCO) kibervédelmi képzések és gyakorlatok projektjeinek létrehozásával és az azokban való részvétellel, mint például az EU kiberakadémiája és innovációs központja (EU CAIH) és a szövetségi kiberbiztonsági gyakorlóterek.

[88] Az (EU) 2021/1058 rendelet 3. cikkének (1) bekezdése és az (EU) 2021/1057 rendelet 4. cikke (1) bekezdésének g) pontja.

[89] Az észt helyreállítási és rezilienciaépítési terv például a digitális készségekre irányuló beruházást (10 millió EUR) irányoz elő, amely magában foglalja az IKT-szakemberek számára elérhető képzések felülvizsgálatát, az IKT-szakemberek kiberbiztonsággal kapcsolatos továbbképzésének és átképzésének finanszírozását, valamint hozzájárul az IKT-szakemberek képesítési keretrendszerének átalakítására irányuló kísérleti program kidolgozásához.

Az Akadémia keretében végzett tevékenységek

Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és az ENISA

- A kiberbiztonsági készségek jelenlegi uniós finanszírozásának **feltérképezése** a piaci igényekhez képest, a **hatékonyság** értékelése és a finanszírozási **prioritások** meghatározása 2024 végéig.

Bizottság

- A digitális készségek és munkahelyek platformján 2023 végéig létrehoz egy **egyablakos ügyintézési pontot** a kiberbiztonsági készségek finanszírozási lehetőségeihez.

7. Az előrehaladás mérése: beépített elszámoltathatóság

Az Akadémia keretében olyan **módszertant** dolgoznak ki, amely lehetővé teszi **a kiberbiztonsági készséghiány megszüntetése terén elért előrehaladás mérését.**

7.1.Kiberbiztonsági mutatók meghatározása a kiberbiztonsági munkaerőpiac fejlődésének nyomon követése érdekében

A **digitális gazdaság és társadalom fejlettségét mérő mutató (DESI)** összefoglalja Európa digitális teljesítményének mutatóit, és nyomon követi az uniós tagállamok fejlődését. A Kiberkészségek Akadémiája keretében az ENISA a Bizottsággal és a Kiberbiztonsági Együttműködési Csoporttal[91] együttműködve – többek között a nemekkel kapcsolatos – **mutatókat** dolgoz ki annak nyomon követésére, hogy az EU tagállamaiban milyen előrelépés történt a kiberbiztonsági szakemberek számának növelése terén, konzultálva az érintett piaci szereplőkkel és a nemzeti együttműködési központokkal is. Az ENISA a DESI módszertanára[92] fog támaszkodni, és biztosítani fogja, hogy a mutatók összhangban legyenek az IKT-szakemberekre és a nemek közötti egyenlőség elérésére vonatkozó európai digitális célokkal. A Bizottság ezután azon fog dolgozni, hogy ezeket a mutatókat beépítse a DESI-be, lehetővé téve ezáltal a kiberbiztonsági készségek és a munkaerőpiac helyzetének éves nyomon követését.

7.2.Adatgyűjtés és a jelentéstétel

Az ENISA az ECCO-projekt és a nemzeti együttműködési központok támogatásával gyűjti össze a mutatókra vonatkozó adatokat. Az összegyűjtött adatok alapján az ENISA **évente jelentést** készít, amely hozzájárul a digitális évtized helyzetéről szóló jelentéshez[93], és amely a DESI-vel együtt az **európai szemeszter** országspecifikus elemzésébe és ajánlásaiba is

---

[90] Az érdekeltek (pl. képzési szolgáltatók és vállalatok, amelyek kiberbiztonsági képzési tevékenységeiket kívánják megtervezni vagy fejleszteni) az InvestEU tanácsadó központhoz fordulhatnak, amely technikai támogatást és segítséget nyújt, beleértve a kapacitásépítést is a projektfejlesztők és szervezetek számára, és felkereshetik az InvestEU portált.

[91] Ennek során arra a módszertanra fog támaszkodni és azt kiegészíteni, amelyet az ENISA dolgoz ki a NIS 2 irányelv 18. cikkének (3) bekezdése szerint kétévente készítendő, a kiberbiztonság uniós helyzetéről szóló jelentése céljából.

[92] Lásd: a digitális gazdaság és társadalom fejlettségét mérő mutató (DESI) 2022 módszertani jegyzet, elérhető a következő címen: A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI) | Európa digitális jövőjének alakítása (europa.eu).

[93] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata (2022. december 14.) a Digitális évtized 2030 szakpolitikai program létrehozásáról.

beépül[94]. A kiberbiztonsági készségekre vonatkozó mutatók továbbá hozzájárulnak az ENISA-nak a kiberbiztonság uniós helyzetéről szóló, a NIS 2 irányelvben előirányzott **kétévente elkészítendő jelentéséhez**, amely a kiberbiztonsági képességekre, tudatosságra és higiéniára terjed ki az EU-ban.

7.3.Kulcsfontosságú teljesítménymutatók (KPI-k) készítése a kiberbiztonságra vonatkozóan

Az európai kiberbiztonsági szakemberhiány megszüntetése érdekében az ENISA a Bizottsággal és a nemzeti együttműködési központokkal szoros együttműködésben a Digitális Évtized 2030 szakpolitikai program módszertanára, valamint az ágazat tapasztalataira támaszkodva KPI-ket fog javasolni a Bizottságnak. Az ENISA megfelelően figyelembe veszi a tagállamok által a nemzeti kiberbiztonsági stratégiáik értékelésére használt KPI-ket[95].

<u>Az Akadémia keretében végzett tevékenységek</u>

ENISA

- A kiberbiztonsági készségekre vonatkozó **mutatók és KPI-k** elkészítése 2023 végéig.
- A mutatókra vonatkozó **adatok összegyűjtése** és az ezekről szóló jelentéstétel, az első adatgyűjtést 2025-ig elvégezve.

Bizottság

- A **kiberbiztonságra vonatkozó mutatóknak a DESI-be** és a **digitális évtized helyzetéről szóló jelentésbe** való beépítésére irányuló munka.

8. Következtetés

Ez a közlemény megteremti az alapjait azon uniós megközelítés megújításának, amely az EU-ban dolgozó szakemberek kiberbiztonsági készségeinek növelésére irányul. A cél a kiberbiztonsági készségekben mutatkozó hiány csökkentése, valamint az EU megfelelő munkaerővel való ellátása, hogy az EU képes legyen reagálni a folyamatosan változó fenyegetettségi helyzetre, és végre tudja hajtani azokat az uniós szakpolitikákat, amelyek célja az EU védelme a kibertámadásokkal szemben, ugyanakkor az üzleti lehetőségeket és a versenyképességet is növelni tudja. A képzett kiberbiztonsági munkaerő a **polgári, védelmi, diplomáciai és bűnüldözési** közösségek javát szolgálhatja, és elősegítheti a köztük lévő szinergiákat.

A Bizottság felszólítja a tagállamokat és az összes érdekelt felet, hogy valósítsák meg a Kiberkészségek Akadémiájának célkitűzéseit.

[94] Ugyanott, (25) preambulumbekezdés.

[95] A NIS 2 irányelv 7. cikkének (4) bekezdése.