Az Európai Unió
Tanácsa

Brüsszel, 2024. december 6.
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Címzett:	a delegációk
Tárgy:	A Tanács következtetései az ENISA-ról

Mellékelten továbbítjuk a delegációknak az ENISA-ról szóló tanácsi következtetéseket, amelyet Tanács a 2024. december 6-i ülésén jóváhagyott.

MELLÉKLET

Tervezet – A Tanács következtetései az ENISA-ról

AZ EURÓPAI UNIÓ TANÁCSA,

1. KIEMELI, hogy a globális kibertérből fakadó kihívások az újonnan felmerülő kiberfenyegetések kifinomultsága, a folyamatosan változó biztonsági környezet és a jelenlegi geopolitikai feszültségek miatt még soha nem voltak olyan összetettek, sokrétűek és súlyosak, mint jelenleg. Ezért a jelenlegi és az újonnan felmerülő fenyegetések és kihívások hatékony azonosítása és kezelése céljából az EU-nak és tagállamainak folytatniuk kell arra irányuló erőfeszítéseiket, hogy reziliensebbé váljanak. KIEMELI, hogy a társadalom egészére kiterjedő megközelítést követve kell folytatni a fokozottabb kiberrezilienciára irányuló munkát. HANGSÚLYOZZA, hogy az elkövetkező években az EU-nak és tagállamainak arra kell összpontosítaniuk, hogy hatékony módon végrehajtásra kerüljenek az e tekintetben eddig tett valamennyi intézkedést alátámasztó és azokhoz hozzájáruló jogalkotási és nem jogalkotási kezdeményezések;

2. EMLÉKEZTETVE arra, hogy a nemzetbiztonság továbbra is az egyes tagállamok kizárólagos felelőssége, NYUGTÁZZA, hogy az EU és tagállamai az elmúlt években hatalmas közös erőfeszítéseket tettek a szükséges intézményi felépítés, valamint nemzeti és uniós szintű együttműködési formák kialakításához a kiberbiztonság területén. ÜDVÖZLI azt a számos jogalkotási és nem jogalkotási kezdeményezést, amelyek ezen a területen erős és szilárd keretet biztosítanak az EU és tagállamai számára, fokozva az Unió általános kiberrezilienciáját. E keret fejlődése nyomán kiterjed a kibertér több aspektusára is: a biztonságra, a diplomáciára, a bűnüldözésre és a védelemre. NYUGTÁZZA, hogy számos szereplő – többek között a tagállamok kiberbiztonsági hatóságai, a Kiberbiztonsági Együttműködési Csoport, a CSIRT-ek hálózata, az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe), a nemzeti koordinációs központok hálózata, az európai kiberbiztonsági tanúsítási csoport, a Bizottság, az Európai Külügyi Szolgálat (EKSZ), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), az Európai Kiberbiztonsági Kompetenciaközpont, a CERT-EU, az Európai Védelmi Ügynökség (EDA) és az Europol Kiberbűnözés Elleni Európai Központja (EC3) – az uniós kiberbiztonsági ökoszisztéma részét képezi, és mindegyikük részt vállal az Unió egészére kiterjedő kiberbiztonsági keret megvalósításában;

3. TUDATÁBAN VAN annak, hogy az elmúlt két évtizedben az ENISA felbecsülhetetlen értékű szervezetnek bizonyult az európai kiberbiztonsági ökoszisztémában, továbbá meghatározó szerepet tölt be a tagállamok, valamint az uniós intézmények, szervek és hivatalok következőkre irányuló aktív támogatásában: kiberbiztonsági politikáik végrehajtása és fejlesztése, kapacitásépítésük és felkészültségük, együttműködésük, valamint kiberbiztonsági tudatosságuk és tanúsításuk előmozdítása;

