EURÓPAI
BIZOTTSÁG

Brüsszel, 2018.9.12.
COM(2018) 630 final

2018/0328 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról

Az Európai Bizottság hozzájárulása a 2018. szeptember 19–20-i salzburgi vezetői értekezlethez

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

INDOKOLÁS

1. A JAVASLAT HÁTTERE

• A javaslat indokai és céljai

Mindennapi életünk és gazdaságunk egyre nagyobb mértékben függ a digitális technológiáktól, ezzel együtt polgárainkra is egyre több komoly kiberfenyegetés leselkedik. Biztonságunk jövőbeni megőrzésének alapja, hogy magasabb szintre emeljük az Unió kiberfenyegetésekkel szembeni védelmét, hiszen mind a polgári infrastruktúra, mind a katonai eszközök nagy mértékben biztonságos digitális rendszerekre épülnek.

Az egyre gyakrabban felmerülő kihívások leküzdése érdekében az EU a 2013-as kiberbiztonsági stratégiára[1], annak céljaira és alapelveire támaszkodva folyamatosan bővítette e területen kifejtett tevékenységét, hogy elősegítse egy megbízható, biztonságos és nyílt kiberbiztonsági ökoszisztéma kialakulását. A hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv[2] elfogadásával az Unió 2016-ban meghozta első, kiberbiztonságot érintő intézkedéseit.

A kiberbiztonság világában zajló rendkívül gyors változások fényében 2017 szeptemberében a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője közös közleményt adott ki[3] „Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése” címmel, amelynek célja az volt, hogy tovább erősítse az EU kibertámadásokkal szembeni ellenálló képességét, visszatartó erejét és válaszadását. A korábbi kezdeményezéseket is figyelembe vevő közös közlemény különböző intézkedéseket javasolt, többek között az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítését, a digitális termékek és szolgáltatások kiberbiztonságának növelését elősegítő önkéntes, uniós kiberbiztonság-tanúsítási keretrendszer kidolgozását, valamint a nagy léptékű kiberbiztonsági események és krízishelyzetek esetén a gyors, összehangolt reagáláshoz felhasználható tervezet megalkotását.

A közös közlemény elismerte, hogy az EU-nak stratégiai érdeke is fűződik a kiberbiztonságot elősegítő alapvető technológiai kapacitások fenntartásához és fejlesztéséhez, hiszen csak így lehet garantálni a digitális egységes piac biztonságát, megvédeni a létfontosságú hálózatokat és információs rendszereket, valamint biztosítani a kulcsfontosságú kiberbiztonsági szolgáltatásokat. Az EU-nak olyan pozícióba kell kerülnie, hogy képes legyen önállóan megvédeni digitális eszközeit és versenyezni a globális kiberbiztonsági piacon.

Jelen pillanatban az EU a kiberbiztonsági termékek és megoldások nettó importőre, amelyek tekintetében elsősorban nem európai szolgáltatókra kell hagyatkoznia[4]. A kiberbiztonság globális szinten egy 600 milliárd EUR-s piac, amely az előrejelzések szerint a következő öt évben a forgalom, a vállalatok száma és a foglalkoztatás terén átlagosan mintegy 17 %-os

---

1 KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, JOIN(2013) 1 final.

2 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

3 KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS AZ EURÓPAI TANÁCSNAK: Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése, JOIN(2017) 450 final.

4 Kiberbiztonsági piactanulmány, 2018, a végleges jelentés tervezete.

növekedést fog elérni. A kiberbiztonság piacát vezető 20 ország között azonban csupán 6 uniós tagállam van[5].

Ugyanakkor jelentős kiberbiztonsági szakértelem és tapasztalat áll rendelkezésre az Unióban: a Bizottság nemrégiben feltérképezte a kiberbiztonsági szakértői központokat, amelynek során több mint 660 szervezetet vett nyilvántartásba az EU különböző részeiből[6]. Amennyiben ezt a szakértelmet sikerülne piacképes termékekre és megoldásokra váltani, az EU képes lenne lefedni a kiberbiztonsági terület teljes értékláncát. A kutatói és az ipari közösségek erőfeszítései azonban nem egységesek, nincsenek összehangolva és nem rendelkeznek közös céllal, ami negatívan befolyásolja az EU e téren fennálló versenyképességét, valamint a digitális eszközök biztonságának biztosítására irányuló képességét. A releváns kiberbiztonsági szektorok (például energetika, űrkutatás, honvédelem, közlekedés) és ezek alterületei jelenleg nem kapnak megfelelő támogatást[7]. Európa a polgári és a katonai kiberbiztonsági szektorok között elérhető szinergiákat sem használja ki teljes mértékben.

A szerződéses kiberbiztonsági köz-magán társulás („cPPP”) 2016-os létrehozásával az Unió megtette az első határozott lépést abba az irányba, hogy a kutatás, az ipar és a közszféra területén tevékenykedő közösségek együttműködése révén megkönnyítse a kiberbiztonsági kutatást és innovációt, ami a várakozások szerint a 2014 és 2020 közötti pénzügyi keret korlátain belül megfelelő, célorientáltabb kutatási és innovációs eredményekhez vezet. A cPPP keretében az ipari partnerek vállalásokat tehettek arra nézve, hogy milyen beruházásokat fognak megvalósítani a társulás Stratégiai kutatási és innovációs tervében meghatározott területeken.

Az EU azonban ennél jóval nagyobb léptékű beruházásokat is képes megvalósítani, és hatékonyabb mechanizmusra van szüksége, amely képes tartós kapacitásokat kiépíteni, összefogni az erőfeszítéseket és kompetenciákat, ösztönözni a kiberbiztonsági iparág kihívásainak leküzdésére alkalmas innovatív megoldások kifejlesztését az új, többcélú technológiák (például mesterséges intelligencia, kvantumszámítógépek, blokklánc és biztonságos digitális identitások) terén, valamint a létfontosságú szektorokban (például közlekedés, energetika, egészségügy, pénzügy, állami szektor, telekommunikáció, gyártás, honvédelem, űrkutatás).

A közös közlemény megfogalmazta annak lehetőségét, hogy az EU kiberbiztonsági képességeit kiberbiztonsági kompetenciaközpontok hálózatával erősítsék meg, amelynek központi intézménye az Európai Kiberbiztonsági Kompetenciaközpont lenne. A hálózat arra törekedne, hogy kiegészítse az uniós és nemzeti szinten tett kapacitásépítési erőfeszítéseket. A közös közleményben a Bizottság hangot adott azon szándékának, hogy 2018-ban hatásvizsgálat keretében megvizsgálja a rendelkezésre álló lehetőségeket, amelyek alapján kidolgozható a struktúra. Első lépésként és a jövőbeni megoldások kidolgozásának elősegítése érdekében a Bizottság a Horizont 2020 program keretei között elindított egy kísérleti fázist azzal a céllal, hogy a nemzeti központok hálózatának létrehozásával lendületet adjon a kiberbiztonsági kompetenciák és technológiák fejlesztésének.

Az állam- és kormányfők a 2017 szeptemberében rendezett tallinni digitális csúcstalálkozón megfogalmazták azt a célkitűzést, hogy az EU „2025-re legyen a kiberbiztonság területének

5 Kiberbiztonsági piactanulmány, 2018, a végleges jelentés tervezete.

6 A JRC műszaki jelentései: Európai kiberbiztonsági szakértői központok, 2018.

7 A JRC műszaki jelentése: A feltérképezési gyakorlat eredményei (részletekért lásd a 4. és az 5. mellékletet).

globális vezetője – erre polgáraink, fogyasztóink és vállalkozásaink bizalmának és online biztonságának megőrzése, valamint az internet szabadságának és törvényes működésének garantálása érdekében van szükség."

A Tanács 2017 novemberében elfogadott következtetéseiben[8] felszólította a Bizottságot, hogy a lehető leghamarabb végezze el a fennálló lehetőségek hatásvizsgálatát, és 2018 közepéig tegyen javaslatot a kezdeményezés megvalósítására alkalmas jogi eszközre.

A Bizottság által 2018 júniusában előterjesztett Digitális Európa program[9] célja, hogy a szakpolitikák megerősítése és a digitális egységes piac törekvéseinek támogatása révén minden releváns uniós szakpolitikai területen biztosítsa, hogy az európai polgárok és vállalkozások teljes körűen ki tudják aknázni a digitális átalakulás előnyeit. A program által javasolt egységes és átfogó megközelítés biztosítja a digitális átalakulás során a fejlett technológiák legjobb használatát, valamint a technikai lehetőségek és az emberi kompetenciák megfelelő egyensúlyát, nem csupán a kiberbiztonság területén, de az intelligens adat-infrastruktúrák, a mesterséges intelligencia, valamint az iparágakban és a közérdekű területeken használt speciális készségek és alkalmazási módok esetében is. Ezek az elemek egymástól függnek, egymást erősítik és együttes fejlesztésükkel elérhető, hogy az adatokon alapuló gazdaság sikeres növekedésnek induljon[10]. A *Horizont Európa program*[11], az EU új kutatási és innovációs keretprogramja szintén prioritásként kezeli a kiberbiztonságot.

Ebben az összefüggésben e javaslat az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának egyszerre történő létrehozásáról szóló rendeletre irányul. Ennek az adott célnak megfelelően kialakított együttműködési modellnek a következők szerint kell működnie ahhoz, hogy képes legyen ösztönözni az európai kiberbiztonsági technológiai és ipari ökoszisztémát: a kompetenciaközpont elősegíti és segít összehangolni a hálózat munkáját és támogatja a kiberbiztonsági kompetenciaközösséget, miközben előmozdítja a kiberbiztonsági menetrendet és megkönnyíti az így összegyűlt szaktudáshoz való hozzáférést. A kompetenciaközpont mindezt különösen a Digitális Európa program és a Horizont Európa program megfelelő részeinek a támogatások odaítélésével és a közbeszerzések végrehajtásával történő végrehajtása révén fogja megvalósítani. Tekintettel a világ más részein tett jelentős kiberbiztonsági beruházásokra, valamint a szóba jövő európai erőforrások koordinálásának és egyesítésének szükségességére, a kompetenciaközpont a javaslat szerint európai partnerségként jön létre[12], ami megkönnyíti az Unió, a tagállamok és/vagy az iparág közös beruházásait. A javaslat ezért arra kötelezi a tagállamokat, hogy arányos összegekkel járuljanak hozzá a kompetenciaközpont és a hálózat tevékenységeihez. A fő döntéshozó szerv az igazgatótanács, amelyben valamennyi tagállam képviselteti magát, de csak azokat a

---

8 A Tanács következtetései az „Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése" című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről, elfogadta az Általános Ügyek Tanácsa 2017. november 20-án.

9 Javaslat Az Európai Parlament és a Tanács rendelete a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról (COM(2018) 434).

10 Lásd: SWD(2018) 305.

11 Javaslat Az Európai Parlament és a Tanács rendelete a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról (COM(2018) 435).

12 A Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatban (COM(2018) 435) meghatározottak, valamint a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatban (COM(2018) 434) hivatkozottak szerint.

tagállamokat illeti szavazati jog, amelyek pénzügyi hozzájárulást tettek. Az igazgatótanács szavazási rendszere a kettős többség elvén alapul, ami azt jelenti, hogy a határozatokhoz egyrészt a szavazatok 75 %-a szükséges, másrészt pedig az, hogy a támogató szavazatok leadói együttesen az összes pénzügyi hozzájárulás legalább 75 %-át képviseljék. Tekintettel az uniós költségvetésével kapcsolatos hatáskörére a Bizottság a szavazatok 50 %-ával rendelkezik. Igazgatótanácsbeli munkájához a Bizottság belátása szerint az Európai Külügyi Szolgálat szakértelmére támaszkodik. A magánszektorral, a fogyasztói szervezetekkel és más érintett érdekeltekkel való rendszeres párbeszéd biztosítása céljából az igazgatótanácsot egy ipari és tudományos tanácsadó testület segíti.

Az e rendelet által létrehozandó Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont szolgálna az EU által javasolt *Digitális Európa program* és *Horizont Európa program* keretében a kiberbiztonsági célokra fordítandó uniós pénzügyi források fő végrehajtási szerveként, és szoros együttműködést folytatna a Nemzeti Koordinációs Központok hálózatával és a kiberbiztonsági kompetenciaközösséggel (amelyhez a kiberbiztonsági technológiák fejlesztésével foglalkozó szereplők nagy és sokszínű csoportja, többek között kutatószervezetek, keresleti és kínálati oldalon és a közszférában tevékenykedő szervezetek tartoznak).

Ezzel az átfogó megközelítéssel a kiberbiztonság az értéklánc minden pontján magasabb szintre emelhető, a kutatástól a kulcsfontosságú technológiák bevezetéséig és elterjesztéséig. A kezdeményezés sikeréhez feltétlenül szükséges, hogy az EU pénzügyi hozzájárulásával arányos mértékben a tagállamok is részt vállaljanak finanszírozásában.

A Horizont 2020 keretében megvalósult szerződéses kiberbiztonsági köz-magán társulásban a Bizottság partnereként részt vevő Európai Kiberbiztonsági Szervezet különleges szakértelemmel rendelkezik a területen, valamint a releváns érdekelt felek széles körét képviseli, ezért fel kell kérni a Központ és a hálózat munkájában való részvételre.

Ezenfelül az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak törekednie kell arra, hogy erősítse a kiberbiztonság polgári és katonai vetületei közötti szinergiákat. A Központnak tanácsadással, a szakértelem megosztásával, továbbá a projektek és tevékenységek terén történő együttműködés elősegítésével támogatást kell nyújtania a tagállamoknak és a többi releváns szereplőnek. Tagállami felkérésre a Központ projektmenedzserként is eljárhat, különösen az Európai Védelmi Alaphoz tartozó projektek viszonylatában. E kezdeményezés az alábbi problémák megoldásához kíván hozzájárulni:

- **Nem kielégítő együttműködés a kiberbiztonság kínálati és keresleti szegmensei között.** Az európai vállalkozások számára kihívást jelent, hogy megőrizzék saját biztonságukat, és egyben biztonságos termékeket és szolgáltatásokat kínáljanak ügyfeleiknek. Sok esetben azonban a vállalkozások nem képesek megfelelő védelemben részesíteni meglévő termékeiket, szolgáltatásaikat és eszközeiket, illetve nem tudnak biztonságos innovatív termékeket és szolgáltatásokat kifejleszteni. A létfontosságú kiberbiztonsági eszközök kifejlesztése gyakran túlzottan magas költségekkel jár, és ezeket olyan önálló szereplők hozzák létre, amelyek alapvető üzleti tevékenysége nem kapcsolódik a kiberbiztonsághoz. Ugyanakkor a kiberbiztonsági piac keresleti és kínálati oldala közötti kapcsolatok nem elég fejlettek, ezért nincs megfelelő kínálat a különböző szektorok igényeihez igazodó európai termékekből és megoldásokból, továbbá nem áll fenn megfelelő mértékű bizalom a piaci szereplők között.

- **Ipari kapacitásépítést célzó, hatékony tagállamok közötti együttműködési mechanizmus hiánya.** Jelenleg nem áll a tagállamok rendelkezésre olyan hatékony együttműködési mechanizmus sem, amellyel közösen kiépíthetnék a különböző iparágak kiberbiztonsági innovációjának és a modern európai kiberbiztonsági megoldások bevezetésének támogatásához szükséges képességeket. Az (EU) 2016/1148 irányelv által létrehozott, tagállamok közötti kiberbiztonságra irányuló együttműködési mechanizmusok céljai között ilyen típusú tevékenységek nem szerepelnek.
- **Elégtelen együttműködés a kutatói és az ipari közösségek között és ezeken belül.** Európa elméletileg képes a kiberbiztonsági értéklánc egészét lefedni, ugyanakkor bizonyos releváns kiberbiztonsági területek (például az energetika, űrkutatás, honvédelem, közlekedés) és ezek alterületei nem kapnak megfelelő támogatást a kutatói közösségektől, vagy csupán korlátozott számú központ biztosít számukra támogatást (például posztkvantum- és kvantum-kriptográfia, megbízhatóság és kiberbiztonság a mesterséges intelligencia területén). Természetesen létezik ilyen jellegű együttműködés, ez azonban általában rövid távú, tanácsadói szerződések formájában valósul meg, ami nem teszi lehetővé a kiberbiztonsági iparág kihívásaira megoldást kínáló hosszú távú kutatási tervek kidolgozását.
- **Elégtelen együttműködés a polgári és a katonai kiberbiztonsági kutatói és innovációs közösségek között.** A kellő intenzitású együttműködés hiánya a polgári és a katonai közösségek viszonylatában is kimutatható. A meglévő szinergiák kiaknázatlanok, mivel nem állnak rendelkezésre olyan hatékony mechanizmusok, amelyek lehetővé tennék e közösségek számára a hatékony együttműködést és a bizalom kiépítését, ez utóbbi e területen kiemelten fontos előfeltétele a sikeres együttműködésnek. Ráadásul az EU kiberbiztonsági piaca korlátozott pénzügyi lehetőségekkel rendelkezik, ami azt is jelenti, hogy nem jut elég forrás az innováció támogatására.
- **Összhang a szabályozási terület jelenlegi rendelkezéseivel**

A kiberbiztonsági kompetenciahálózat és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont célja, hogy kiegészítő támogatást nyújtson a meglévő kiberbiztonsági szakpolitikai rendelkezések és szereplők számára. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont feladatkörét tekintve kiegészíti az ENISA tevékenységét, ugyanakkor más területekre fókuszál és más készségekre támaszkodik. Míg az ENISA felhatalmazása szerint tanácsadói szerepet tölt be az EU-ban zajló kiberbiztonsági kutatás és innováció terén, a kompetenciaközpont javasolt megbízása elsősorban az EU kiberbiztonsági ellenálló képességének megerősítéséhez szükséges más fontos feladatokat helyez előtérbe. Ezenfelül az ENISA célkitűzései között nem szerepelnek a kompetenciaközpont és a hálózat alapvető feladatainak számító tevékenységek, vagyis a kiberbiztonsági technológiák kifejlesztésének és bevezetésének ösztönzése, valamint az e területen tett kapacitásépítési erőfeszítések uniós és nemzeti szintű kiegészítése.

Ezenfelül az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a kiberbiztonsági kompetenciahálózat feladatai közé tartozik majd a szabványosítási és tanúsítási folyamatok, különösen a javasolt Kiberbiztonsági jogszabály[13][14] szerinti

[13] Javaslat: AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”, COM(2017) 477 final/3).

[14] Ez nem befolyásolja az általános adatvédelmi rendelet, azaz a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a

kiberbiztonsági tanúsítási rendszerekhez kapcsolódó szabványosítási és tanúsítási folyamatok elősegítését és felgyorsítását célzó kutatások támogatása is.

Ez a kezdeményezés ténylegesen továbbfejleszti a szerződéses kiberbiztonsági köz-magán társulást (cPPP), amely az első uniós léptékű próbálkozást jelentette a kiberbiztonsági iparág, a keresleti oldal (a kiberbiztonsági termékeket és megoldásokat vásárló felek, köztük a közigazgatási szervek és fontos szektorok, például közlekedés, egészségügy, energetika, pénzügy) és a kutatói közösségek összehangolására, a felek közötti fenntartható párbeszéd kiépítésére és az önkéntes társberuházás feltételeinek megteremtésére. A cPPP 2016-ban jött létre, és 2020-ig mintegy 1,8 milliárd EUR beruházást hívott életre. Ugyanakkor a világ többi részén megvalósuló beruházások mértéke (például az Egyesült Államok csak 2017-ben 19 milliárd dollárt fektetett a kiberbiztonságba) azt támasztja alá, hogy az EU-nak többet kell tennie azért, hogy a beruházások elérjék a kritikus tömeget, és leküzdje az EU különböző részein meglévő kapacitások széttagoltságából fakadó hátrányokat.

- **Összhang az Unió egyéb szakpolitikáival**

Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont több uniós kiberbiztonsági program (a Digitális Európa program és a Horizont Európa program) közös végrehajtó testületeként fog működni, összehangolva tevékenységeiket és növelve a közöttük kialakuló szinergiákat.