ÁLTALÁNOS SZAKPOLITIKAI AJÁNLÁSOK

4. FELKÉRI a Bizottságot, hogy éljen **a kiberbiztonsági jogszabály értékelésének** lehetőségével, és vizsgálja meg, hogy az miként járulhat hozzá az összetett kiberbiztonsági ökoszisztéma egyszerűsítéséhez, javítva ezáltal az erőforrások eredményességét és hatékony felhasználását. Ezért FELSZÓLÍTJA a Bizottságot annak biztosítására, hogy az ENISA-nak a tagállamok, valamint az uniós intézmények, szervek és hivatalok támogatására vonatkozó megbízatása célzott és egyértelműen meghatározott legyen, tartalmazzon konkrét stratégiai célkitűzéseket és rangsorolt feladatokat, a többi szereplő tekintetében fennálló feladatok és hatáskörök pontosabb megosztása mellett. E tekintetben FELKÉRI a Bizottságot, hogy vizsgálja meg és erősítse tovább az ENISA által a kiberreziliencia javítása terén uniós szinten és a tagállamok között megvalósuló operatív együttműködés támogatásában betöltött szerepet, figyelembe véve a tagállamok e területen meglévő hatásköreit. Emellett FELSZÓLÍTJA a Bizottságot, hogy erősítse meg a hatályos és jövőbeli uniós jogalkotási és nem jogalkotási kezdeményezések végrehajtása tekintetében a szakértői és tényeken alapuló iránymutatás és ajánlások terén az ENISA által betöltött szerepet, biztosítva egyúttal az uniós kiberbiztonsági keret koherenciáját;

5. ugyanebben a szellemben ÖSZTÖNZI a Bizottságot, hogy fontolja meg az ENISA által az olyan feladatok tekintetében betöltött szerep észszerűsítését, amelyek nem képezik az ENISA küldetésének központi elemét. HANGSÚLYOZZA, hogy közelmúltbeli jogalkotási kezdeményezések – így többek között a NIS 2 irányelv, a kiberrezilienciáról szóló jogszabály és a kiberszolidaritásról szóló jogszabály – **jelentősen kibővítették** az ENISA **feladatkörét**. NYUGTÁZVA, hogy e kezdeményezések némelyikének eredményeként az ENISA kiegészítő forrásokban részesült, KIEMELI, hogy az ENISA feladatkörének kibővítése, valamint a kiberfenyegetések és a kiberbiztonsági kihívások egyre összetettebbé válása az ENISA feladatainak jelentős növekedéséhez vezetett, aminek tükröződnie kell a **megfelelő** – emberi, pénzügyi és technikai – **erőforrásokban** annak érdekében, hogy az Ügynökség teljes mértékben képes legyen ellátni a hatáskörébe tartozó valamennyi feladatot, a többéves pénzügyi keretről folytatott tárgyalások sérelme nélkül. E célból FELSZÓLÍTJA a Bizottságot, hogy az Unió általános költségvetése tervezetének elkészítésekor helyezze előtérbe a tagállamok részére a kiberrezilienciájuk és operatív együttműködésük javításához, valamint az uniós jog kidolgozásához és végrehajtásához nyújtott támogatással kapcsolatos intézkedéseket, és állítsa fontossági sorrendbe az ezekkel kapcsolatos feladatokat;

AZ ENISA ÁLTAL A SZAKPOLITIKÁK KIDOLGOZÁSÁHOZ ÉS VÉGREHAJTÁSÁHOZ NYÚJTOTT TÁMOGATÁS

6. EMLÉKEZTET arra, hogy a hatályos kiberbiztonsági jogi keret alapján több kulcsfontosságú, az Unió egészére kiterjedő támogató és tanácsadói feladatkörrel is megbízták az ENISA-t. ÜDVÖZLI, hogy az ENISA szerepe e tekintetben az, hogy **támogatást** nyújtson **a tagállamoknak** a jogalkotási és a nem jogalkotási kezdeményezések hatékony végrehajtásához. FELSZÓLÍTJA az ENISA-t, hogy – a Kiberbiztonsági Együttműködési Csoporttal és a Bizottsággal szoros együttműködésben – továbbra is biztosítson általános betekintést és elemzést a kiberbiztonsággal kapcsolatos hatályos jogi környezetre vonatkozóan. ÖSZTÖNZI az ENISA-t, hogy rendszeresen és strukturált módon ossza meg és aktívan mozdítsa elő a technikai iránymutatásokat és a legjobb gyakorlatokat, támogatva a tagállamokat a kiberbiztonsági politika és jogszabályok végrehajtásában;