E kezdeményezés ezenfelül hozzájárul a tagállami erőfeszítések kiegészítéséhez: megfelelő támogatást tud nyújtani az oktatás területén dolgozó döntéshozóknak a kiberbiztonsági készségek fejlesztéséhez (például a polgári és a katonai oktatásban használható kiberbiztonsági tantervek kidolgozásával), és így hozzájárulhat egy képzett európai kiberbiztonsági munkavállalói réteg kialakulásához, ami rendkívül hasznos lenne a kiberbiztonsággal foglalkozó vállalatok és a kiberbiztonságban érdekelt más iparágak számára. Ami a kibervédelmi oktatást és képzést illeti, a kezdeményezés összhangban van az Európai Biztonsági és Védelmi Főiskola keretében létrejött kibervédelmi oktatási, képzési és gyakorlati platformon belül folyó munkával.

A kezdeményezés kiegészíti és támogatja majd a Digitális Európa program keretében létrehozandó digitális innovációs központok erőfeszítéseit. A digitális innovációs központok olyan nyereségérdekeltség nélküli szervezetek, amelyek célja, hogy digitális technológiákra épülő intelligens és innovatív megoldások révén segítséget nyújtsanak az induló vállalkozásoknak, a kkv-knek és a közepes tőkeértékű vállalkozásoknak üzleti/termelési folyamataik, valamint termékeik és szolgáltatásaik fejlesztéséhez, és ezen keresztül versenyképességük növeléséhez. A digitális innovációs központok az új termékek és szolgáltatások sikeres piacra vitele, illetve a hatékonyabb termelési folyamatok bevezetése érdekében üzletközpontú, innovációs szolgáltatásokat nyújtanak, például piaci intelligenciát, finanszírozási tanácsadást, tesztelési és kísérleti létesítményekhez való hozzáférést, képzést és készségfejlesztést. Egyes, konkrét kiberbiztonsági szakértelemmel rendelkező digitális innovációs központok közvetlenül is részt vállalhatnak a kezdeményezés által kialakítandó kiberbiztonsági kompetenciaközösség munkájában. A legtöbb digitális innovációs központ azonban nem a kiberbiztonságra összpontosít, ezért feladatuk főként az lesz, hogy a nemzeti koordinációs központok hálózatával és az Európai Kiberbiztonsági Ipari, Technológiai és

95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) által meghatározott, az adatvédelmi hatóságok szerepvállalásával megvalósuló tanúsítási mechanizmusokat.

Kutatási Kompetenciaközponttal szorosan együttműködve hozzáférést biztosítsanak az általuk kiszolgált feleknek a kiberbiztonsági kompetenciaközösség által kínált szakértelemhez, ismeretekhez és kapacitásokhoz. A digitális innovációs központok ezenfelül elősegíthetik azt is, hogy az általuk kiszolgált vállalatok és más végfelhasználók igényeinek megfelelő innovatív kiberbiztonsági termékek és megoldások kerüljenek a piacra. Végül az ágazatspecifikus digitális innovációs központok megoszthatják a különböző ágazatok valós igényeire vonatkozó ismereteiket a hálózattal és a kompetenciaközponttal, és ezzel elősegíthetik, hogy a kutatási és innovációs tervek a valódi ipari szükségletekhez igazodjanak.

Fontos szempont az Európai Innovációs és Technológiai Intézet alá tartozó tudományos és innovációs társulásokkal, különösen a digitális társulással való szinergiák feltárása.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

• Jogalap

Jellegének és konkrét célkitűzéseinek tükrében a kompetenciaközpont létrehozása szempontjából két jogalapot kell figyelembe venni. Az EUMSZ uniós kutatási, technológiafejlesztési és demonstrációs programok hatékony végrehajtásához szükséges struktúrákat kidolgozó 187. cikke lehetővé teszi, hogy a kompetenciaközpont szinergiák kialakításával és különböző erőforrások összefogásával beruházzon a tagállami szinten szükséges kapacitásokba, és közös európai eszközöket hozzon létre (például a kiberbiztonsági tesztekhez és kísérletekhez szükséges infrastruktúra közös beszerzése révén). A 188. cikk első bekezdése lehetővé teszi az ilyen intézkedések meghozatalát. Ha azonban csak a 188. cikk első albekezdése szolgálna egyedüli jogalapként, akkor nem lehetne a kutatás-fejlesztés területén túlmutató tevékenységeket végezni, amelyekre pedig a kompetenciaközpont e rendeletben lefektetett céljainak megvalósításához szükség van, hiszen e célok között szerepel a kiberbiztonsági termékek és megoldások piacra vitelének támogatása, az európai kiberbiztonsági iparág versenyképességének és piaci részesedésének növelése, valamint a kiberbiztonsági készségek terén jelentkező hiányosságok leküzdését célzó nemzeti erőfeszítésekhez való hozzájárulás. A fenti célkitűzések teljesítése érdekében a 173. cikk (3) bekezdésére is jogalapként kell hivatkoznunk, amely lehetővé teszi, hogy az EU intézkedések révén támogassa az ipar versenyképességét.

• A javaslat indokolása a szubszidiaritás és az arányosság elve alapján

A kiberbiztonság az Unió egészének közös érdeke, amelyet a fent említett tanácsi következtetések is megerősítenek. A *WannaCry*, a *NonPetya* és hasonló incidensek jelentős kihatása és határokon átnyúló jellege szintén alátámasztja ezt a megállapítást. A kiberbiztonság terén fennálló technológiai kihívások jellege és léptéke, valamint az ipar, a közszféra és a kutatói közösségek közötti és azokon belüli elégtelen együttműködés szükségessé teszi, hogy az EU további támogatást nyújtson az erőfeszítések összehangolásához, egyfelől az erőforrások kritikus tömegének biztosítása, másfelől a jobb tudás- és eszközkezelés érdekében. Ezt teszik szükségessé a kiberbiztonsági kutatáshoz, fejlesztéshez és a kiberbiztonsági megoldások bevezetéséhez kapcsolódó bizonyos képességek erőforrásigényei; az interdiszciplináris kiberbiztonsági szakismerethez való hozzáférés különböző diszciplínák számára történő biztosítására irányuló igények (ez a szakismeret általában nemzeti szinten csak részlegesen áll rendelkezésre); továbbá az iparági értékláncok globális jellege, valamint a piacokon működő nemzetközi versenytársak tevékenysége.

A fentiekhez olyan léptékű erőforrások és szakértelem szükséges, amelyet egyetlen tagállam sem tud önálló intézkedésekkel biztosítani. Például egy összeurópai kvantumkommunikációs hálózat kiépítése az összekapcsolni/bevonni kívánt tagállamok által tett beruházások, valamint a meglévő infrastruktúra felhasználhatóságától függően akár mintegy 900 millió EUR uniós beruházást is igényelhet. A kezdeményezés létfontosságú segítséget fog nyújtani a finanszírozás összehangolásához és az ilyen jellegű uniós beruházások lehetővé tételéhez.

E kezdeményezés célkitűzéseit önmagukban a tagállamok nem képesek maradéktalanul megvalósítani. Ahogy azt a fentiekben bemutattuk, ezek a célkitűzések hatékonyabban megvalósíthatók uniós szinten az erőfeszítések összehangolásával, mivel ezáltal elkerülhetők a szükségtelen párhuzamos tevékenységek, elérhető a kritikus tömegű beruházás, és garantálható a közpénzek optimális felhasználása. Emellett azonban az arányosság elvének megfelelően e rendelet nem lépi túl a célkitűzés eléréséhez szükséges mértéket. A szubszidiaritás és arányosság elve alapján ezért indokolt az uniós szintű fellépés.

E kezdeményezés nem ró új szabályozási kötelezettségeket a vállalkozásokra. Sőt, valószínűleg csökkenni fognak a vállalkozások, különösen a kkv-k innovatív kiberbiztonsági termékek kifejlesztésére irányuló erőfeszítéseihez kapcsolódó költségei, hiszen a kezdeményezés lehetővé teszi az erőforrások összehangolását a szükséges kapacitásokba történő tagállami beruházásokhoz, illetve a közös európai eszközök kifejlesztéséhez (például a kiberbiztonsági tesztekhez és kísérletekhez szükséges infrastruktúra közös beszerzése révén). Ezekkel az eszközökkel a különböző szektorokban tevékenykedő iparági szereplők és kkv-k garantálhatják termékeik biztonságosságát, és versenyelőnyt kovácsolhatnak a kiberbiztonságból.

- **A jogi aktus típusának megválasztása**

A javasolt jogi aktus létrehoz egy, a Digitális Európa program és a Horizont Európa program keretében végzett kiberbiztonsági tevékenységek végrehajtására szolgáló szervet. A javaslat ismerteti az új szerv megbízatását, feladatkörét, valamint igazgatási struktúráját. Az ilyen uniós szervek létrehozásához rendelet elfogadása szükséges.

3. KONZULTÁCIÓK AZ ÉRDEKELTEKKEL ÉS HATÁSVIZSGÁLATOK

Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont vezetésével működő kiberbiztonsági kompetenciahálózat létrehozására vonatkozó javaslat egy új kezdeményezés. A kezdeményezés a 2016-ban létrehozott szerződéses kiberbiztonsági közmagán társulás folytatásának és kibővítésének minősül.

- **Az érdekelt felekkel folytatott konzultációk**

A kiberbiztonság szerteágazó, több szektort érintő témakör. A Bizottság különböző konzultációs módszerekre támaszkodott annak garantálása érdekében, hogy a kezdeményezés az általános uniós közérdeket, és ne az érdekeltek szűk csoportjainak érdekeit tükrözze. Ez a módszer biztosítja a Bizottság munkájának átláthatóságát és elszámoltathatóságát. Bár az ipari és a kutatói közösségből, valamint a tagállamokból álló célközönség miatt kifejezetten erről a kezdeményezésről nem folyt nyílt és nyilvános konzultáció, a témakört már számos ilyen jellegű konzultáció lefedte:

- A 2018-ban a beruházás, a kutatás és innováció, a kis- és középvállalkozások és az egységes piac témájában megrendezett általános, nyílt és nyilvános konzultáció.

- A 2017-ben 12 héten át tartó online nyilvános konzultáció, amelynek során az ENISA értékelésére és felülvizsgálatára kérték fel a szélesebb nyilvánosságot (körülbelül 90 válasz érkezett).
- A 2016-ban a szerződéses kiberbiztonsági köz-magán társulás elindításakor 12 héten keresztül zajló online nyilvános konzultáció (körülbelül 240 válasz érkezett).

A Bizottság ezenfelül célzott konzultációkat is tartott a kezdeményezésről, többek között műhelytalálkozókat, megbeszéléseket szervezett, és véleménynyilvánítást kért (az ENISA-tól és az Európai Védelmi Ügynökségtől). A konzultációs időszak 6 hónapig tartott, 2017 novembere és 2018 márciusa között. A Bizottság ezenfelül feltérképezte a szakértői központokat, és e gyakorlat keretében 665 kiberbiztonsági szakértői központ szaktudásáról, tevékenységéről, munkaterületeiről és nemzetközi együttműködéseiről gyűjtött információkat. A felmérés januárban vette kezdetét, az elemzés során a Bizottság a 2018. március 8-ig visszaküldött kérdőíveket vette figyelembe.

Az ipari és a kutatói közösségek érdekelt szereplői úgy vélték, hogy a kompetenciaközpont és a hálózat hozzáadott értéket tudna nyújtani a jelenlegi nemzeti szintű erőfeszítésekhez, hiszen hozzájárulna az uniós kiberbiztonsági ökoszisztéma kialakításához, ami elősegítené a kutatói és az ipari közösségek közötti együttműködést. Az érdekeltek ezenfelül szükségesnek ítélték, hogy az EU és a tagállamok proaktív, hosszú távú és stratégiai szempontból közelítsék meg a kiberbiztonsági iparra vonatkozó szakpolitikai tevékenységeket, és ne csak a kutatásra és az innovációra fókuszáljanak. Az érdekelt felek szerint hasznos lenne, ha hozzáférhetnének olyan fontos eszközökhöz, mint a tesztelésre és kísérletezésre használható létesítmények, valamint ha az EU hathatósabban tevékenykedne a kiberbiztonság terén fennálló szakképzettségi hiányosságok megszüntetésén, például a legtehetségesebb szakembereket vonzó nagy léptékű európai projektek révén. A felek ahhoz is szükségesnek tartják a fenti intézkedéseket, hogy az EU a kiberbiztonság területének globálisan elismert vezetőjévé váljon.

A tagállamok a tavaly szeptember óta lebonyolított konzultációs tevékenységek[15] keretében és a témában elfogadott tanácsi következtetésekben[16] üdvözölték a kiberbiztonsági technológiák fejlesztésének és bevezetésének ösztönzését célzó kiberbiztonsági kompetenciahálózat létrehozásának szándékát, és hangsúlyozták, hogy a kezdeményezésnek ki kell terjednie minden tagállamra, valamint azok meglévő kiválósági és kompetenciaközpontjaira, továbbá hogy különös figyelmet kell fordítani a komplementaritás elvére. A jövőben létrehozandó kompetenciaközponttal kapcsolatban a tagállamok a hálózat támogatásában betöltött koordinációs szerepének fontosságát emelték ki. Ami a nemzeti tevékenységeket és a kibervédelmi igényeket illeti, az Európai Külügyi Szolgálat által 2018 márciusában a tagállamok kibervédemi igényeinek feltérképezése céljából végzett felmérés azt mutatta, hogy a tagállamok többsége számára a hozzáadott értéket a kibervédelmi képzés és oktatás uniós támogatása, valamint az iparág kutatás-fejlesztésen keresztül történő támogatása jelentené[17]. A kezdeményezés végrehajtása a tagállamokkal vagy a tagállamok által támogatott szervezetekkel közösen történne. Az iparban, a kutatásban és/vagy a közszférában tevékenykedő közösségek együttműködése nem új szervezeteket és tevékenységeket hozna létre, hanem összefogná és megerősítené a meglévőket. A tagállamok a közszférát mint a

[15] Például magas szintű kerekasztal-beszélgetés a tagállamokkal, Ansip alelnök, Gabriel biztos, 2017. december 5.

[16] Általános Ügyek Tanácsa: A Tanács következtetései az „Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről (2017. november 20.).

[17] EKSZ, 2018. március.

kiberbiztonsági technológiák és szakismeretek közvetlen felhasználóját célzó konkrét tevékenységek meghatározásában is részt vennének.

- **Hatásvizsgálat**

A kezdeményezést támogató hatásvizsgálatot 2017. április 11-én benyújtották a Szabályozói Ellenőrzési Testületnek, amely – bizonyos fenntartások mellett – kedvező véleményt fogalmazott meg. A hatásvizsgálatot a Testület megjegyzései alapján felülvizsgálták. A Testület által adott vélemény és a Testület észrevételeinek figyelembevételét magyarázó melléklet e javaslattal együtt kerül közzétételre.

A hatásvizsgálat több különböző jogalkotási és nem jogalkotási lehetőséget is megvizsgált. A Bizottság az alábbi lehetőségeket részletes vizsgálatnak is alávetette:

- Az alapforgatókönyv – együttműködésre építő lehetőség – azt veszi alapul, hogy tovább folytatódik az uniós ipari és technológiai kiberbiztonsági kapacitások kiépítésének jelenlegi megközelítése, azaz a kutatás, az innováció és a kapcsolódó együttműködési mechanizmusok kilencedik keretprogram keretében történő támogatása.
- 1. lehetőség: Kiberbiztonsági kompetenciahálózat, élén egy Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközponttal és két fő feladattal: az ipari technológiákat támogató intézkedések, valamint a kutatást és innovációt érintő intézkedések meghozatala.
- 2. lehetőség: Kiberbiztonsági kompetenciahálózat, élén egy Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközponttal, amely kutatási és innovációs tevékenységekre összpontosít.

A korai szakaszban elvetett lehetőségek között szerepeltek a következők: 1) nem történik fellépés e téren, 2) csak a kiberbiztonsági kompetenciahálózat létrehozása, 3) csak a központi struktúra létrehozása és 4) valamelyik meglévő szervezet (az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA), a Kutatási Végrehajtó Ügynökség (REA) vagy az Innovációs és Hálózati Projektek Végrehajtó Ügynökség (INEA)) használata.

Az elemzés megállapította, hogy a kezdeményezés céljainak teljesítésére az 1. lehetőség a legalkalmasabb, továbbá ez biztosítja a legjelentősebb gazdasági, társadalmi és környezetvédelmi hatást, és ez képviseli a legjobban az EU érdekeit. Az e lehetőség mellett felhozott legerősebb érvek a következők: ez a megoldás lehetővé teszi a valódi, átfogó kiberbiztonsági szakpolitika kidolgozását, mivel nem csupán a kutatás-fejlesztéssel, hanem a piacfejlesztéssel összefüggő tevékenységeket is támogat; rugalmas, hiszen a meglévő ismeretek és erőforrások felhasználásának optimalizálása érdekében több együttműködési modellt is megenged a kompetenciaközpontok hálózata számára; lehetővé teszi az összes releváns szektor, köztük a védelmi ágazat állami és magánszférában tevékenykedő szereplői közötti együttműködés és a közös vállalások összefogását. Végül pedig az 1. lehetőség elősegíti a szinergiák növelését, és két különböző uniós kiberbiztonsági finanszírozási forrás (a Digitális Európa program és a Horizont Európa program) végrehajtási mechanizmusaként szolgálhat a következő többéves pénzügyi keret során.

- **Alapjogok**

E kezdeményezés lehetővé teszi, hogy biztonságosabb termékek és megoldások kidolgozása és beszerzése révén a tagállamok hatóságai és iparági szereplői hatékonyabban állják útját a kibertámadásoknak és reagáljanak azokra. Ez különösen fontos az alapvető szolgáltatások

(például a közlekedés, egészségügy, banki és pénzügyi szolgáltatások) elérhetőségének védelme szempontjából.

Az, hogy az Európai Unió képes lesz önállóan védelmet nyújtani termékeinek és szolgáltatásainak, minden bizonnyal azt is elősegíti, hogy a polgárok hatékonyabban élhessenek demokratikus jogaikkal (például az adatokra vonatkozóan az Alapjogi Chartában lefektetett jogok, különösen a személyes adatok és a magánélet védelméhez való jog magasabb szintű védelme révén), aminek köszönhetően a jövőben bizonyára jobban meg fognak bízni a digitális társadalomban és gazdaságban.

4. KÖLTSÉGVETÉSI VONZATOK

A kiberbiztonsági kompetenciahálózattal együttműködő Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont lesz a Digitális Európa program és a Horizont Európa program keretében a kiberbiztonságra fordítható uniós pénzügyi források fő végrehajtó szerve.

A Digitális Európa program megvalósításának költségvetési vonzatait részletesen ismerteti az e javaslathoz mellékelt pénzügyi kimutatás. A Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez a 21. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR). A javaslat az XXX rendelet [a Horizont Európa keretprogramja] 6. cikkének (6) bekezdésében meghatározott stratégiai tervezési folyamat eredményein fog alapulni.

5. EGYÉB ELEMEK

- **Végrehajtási tervek, valamint a nyomon követés, az értékelés és a jelentéstétel szabályai**

E javaslat értékelésre vonatkozó rendelkezést tartalmaz (38. cikk), amelynek értelmében a Bizottság független értékelést fog végezni. A jogi aktus hatásának és hozzáadott értékének felmérése érdekében a Bizottság ezt követően jelentést készít az Európai Parlamentnek és a Tanácsnak az értékeléséről, amelyet adott esetben egy felülvizsgálatra irányuló javaslat kísér. Az értékelés során a minőségi jogalkotást ösztönző bizottsági módszert fogják alkalmazni.

E javaslat 17. cikkének értelmében az ügyvezető igazgató köteles kétévente utólagos értékelést benyújtani az igazgatótanácsnak az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a hálózat tevékenységéről. Az ügyvezető igazgatónak továbbá nyomonkövetési cselekvési tervet kell készítenie a visszamenőleges értékelések következtetéseiről, és kétévente jelentést kell benyújtania a Bizottságnak az elért eredményekről. E javaslat 16. cikke értelmében az igazgatótanács felelős a következtetések megfelelő nyomon követésének felügyeletéért.

A szervezet tevékenységei során felmerülő hivatali visszásságok eseteit az európai ombudsman vizsgálja a Szerződés 228. cikkével összhangban.

2018/0328 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról

Az Európai Bizottság hozzájárulása a 2018. szeptember 19–20-i salzburgi vezetői értekezlethez

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 173. cikke (3) bekezdésére és 188. cikke első bekezdésére,

tekintettel az Európai Bizottság javaslatára,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[18],

tekintettel a Régiók Bizottságának véleményére[19],

rendes jogalkotási eljárás keretében,

mivel:

(1) Mindennapi életünk és gazdaságunk egyre nagyobb mértékben függ a digitális technológiáktól, ezzel együtt polgárainkra is egyre több komoly kiberfenyegetés leselkedik. Tekintve, hogy mind a polgári infrastruktúra, mind a katonai eszközök biztonságos digitális rendszerekre épülnek, jövőbeli biztonságunk egyik feltétele, hogy az Unió kiberfenyegetésekkel szembeni védelme érdekében javítsunk technológiai és ipari képességeinken.

(2) A megbízható, biztonságos és nyílt kiberbiztonsági ökoszisztéma kialakítására törekvő 2013-as kiberbiztonsági stratégia[20] létrehozását követően az EU folyamatosan bővítette az egyre gyakrabban fellépő kiberbiztonsági kihívások leküzdését célzó tevékenységeit. A hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv[21] elfogadásával az EU 2016-ban meghozta a kiberbiztonságot érintő első intézkedéseket.

---

18 HL C […]., […], […]. o.

19 HL C […]., […]., […]. o.

20 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, JOIN(2013) 1 final.

21 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

(3) 2017 szeptemberében a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője közös közleményt[22] adott ki „Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése” címmel, amelynek célja az volt, hogy tovább erősítse az EU kibertámadásokkal szembeni ellenálló képességét, visszatartó erejét és válaszadását.

(4) Az állam- és kormányfők a 2017 szeptemberében rendezett tallinni digitális csúcstalálkozón megfogalmazták azt a célkitűzést, hogy az EU „2025-re legyen a kiberbiztonság területének globális vezetője – erre polgáraink, fogyasztóink és vállalkozásaink bizalmának és online biztonságának megőrzése, valamint az internet szabadságának és törvényes működésének garantálása érdekében van szükség.”

(5) A hálózati és információs rendszerekben fellépő jelentős zavarok befolyásolhatják az egyes tagállamok és az EU egészének életét. A hálózati és információs rendszerek biztonsága ezért alapvető fontosságú a belső piac zavartalan működése szempontjából. Az EU jelenleg kénytelen nem európai kiberbiztonsági szolgáltatókra hagyatkozni. Ugyanakkor az EU stratégiai érdeke a kiberbiztonságot elősegítő alapvető technológiai kapacitások fenntartása és fejlesztése, hiszen csak így lehet garantálni a digitális egységes piac biztonságát, megvédeni a létfontosságú hálózatokat és információs rendszereket, valamint biztosítani a kulcsfontosságú kiberbiztonsági szolgáltatásokat.

(6) Az EU-ban jelentős szakértelem és tapasztalat áll rendelkezésre a kiberbiztonság kutatása, technológiai háttere és iparági fejlesztése terén, ugyanakkor az ipari és a kutatói közösségek erőfeszítései nem egységesek, nincsenek összehangolva és nem rendelkeznek közös céllal, ami negatívan befolyásolja e terület versenyképességét. Fontos, hogy az uniós és tagállami szinten meglévő kutatási, technológiai és ipari kapacitások megerősítése és kiegészítése érdekében ezt az erőfeszítést és szakértelmet összehangoljuk, hálózatba kössük és hatékonyan használjuk fel.

(7) A Tanács 2017 novemberében elfogadott következtetéseiben felszólította a Bizottságot, hogy a lehető leghamarabb végezzen hatásvizsgálatot a kiberbiztonsági kompetenciaközpontok hálózata és az Európai Kutatási és Kompetenciaközpont kialakításának lehetőségeiről, és 2018 közepéig tegyen javaslatot az ehhez szükséges jogi eszközre vonatkozóan.

(8) A kompetenciaközpont feladata, hogy az EU fő eszközeként összehangolja a kiberbiztonság területén végzett kutatásokat, technológiai és ipari fejlesztéseket támogató beruházásokat, valamint a kiberbiztonsági kompetenciahálózattal együttműködve megvalósítsa a releváns projekteket és kezdeményezéseket. További feladata, hogy a Horizont Európa és a Digitális Európa program keretéből pénzügyi támogatást nyújtson a kiberbiztonsághoz köthető célokra, és ahol ez megvalósítható, hozzáférést biztosítson az Európai Regionális Fejlesztési Alaphoz és más programokhoz. Ez a megközelítés hozzájárul a szinergiák kialakításához, a kiberbiztonsági kutatás, innováció, technológiai és ipari fejlesztés céljaira juttatott pénzügyi támogatások összehangolásához, valamint a párhuzamosságok elkerüléséhez.

(9) Mivel a kezdeményezés céljai akkor teljesülhetnek a leghatékonyabban, ha az összes vagy a lehető legtöbb tagállam részt vesz benne, és a tagállamok részvételének ösztönzése érdekében csak azok a tagállamok kaphatnak szavazati jogot, amelyek

[22] Közös közlemény az Európai Parlamentnek és a Tanácsnak: Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése, JOIN(2017) 450 final.

pénzügyileg hozzájárulnak a kompetenciaközpont igazgatási és üzemeltetési költségeinek fedezéséhez.

(10) A részt vevő tagállamok az uniós pénzügyi hozzájárulással arányos mértékben járulnak hozzá a kezdeményezéshez.

(11) A kompetenciaközpont feladata, hogy megkönnyítse és segítse az egyes tagállamokban felállított nemzeti koordinációs központokból álló kiberbiztonsági kompetenciahálózat (a „hálózat”) munkáját. Ahhoz, hogy elvégezhessék az e rendeletben meghatározott tevékenységeket, a nemzeti koordinációs központoknak közvetlen uniós pénzügyi támogatásban, többek között pályázati felhívás nélkül odaítélt támogatásban kell részesülniük.

(12) A nemzeti koordinációs központokat a tagállamoknak kell kiválasztaniuk. A szükséges igazgatási kapacitás mellett a központoknak saját kiberbiztonság-technológiai szaktudással vagy ehhez való közvetlen hozzáféréssel kell rendelkezniük, különösen a kriptográfia, az IKT biztonsági szolgáltatások, a behatolásérzékelés, a rendszerbiztonság, a hálózati biztonság, a szoftver- és alkalmazásbiztonság, valamint a biztonság és az adatvédelem emberi és társadalmi szempontjai terén. Ezenfelül alkalmasnak kell lenniük az ágazattal, a közszférával – beleértve az (EU) 2016/1148 európai parlamenti és tanácsi irányelv[23] alapján kijelölt hatóságokat is – és a kutatói közösséggel való hatékony együttműködésre és koordinációra.

(13) Amennyiben a nemzeti koordinációs központok nemzeti szinten tevékenykedő harmadik feleknek juttatandó támogatást kapnak, ezt több lépcsős támogatási megállapodások keretében kell kifizetni a releváns feleknek.

(14) Az új technológiák, például a mesterséges intelligencia, a dolgok internete, a nagy teljesítményű számítástechnika, a kvantum-számítástechnika, a blokklánc és a biztonságos digitális személyazonosításhoz hasonló koncepciók nem csupán új kihívásokat támasztanak, de megoldásokat is kínálnak a kiberbiztonság területén. A meglévő és jövőbeni IKT-rendszerek ellenálló képességének felméréséhez és igazolásához szükséges lesz, hogy a biztonsági megoldásokat nagy teljesítményű és kvantumszámítógépekről levezényelt támadásokkal szemben teszteljék. A kompetenciaközpont, a hálózat és a kiberbiztonsági kompetenciaközösség feladata az is, hogy segítséget nyújtson a legújabb kiberbiztonsági megoldások kifejlesztéséhez és elterjesztéséhez. Emellett fontos, hogy a kompetenciaközpont és a hálózat a létfontosságú szektorokban (például közlekedés, energetika, egészségügy, pénzügy, kormányzat, telekommunikáció, gyártás, védelem és űrkutatás) tevékenykedő fejlesztők és szolgáltatók rendelkezésére álljon, és segítse őket a kiberbiztonsági kihívások leküzdésében.

(15) A kompetenciaközpont a tervek szerint számos központi funkciót fog betölteni. Először: a kompetenciaközpont feladata, hogy megkönnyítse és segítse az európai kiberbiztonsági kompetenciahálózat munkájának összehangolását, valamint támogassa a kiberbiztonsági kompetenciaközösséget. A kompetenciaközpont meghatározza a kiberbiztonság területének legfontosabb technológiai feladatait, és hozzáférést biztosít a hálózat és a kiberbiztonsági kompetenciaközösség által összegyűjtött tudáshoz. Másodszor: végre kell hajtania a Digitális Európa és a Horizont Európa program

[23] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19, 1. o.).

releváns részeit, azaz ki kell osztania a jellemzően versenypályázati felhívások útján odaítélt támogatásokat. Harmadszor: a kompetenciaközpont feladata az is, hogy megkönnyítse az EU, a tagállamok és/vagy az iparági szereplők közös beruházásait.

(16) A kompetenciaközpont ösztönzi és támogatja a kiberbiztonsági kompetenciaközösség tagjainak együttműködését és tevékenységeinek összehangolását, amely közösség a kiberbiztonsági technológiákkal foglalkozó szereplők nagy, nyílt és sokszínű csoportja. A közösségben különösen a kutatóintézeteknek, a kereslet és a kínálat oldalán tevékenykedő szervezeteknek, valamint a közszférának kell részt vennie. A kiberbiztonsági kompetenciaközösség feladata, hogy véleményezze a kompetenciaközpont tevékenységeit és munkatervét; részesülnie kell a kompetenciaközpont és a hálózat által szervezett közösségépítő kezdeményezések előnyeiből, de nem élvezhet kivételes bánásmódot az ajánlattételi vagy pályázati felhívások során.

(17) A keresleti és a kínálati oldal iparági igényeinek kielégítése érdekében a kompetenciaközpontnak nem csupán az IKT-termékek és -szolgáltatások, hanem minden más, kiberbiztonsági megoldásokat tartalmazó iparági és technológiai termék és megoldás terén képesnek kell lennie kiberbiztonsági ismereteket és technikai támogatást nyújtani.

(18) Míg a kompetenciaközpontnak és a hálózatnak arra kell törekednie, hogy biztosítsa a kiberbiztonság polgári és katonai területe közötti szinergiákat, a Horizont Európa program által finanszírozott projekteket az XXX rendelettel [a Horizont Európa rendelet] összhangban kell végrehajtani, amely előírja, hogy a Horizont Európa égisze alatt megvalósuló kutatási és innovációs tevékenységeknek a polgári alkalmazási területekre kell összpontosítaniuk.

(19) A strukturált és fenntartható együttműködés érdekében a kompetenciaközpont és a nemzeti koordinációs központok között szerződéses kapcsolatot kell kialakítani.

(20) Megfelelő rendelkezéseket kell hozni a kompetenciaközpont felelősségének és átláthatóságának biztosítására.

(21) A Bizottság Közös Kutatóközpontja és az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) komoly kiberbiztonsági szakértelmet tudhat magáénak, ezért tevékenyen részt kell venniük a kiberbiztonsági kompetenciaközösségben, valamint az ipari és tudományos tanácsadó testületben.

(22) Az EU általános költségvetéséből pénzügyi hozzájárulásban részesülő nemzeti koordinációs központoknak és kiberbiztonsági kompetenciaközösséghez tartozó szereplőknek nyilvánosságra kell hozniuk, hogy releváns tevékenységeiket e kezdeményezés keretében végzik.

(23) A kompetenciaközpontnak biztosított uniós hozzájárulásnak a kompetenciaközpont létrehozásához, irányításához és koordinációjához szükséges tevékenységek költségeinek felét kell fedeznie. A kettős finanszírozás elkerülése érdekében ezek a tevékenységek más uniós programokból nem kaphatnak támogatást.

(24) A kompetenciaközpont tevékenységének általános irányát a kompetenciaközpont tagállami és bizottsági képviselőkből álló igazgatótanácsának kell megszabnia, és arról is az igazgatótanácsnak kell gondoskodnia, hogy a kompetenciaközpont e rendelettel összhangban ellássa kijelölt feladatait. Az igazgatótanácsot fel kell ruházni mindazokkal a hatáskörökkel, amelyek a költségvetés meghatározásához és végrehajtásának ellenőrzéséhez, a vonatkozó pénzügyi szabályzat elfogadásához, a kompetenciaközpont átlátható határozathozatali eljárásainak kialakításához, a

kompetenciaközpontnak – a célkitűzéseinek megvalósítása és feladatainak teljesítése céljából prioritásként kezelt szempontokat tükröző – munkaterve és többéves stratégiai terve elfogadásához, saját eljárási szabályzatának elfogadásához, az ügyvezető igazgató kinevezéséhez, az ügyvezető igazgató hivatali idejének meghosszabbításához és az ügyvezető igazgató felmentéséhez szükségesek.

(25) A kompetenciaközpont megfelelő és hatékony működése érdekében a Bizottságnak és a tagállamoknak biztosítaniuk kell, hogy az igazgatótanács tagjainak kinevezendő személyek a funkcionális területeken megfelelő szakértelemmel és tapasztalattal rendelkezzenek. Az igazgatótanács munkájának folytonosságát biztosítandó, a Bizottságnak és a tagállamoknak erőfeszítéseket kell tenniük annak érdekében, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban.

(26) A kompetenciaközpont zavartalan működése azt kívánja, hogy az ügyvezető igazgató kinevezése érdemei, igazolt igazgatási és vezetői készségei, valamint a kiberbiztonság területén szerzett szakmai hozzáértése és tapasztalatai alapján történjék, és hogy az ügyvezető igazgató feladatait teljes mértékben független módon végezze.

(27) A magánszektorral, a fogyasztói szervezetekkel és más érdekeltekkel való rendszeres párbeszéd biztosítása céljából a kompetenciaközponton belül tanácsadó szervként indokolt létrehozni egy ipari és tudományos tanácsadó testületet. Az ipari és tudományos tanácsadó testületnek az érdekelt felek számára releváns kérdésekre kell összpontosítania, és fel kell hívnia ezekre a kompetenciaközpont igazgatótanácsának figyelmét. Az ipari és tudományos tanácsadó testület összetételét és feladatait (például a munkatervhez kapcsolódó tanácsadói tevékenységét) úgy kell meghatározni, hogy az érdekelt felek kellő mértékben képviseltessék magukat a kompetenciaközpont munkájában.

(28) A kompetenciaközpontnak az ipari és tudományos tanácsadó testületen keresztül részesülnie kell a szerződéses kiberbiztonsági köz-magán társulás által a Horizont 2020 időtartama alatt megszerzett konkrét szakértelem és a releváns érdekelt felek széles körű bevonásának előnyeiből.

(29) A kompetenciaközpontnak szabályokat kell kidolgoznia az összeférhetetlenségek megelőzésére és kezelésére. Alkalmaznia kell továbbá a dokumentumokhoz való nyilvános hozzáférésről szóló 1049/2001/EK európai parlamenti és tanácsi rendeletben[24] meghatározott idevágó uniós rendelkezéseket is. A személyes adatok kompetenciaközpont általi kezelésére az (EU) 2018/XXX európai parlamenti és tanácsi rendelet alkalmazandó. Be kell tartania továbbá az uniós intézményekre vonatkozó rendelkezéseket, valamint az adatok – különösen a nem minősített különleges adatok és az EU-minősített adatok – kezelésére vonatkozó nemzeti jogszabályokat is.

(30) Az Unió és a tagállamok pénzügyi érdekeit a teljes kiadási ciklusban arányos intézkedésekkel kell védeni a kiadási ciklus egészében, ideértve a szabálytalanságok megelőzését, feltárását és kivizsgálását, a kárba veszett, nem megfelelően kifizetett vagy helytelenül felhasznált pénzeszközök visszatéríttetését, valamint adott esetben az (EU, Euratom) XXX európai parlamenti és tanácsi rendelet[25] (a továbbiakban: költségvetési rendelet) szerinti közigazgatási és pénzügyi szankciók kiszabását.

---

[24] Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről (HL L 145., 2001.5.31., 43. o.).

[25] [cím és HL-hivatkozás]

(31) A kompetenciaközpontnak nyílt és átlátható módon kell működnie, és ennek keretében valamennyi releváns információt kellő időben rendelkezésre kell bocsátania, valamint gondoskodnia kell tevékenységeinek promóciójáról, többek között a nagyközönséget célzó tájékoztató és ismeretterjesztő kampányok révén. A kompetenciaközpont testületeinek eljárási szabályzatát a nyilvánosság számára hozzáférhetővé kell tenni.

(32) A Bizottság belső ellenőrének ugyanolyan hatásköröket kell gyakorolnia a kompetenciaközpont felett, mint a Bizottság szervezeti egységei felett.

(33) A Bizottság, a kompetenciaközpont, a Számvevőszék és az Európai Csalás Elleni Hivatal számára minden szükséges információhoz és helyszínhez hozzáférést kell biztosítani, hogy lefolytathassák a kompetenciaközpont által aláírt támogatásokra, szerződésekre és megállapodásokra vonatkozó ellenőrzéseket és vizsgálatokat.

(34) Mivel a meglévő, korlátozott erőforrások szétszórtan helyezkednek el és jelentős mértékű beruházásra van szükség, a tagállamok önállóan nem tudják teljes mértékben megvalósítani e rendelet célkitűzéseit, vagyis az EU kiberbiztonsági technológiai és ipari kapacitásaink megőrzését és bővítését, az uniós kiberbiztonsági ipar versenyképességének növelését és a kiberbiztonság versenyelőnnyé kovácsolását más uniós iparágak számára, ugyanakkor e célkitűzések az erőfeszítések felesleges párhuzamosságának elkerülése, a beruházások kritikus tömegének elérése és a közpénzek optimális felhasználásának biztosítása révén hatékonyabban teljesíthetők uniós szinten, az EU jogosult az Európai Unió működéséről szóló szerződés 5. cikkében lefektetett szubszidiaritási elvvel összhangban intézkedéseket hozni. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl a célkitűzések eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

A KOMPETENCIAKÖZPONTRA ÉS A HÁLÓZATRA VONATKOZÓ ÁLTALÁNOS RENDELKEZÉSEK ÉS ALAPELVEK

1. cikk

Tárgy

(1) E rendelet létrehozza az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontot („kompetenciaközpont”) és a nemzeti koordinációs központok hálózatát, továbbá lefekteti a nemzeti koordinációs központok kijelölésének és a kiberbiztonsági kompetenciaközösség kialakításának szabályait.

(2) A kompetenciaközpont hozzájárul az XXX rendelet által létrehozott Digitális Európa program kiberbiztonsági részének, különösen az (EU) XXX rendelet [Digitális Európa program] 6. cikkéhez kapcsolódó tevékenységek végrehajtásához, valamint az XXX rendelet által létrehozott Horizont Európa program, különösen a Horizont Európa kutatási és innovációs keretprogram végrehajtását szolgáló egyedi program létrehozásáról szóló XXX határozat [az egyedi program hivatkozási száma] I. mellékletében szereplő II. pillér 2.2.6. pontjának végrehajtásához.

(3) A kompetenciaközpont székhelye [Brüsszel, Belgium].

(4) A kompetenciaközpont jogi személy. Valamennyi tagállamban az adott tagállam jogszabályai alapján a jogi személyeket megillető legteljesebb jogképességgel rendelkezik. Jogosult különösen ingó és ingatlan vagyont szerezni, illetve azt elidegeníteni, továbbá bírósági eljárásban félként részt venni.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „kiberbiztonság”: a hálózati és információs rendszereknek, azok felhasználóinak, valamint más személyeknek a kiberfenyegetésekkel szembeni védelme;
2. „kiberbiztonsági termékek és megoldások”: olyan IKT-termékek, -szolgáltatások és -eljárások, amelyek kifejezett célja, hogy védelmet nyújtsanak a hálózati és információs rendszereknek, azok felhasználóinak, valamint az érintett személyeknek a kiberfenyegetésekkel szemben;
3. „hatóság”: országos, regionális vagy helyi kormányzati vagy más közigazgatási szerv, ideértve az állami tanácsadó testületeket, valamint a nemzeti jogszabályok alapján közigazgatási funkciókat – ezen belül konkrét feladatokat – ellátó természetes vagy jogi személy;
4. „részt vevő tagállam”: a kompetenciaközpont igazgatási és működési költségeihez önkéntesen pénzügyi hozzájárulást nyújtó tagállam.

3. cikk

A kompetenciaközpont és a hálózat küldetése

(1) A kompetenciaközpont és a hálózat segíti az Uniót abban, hogy:

a) fenntartsa és továbbfejlessze a digitális egységes piac biztonságának garantálásához szükséges kiberbiztonsági technológiai és ipari kapacitásokat;

b) javítsa az uniós kiberbiztonsági ipar versenyképességét, és a kiberbiztonságot versenyelőnnyé tegye a többi uniós iparág számára.

(2) A kompetenciaközpont adott esetben a nemzeti koordinációs központok hálózatával és a kiberbiztonsági kompetenciaközösséggel együttműködésben végzi feladatait.

4. cikk

A központ célkitűzései és feladatai

A kompetenciaközpont célkitűzései és ezekhez kapcsolódó feladatai a következők:

1. elősegíti és segít összehangolni a 6. cikkben említett nemzeti koordinációs központok hálózatának („hálózat”) és a 8. cikkben említett kiberbiztonsági kompetenciaközösségnek a munkáját;
2. hozzájárul az XXX rendelet[26] által létrehozott Digitális Európa program kiberbiztonsági részének, különösen az (EU) XXX rendelet [Digitális Európa program] 6. cikkéhez kapcsolódó tevékenységek végrehajtásához, valamint az XXX

[26] [teljes cím és HL-hivatkozás]

rendelet[27] által létrehozott Horizont Európa program, különösen a Horizont Európa kutatási és innovációs keretprogram végrehajtását szolgáló egyedi program létrehozásáról szóló XXX határozat [az egyedi program hivatkozási száma] I. mellékletében szereplő II. pillér 2.2.6. pontjának végrehajtásához, valamint más uniós programok végrehajtásához, amennyiben azt uniós jogi aktusok előírják;

3. javítja az iparágak, a közszféra és a kutatói közösségek rendelkezésére álló kiberbiztonsági képességeket, ismereteket és infrastruktúrát, az alábbi feladatok ellátása révén:

   a) a legmodernebb kiberbiztonsági ipari és kutatási infrastruktúrát és az ezekhez kapcsolódó szolgáltatásokat figyelembe véve beszerzi, továbbfejleszti, üzemelteti és az EU különböző részein tevékenykedő széles felhasználói réteg – az ipar (ezen belül a kkv-k), a közszféra, valamint a kutatói és tudományos közösség – számára elérhetővé teszi az ilyen jellegű infrastruktúrát és a kapcsolódó szolgáltatásokat;

   b) a legmodernebb kiberbiztonsági ipari és kutatási infrastruktúrát és az ezekhez kapcsolódó szolgáltatásokat figyelembe véve – többek között pénzügyi – támogatást nyújt más szervezeteknek ahhoz, hogy beszerezzék, továbbfejlesszék, üzemeltessék és az EU különböző részein tevékenykedő széles felhasználói réteg – az ipar (ezen belül a kkv-k), a közszféra, valamint a kutatói és tudományos közösség – számára elérhetővé tegyék az ilyen jellegű infrastruktúrát és a kapcsolódó szolgáltatásokat;

   c) kiberbiztonsági ismereteket és technikai támogatást nyújt az ipari szereplők és a hatóságok számára, különösen azáltal, hogy támogatja a hálózatban és a kiberbiztonsági kompetenciaközösségben fellelhető szaktudáshoz való hozzáférés megkönnyítésére irányuló tevékenységeket;

4. hozzájárul a legmodernebb kiberbiztonsági termékek és megoldások széles körű bevezetéséhez a gazdaság minden szegmensében, az alábbi feladatok ellátása révén:

   a) ösztönzi a kiberbiztonsági kutatást, fejlesztést, valamint az uniós kiberbiztonsági termékek és megoldások hatóságok és felhasználó iparágak körében történő bevezetését;

   b) segítséget nyújt a hatóságok, a keresleti oldali iparágak és más felhasználók számára a legújabb kiberbiztonsági megoldások bevezetéséhez és integrálásához;

   c) segítséget nyújt különösen a hatóságok számára a legmodernebb kiberbiztonsági termékekre és megoldásokra irányuló közbeszerzések megszervezéséhez, illetve nevükben lebonyolítja az ilyen jellegű közbeszerzéseket;

   d) pénzügyi támogatást és technikai támogatás nyújt a kiberbiztonság területén tevékenykedő induló vállalkozásoknak és kkv-knek ahhoz, hogy eljussanak a potenciális piacokra és befektetőket szerezzenek;

[27] [teljes cím és HL-hivatkozás]

5. előmozdítja a kiberbiztonság jobb megértését, és hozzájárul a kiberbiztonság terén az Unióban tapasztalható készséghiány csökkentéséhez, az alábbi feladatok ellátása révén:

    a) támogatja a kiberbiztonsági készségek továbbfejlesztését, adott esetben az érintett uniós hivatalokkal és szervekkel (például az ENISA-val) együttműködésben;

6. hozzájárul az uniós kiberbiztonsági kutatás és fejlesztés megerősítéséhez, az alábbiak révén:

    a) meghatároz egy közös, folyamatosan értékelt és fejlesztett többéves stratégiai, ipari, technológiai és kutatási menetrendet, és ennek alapján pénzügyi támogatást nyújt a kiberbiztonság terén zajló kutatási tevékenységekhez;

    b) az iparral és a hálózattal együttműködve támogatja az új generációs kiberbiztonsági technológiai képességekre irányuló nagy léptékű kutatási és demonstrációs projekteket;

    c) támogatja a kiberbiztonsági technológiák szabványosítását célzó kutatást és innovációt;

7. a kiberbiztonság területén fokozza a kettős felhasználású technológiák és alkalmazások terén a polgári és a katonai terület között fennálló együttműködést, az alábbi feladatok ellátása révén:

    a) támogatást nyújt a tagállamoknak, valamint az iparban és a kutatásban tevékenykedő érdekelteknek a kutatáshoz, a fejlesztéshez és a bevezetéshez;

    b) hozzájárul a tagállamok közötti együttműködéshez az oktatás, a képzés és a gyakorlatok támogatásával;

    c) összekapcsolja az érdekelt feleket a polgári és a katonai kiberbiztonsági kutatások és piacok közötti szinergiák növelése érdekében;

8. az Európai Védelmi Alaphoz kapcsolódóan növeli a kiberbiztonság polgári és katonai vetületei közötti szinergiákat, az alábbi feladatok ellátása révén:

    a) tanácsot ad, megosztja a szakértelmet és elősegíti az érintett érdekelt felek közötti együttműködést;

    b) tagállami felkérés esetén több országot érintő kibervédelmi projekteket bonyolít le, így az XXX rendelet [az Európai Védelmi Alapot létrehozó rendelet] értelmében projektmenedzserként jár el.

5. cikk

Beruházás infrastruktúrákba, képességekbe, termékekbe és megoldásokba, és ezek használata

(1) Amennyiben a kompetenciaközpont a 4. cikk 3. és 4. pontja szerint támogatás vagy díj formájában finanszírozást nyújt infrastruktúra, képességek, termékek vagy megoldások előállításához, a kompetenciaközpont munkaterve tartalmazhatja az alábbiakat:

    a) az infrastruktúra vagy képesség működésére vonatkozó szabályok, adott esetben jelezve, hogy a kompetenciaközpont az általa meghatározott feltételek

mellett az adott infrastruktúra vagy képesség üzemeltetését egy üzemeltető szervezetre bízza;

b) az infrastruktúrához vagy képességhez való hozzáférésre és a használatukra vonatkozó szabályok.

(2) A kompetenciaközpont a hálózat tagjai, a kiberbiztonsági kompetenciaközösség tagjai és a kiberbiztonsági termékek és megoldások felhasználóit képviselő más harmadik felek megbízásából a területet érintő közös beszerzési tevékenységek, többek között kereskedelmi hasznosítást megelőző beszerzések általános lebonyolítására is felkérést kaphat. E feladatok teljesítéséhez a kompetenciaközpontnak egy vagy több nemzeti koordinációs központ vagy a kiberbiztonsági kompetenciaközösség tagjai is segítséget nyújthatnak.

6. cikk

A nemzeti koordinációs központok kijelölése

(1) Minden tagállam köteles [dátum]-ig kijelölni azt a szervezetet, amely e rendelet alkalmazásában nemzeti koordinációs központként fog működni, és köteles értesíteni választásáról a Bizottságot.

(2) A Bizottság az adott szervezet (4) bekezdésben meghatározott követelményeknek való megfelelésének értékelése alapján a tagállami értesítést követő 6 hónapon belül meghozza határozatát, amelyben nemzeti koordinációs központként akkreditálja a szervezet, vagy elutasítja a jelölést. A Bizottság közzéteszi a nemzeti koordinációs központok jegyzékét.

(3) A tagállamok bármikor kijelölhetnek az e rendelet alkalmazásában nemzeti koordinációs központként működő új szervezetet. Új szervezet kijelölésekor minden esetben az (1) és (2) bekezdésben foglaltak alkalmazandók.

(4) Olyan szervezetet kell nemzeti koordinációs központnak jelölni, amely alkalmas arra, hogy támogatást nyújtson a kompetenciaközpontnak és a hálózatnak az e rendelet 3. cikkében meghatározott küldetésük teljesítéséhez. A koordinációs központoknak saját kiberbiztonság-technológiai szaktudással vagy ehhez való közvetlen hozzáféréssel kell rendelkezniük, és alkalmasnak kell lenniük az ágazattal, a közszférával és a kutatói közösséggel való hatékony együttműködésre és koordinációra.

(5) A kompetenciaközpont és a nemzeti koordinációs központok közötti kapcsolat alapját a kompetenciaközpont és az egyes nemzeti koordinációs központok által kötött szerződéses megállapodások képezik. E megállapodásoknak tartalmazniuk kell a kompetenciaközpont és az adott nemzeti koordinációs központ közötti kapcsolatot meghatározó szabályokat, valamint a feladatok felosztását a két fél között.

(6) A nemzeti koordinációs központok hálózatát a tagállamok által kijelölt valamennyi nemzeti koordinációs központ együttesen alkotja.

7. cikk

A nemzeti koordinációs központok feladatai

(1) A nemzeti koordinációs központok az alábbi feladatokat látják el:

a) támogatják a kompetenciaközpontot célkitűzései teljesítésében, különösen a kiberbiztonsági kompetenciaközösség koordinálásában;

b) elősegítik a tagállami szintű ipari és más szereplők határokon átnyúló projektekben való részvételét;

c) a kompetenciaközponttal együtt hozzájárulnak az ágazatspecifikus kiberbiztonsági ipari kihívások azonosításához és leküzdéséhez;

d) országos szintű kapcsolattartási pontként szolgálnak a kiberbiztonsági kompetenciaközösség és a kompetenciaközpont számára;

e) igyekeznek szinergiákat kialakítani az érintett nemzeti és regionális szintű tevékenységekkel;

f) végrehajtják a kompetenciaközpont által támogatásban részesített konkrét tevékenységeket, e célból pedig egyebek mellett az adott támogatási megállapodásokban lefektetett feltételek mellett az XXX rendelet [új költségvetési rendelet] 204. cikke szerinti pénzügyi támogatást nyújtanak harmadik feleknek;

g) nemzeti és regionális szinten népszerűsítik és terjesztik a hálózat, a kiberbiztonsági kompetenciaközösség és a kompetenciaközpont munkájának releváns eredményeit;

h) elbírálják a velük azonos tagállamban bejegyzett szervezetek által benyújtott, a kiberbiztonsági kompetenciaközösségbe való felvételre vonatkozó kérvényeket.

(2) Az f) pont alkalmazásában a harmadik feleknek nyújtott pénzügyi támogatás az XXX rendelet [új költségvetési rendelet] 125. cikkében meghatározott formák bármelyikét öltheti, akár egyösszegű támogatás is lehet.

(3) Az XXX rendelet [új költségvetési rendelet] 195. cikkének d) pontja szerint az e cikkben meghatározott feladatok teljesítéséhez a nemzeti koordinációs központok is kaphatnak uniós támogatást.

(4) A nemzeti koordinációs központok az (1) bekezdés a), b), c), e) és g) pontjában említett feladatok végrehajtása érdekében szükség esetén együttműködnek a hálózat többi tagjával.

8. cikk

A kiberbiztonsági kompetenciaközösség

(1) A kiberbiztonsági kompetenciaközösség feladata, hogy támogassa a kompetenciaközpontot a 3. cikkben meghatározott küldetésének teljesítésében, továbbá magasabb szintre emelje és elterjessze a kiberbiztonsági szaktudást az Unióban.

(2) A kiberbiztonsági kompetenciaközösség ipari, tudományos és nonprofit kutatószervezetekből, társulásokból, ezenkívül közigazgatási intézményekből, valamint üzemeltetési és műszaki ügyekkel foglalkozó egyéb szervezetekből áll. Összefogja az Unióban a kiberbiztonsági technológiai és ipari kapacitásokban érdekelt főbb szereplőket. Tevékenységében a nemzeti koordinációs központok, valamint a releváns szaktudással rendelkező uniós intézmények és szervek is részt vesznek.

(3) A kiberbiztonsági kompetenciaközösség akkreditált tagjai csak az Unióban bejegyzett szervezetek lehetnek. A tagoknak igazolniuk kell, hogy kiberbiztonsági szaktudással rendelkeznek legalább az alábbi területek egyikén:

a) kutatás;

b) iparfejlesztés;

c) szakképzés és oktatás.

(4) A kompetenciaközpont azt követően akkreditál a kiberbiztonsági kompetenciaközösség tagjaként egy, a nemzeti jogszabályok szerint bejegyzett szervezetet, hogy a szervezet bejegyzése szerinti tagállamban működő nemzeti koordinációs központ felmérte, hogy a szervezet megfelel-e a (3) bekezdésben szereplő követelményeknek. Az akkreditáció határozatlan időre szól, de a kompetenciaközpont bármikor visszavonhatja, ha a kompetenciaközpont vagy az illetékes nemzeti koordinációs központ úgy ítéli meg, hogy a szervezet már nem felel meg a (3) bekezdésben meghatározott kritériumoknak, vagy az XXX rendelet [új költségvetési rendelet] 136. cikkében szereplő idevágó rendelkezések hatálya alá esik.

(5) A kompetenciaközpont a releváns uniós szerveket és hivatalokat azután akkreditálja a kiberbiztonsági kompetenciaközösség tagjaként, hogy felmérte, hogy azok megfelelnek-e a (3) bekezdésben meghatározott kritériumoknak. Az akkreditáció határozatlan időre szól, de a kompetenciaközpont bármikor visszavonhatja, ha úgy ítéli meg, hogy a szervezet már nem felel meg a (3) bekezdésben meghatározott kritériumoknak, vagy az XXX rendelet [új költségvetési rendelet] 136. cikkében szereplő idevágó rendelkezések hatálya alá esik.

(6) A Bizottság képviselői részt vehetnek a közösség munkájában.

9. cikk

A kiberbiztonsági kompetenciaközösség tagjainak feladatai

A kiberbiztonsági kompetenciaközösség tagjai:

1. támogatják a kompetenciaközpontot a 3. cikkben meghatározott küldetése és a 4. cikkben részletezett célkitűzései teljesítésében, és ebből a célból szorosan együttműködnek a kompetenciaközponttal és az illetékes nemzeti koordinációs központokkal;

2. részt vesznek a kompetenciaközpont és a nemzeti koordinációs központok által népszerűsített tevékenységekben;

3. ha szükséges, részt vesznek azokban a munkacsoportokban, amelyeket a kompetenciaközpont igazgatótanácsa hoz létre a kompetenciaközpont munkatervében kijelölt konkrét feladatok elvégzésére;

4. ha szükséges, támogatják a kompetenciaközpontot és a nemzeti koordinációs központokat konkrét projektek népszerűsítésében;

5. népszerűsítik és terjesztik a közösségen belül zajló tevékenységek és projektek releváns eredményeit.

10. cikk

Együttműködés a kompetenciaközpont és az EU intézményei, szervei és hivatalai között

(1) A kompetenciaközpont együttműködik a releváns uniós intézményekkel, szervekkel és hivatalokkal, köztük az Európai Uniós Hálózat- és Információbiztonsági Ügynökséggel, a hálózatbiztonsági vészhelyzeteket elhárító csoporttal (CERT-EU),

az Európai Külügyi Szolgálattal, a Bizottság Közös Kutatóközpontjával, a Kutatási Tanács Végrehajtó Ügynökségével, az Innovációs és Hálózati Projektek Végrehajtó Ügynökségével, az Europol Számítástechnikai Bűnözés Elleni Európai Központjával és az Európai Védelmi Ügynökséggel.

(2) Az együttműködés mindig munkaszerződések keretei között zajlik. A szerződéseket előzetes jóváhagyásra be kell nyújtani a Bizottsághoz.

II. FEJEZET

A KOMPETENCIAKÖZPONT SZERVEZETI FELÉPÍTÉSE

11. cikk

Tagság és szervezet

(1) A kompetenciaközpont tagsága az Unióból (amelyet a Bizottság képvisel) és a tagállamokból tevődik össze.

(2) A kompetenciaközpont szervezetét az alábbiak alkotják:

a) az igazgatótanács, amely ellátja a 13. cikkben meghatározott feladatokat;

b) az ügyvezető igazgató, aki ellátja a 16. cikkben meghatározott feladatokat;

c) az ipari és tudományos tanácsadó testület, amely ellátja a 20. cikkben meghatározott feladatokat.

I. SZAKASZ

IGAZGATÓTANÁCS

12. cikk

Az igazgatótanács összetétele

(3) Az igazgatótanács a tagállamok egy-egy képviselőjéből és az Uniót képviselő Bizottság öt képviselőjéből áll.

(4) Az igazgatótanács minden egyes tagja rendelkezik egy helyettessel, aki a tagot annak távollétében képviseli.

(5) Az igazgatótanács tagjait és a póttagokat a technológia világában szerzett ismereteik alapján nevezik ki, a megfelelő vezetői, igazgatási és költségvetési készségek figyelembevételével. Az igazgatótanács munkájának folytonosságát biztosítandó a Bizottság és a tagállamok törekednek arra, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban. A Bizottság és a tagállamok törekednek a nők és férfiak igazgatótanácsbeli kiegyensúlyozott képviseletének kialakítására.

(6) Az igazgatótanács tagjai és a póttagok hivatali ideje négy év. A hivatali idő megújítható.

(7) Az igazgatótanács tagjai a kompetenciaközpont érdekében, független és átlátható módon járnak el, őrködnek céljai és küldetése, identitása, önállósága és koherenciája felett.

(8) A Bizottság az igazgatótanács ülésein való részvétel céljából belátása szerint megfigyelőket hívhat meg, ideértve az Unió érintett szerveinek és hivatalainak képviselőit is.

(9) Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) állandó megfigyelői szerepet kap az igazgatótanácsban.

13. cikk

Az igazgatótanács feladatai

(1) Általánosságban az igazgatótanács felel a kompetenciaközpont stratégiai irányításáért és működéséért, és felügyeli a tevékenységeinek végrehajtását.

(2) Az igazgatótanács elfogadja saját eljárási szabályzatát. Az eljárási szabályzatnak konkrét eljárásokat kell tartalmazniuk az összeférhetetlenség azonosítására és elkerülésére, valamint a különleges adatok bizalmas kezelésének biztosítására.

(3) Az igazgatótanács meghozza a szükséges stratégiai döntéseket, nevezetesen:

a) elfogadja a többéves stratégiai tervet, amely a kompetenciaközpont legfontosabb prioritásait és tervezett kezdeményezéseit felvázoló nyilatkozatból, valamint a becsült finanszírozási igények és források ismertetéséből áll;

b) az ügyvezető igazgató által benyújtott javaslat alapján elfogadja a kompetenciaközpont munkatervét, éves beszámolóját, mérlegét és éves tevékenységjelentését;

c) elfogadja a kompetenciaközpontra vonatkozó pénzügyi szabályokat a [költségvetési rendelet 70. cikke] szerint;

d) elfogadja az ügyvezető igazgató kinevezési eljárását;

e) elfogadja a kiberbiztonsági kompetenciaközösségbe jelentkező szervezetek felmérésére és akkreditálására szolgáló követelményeket és eljárásokat;

f) kinevezi és felmenti az ügyvezető igazgatót, meghosszabbítja az ügyvezető igazgató kinevezését, valamint útmutatást nyújt számára és nyomon követi a teljesítményét, továbbá kinevezi a számvitelért felelős tisztviselőt;

g) elfogadja a kompetenciaközpont éves költségvetését, ideértve a vonatkozó létszámtervet is, amely tisztségcsoportok és besorolási fokozatok szerinti bontásban feltünteti az ideiglenes álláshelyek számát, valamint a szerződéses alkalmazottak és a kirendelt nemzeti szakértők teljes munkaidős egyenértékben kifejezett létszámát;

h) elfogadja az összeférhetetlenségre vonatkozó szabályokat;

i) a kiberbiztonsági kompetenciaközösség tagjaival közösen munkacsoportokat állít fel;

j) kinevezi az ipari és tudományos tanácsadó testület tagjait;

k) belső ellenőrzési szervet hoz létre az 1271/2013/EU felhatalmazáson alapuló bizottsági rendelet[28] alapján;

[28] A Bizottság 1271/2013/EU felhatalmazáson alapuló rendelete (2013. szeptember 30.) a 966/2012/EU, Euratom európai parlamenti és tanácsi rendelet 208. cikkében említett szervekre vonatkozó pénzügyi keretszabályzatról (HL L 328., 2013.12.7., 42. o.).

l) nemzetközi szinten népszerűsíti a kompetenciaközpontot, hogy növelje annak vonzerejét, és hogy az a kiberbiztonság terén világszínvonalú szervvé válhasson;

m) az ügyvezető igazgató ajánlása alapján megállapítja a kompetenciaközpont kommunikációs politikáját;

n) felelős az utólagos értékelésekben megfogalmazott következtetések megfelelő nyomon követésének felügyeletéért;

o) adott esetben megállapítja a személyzeti szabályzatra és az alkalmazási feltételekre vonatkozó végrehajtási szabályokat a 31. cikk (3) bekezdésével összhangban;

p) adott esetben meghatározza a nemzeti szakértők kompetenciaközpontba való kirendelésére és a gyakornokok alkalmazására vonatkozó szabályokat, az e rendelet 32. cikkének (2) bekezdésének megfelelően;

q) meghatározza a kompetenciaközpontra vonatkozó biztonsági szabályokat;

r) csalás elleni stratégiát fogad el, amely – figyelemmel a végrehajtandó intézkedések költség-haszon elemzésére – arányos a csalási kockázatokkal;

s) elfogadja a tagállamok pénzügyi hozzájárulásának kiszámítására szolgáló módszereket;

t) felelős minden olyan feladatért, amely nincs kifejezetten a kompetenciaközpont valamely szervéhez rendelve; az ilyen feladatokat a kompetenciaközpont bármely tagjához rendelheti.

14. cikk

Az igazgatótanács elnöke és ülései

(1) Az igazgatótanács a szavazati joggal rendelkező tagok közül elnököt és alelnököt választ, akik megbízatása két évre szól. Az elnök és az alelnök mandátuma az igazgatótanács határozata alapján egyszer meghosszabbítható. Ha azonban igazgatótanácsbeli tagságuk hivatali idejük alatt bármikor megszűnik, ugyanezen a napon hivatali idejük is automatikusan megszűnik. Az elnökhelyettes hivatalból helyettesíti az elnököt abban az esetben, ha az elnök nem tudja ellátni feladatait. Az elnök részt vesz a szavazásban.

(2) Az igazgatótanács évente legalább három alkalommal rendes ülést tart. A testület a Bizottság kérésére rendkívüli üléseket is tarthat, vagy ha legalább tagjainak harmada, az elnök vagy az ügyvezető igazgató feladatainak teljesítése érdekében e mellett dönt.

(3) Az ügyvezető igazgató a tanácskozásokon – az igazgatótanács eltérő határozata hiányában – részt vesz, de szavazati joggal nem rendelkezik. Az igazgatótanács eseti alapon meghívhat más személyeket, hogy ülésein megfigyelőként részt vegyenek.

(4) Az ipari és tudományos tanácsadó testület tagjai az elnök felkérésére szavazati jog nélkül részt vehetnek az igazgatótanács ülésein.

(5) Az igazgatótanács tagjai és a póttagok – az eljárási szabályzatra figyelemmel – tanácsadók és szakértők segítségét is igénybe vehetik az üléseken.

(6) Az igazgatótanács titkárságát a kompetenciaközpont biztosítja.

15. cikk

Az igazgatótanács szavazási szabályai

(1) Az Unió a szavazati jogok 50 %-át birtokolja. Az Unió szavazati joga nem osztható meg.

(2) Minden résztvevő tagállam egy szavazattal rendelkezik.

(3) Az igazgatótanács az összes szavazat legalább 75 %-os többségével hozza meg határozatait, amelybe beletartoznak a távollévő tagok szavazatai is, tehát azok a határozatok érvényesek, amelyeket a kompetenciaközponthoz pénzügyi hozzájárulást biztosító felek legalább 75 %-a támogat. A pénzügyi hozzájárulás kiszámításának alapját a tagállamok által javasolt becsült kiadások (lásd a 17. cikk (2) bekezdésének c) pontját), valamint a részt vevő tagállamok hozzájárulásának értékét meghatározó jelentés (lásd a 22. cikk (5) bekezdését) képezi.

(4) Szavazati joggal kizárólag a Bizottság képviselői és a részt vevő tagállamok képviselői rendelkeznek.

(5) Az elnök részt vesz a szavazásban.

II. SZAKASZ

ÜGYVEZETŐ IGAZGATÓ

16. cikk

Az ügyvezető igazgató kinevezése, felmentése, valamint megbízatásának meghosszabbítása

(1) Az ügyvezető igazgató a kompetenciaközpont működési területén tapasztalattal és nagy tekintéllyel rendelkező személy.

(2) Az ügyvezető igazgató az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 2. cikkének a) pontja értelmében a kompetenciaközpont ideiglenes alkalmazottjaként látja el feladatkörét.

(3) Az ügyvezető igazgatót az igazgatótanács nevezi ki, a Bizottság által egy nyílt és átlátható kiválasztási eljárást követően összeállított jelöltlistáról.

(4) Az ügyvezető igazgatói szerződés megkötése során a kompetenciaközpontot az igazgatótanács elnöke képviseli.

(5) Az ügyvezető igazgató hivatali ideje négy év. Ezen időszak lejárta előtt a Bizottság értékelést készít, amely figyelembe veszi az ügyvezető igazgató teljesítményét, valamint a kompetenciaközpont jövőbeni feladatait és az előtte álló kihívásokat.

(6) Az igazgatótanács az (5) bekezdésben említett értékelést figyelembe vevő bizottsági javaslat alapján eljárva az ügyvezető igazgató hivatali idejét egy alkalommal, legfeljebb négy évre meghosszabbíthatja.

(7) Az az ügyvezető igazgató, akinek hivatali idejét már meghosszabbították, nem vehet részt az ugyanazon tisztség betöltését célzó kiválasztási eljárásban.

(8) Az ügyvezető igazgató csak a Bizottság javaslata alapján, az igazgatótanács által hozott határozattal menthető fel.

17. cikk

Az ügyvezető igazgató feladatai

(1) Az ügyvezető igazgató felelős a kompetenciaközpont működéséért, napi ügyvezetéséért, és ő a kompetenciaközpont törvényes képviselője. Az ügyvezető igazgató az igazgatótanácsnak tartozik elszámolással, és a rá ruházott hatáskörön belül teljes mértékben független módon végzi feladatát.

(2) Az ügyvezető igazgató mindenekelőtt a következő feladatokat hajtja végre, függetlenül eljárva:

a) végrehajtja az igazgatótanács által elfogadott határozatokat;

b) segíti az igazgatótanács munkáját, és üléseik idejére biztosítja a titkári feladatok ellátását, valamint a feladataik ellátáshoz szükséges valamennyi információt biztosítja számukra;

c) az igazgatótanáccsal és a Bizottsággal való konzultációt követően elkészíti és az igazgatótanács elé terjeszti jóváhagyásra a kompetenciaközpont többéves stratégiai tervének és éves munkatervének tervezetét, amely tartalmazza a munkaterv végrehajtásához szükséges ajánlattételi felhívások, részvételi szándék kifejezésére való felhívások és ajánlati felhívások hatókörét, valamint az ezeknek megfelelő, a tagállamok és a Bizottság által javasolt kiadási előirányzatokat;

d) elkészíti és az igazgatótanács elé terjeszti jóváhagyásra az éves költségvetési tervet, ideértve a létszámtervet is, amely csoportok és besorolási fokozatok szerinti bontásban tünteti fel az ideiglenes álláshelyek számát, valamint a szerződéses alkalmazottak és a kirendelt nemzeti szakértők teljes munkaidős egyenértékben kifejezett létszámát;

e) végrehajtja a munkatervet, és jelentést tesz erről az igazgatótanácsnak;

f) elkészíti a kompetenciaközpont éves tevékenységi jelentésének tervezetét, amely tartalmazza a vonatkozó kiadások adatait is;

g) garantálja a kompetenciaközpont teljesítményére vonatkozó hatékony felügyeleti és értékelési eljárások végrehajtását;

h) az utólagos értékelések következtetéseinek alapján elkészíti a cselekvési tervet, és kétévente beszámol a Bizottságnak az eredményekről;

i) előkészíti, letárgyalja és megköti a szerződéseket a nemzeti koordinációs központokkal;

j) felelősséget vállal az igazgatási, pénzügyi és személyzeti ügyekért, egyebek mellett – az igazgatótanács által ráruházott jogkörök korlátain belül – a kompetenciaközpont költségvetésének végrehajtásáért, kellő figyelmet fordítva a belső ellenőrzési szervtől kapott tanácsokra;

k) a munkatervvel összhangban jóváhagyja és felügyeli az ajánlattételi felhívások közzétételét, továbbá adminisztrálja a támogatási megállapodásokat és határozatokat;

l) jóváhagyja a finanszírozásra kiválasztott intézkedések listáját egy független szakértői csoport által összeállított ranglista alapján;

m) a munkatervvel összhangban jóváhagyja és felügyeli az ajánlati felhívások közzétételét, és adminisztrálja a szerződéseket;

n) jóváhagyja a finanszírozásra kiválasztott ajánlatokat;

o) benyújtja az éves beszámoló és mérleg tervezetét a belső ellenőrzési szervnek, majd azt követően az igazgatótanácsnak;

p) gondoskodik a kockázatértékelésről és a kockázatkezelésről;

q) aláírja az egyes támogatási megállapodásokat, határozatokat és szerződéseket;

r) aláírja a beszerzési szerződéseket;

s) elkészíti a cselekvési tervet a belső és külső ellenőrzési jelentésekből, valamint az Európai Csalás Elleni Hivatal (OLAF) vizsgálataiból származó megállapítások nyomán meghozandó intézkedésekről, évente két alkalommal jelentést tesz az eredményekről a Bizottságnak, valamint rendszeresen az igazgatótanácsnak;

t) elkészíti a kompetenciaközpontra alkalmazandó pénzügyi szabályzat tervezetét;

u) kialakít egy eredményes és hatékony belső ellenőrzési rendszert, és gondoskodik annak működtetéséről, valamint tájékoztatja az igazgatótanácsot az ellenőrzési rendszert érintő jelentős változásokról;

v) biztosítja az uniós intézményekkel folytatott hatékony kommunikációt;

w) meghoz minden egyéb intézkedést, amelyek révén felmérhető a kompetenciaközpont előrehaladása az e rendelet 3. és 4. cikkében meghatározott küldetés és célkitűzések teljesítése terén;

x) elvégzi az igazgatótanács által rábízott vagy láruházott feladatokat.

III. SZAKASZ

AZ IPARI ÉS TUDOMÁNYOS TANÁCSADÓ TESTÜLET

18. cikk

Az ipari és tudományos tanácsadó testület összetétele

(1) Az ipari és tudományos tanácsadó testület legfeljebb 16 tagból áll. Tagjait az igazgatótanács nevezi ki a kiberbiztonsági kompetenciaközösséget alkotó szervezetek képviselői közül.

(2) Az ipari és tudományos tanácsadó testület tagjai szakértelemmel rendelkeznek a kiberbiztonsági kutatások, az ipari fejlesztések, a professzionális szolgáltatások vagy ezek bevezetése terén. Az e szakértelemre vonatkozó részletes követelményeket az igazgatótanács határozza meg.

(3) A tanácsadó testület tagjainak az igazgatótanács általi kinevezésére, valamint a tanácsadó testület működésére vonatkozó eljárásokat a kompetenciaközpont eljárási szabályzatában kell meghatározni, és nyilvánosságra kell hozni.

(4) Az ipari és tudományos tanácsadó testület tagjainak hivatali ideje három év. A hivatali idő megújítható.

(5) A Bizottság és az Európai Uniós Hálózat- és Információbiztonsági Ügynökség képviselői részt vehetnek az ipari és tudományos tanácsadó testület munkájában, valamint támogathatják azt.

19. cikk

Az ipari és tudományos tanácsadó testület működése

(1) Az ipari és tudományos tanácsadó testület legalább évente kétszer ülésezik.

(2) Az ipari és tudományos tanácsadó testület tanácsot adhat az igazgatótanácsnak a kompetenciaközpont tevékenységét érintő konkrét kérdésekkel foglalkozó munkacsoportok létrehozásáról, amit szükség esetén az ipari és tudományos tanácsadó testület egy vagy több tagja koordinál.

(3) Az ipari és tudományos tanácsadó testület maga választja meg elnökét.

(4) Az ipari és tudományos tanácsadó testület elfogadja saját eljárási szabályzatát, beleértve az adott esetben a tanácsadó testületet képviselő személyek kinevezését és kinevezésük időtartamát is.

20. cikk

Az ipari és tudományos tanácsadó testület feladatai

Az ipari és tudományos tanácsadó testület tanácsot ad a kompetenciaközpontnak az általa végzett különböző tevékenységekkel kapcsolatban, továbbá:

1. az igazgatótanács által megszabott határidőkig benyújtja stratégiai tanácsait és észrevételeit az ügyvezető igazgatónak és az igazgatótanácsnak a munkaterv és a többéves stratégiai terv kidolgozásához;
2. a kiberbiztonság területén érdekelt, köz- és magánszférában tevékenykedő felek számára egyaránt nyitva álló nyilvános konzultációkat szervez, és így beszerzi az 1. pontban említett stratégiai tanácsadáshoz szükséges információkat;
3. népszerűsíti a kompetenciaközpont munkatervét és többéves stratégiai tervét, és visszajelzéseket gyűjt arról.

III. FEJEZET

PÉNZÜGYI RENDELKEZÉSEK

21. cikk

Az EU pénzügyi hozzájárulása

(1) Az Unió az alábbiakkal járul hozzá a kompetenciaközpont igazgatási és üzemeltetési költségeinek fedezéséhez:

a) 1 981 668 000 EUR a Digitális Európa programból, ezen belül legfeljebb 23 746 000 EUR igazgatási költségekre;

b) a Horizont Európa programból biztosított összeg, többek között az igazgatási költségek fedezésére, amely az XXX rendelet [a Horizont Európa rendelet] 6. cikkének (6) bekezdése szerint végzendő stratégiai tervezési folyamat figyelembevételével kerül meghatározásra.

(2) A teljes uniós hozzájárulás az Unió általános költségvetéséből a [Digitális Európa program] és az XXX határozat által létrehozott Horizont Európa programot végrehajtó program számára elkülönített előirányzatokból fizetendő ki.

(3) A kompetenciaközpont a [Digitális Európa program] és a [Horizont Európa program] kiberbiztonsági tevékenységeit az (EU, Euratom) XXX rendelet[29] [költségvetési rendelet] 62. cikke c) pontjának iv. alpontjában leírtaknak megfelelően hajtja végre.

(4) Az uniós pénzügyi hozzájárulás nem fordítható a 4. cikk 8. b) pontjában szereplő feladatokra.

22. cikk

A részt vevő tagállamok hozzájárulása

(1) A részt vevő tagállamok kötelesek összesen legalább az e rendelet 21. cikkének (1) bekezdésében szereplő összegekkel azonos mértékben hozzájárulni a kompetenciaközpont működtetési és igazgatási költségeihez.

(2) Az (1) bekezdésben és a 23. cikk (3) bekezdése b) pontjának ii. alpontjában említett hozzájárulások felméréséhez a költségeket az érintett tagállam szokásos költségelszámolási gyakorlatának, a tagállamban alkalmazandó számviteli standardoknak és az alkalmazandó nemzetközi számviteli standardoknak és nemzetközi pénzügyi beszámolási standardoknak megfelelően kell megállapítani. A költségeket az érintett tagállam által kijelölt független külső könyvvizsgálónak kell igazolnia. Fennmaradó bizonytalanságok esetén a kompetenciaközpont ellenőrizheti az értékmegállapítás céljára alkalmazott módszert.

(3) Amennyiben valamely részt vevő tagállam nem teljesíti a pénzügyi hozzájárulásra vonatkozó kötelezettségvállalását, az ügyvezető igazgató erről írásban értesíti a tagot, és észszerű határidőt állapít meg a mulasztás pótlására. Amennyiben a mulasztás pótlására a megadott határidőn belül nem kerül sor, az ügyvezető igazgató összehívja az igazgatótanácsot annak eldöntésére, hogy a mulasztást elkövető részt vevő tagállam szavazati jogát felfüggesszék-e, vagy egyéb intézkedésre kerüljön-e sor, amíg a kötelezettségei teljesítése meg nem történik. A nem fizető tagállam szavazati jogát mindaddig felfüggesztik, amíg ismét teljesíti kötelezettségét.

(4) A Bizottság jogosult megszüntetni, arányosan csökkenteni vagy felfüggeszteni a kompetenciaközpont számára biztosított uniós pénzügyi hozzájárulást, amennyiben a részt vevő tagállamok nem fizetik be, csak részlegesen fizetik be vagy késedelmesen fizetik be az (1) bekezdésben részletezett hozzájárulást.

(5) A részt vevő tagállamok kötelesek minden év január 31-ig jelentést tenni az igazgatótanácsnak az előző pénzügyi évben teljesített, (1) bekezdés szerinti hozzájárulásuk értékéről.

23. cikk

A kompetenciaközpont költségei és erőforrásai

(1) A kompetenciaközpont finanszírozását az Unió és a tagállamok közösen biztosítják részletekben fizetett pénzügyi hozzájárulások, valamint a nemzeti koordinációs központok és a kedvezményezettek által megvalósított, a kompetenciaközpont támogatásában nem részesülő tevékenységek költségeiből álló hozzájárulások formájában.

(2) A kompetenciaközpont igazgatási költségei nem haladhatják meg a(z) [szám] EUR-t; ezt az összeget az Unió és a részt vevő tagállamok által fizetett, köztük éves alapon

[29] [teljes cím és HL-hivatkozás]

egyenlően megosztott pénzügyi hozzájárulások biztosítják. Amennyiben az igazgatási költségekre szánt hozzájárulás egy része nem kerül felhasználásra, az a kompetenciaközpont működési költségeire fordítható.

(3) A kompetenciaközpont működési költségeit az alábbiak fedezik:

a) az Unió pénzügyi hozzájárulása;

b) a részt vevő tagállamok által az alábbi formában biztosított hozzájárulások:

i. pénzügyi hozzájárulások; valamint

ii. adott esetben a részt vevő tagállamoknak a nemzeti koordinációs központok és a kedvezményezettek által végzett közvetett tevékenységek során felmerült költségekhez való természetbeni hozzájárulásai, amelyek nem foglalják magukban a kompetenciaközpont és más uniós felek e költségekhez való hozzájárulását;

(4) A kompetenciaközpont költségvetését alkotó források az alábbi hozzájárulásokból állnak:

a) a részt vevő tagállamok pénzügyi hozzájárulásai az igazgatási költségekhez;

b) a részt vevő tagállamok pénzügyi hozzájárulásai az üzemeltetési költségekhez;

c) a kompetenciaközpont által generált bevételek;

d) bármely más pénzügyi hozzájárulás, forrás és bevétel.

(5) A részt vevő tagállamok által a kompetenciaközpontnak fizetett hozzájárulások kamata a kompetenciaközpont bevételének tekintendő.

(6) A kompetenciaközpont minden erőforrásával és tevékenységével a 4. cikkben lefektetett célkitűzések elérésén munkálkodik.

(7) Az általa létrehozott, vagy a célkitűzéseinek teljesítése céljából ráruházott eszközök a kompetenciaközpont tulajdonát képezik.

(8) A kompetenciaközpont végelszámolásának az esetét kivéve a bevétel kiadásokat meghaladó része nem kerül kifizetésre a kompetenciaközpont munkájában részt vevő tagállamoknak.

24. cikk

Pénzügyi kötelezettségvállalások

A kompetenciaközpont pénzügyi kötelezettségvállalásai nem haladhatják meg a rendelkezésre álló vagy a költségvetése számára a tagjai által lekötött pénzügyi források összegét.

25. cikk

Pénzügyi év

A pénzügyi év január 1-jétől december 31-ig tart.

26. cikk

A költségvetés megállapítása

(1) Az ügyvezető igazgató minden évben elkészíti és a létszámterv tervezetével együtt továbbítja az igazgatótanácsnak a kompetenciaközpont következő pénzügyi évre tervezett bevételeire és kiadásaira vonatkozó kimutatás tervezetét. A bevételeknek és kiadásoknak egyensúlyban kell lenniük. A kompetenciaközpont kiadásai magukban foglalják a személyzeti, adminisztratív, infrastrukturális és működési költségeket. Az adminisztratív költségeket minimális szinten kell tartani.

(2) Az igazgatótanács a tervezett bevételekről és kiadásokról szóló kimutatás (1) bekezdésben említett tervezete alapján minden évben elkészíti a kompetenciaközpont következő költségvetési évre vonatkozó tervezett bevételeiről és kiadásairól szóló kimutatást.

(3) Az igazgatótanács minden év január 31-ig benyújtja a Bizottságnak a (2) bekezdésben említett kimutatástervezetet, amely az egységes programozási dokumentum tervezetének részévé válik.

(4) A Bizottság e kimutatástervezet alapján bevezeti az Unió költségvetésének tervezetébe a létszámtervhez szükségesnek ítélt becsléseket és az általános költségvetést terhelő hozzájárulás összegét, majd az EUMSZ 313. és 314. cikkének megfelelően a tervezetet benyújtja az Európai Parlamentnek és a Tanácsnak.

(5) Az Európai Parlament és a Tanács engedélyezi a kompetenciaközpontnak nyújtandó hozzájárulás előirányzatait.

(6) Az Európai Parlament és a Tanács elfogadja a kompetenciaközpont létszámtervét.

(7) Az igazgatótanács a munkatervvel együtt elfogadja a kompetenciaközpont költségvetését. A költségvetés az Unió általános költségvetésének végleges elfogadásával válik véglegessé. Az igazgatótanács a kompetenciaközpont költségvetését és munkaprogramját szükség szerint az Unió általános költségvetéséhez igazítja.

27. cikk

A kompetenciaközpont elszámolásainak benyújtása és a mentesítés

A kompetenciaközpont előzetes és végleges elszámolásainak benyújtása és a mentesítés során be kell tartani a költségvetési rendelet és a 29. cikk értelmében bevezetett saját pénzügyi szabályzata által meghatározott szabályokat és határidőket.

28. cikk

Operatív és pénzügyi beszámolás

(1) Az ügyvezető igazgató minden évben jelentést készít az igazgatótanács részére feladatainak a kompetenciaközpont pénzügyi szabályzata szerinti teljesítéséről.

(2) Az ügyvezető igazgató a pénzügyi év lezárásától számított két hónapon belül jóváhagyásra az igazgatótanács elé terjeszti a kompetenciaközpont által az előző naptári évben – különösen az adott évre szóló éves munkatervhez képest – elért eredményekről szóló éves tevékenységi jelentést. A jelentésben tájékoztatást ad többek között az alábbiakról:

a) üzemeltetési intézkedések és az azokhoz kapcsolódó ráfordítások;

b) a benyújtott tevékenységek a résztvevők típusa – a kkv-kat is beleértve – és tagállamok szerinti bontásban;

c) a finanszírozásra kiválasztott tevékenységek a résztvevők típusa – a kkv-kat is beleértve – és tagállamok szerinti bontásban, feltüntetve a kompetenciaközpontnak az egyes résztvevők és tevékenységek számára juttatott hozzájárulását;

d) előrelépés a 4. cikkben meghatározott célkitűzések elérése felé, és az e célkitűzések eléréséhez szükséges további munkára vonatkozó javaslatok.

(3) Az igazgatótanács által jóváhagyott éves tevékenységi jelentést nyilvánosan elérhetővé kell tenni.

29. cikk

Pénzügyi szabályzat

A kompetenciaközpont az XXX rendelet [új költségvetési rendelet] 70. cikkében szereplő előírásoknak megfelelően elfogadja saját pénzügyi szabályzatát.

30. cikk

A pénzügyi érdekek védelme

(1) A kompetenciaközpont megfelelő intézkedésekkel – csalás, korrupció és más jogellenes cselekmények elleni megelőző intézkedésekkel, hatásos ellenőrzésekkel, szabálytalanság feltárása esetén a jogtalanul kifizetett összegek visszafizettetésével, valamint szükség esetén hatékony, arányos és visszatartó erejű közigazgatási szankciókkal – biztosítja, hogy az Európai Unió pénzügyi érdekei az e rendelet alapján finanszírozott cselekvések végrehajtása során ne sérüljenek.

(2) A kompetenciaközpontnak a Bizottság alkalmazottai, valamint a Bizottság által felhatalmazott más személyek, illetve a Számvevőszék számára hozzáférést kell biztosítania a telephelyeihez és helyiségeihez, továbbá az ellenőrzések elvégzéséhez szükséges valamennyi információhoz, az elektronikus információkat is ideértve.

(3) A 2185/96/Euratom, EK tanácsi rendeletben[30] és a 883/2013/EU, Euratom európai parlamenti és tanácsi rendeletben[31] megállapított rendelkezéseknek és eljárásoknak megfelelően az Európai Csalás Elleni Hivatal (OLAF) vizsgálatokat, köztük helyszíni ellenőrzéseket és egyéb ellenőrzéseket végezhet annak megállapítása érdekében, hogy az e rendelettel összhangban finanszírozott támogatási megállapodással, illetve közvetve vagy közvetlenül támogatott szerződéssel kapcsolatban csalás, korrupció vagy bármely egyéb jogellenes tevékenység révén sérültek-e az Unió pénzügyi érdekei.

(4) E cikk (1), (2) és (3) bekezdésében foglaltak sérelme nélkül az e rendelet végrehajtásának eredményeként létrejövő szerződéseknek és támogatási megállapodásoknak tartalmazniuk kell olyan rendelkezéseket, amelyek kifejezetten felhatalmazzák a Bizottságot, a kompetenciaközpontot, a Számvevőszéket és az

[30] A Tanács 2185/96/Euratom, EK rendelete (1996. november 11.) az Európai Közösségek pénzügyi érdekeinek csalással és egyéb szabálytalanságokkal szembeni védelmében a Bizottság által végzett helyszíni ellenőrzésekről és vizsgálatokról (HL L 292., 1996.11.15., 2. o.).

[31] Az Európai Parlament és a Tanács 883/2013/EU, Euratom rendelete (2013. szeptember 11.) az Európai Csalás Elleni Hivatal (OLAF) által lefolytatott vizsgálatokról, valamint az 1073/1999/EK európai parlamenti és tanácsi rendelet és az 1074/1999/Euratom tanácsi rendelet hatályon kívül helyezéséről (HL L 248., 2013.9.18., 1. o.).

Európai Csalás Elleni Hivatalt az ilyen ellenőrzések és vizsgálatok hatáskörüknek megfelelően történő elvégzésére. Amennyiben valamely cselekvés végrehajtását részben vagy egészben kiszervezték vagy azzal mást bíztak meg, vagy amennyiben az közbeszerzési szerződés vagy pénzügyi támogatás harmadik félnek való odaítélését igényli, a szerződésben, illetőleg a támogatási megállapodásban rendelkezni kell a szerződő fél vagy a kedvezményezett azon kötelezettségéről, hogy az érintett harmadik felekkel kifejezetten elfogadtassa a Bizottság, a kompetenciaközpont, a Számvevőszék és az Európai Csalás Elleni Hivatal említett hatáskörét.

IV. FEJEZET

A KOMPETENCIAKÖZPONT SZEMÉLYI ÁLLOMÁNYA

31. cikk

Személyi állomány

(1) A kompetenciaközpont személyi állományára a Tisztviselők személyzeti szabályzata (a „személyzeti szabályzat”) és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételek (az „alkalmazási feltételek”) – amelyeket a 259/68/EGK, Euratom, ESZAK tanácsi rendelet[32] állapított meg –, valamint a személyzeti szabályzat és az alkalmazási feltételek alkalmazása céljából az uniós intézmények által együttesen elfogadott szabályok alkalmazandók.

(2) A kompetenciaközpont személyi állományának vonatkozásában az igazgatótanács gyakorolja a személyzeti szabályzat értelmében kinevezésre jogosult hatóságra ruházott hatásköröket, valamint az alkalmazási feltételek értelmében a szerződéskötési jogosultsággal rendelkező hatóságra ruházott hatásköröket (a „kinevezésre jogosult hatóság hatáskörei”).

(3) A személyzeti szabályzat 110. cikke szerint az igazgatótanács határozatot fogad el a személyzeti szabályzat 2. cikkének (1) bekezdése és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 6. cikke alapján, amelyben a kinevezésre jogosult hatóság megfelelő hatásköreit átruházza az ügyvezető igazgatóra, és meghatározza az említett átruházás felfüggesztésére vonatkozó feltételeket. Az ügyvezető igazgató felhatalmazást kap e hatáskör további átruházására.

(4) Amennyiben kivételes körülmények szükségessé teszik, az igazgatótanács határozat útján ideiglenesen felfüggesztheti a kinevezésre jogosult hatóság hatásköreinek az ügyvezető igazgatóra történő átruházását, illetve az ügyvezető igazgató általi további átruházást. Ilyen esetben az igazgatótanács a kinevezésre jogosult hatóság hatáskörét maga gyakorolja, vagy azt az ügyvezető igazgatótól eltérő, valamely más tagjára vagy a kompetenciaközpont személyi állományának valamely más tagjára ruházhatja.

(5) Az igazgatótanács a személyzeti szabályzat 110. cikkével összhangban végrehajtási szabályokat fogad el a személyzeti szabályzat és az alkalmazási feltételek tekintetében.

[32] A Tanács 259/68/EGK, Euratom, ESZAK rendelete (1968. február 29.) az Európai Közösségek tisztviselőinek személyzeti szabályzatáról, egyéb alkalmazottainak alkalmazási feltételeiről, valamint a Bizottság tisztviselőire ideiglenesen alkalmazandó különleges intézkedések bevezetéséről (HL L 56., 1968.3.4., 1. o.).

(6) A személyi erőforrásokat a kompetenciaközpont létszámtervében kell meghatározni, az éves költségvetésnek megfelelően tisztségcsoportok és besorolási fokozatok szerinti bontásban feltüntetve az ideiglenes álláshelyek számát, valamint a szerződéses alkalmazottak teljes munkaidős egyenértékben kifejezett létszámát.

(7) A kompetenciaközpont személyi állománya ideiglenes alkalmazottakból és szerződéses alkalmazottakból áll.

(8) A személyi állománnyal kapcsolatos minden költséget a kompetenciaközpont visel.

32. cikk

Kirendelt nemzeti szakértők és egyéb alkalmazottak

(1) A kompetenciaközpont igénybe vehet kirendelt nemzeti szakértőket és egyéb, nem a kompetenciaközpont alkalmazásában álló személyzetet.

(2) Az igazgatótanács a Bizottsággal egyetértésben határozatot fogad el a nemzeti szakértők kompetenciaközponthoz történő kirendelése szabályainak megállapításáról.

33. cikk

Kiváltságok és mentességek

A kompetenciaközpontra és személyi állományára az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyv alkalmazandó.

V. FEJEZET
KÖZÖS RENDELKEZÉSEK

34. cikk

Biztonsági szabályok

(1) A kompetenciaközpont által finanszírozott minden tevékenységben való részvételre az (EU) XXX rendelet [a Digitális Európa program] 12. cikkének (7) bekezdése alkalmazandó.

(2) A Horizont Európa program keretében finanszírozott tevékenységekre külön biztonsági szabályok alkalmazandók:

a) az (EU) XXX rendelet [a Horizont Európa program] 34. cikke (1) bekezdésének [Tulajdon és védelem] alkalmazásában, amennyiben a munkaterv rendelkezik erről, a nem kizárólagos engedélyek odaítélése a tagállamokban bejegyzett vagy bejegyzettnek minősülő harmadik felekre korlátozható, valamint a tagállamok és/vagy tagállami állampolgárok által ellenőrizhető;

b) az (EU) XXX rendelet [a Horizont Európa program] 36. cikke (4) bekezdésének b) pontja [Átruházás és engedélyezés] alkalmazásában, az eredmények tulajdonjogának átruházása vagy az eredményekre vonatkozó kizárólagos engedély odaítélése ellen azon az alapon is kifogás emelhető, hogy az átruházás vagy az engedélyezés alanya egy társult országban bejegyzett

vagy az Unió területén bejegyzett, de harmadik országból irányított jogi személy;

c) az (EU) XXX rendelet [a Horizont Európa program] 37. cikke (3) bekezdése a) pontjának [Hozzáférési jogok] alkalmazásában, amennyiben a munkaterv rendelkezik erről, az eredményekhez és azok háttérhez való hozzáférés biztosítása a tagállamokban bejegyzett vagy bejegyzettnek minősülő jogi személyekre korlátozható, valamint a tagállamok és/vagy tagállami állampolgárok által ellenőrizhető;

35. cikk

Átláthatóság

(1) A kompetenciaközpont valamennyi tevékenységét magas fokú átláthatósággal végzi.

(2) A kompetenciaközpont biztosítja, hogy a nyilvánosság és minden érdekelt fél – különösen a kompetenciaközpont munkájának eredményeiről – megfelelő, tárgyilagos, megbízható és könnyen hozzáférhető tájékoztatást kapjon. A kompetenciaközpont továbbá köteles a nyilvánosság elé tárni a 41. cikkel összhangban tett érdekeltségi nyilatkozatokat.

(3) Az igazgatótanács az ügyvezető igazgató javaslatára engedélyezheti, hogy meghatározott érdekelt felek a kompetenciaközpont egyes tevékenységeiben megfigyelőként részt vegyenek.

(4) A kompetenciaközpont eljárási szabályzatában megállapítja az (1) és (2) bekezdésben említett átláthatósági szabályok végrehajtására vonatkozó gyakorlati intézkedéseket. A Horizont Európa program által finanszírozott intézkedések esetében figyelembe kell venni a Horizont Európa rendelet III. mellékletében szereplő előírásokat is.

36. cikk

A minősített adatok és a nem minősített különleges adatok védelmére vonatkozó biztonsági szabályok

(1) A 35. cikk sérelme nélkül a kompetenciaközpont nem adhatja tovább harmadik felek részére az általa kezelt vagy hozzá beérkezett olyan információkat, amelyek tekintetében indokolással ellátott kérelmet nyújtottak be teljes vagy részben bizalmas kezelés iránt.

(2) Az igazgatótanács tagjai, az ügyvezető igazgató, az ipari és tudományos tanácsadó testület tagjai, az eseti munkacsoportok tevékenységében részt vevő külső szakértők és a kompetenciaközpont személyzetének tagjai még feladataik megszűnését követően is az Európai Unió működéséről szóló szerződés 339. cikke szerinti titoktartási kötelezettségek hatálya alá tartoznak.

(3) A kompetenciaközpont igazgatótanácsa a bizottsági jóváhagyást követően elfogadja a kompetenciaközpont biztonsági szabályait, amelyek alapját az EU-minősített adatok és a nem minősített különleges adatok védelmét szolgáló bizottsági biztonsági szabályokban megfogalmazott elvek és előírások, többek között az (EU, Euratom)

2015/443[33] és az (EU, Euratom) 2015/444[34] bizottsági határozatban szereplő, az ilyen adatok kezelésére és tárolására vonatkozó rendelkezések képezik.

(4) A kompetenciaközpont minden szükséges intézkedést megtehet annak érdekében, hogy megkönnyítse a feladatai szempontjából lényeges adatoknak a Bizottsággal és a tagállamokkal, és adott esetben az érintett uniós hivatalokkal és szervekkel történő cseréjét. Az ebből a célból az EU-minősített adatok megosztására vonatkozóan kötött igazgatási megállapodásokhoz, valamint ilyen megállapodások hiányában az EU-minősített adatok rendkívüli eseti átadásához minden esetben ki kell kérni a Bizottság előzetes jóváhagyását.

37. cikk

Dokumentumokhoz való hozzáférés

(1) A kompetenciaközpont birtokában lévő dokumentumokra alkalmazni kell az 1049/2001/EK rendeletet.

(2) Az igazgatótanács a kompetenciaközpont létrejöttét követően hat hónapon belül elfogadja az 1049/2001/EK rendelet végrehajtására vonatkozó rendelkezéseket.

(3) A kompetenciaközpont által az 1049/2001/EK rendelet 8. cikke alapján hozott határozatok ellen az Európai Unió működéséről szóló szerződés 228. cikke értelmében panasszal lehet fordulni az ombudsmanhoz, valamint az Európai Unió működéséről szóló szerződés 263. cikke szerint keresetet lehet benyújtani az Európai Unió Bíróságához.

38. cikk

Felügyelet, értékelés és felülvizsgálat

(1) A kompetenciaközpont köteles folyamatos és módszeres ellenőrzésnek, valamint rendszeres értékeléseknek alávetni minden tevékenységét, ideértve a nemzeti koordinációs központokon és a hálózaton keresztül irányított tevékenységeket is. A kompetenciaközpont biztosítja a felügyeleti program végrehajtására és eredményeire vonatkozó adatok hatékony, eredményes és időszerű összegyűjtését, valamint hogy az uniós támogatásban részesülő kedvezményezettekre és a tagállamokra arányos adatszolgáltatási kötelezettség háruljon. Az értékelés eredményét nyilvánosságra kell hozni.

(2) Amikor már elegendő információ áll rendelkezésre e rendelet végrehajtásáról, de legkésőbb három és fél évvel a rendelet végrehajtásának megkezdését követően a Bizottság elvégzi a kompetenciaközpont időközi értékelését. A Bizottság jelentést készít erről az értékelésről, és 2024. december 31-ig benyújtja azt az Európai Parlamentnek és a Tanácsnak. A kompetenciaközpont és a tagállamok ellátják a Bizottságot a jelentés elkészítéséhez szükséges információkkal.

(3) A (2) bekezdésben említett értékelés keretében fel kell mérni a kompetenciaközpont által elért eredményeket a számára meghatározott célok, megbízatás és feladatok tükrében. Amennyiben a Bizottság indokoltnak tartja a kompetenciaközpont további

[33] A Bizottság (EU, Euratom) 2015/443 határozata (2015. március 13.) a Bizottságon belüli biztonságról (HL L 72., 2015.3.17., 41. o.).

[34] A Bizottság (EU, Euratom) 2015/444 határozata (2015. március 13.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 72., 2015.3.17., 53. o.).

működtetését annak céljaira, megbízatására és feladataira tekintettel, javasolhatja a kompetenciaközpont 46. cikkben meghatározott megbízatásának meghosszabbítását.

(4) A (2) bekezdésben említett időközi értékelés megállapításai alapján a Bizottság [a 22. cikk (5) bekezdésével] összhangban járhat el, vagy más megfelelő intézkedést tehet.

(5) A Horizont Európa program keretében biztosított hozzájárulás ellenőrzését, értékelését, kivezetését és megújítását a Horizont Európa rendelet 8., 45. és 47. cikkében, valamint III. mellékletében foglalt rendelkezéseknek és az elfogadott végrehajtási módozatoknak megfelelően kell végezni.

(6) A Digitális Európa program keretében biztosított hozzájárulás ellenőrzését, jelentését és értékelését a Digitális Európa program 24. és 25. cikkének előírásai szerint kell végezni.

(7) A kompetenciaközpont végelszámolása esetén a Bizottság a kompetenciaközpont végelszámolását követő hat hónapon belül, de legkésőbb két évvel az e rendelet 46. cikkében említett végelszámolási eljárás megindítását követően elvégzi a kompetenciaközpont záróértékelését. A záróértékelés eredményeit az Európai Parlament és a Tanács elé kell terjeszteni.

39. cikk

A kompetenciaközpont felelőssége

(1) A kompetenciaközpont szerződéses felelősségét az adott megállapodásra, határozatra vagy szerződésre alkalmazandó jog szabályozza.

(2) Szerződésen kívüli felelősség esetén a kompetenciaközpont a tagállamok jogában közös általános elveknek megfelelően megtéríti az alkalmazottai által feladataik teljesítése során okozott károkat.

(3) A kompetenciaközpont által az (1) és (2) bekezdésben említett felelősség tekintetében teljesített bármely kifizetés, valamint az azzal kapcsolatban felmerülő költségek és ráfordítások a kompetenciaközpont kiadásának minősülnek, és azokat annak forrásaiból kell fedezni.

(4) A kompetenciaközpont a kötelezettségei teljesítéséért kizárólagos felelősséggel tartozik.

40. cikk

Az Európai Unió Bíróságának hatásköre és az alkalmazandó jog

(1) Az Európai Unió Bíróságának hatásköre az alábbi esetekben áll fenn:

1. ha azt a kompetenciaközpont által kötött megállapodásban, határozatban vagy szerződésben szereplő választottbírósági záradék előírja;
2. a kompetenciaközpont személyzete által a feladatai ellátása során okozott károkra vonatkozó kártérítéssel kapcsolatos jogvitákban;
3. a kompetenciaközpont és alkalmazottai közötti jogvitákban az Európai Unió tisztviselőinek személyzeti szabályzatában és az

Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben meghatározott korlátok között és feltételek mellett.

(2) Minden olyan kérdésben, amelyről e rendelet vagy más uniós jogi aktus nem rendelkezik, azon tagállam joga alkalmazandó, amelyben a kompetenciaközpont székhelye található.

41. cikk

A tagok felelőssége és biztosítás

(1) A tagoknak a kompetenciaközpont adósságaiért viselt pénzügyi felelőssége nem haladja meg az igazgatási költségekhez való, már befizetett hozzájárulásaik összegét.

(2) A kompetenciaközpontnak megfelelő biztosítást kell kötnie és fenntartania.

42. cikk

Összeférhetetlenség

A kompetenciaközpont igazgatótanácsának szabályokat kell elfogadnia a tagokra, a szervekre és a személyi állományra vonatkozóan az összeférhetetlenség megelőzése és kezelése céljából. Ezeknek a szabályoknak az XXX rendelet [új költségvetési rendelet] értelmében tartalmazniuk kell az igazgatótanács és az ipari és tudományos tanácsadó testület tagjainak képviselőivel kapcsolatos összeférhetetlenség elkerülésére szolgáló rendelkezéseket.

43. cikk

Személyes adatok védelme

(1) A személyes adatok kompetenciaközpont általi kezelésére az (EU) 2018/XXX európai parlamenti és tanácsi rendelet alkalmazandó.

(2) Az igazgatótanács elfogadja az (EU) 2018/xxx rendelet xx. cikkének (3) bekezdésében említett végrehajtási intézkedéseket. Az igazgatótanács további, az (EU) 2018/xxx rendelet kompetenciaközpont általi alkalmazásához szükséges intézkedéseket fogadhat el.

44. cikk

A fogadó tagállam által nyújtott támogatás

A kompetenciaközpont és a székhelye szerinti tagállam [Belgium] között igazgatási megállapodás jöhet létre, amelyben az adott tagállam kiváltságokat és mentességeket, valamint egyéb támogatást biztosíthat a kompetenciaközpont részére.

VII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

45. cikk

Első intézkedések

(1) Mindaddig, amíg a kompetenciaközpont nem rendelkezik a saját költségvetésének végrehajtásához szükséges működési kapacitással, a Bizottság felel a kompetenciaközpont létrehozásáért és kezdeti működtetéséért. A Bizottság az uniós joggal összhangban valamennyi szükséges intézkedést a kompetenciaközpont illetékes szerveinek bevonásával hajtja végre.

(2) Az (1) bekezdés alkalmazásában, az igazgatótanács által a 16. cikk szerint kinevezett ügyvezető igazgató hivatalba lépéséig a Bizottság kijelölhet egy ideiglenes ügyvezető igazgatót, aki ellátja az ügyvezető igazgatói feladatokat, és akit ebben korlátozott számú bizottsági tisztviselő segíthet. A Bizottság ideiglenesen korlátozott számú bizottsági tisztviselőt bízhat meg.

(3) Az ideiglenes ügyvezető igazgató engedélyezhet minden kifizetést, amelyet a kompetenciaközpont éves költségvetésében szereplő előirányzatok fedeznek és amelyeket az igazgatótanács jóváhagyott, valamint megállapodásokat és szerződéseket köthet, illetve döntéseket hozhat, ideértve – a kompetenciaközpont létszámtervének elfogadását követően – a munkavállalói szerződéseket is.

(4) Az ideiglenes ügyvezető igazgató a kompetenciaközpont ügyvezető igazgatójával egyetértésben, az igazgatótanács jóváhagyásával meghatározza azt a napot, amelyen a kompetenciaközpont képessé válik saját költségvetésének a végrehajtására. E naptól kezdve a Bizottság nem tesz kötelezettségvállalásokat és nem teljesít kifizetéseket a kompetenciaközpont tevékenységeivel kapcsolatban.

46. cikk

Időtartam

(1) A kompetenciaközpont a 2021. január 1-jétől 2029. december 31-ig tartó időszakra jön létre.

(2) Ezen időszak végén, amennyiben e rendelet felülvizsgálata alapján nem születik ezzel ellentétes döntés, el kell indítani a végelszámolási eljárást. A végelszámolási eljárás automatikusan elindul, ha az Unió vagy az összes részt vevő tagállam kilép a kompetenciaközpontból.

(3) A kompetenciaközpont végelszámolását célzó eljárás lebonyolítására az igazgatótanács kinevez egy vagy több végelszámolót, aki(k)nek eleget kell tennie/tenniük az igazgatótanács határozatainak.

(4) A kompetenciaközpont végelszámolásakor a kompetenciaközpont vagyona szolgál a kötelezettségei és a végelszámolási költségek fedezeteként. Az esetleges többletet a kompetenciaközpont számára biztosított pénzügyi hozzájárulásukkal arányosan szét kell osztani az Unió és a részt vevő tagállamok között. A felosztás során az Uniónak jutó rész visszakerül az Unió költségvetésébe.

47. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, -án/-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

1.2. A tevékenységalapú irányítás / tevékenységalapú költségvetés-tervezés keretébe tartozó érintett szakpolitikai terület(ek)

1.3. A javaslat/kezdeményezés típusa

1.4. Célkitűzés(ek)

1.5. A javaslat/kezdeményezés indoklása

1.6. Az intézkedés és a pénzügyi hatás időtartama

1.7. Tervezett irányítási módszer(ek)

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

2.2. Irányítási és kontrollrendszer

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret mely fejezetét/fejezeteit és a költségvetés mely kiadási tételét/tételeit érintik a kiadások?

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összegzése

3.2.2. Az operatív előirányzatokra gyakorolt becsült hatás

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

3.2.5. Harmadik felek részvétele a finanszírozásban

3.3. A bevételre gyakorolt becsült hatás

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

Rendelet az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont létrehozásáról

1.2. A tevékenységalapú irányítás / tevékenységalapú költségvetés-tervezés keretébe tartozó érintett szakpolitikai terület(ek)[35]

Kutatás és innováció

Európai stratégiai beruházások

1.3. A javaslat/kezdeményezés típusa

☒A javaslat/kezdeményezés **új intézkedésre** irányul

☐ A javaslat/kezdeményezés **kísérleti projektet / előkészítő intézkedést követő új intézkedésre** [36]irányul

☐ A javaslat/kezdeményezés **jelenlegi intézkedés meghosszabbítására** irányul

☐ A javaslat/kezdeményezés **új intézkedésnek megfelelően módosított intézkedésre** irányul

1.4. Célkitűzés(ek)

1.4.1. A javaslat/kezdeményezés által érintett többéves bizottsági stratégiai célkitűzés(ek)

1. Összekapcsolt digitális egységes piac

2. Új lendület a foglalkoztatásnak, a növekedésnek és a beruházásoknak

1.4.2. Érintett konkrét célkitűzés(ek)

Konkrét célkitűzések

1.3. A digitális gazdaságban rejlő lehetőségek teljes mértékű kibontakoztatása a digitális és adatalapú technológiák teljes növekedési potenciáljának kiaknázását lehetővé tévő kezdeményezések által.

2.1. Európa megőrzi a digitális világgazdaságban betöltött vezető szerepét, ahol az európai vállalkozások erős digitális vállalkozási készségekre és jól teljesítő induló vállalkozásokra építve képesek globális növekedést elérni, és ahol az iparág és a közszolgáltatások alakítják a digitális átalakulás folyamatát és kiaknázzák az abban rejlő lehetőségeket.

2.2. Az európai kutatás beruházási lehetőségeket talál a potenciális technológiai áttörésekhez és úttörő kezdeményezésekhez, elsősorban a Horizont 2020/Horizont Európa program keretein belül, köz-magán társulások létrehozása révén.

[35] ABM: tevékenységalapú irányítás; ABB: tevékenységalapú költségvetés-tervezés.

[36] A költségvetési rendelet 54. cikke (2) bekezdésének a) vagy b) pontja szerint.

1.4.3. Várható eredmény(ek) és hatás(ok)

Tüntesse fel, milyen hatásokat gyakorolhat a javaslat/kezdeményezés a kedvezményezettekre/célcsoportokra.

A kompetenciaközpont a hálózattal és a közösséggel együtt az alábbi célok megvalósításán fog dolgozni:

1. hozzájárulás az XXX rendelet által létrehozott Digitális Európa program kiberbiztonsági részének, különösen az (EU) XXX rendelet [a Digitális Európa program] 6. cikkéhez kapcsolódó tevékenységek végrehajtásához, valamint az XXX rendelet által létrehozott Horizont Európa program, különösen a Horizont Európa kezdeményezést végrehajtó konkrét programot – a kutatási és innovációs keretprogramot létrehozó XXX határozat I. melléklete 2.2.6. szakaszának végrehajtásához, valamint más uniós programok végrehajtásához, amennyiben ezt az uniós jogi aktusok előírják számára,

2. az iparágak, a közszféra és a kutatói közösségek rendelkezésére álló kiberbiztonsági képességek, ismeretek és infrastruktúra javítása,

3. hozzájárulás a legmodernebb kiberbiztonsági termékek és megoldások széles körű bevezetéséhez a gazdaság minden szegmensében,

4. a kiberbiztonság jobb megértésének előmozdítása és hozzájárulás a kiberbiztonság terén az Unióban tapasztalható szakképzettségi hiányosságok csökkentéséhez,

5. hozzájárulás az uniós kiberbiztonsági kutatás és fejlesztés megerősítéséhez,

6. a kettős felhasználású technológiák és alkalmazások terén a polgári és a katonai terület között fennálló együttműködés fokozása,

7. a kiberbiztonság polgári és a katonai vetületei közötti szinergiák növelése,

8. a 10. cikkben említett nemzeti koordinációs központok hálózata (a „hálózat”) és a 12. cikkben említett kiberbiztonsági kompetenciaközösség által végzett munka összehangolásának támogatása és elősegítése.

1.4.4. Eredmény- és hatásmutatók

Tüntesse fel a javaslat/kezdeményezés megvalósításának nyomon követését lehetővé tevő mutatókat.

· A közös beszerzésű kiberbiztonsági infrastruktúra/eszközök száma.

· Az európai kutatók és ipari szereplők számára a hálózaton és a kompetenciaközponton keresztül biztosított, tesztelésre és kísérletezésre fordítható idő. Meglévő létesítmények esetén a közösségek által jelenleg elérhető órák számához képest elért óraszám-növekedés.

· Az ellátott felhasználói közösségek száma és az európai kiberbiztonsági létesítményekhez hozzáférő kutatók számának növekedése azokhoz képest, akiknek Európán kívüli erőforrásokat kell keresniük.

· Az európai szolgáltatók versenyképessége javulni kezd, amelyet a világpiaci részesedés (cél a 25 %-os részesedés elérése 2027-re), valamint az iparban hasznosuló európai kutatás-fejlesztési eredmények aránya alapján kell mérni.

· Hozzájárulás a jövő kiberbiztonsági technológiáihoz, amelyet a bejegyzett szerzői jogok, szabadalmak, tudományos kiadványok és kereskedelmi forgalomba hozott termékek száma alapján kell mérni.

· A kiberbiztonsági készségeket biztosító felmért és harmonizált tantervek száma, a felmért kiberbiztonsági szakmai tanúsítást nyújtó programok száma.

· Képzésben részesült kutatók, diákok, valamint (ipari és közigazgatási) felhasználók száma.

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek)

A kiberbiztonsági technológiai és ipari fejlődést célzó beruházások kritikus tömegének elérése, és az EU különböző részein meglévő kapacitások széttagoltságából fakadó hátrányok leküzdése.

1.5.2. Az uniós részvételből adódó többletérték

A kiberbiztonság az Unió egészének közös érdeke, amelyet a fent említett tanácsi következtetések is megerősítenek. A WannaCry, a NonPetya és hasonló incidensek jelentős kihatása és határokon átnyúló jellege szintén alátámasztja ezt a megállapítást. A kiberbiztonság terén fennálló technológiai kihívások jellege és léptéke, valamint az ipar, a közszféra és a kutatói közösségek közötti és azokon belüli elégtelen együttműködés szükségessé teszi, hogy az EU további támogatást nyújtson az erőfeszítések összehangolásához, egyfelől az erőforrások kritikus tömegének biztosítása, másfelől a jobb tudás- és eszközkezelés érdekében. Ezt teszik szükségessé a kiberbiztonsági kutatáshoz, fejlesztéshez és a kiberbiztonsági megoldások bevezetéséhez kapcsolódó bizonyos képességek erőforrásigényei; az interdiszciplináris kiberbiztonsági szakismerethez való hozzáférés különböző diszciplínák számára történő biztosítására irányuló igények (ez a szakismeret általában nemzeti szinten csak részlegesen áll rendelkezésre); továbbá az iparági értékláncok globális jellege, valamint a piacokon működő nemzetközi versenytársak tevékenysége.

A fentiekhez olyan léptékű erőforrások és szakértelem szükséges, amelyet egyetlen tagállam sem tud önálló intézkedésekkel biztosítani. Például egy összeurópai kvantumkommunikációs hálózat kiépítése az összekapcsolni/bevonni kívánt tagállamok által tett beruházások, valamint a meglévő infrastruktúra felhasználhatóságától függően akár mintegy 900 millió EUR uniós beruházást is igényelhet.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

A Horizont 2020 program időközi értékelése egyebek mellett azt is megerősítette, hogy továbbra is szükség van az uniós támogatásra a kutatás-fejlesztés és a társadalmi kihívások leküzdése terén (a program része többek között a kiberbiztonsági kutatás-fejlesztést támogató „Biztonságos társadalmak” alprogram). Az értékelés ugyanakkor rámutat arra, hogy az ipari vezető szerep megerősítése továbbra is kihívást jelent, illetve hogy még mindig létezik az innovációs szakadék, ami azt jelenti, hogy az EU a komoly áttörésnek számító, piacokat teremtő innovációk terén elmarad a világ más részeitől.

Bár az Európai Hálózatfinanszírozási Eszköz (CEF) a kiberbiztonság másik aspektusára (a működésbiztonságra) helyezte a hangsúlyt, és némiképp eltérő beavatkozási logikára támaszkodott, a CEF félidős értékelése megerősíti a kutatás-fejlesztés területén túlmutató uniós beavatkozás hozzáadott értékét. Emellett a CEF keretében kiberbiztonsági célú támogatásban részesülő kedvezményezettek többsége

(a nemzeti számítógép-biztonsági és incidenskezelő csoportok közössége) kifejezte igényét egy, a következő többéves pénzügyi keret alatt megvalósítandó külön támogatási programra.

A szerződéses kiberbiztonsági köz-magán társulás („cPPP”) 2016-os létrehozásával az EU megtette az első határozott lépést abba az irányba, hogy a kutatás, az ipar és a közszféra területén tevékenykedő közösségek együttműködése révén megkönnyítse a kiberbiztonsági kutatást és innovációt, ami a várakozások szerint a 2014 és 2020 közötti pénzügyi keret korlátain belül megfelelő, célorientáltabb kutatási és innovációs eredményekhez vezet. A cPPP keretében az ipari partnerek vállalásokat tehettek arra nézve, hogy milyen beruházásokat fognak megvalósítani a társulás Stratégiai kutatási és innovációs tervében meghatározott területeken.

1.5.4. Egyéb releváns eszközökkel való összeegyeztethetőség és lehetséges szinergia

A kiberbiztonsági kompetenciahálózat és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont célja, hogy kiegészítő támogatást nyújtson a meglévő kiberbiztonsági szakpolitikai rendelkezések és szereplők számára. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont feladatkörét tekintve kiegészíti az ENISA tevékenységét, ugyanakkor más területekre fókuszál és más készségekre támaszkodik. Míg az ENISA tanácsadói szerepet tölt be az EU-ban zajló kiberbiztonsági kutatások és innováció terén, a kompetenciaközpont javasolt megbízása elsősorban az EU kiberbiztonsági ellenálló képességének megerősítéséhez szükséges más fontos feladatokat helyez előtérbe. A kompetenciaközpontnak ösztönöznie kell a kiberbiztonsági technológia fejlesztését és bevezetését, valamint ki kell egészítenie a kiberbiztonság területén zajló uniós és nemzeti kapacitásépítési tevékenységeket.

Ezenfelül az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a kiberbiztonsági kompetenciahálózat feladatai közé tartozik majd a szabványosítási és tanúsítási folyamatok, különösen a Kiberbiztonsági jogszabály szerinti kiberbiztonsági tanúsítási rendszerekhez kapcsolódó szabványosítási és tanúsítási folyamatok elősegítését és felgyorsítását célzó kutatások támogatása is.

Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont két kiberbiztonságot támogató európai program, a Digitális Európa program és a Horizont Európa program közös végrehajtó testületeként fog működni, összehangolva tevékenységeiket és növelve a közöttük kialakuló szinergiákat.

Ez a kezdeményezés lehetővé teszi a tagállamok által tett erőfeszítések kiegészítését, mivel hasznos információkat tud nyújtani az oktatási döntéshozóknak a kiberbiztonsági képzések minőségének javításához (például a polgári és katonai oktatásban felhasználható kiberbiztonsági tananyagok kidolgozásával, de akár az alapszintű kiberbiztonsági oktatáshoz való hozzájárulással). A kezdeményezés ezenfelül lehetővé tehetné a kiberbiztonsági szakmai tanúsítást nyújtó programok harmonizálását és folyamatos értékelését – e tevékenységek mind szükségesek a kiberbiztonság terén tapasztalható szakképzettségi hiány megszüntetéséhez, valamint az ipari és más szereplők kiberbiztonsági szakemberekhez való hozzáférésének elősegítéséhez. A képzések és készségek harmonizálása hozzájárul egy képzett európai kiberbiztonsági munkavállalói réteg kialakulásához, ami rendkívül hasznos lenne a kiberbiztonsággal foglalkozó vállalatok és a kiberbiztonságban érdekelt más iparágak számára.

1.6. Az intézkedés és a pénzügyi hatás időtartama

☒ A javaslat/kezdeményezés **határozott időtartamra** vonatkozik

– ☒ A javaslat/kezdeményezés időtartama: 2021.1.1-től 2029.12.31-ig

– ☒ Pénzügyi hatás: 2021-től 2027-ig a kötelezettségvállalási előirányzatok esetében és 2021-től 2031-ig a kifizetési előirányzatok esetében.

☐ A javaslat/kezdeményezés **határozatlan időtartamra** vonatkozik

– Beindítási időszak: ÉÉÉÉ-tól/-től ÉÉÉÉ-ig

– azt követően: rendes ütem.

1.7. Tervezett irányítási módszer(ek)[37]

☐ Bizottság általi **közvetlen irányítás**

– ☐ a Bizottság szervezeti egységein keresztül, ideértve az uniós küldöttségek személyzetét;

– ☐ végrehajtó ügynökségen keresztül.

☐ **Megosztott irányítás** a tagállamokkal

☒

Közvetett irányítás a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

– ☐ harmadik országok vagy az általuk kijelölt szervek;

– ☐ nemzetközi szervezetek és ügynökségeik (nevezze meg);

– ☐ az EBB és az Európai Beruházási Alap;

– ☒ a költségvetési rendelet 70. és 71. cikkében említett szervek;

– ☐ közjogi szervek;

– ☐ magánjog alapján működő, közfeladatot ellátó szervek, olyan mértékben, amennyiben megfelelő pénzügyi garanciákat nyújtanak;

– ☐ a valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek;

– ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek.

– *Egynél több irányítási módszer feltüntetése esetén kérjük, adjon részletes felvilágosítást a „Megjegyzések” rovatban.*

[37] Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a Költségvetési Főigazgatóság honlapján: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Gyakoriság és feltételek.

A nyomon követésre és a jelentéstételre vonatkozó részletes rendelkezéseket a 28. cikk tartalmazza.

2.2. Irányítási és kontrollrendszer

2.2.1. Felismert kockázat(ok)

A kompetenciaközpont felállítását követően a működéssel kapcsolatos kockázatok mérséklése és a késedelmek elkerülése érdekében a Bizottság ebben az időszakban támogatást nyújt a kompetenciaközpontnak a kulcsfontosságú személyzet gyors alkalmazásba vételéhez, valamint a hatékony belső kontrollrendszer és a megbízható eljárások bevezetéséhez.

2.2.2. A működő belső kontrollrendszerrel kapcsolatos információk

Az ügyvezető igazgató felelős a kompetenciaközpont működéséért, napi ügyvezetéséért, és ő a kompetenciaközpont törvényes képviselője. Az igazgató elszámoltatható az igazgatótanács felé, és folyamatosan jelent neki a kompetenciaközpont tevékenységeinek alakulásáról.

Általánosságban az igazgatótanács felel a kompetenciaközpont stratégiai irányításáért és működéséért, és felügyeli a tevékenységeinek végrehajtását.

A kompetenciaközpontra alkalmazandó pénzügyi szabályokat a Bizottsággal folytatott konzultációt követően az igazgatótanács fogadja el. Ezek a szabályok nem térhetnek el az 1271/2013/EU rendelettől, kivéve, ha az eltérés a kompetenciaközpont működéséhez kifejezetten szükséges, és ahhoz a Bizottság előzetesen hozzájárult.

A Bizottság belső ellenőre ugyanazon hatásköröket gyakorolja a kompetenciaközpont felett, mint a Bizottság szervezeti egységei felett. A Számvevőszék jogosult dokumentumalapú és helyszíni ellenőrzést végezni a támogatások kedvezményezettjeinél, valamint a kompetenciaközponttól uniós forrásokban részesülő vállalkozóknál és alvállalkozóknál.

2.2.3. Az ellenőrzések költsége és haszna, a várt hibaarány értékelése

Az ellenőrzésekkel járó költségek és előnyök

Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközponthoz kapcsolódó ellenőrzési költségek a bizottsági szintű felügyelet költségeiből és a végrehajtó szerv szintjén jelentkező, működési ellenőrzésekhez kapcsolódó költségekből tevődnek össze.

A kompetenciaközpont szintjén jelentkező ellenőrzési költségek a becslések szerint a kompetenciaközpont szintjén biztosított operatív kifizetési előirányzatok mintegy 1,19 %-át fogják kitenni.

A bizottsági szintű felügyelet költségei várhatóan a kompetenciaközpont szintjén biztosított operatív kifizetési előirányzatok 1,20 %-át fogják kitenni.

Amennyiben a Bizottság önállóan, a végrehajtó szerv támogatása nélkül irányítaná a tevékenységeket, az ellenőrzési költségek lényegesen magasabbak lennének: elérhetnék a kifizetési előirányzatok mintegy 7,7 %-át.

A tervezett kontrollok célja, hogy a Bizottság hatékonyan és zökkenőmentesen felügyelhesse a végrehajtó szerveket, és megfelelő mértékű bizonyosságot szerezhessen.

A kontrollok hasznai a következők:

- Gyengébb vagy nem megfelelő pályázatok választásának elkerülése.
- Az uniós finanszírozás tervezésének és felhasználásának optimalizálása az uniós hozzáadott érték megőrzése mellett.
- A támogatási megállapodások minőségének biztosítása, a jogi személyek azonosításában fellépő hibák elkerülése, az EU-hozzájárulások megfelelő kiszámításának biztosítása és a támogatások megfelelő működésének garantálása.
- A nem elszámolható költségek feltárása a kifizetési szakaszban.
- A tevékenységek jogszerűségét és szabályszerűségét befolyásoló hibák feltárása az ellenőrzési szakaszban.

Becsült hibaszint

A cél az, hogy a fennmaradó hibaarány a program egészében a 2 %-os küszöb alatt maradjon, ugyanakkor a kedvezményezetteknél jelentkező ellenőrzési terhek ne növekedjenek, ezzel megfelelő egyensúly jöjjön létre a törvényesség és jogszerűség célja és egyéb célok, például a program különösen a kkv-k számára mutatkozó vonzereje és a kontrollok költségei között.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket.

Az Európai Csalás Elleni Hivatal a 883/2013/EU, Euratom európai parlamenti és tanácsi rendeletben és az Európai Közösségek pénzügyi érdekeinek csalással és egyéb szabálytalanságokkal szembeni védelmében a Bizottság által végzett helyszíni ellenőrzésekről és vizsgálatokról szóló, 1996. november 11-i 2185/96/Euratom, EK tanácsi rendeletben előírt rendelkezéseknek és eljárásoknak megfelelően vizsgálatokat, ezen belül helyszíni ellenőrzéseket és vizsgálatokat is végezhet annak megállapítására, hogy a kompetenciaközpont által finanszírozott támogatással vagy szerződéssel összefüggésben történt-e az Unió pénzügyi érdekeit sértő csalás, korrupció vagy más jogellenes cselekmény.

Az e rendelet végrehajtásából eredő megállapodásokban, határozatokban és szerződésekben kifejezetten rendelkezni kell arról, hogy a Bizottság, a kompetenciaközpont, a Számvevőszék és az Európai Csalás Elleni Hivatal saját hatáskörben jogosult ellenőrzéseket és vizsgálatokat végezni.

A kompetenciaközpont megfelelő belső és külső ellenőrzések végzése vagy végeztetése révén gondoskodik arról, hogy tagjainak pénzügyi érdekei kellő védelemben részesüljenek.

A kompetenciaközpont csatlakozik az Európai Parlament, az Európai Unió Tanácsa és az Európai Közösségek Bizottsága közötti, az Európai Csalás Elleni Hivatal (OLAF) belső vizsgálatairól szóló, 1999. május 25-i intézményközi megállapodáshoz. A kompetenciaközpont meghozza az Európai Csalás Elleni Hivatal által végzett belső vizsgálatok megkönnyítéséhez szükséges intézkedéseket.

A kompetenciaközpont csalással kapcsolatos kockázatértékelésen és költség-haszon elemzésen alapuló csalás elleni stratégiát fogad el. A központ a csalás, vesztegetés és egyéb illegális tevékenységek elleni megelőző intézkedések alkalmazásával, hatékony ellenőrzésekkel, illetve szabálytalanságok észlelése esetén a jogtalanul kifizetett összegek behajtásával és adott esetben hatékony, arányos és visszatartó erejű igazgatási és pénzügyi büntetésekkel védi az Unió pénzügyi érdekeit.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret fejezete és a költségvetés javasolt új kiadási tétele/tételei

- Létrehozandó új költségvetési tételek

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési tételek sorrendjében:

A többéves pénzügyi keret fejezete	Költségvetési tétel	Kiadás típusa	Hozzájárulás			
	Szám	diff./nem diff[38].	EFTA-országoktól[39]	tagjelölt országoktól[40]	harmadik országoktól	a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében
1. fejezet: Egységes piac, innováció és digitális gazdaság	01 02 XX XX Horizont Európa Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont – támogatási kiadások 01 02 XX XX Horizont Európa Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont 02 06 01 XX Digitális Európa program Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont – támogatási kiadások 02 06 01 XX Digitális Európa program Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont	Diff.	IGEN	IGEN (ha meg van adva az éves munkaprogramban)	IGEN (a program egyes részeire korlátozva)	NEM

- Az e költségvetési tételekbe beérkező hozzájárulások várt forrása:

[38] Diff. = Differenciált előirányzatok / Nem diff. = Nem differenciált előirányzatok.
[39] EFTA: Európai Szabadkereskedelmi Társulás.
[40] Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelöltek.

millió EUR (három tizedesjegyig)

Költségvetési tétel	2021. év	2022. év	2023. év	2024. év	2025. év	2026. év	2027. év	**Összesen**
01 01 01 01 Kutatási tisztviselőkkel és ideiglenes alkalmazottakkal kapcsolatos kiadások – Horizont Európa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 A kutatási programokat: a Horizont Európa keretprogramot végrehajtó külső munkatársakkal kapcsolatos kiadások	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 A kutatással kapcsolatos egyéb igazgatási kiadások – Horizont Európa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globális kihívások és ipari versenyképesség	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Igazgatási támogatás – Digitális Európa program	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Kiberbiztonság – Digitális Európa program	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Kiadások összesen	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

A Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez a 21. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR). A javaslat az XXX rendelet [a Horizont Európa keretprogramja] 6. cikkének (6) bekezdésében meghatározott stratégiai tervezési folyamat eredményein fog alapulni.

A fenti összegek nem tartalmazzák a tagállamok által a kompetenciaközpont igazgatási és működési költségeihez biztosított, az uniós pénzügyi hozzájárulással arányos hozzájárulást.

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összegzése

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret fejezete	**1**	Egységes piac, innováció és digitális gazdaság

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***2027 után***	**ÖSSZESEN**
1. cím (személyzeti kiadások)	Kötelezettségvállalási előirányzatok = kifizetési előirányzatok	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
2. cím (infrastrukturális és működési kiadások)	Kötelezettségvállalási előirányzatok = kifizetési előirányzatok	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
3. cím (operatív kiadások)	Kötelezettségvállalási előirányzatok	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Kifizetési előirányzatok	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
A programkeretre szóló előirányzatok	Kötelezettségvállalási	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] A Bizottság a személyzeti előirányzatokat 2021-re vonatkozóan csak fél évre határozta meg.

ÖSSZESEN[42]	előirányzatok										
	Kifizetési előirányzatok	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] Az itt szereplő összesített előirányzatok csak a Digitális Európa program keretei között a kiberbiztonságra szánt uniós pénzügyi erőforrásokra vonatkoznak. A Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez az 5. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR). A javaslat az XXX rendelet [a Horizont Európa keretprogramja] 6. cikkének (6) bekezdésében meghatározott stratégiai tervezési folyamat eredményein fog alapulni.

A többéves pénzügyi keret fejezete	7	„Igazgatási kiadások”

millió EUR (három tizedesjegyig)

		2021	2022	2023	2024	2025	2026	2027	*2027 után*	ÖSSZESEN
Humánerőforrás		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Egyéb igazgatási kiadások		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
A többéves pénzügyi keret 7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN	(Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

millió EUR (három tizedesjegyig)

		2021	2022	2023	2024	2025	2026	2027	*2027 után*	ÖSSZESEN
A többéves pénzügyi keret **FEJEZETEIHEZ tartozó előirányzatok ÖSSZESEN**	Kötelezettségvállalási előirányzatok	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Kifizetési előirányzatok	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 061,715**	**2 005,637**

3.2.2. Az igazgatási előirányzatokra gyakorolt becsült hatás összefoglalása

– ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását

– ☒ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

Évek	2021	2022	2023	2024	2025	2026	2027	ÖSSZESEN
A többéves pénzügyi keret 7. FEJEZETÉHEZ tartozó előirányzatok								
Humánerőforrás	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Egyéb igazgatási kiadások	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
A többéves pénzügyi keret 7. FEJEZETÉHEZ tartozó előirányzatok részösszege	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

A többéves pénzügyi keret 7. FEJEZETÉBE[43] bele nem tartozó előirányzatok								
Humánerőforrás								
Egyéb igazgatási kiadások	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
A többéves pénzügyi keret 7. FEJEZETÉBE bele nem tartozó előirányzatok részösszege	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

ÖSSZESEN	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

A humánerőforrással és más igazgatási kiadásokkal kapcsolatos előirányzat-igényeket az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt előirányzatokkal és/vagy az adott főigazgatóságon belüli átcsoportosítással kell teljesíteni. A források adott esetben a költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

A humánerőforrással és az egyéb igazgatási kiadásokkal kapcsolatos 7. fejezetbe bele nem tartozó kívüli fenti előirányzatok a Digitális Európa program keretében biztosított uniós pénzügyi hozzájárulás által fedezett összegeknek felelnek meg.

[43] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

A humánerőforrással és az egyéb igazgatási kiadásokkal kapcsolatos 7. fejezetbe bele nem tartozó előirányzatok mértékét növelni fogják a Horizont Európa program keretében biztosított uniós pénzügyi hozzájárulás által fedezett összegek, mivel a Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez a 21. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR).

A humánerőforrással és az egyéb igazgatási kiadásokkal kapcsolatos 7. fejezet bele nem tartozó fenti előirányzatok összege nem tartalmazza a tagállamok által a kompetenciaközpont igazgatási költségeihez biztosított, az uniós pénzügyi hozzájárulással arányos hozzájárulást.

3.2.2.1. A Bizottságnál felmerülő, becsült humánerőforrás-szükségletek

– ☐ A javaslat/kezdeményezés nem igényel humánerőforrást.

– ■ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

A becsléseket teljes munkaidős egyenértékben kell kifejezni

Évek		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)								
a központban és a bizottsági képviseleteken		20	21	21	21	21	21	22
a küldöttségeknél								
Kutatás								
• Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve: AC, AL, END, INT és JED [44]								
7. fejezet:								
A többéves pénzügyi keret 7. FEJEZETÉHEZ tartozó előirányzatokból finanszírozva	- a központban	3	3	3	3	3	3	3
	- a küldöttségeknél							
A programkeretből finanszírozva [45]	- a központban							
	- a küldöttségeknél							
Kutatás								
Egyéb (meghatározandó)								
ÖSSZESEN		**23**	**23**	**24**	**24**	**24**	**25**	**25**

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra bízott feladatok összehangolása, felügyelete és irányítása, ideértve a támogatási és koordinációs költségek kezelését. A kiberbiztonsági szakpolitika alakítása és koordinálása az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra bízott feladatok, például a kutatási és iparpolitikai prioritások meghatározása, a tagállamok és a gazdasági szereplők közötti általános együttműködés, a jövőbeni uniós kiberbiztonsági tanúsítási

[44] AC=szerződéses alkalmazott; AL=helyi alkalmazott; END=kirendelt nemzeti szakértő; INT=kölcsönmunkaerő (átmeneti alkalmazott); JPD=küldöttségi pályakezdő szakértő.

[45] Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

	keretrendszerrel való összhang, a felelősség és gondosság kidolgozása, valamint a nagy teljesítményű számítástechnikára, a mesterséges intelligenciára és a digitális készségekre vonatkozó szakpolitikákkal való összhang kialakítása tekintetében. .
Külső munkatársak	Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra bízott feladatok összehangolása, felügyelete és irányítása, ideértve a támogatási és koordinációs költségek kezelését. A kiberbiztonsági szakpolitika alakítása és koordinálása az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra bízott feladatok, például a kutatási és iparpolitikai prioritások meghatározása, a tagállamok és a gazdasági szereplők közötti általános együttműködés, a jövőbeni uniós kiberbiztonsági tanúsítási keretrendszerrel való összhang, a felelősség és gondosság kidolgozása, valamint a nagy teljesítményű számítástechnikára, a mesterséges intelligenciára és a digitális készségekre vonatkozó szakpolitikákkal való összhang kialakítása tekintetében. .

3.2.2.2. A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont becsült humánerőforrás-szükséglete

	2021	2022	2023	2024	2025	2026	2027
Bizottsági tisztviselők							
ebből AD							
ebből AST							
ebből AST-SC							
Ideiglenes alkalmazottak							
ebből AD	10	11	13	13	13	13	13
ebből AST							
ebből AST-SC							
Szerződéses alkalmazottak	26	32	39	39	39	39	39
Kirendelt nemzeti szakértők (SNE)	1	1	1	1	1	1	1
Összesen	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	Az e rendelet 4. cikke által az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra rótt feladatok operatív végrehajtása, ideértve a támogatási és koordinációs költségek kezelését.
Külső munkatársak	Az e rendelet 4. cikke által az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra rótt feladatok operatív végrehajtása, ideértve a támogatási és koordinációs költségek kezelését.

A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra vonatkozóan a fentiekben megállapított becsült humánerőforrás-szükséglet a Digitális Európa program keretében biztosított uniós pénzügyi hozzájárulás végrehajtásához szükséges becsült igényeknek felel meg.

A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont fentiekben megállapított becsült humánerőforrás-szükségletét növelni fogják a Horizont Európa program keretében biztosított uniós pénzügyi hozzájárulás végrehajtásához szükséges becsült igények, mivel a Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez a 21. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR).

3.2.2.3. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont létszámterve

Tisztviselői besorolások és fokozatok	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD összesen	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST összesen							

AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
AST/SC összesen							
MINDÖSSZESEN	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. A személyi állományra gyakorolt becsült hatás (további alkalmazottak) – a Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont külső személyzete

Szerződéses alkalmazottak	2021	2022	2023	2024	2025	2026	2027
IV. besorolási csoport	20	22	29	29	29	29	29
III. besorolási csoport	2	4	4	4	4	4	4
II. besorolási csoport	4	6	6	6	6	6	6
I. besorolási csoport							
Összesen	**26**	**32**	**39**	**39**	**39**	**39**	**39**

A létszámnövekedés elkerülése érdekében a Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont létszámának növelését részben ellensúlyozza majd a releváns bizottsági szolgálatoknál dolgozó tisztviselők és külső alkalmazottak (azaz a jelenlegi létszámterv és külső alkalmazottak) számának csökkentése.

A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont 3.2.2.2–4. pontokban meghatározott alkalmazotti létszáma az alábbi módon kerül kompenzálásra[46]:

ÖSSZESEN	2021	2022	2023	2024	2025	2026	2027
Bizottsági tisztviselők	5	5	6	6	6	6	6
Ideiglenes alkalmazottak							
Szerződéses	14	17	20	20	20	20	20

[46] Függ a költségvetés végleges összegétől, amelynek végrehajtása a kompetenciaközpont feladata lesz.

alkalmazottak							
Kirendelt nemzeti szakértők (SNE)							
Teljes munkaidős munkavállalók száma összesen	19	22	26	26	26	26	26
Létszám	19	22	26	26	26	26	26

A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont humánerőforrásának kompenzációja arányos lesz az uniós pénzügyi hozzájárulás mértékével, ami 50 %.

A Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra vonatkozóan fent megállapított kompenzáció a Digitális Európa program keretében biztosított uniós pénzügyi hozzájárulás megvalósításához szükséges becsült humánerőforrás-szükségletének felel meg.

A fenti kompenzációt növelni fogják a Horizont Európa program keretében biztosított uniós pénzügyi hozzájárulás végrehajtásához szükséges becsült igények, mivel a Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez a 21. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR).

3.2.3. Harmadik felek részvétele a finanszírozásban

A javaslat/kezdeményezés:

– ☐ nem irányoz elő harmadik felek általi társfinanszírozást;

– ☒ előirányoz harmadik felek általi társfinanszírozást[47] az alábbi becslések szerint:

előirányzatok, millió EUR (három tizedesjegyig)

Évek	2021	2022	2023	2024	2025	2026	2027	ÖSSZESEN
Tagállamok – hozzájárulás a személyzeti kiadásokhoz	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Tagállamok – hozzájárulás az infrastrukturális és üzemeltetési kiadásokhoz	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Tagállamok – hozzájárulás a működési kiadásokhoz	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Társfinanszírozott előirányzatok ÖSSZESEN	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

A fenti, harmadik felek általi hozzájárulás csak a Digitális Európa program keretében a kiberbiztonságra szánt uniós pénzügyi erőforrásokkal arányos társfinanszírozást veszi figyelembe. A fenti, harmadik felek általi hozzájárulás növekedni fog, mivel a Bizottság a jogalkotási folyamat során, még a politikai megállapodás véglegesítése előtt javaslatot fog tenni arra, hogy milyen összeget használjanak fel a kezdeményezéshez a 21. cikk (1) bekezdésének b) pontjában említett Horizont Európa II. pillérének („Globális kihívások és ipari versenyképesség”) az „Inkluzív és biztonságos társadalom” című klaszteréhez tartozó pénzügyi keretösszegből (a teljes keretösszeg 2 800 000 000 EUR). A javaslat az XXX rendelet [a Horizont Európa keretprogramja] 6. cikkének (6) bekezdésében meghatározott stratégiai tervezési folyamat eredményein fog alapulni.

3.3. A bevételre gyakorolt becsült hatás

– ☒ A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre.

– ☐ A javaslatnak/kezdeményezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:

☐ a javaslat a saját forrásokra gyakorol hatást

☐ a javaslat más bevételre gyakorol hatást

kérjük, adja meg, hogy a bevétel költségvetési tételhez van-e rendelve ☐

millió EUR (három tizedesjegyig)

Bevételi költségvetési	A javaslat/kezdeményezés hatása[48]

[47] A tagállamok által biztosított természetbeni hozzájárulás becsült értéke.

[48] A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összegeket, vagyis a 20 %-kal (beszedési költségek) csökkentett bruttó összegeket kell megadni.

tétel:	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
… jogcímcsoport							

A címzett bevételek esetében tüntesse fel az érintett kiadáshoz tartozó költségvetési tétel(eke)t.

Egyéb megjegyzések (pl. a bevételre gyakorolt hatás számítására használt módszer/képlet vagy egyéb információ).