7. TUDATÁBAN VAN annak, hogy az ENISA meghatározó szerepet tölt be **európai kiberbiztonsági tanúsítási rendszerek** kidolgozásában, amelyek alátámasztják az IKT-termékekbe, -szolgáltatásokba és -folyamatokba, valamint ezenkívül az irányított biztonsági szolgáltatásokba vetett bizalmat, tekintettel a kiberbiztonsági jogszabály közelgő célzott módosítására. HANGSÚLYOZZA, hogy a tagállamokat és az ipart aggodalommal tölti el a kiberbiztonsági tanúsítási rendszerek kiválasztásának, kidolgozásának és elfogadásának hosszadalmas folyamata, ezért SÜRGETI a Bizottságot, hogy éljen a kiberbiztonsági jogszabály értékelése által kínált lehetőséggel, és tárja fel, hogy az uniós kiberbiztonsági tanúsítási rendszerek kidolgozása tekintetében miként rendelkezhetnénk egy egyszerűbb, kockázatalapú, valamint átláthatóbb és gyorsabb megközelítéssel, HANGSÚLYOZVA egyúttal a tagállamok által az erre irányuló folyamatban betöltött fontos szerepet. Emellett HANGSÚLYOZZA annak fontosságát, hogy az egyes tanúsítási rendszerek fenntartása tekintetében kifejezetten meg kell állapítani a felelősséget. EMLÉKEZTET továbbá arra, hogy az ENISA-nak a javasolt tanúsítási rendszerek kidolgozása során hivatalos, nyílt, átlátható és inkluzív folyamat keretében kellő időben konzultálnia kell valamennyi érintett érdekelt féllel, és hogy a Bizottságnak nyílt, átlátható és inkluzív módon kell konzultálnia az elfogadott rendszerek hatékonyságának és alkalmazásának értékelése során. ÖSZTÖNZI az ENISA-t, hogy erősítse tovább az adatvédelmi közösséggel, különösen – adott esetben – az Európai Adatvédelmi Testülettel és az illetékes nemzeti hatóságokkal folytatott együttműködést, különös figyelmet fordítva a szinergiák előmozdítására a jövőbeli európai kiberbiztonsági tanúsítási rendszerek kidolgozásával összefüggésben;

8. az összetett jelentéstételi keret miatt esetlegesen felmerülő szükségtelen adminisztratív terhek megelőzése érdekében FELSZÓLÍTJA az ENISA-t, hogy – a Bizottsággal együttműködve – folytassa a tagállamokkal való, a jelentéstételi eljárás gyakorlati vonatkozásaira, egyszerűsítésére és észszerűsítésére irányuló párbeszédet. EMLÉKEZTET továbbá arra, hogy felkérte a Bizottságot, hogy – az ENISA és más megfelelő uniós szervezetek támogatásával – térképezze fel a kiber- és digitális kérdésekkel foglalkozó vonatkozó uniós jogalkotási aktusokban meghatározott releváns jelentéstételi kötelezettségeket. EMLÉKEZTET arra, hogy az ENISA és a tagállamok közötti információcsere bizalmi viszonyon alapul, amelynek keretében a biztonság és a titoktartás a kiberbiztonsági jogszabálynak, valamint a vonatkozó szabályoknak és eljárásoknak megfelelően garantált, továbbá arra kell korlátozódnia, ami az információcsere céljából releváns és arányos. HANGSÚLYOZZA, hogy az adatokat és az információkat kellő gondossággal kell kezelni;

9. KIEMELI, hogy az ENISA feladata **a kiberrezilienciáról szóló jogszabály szerinti egységes jelentéstételi platform** létrehozása és fenntartása. Ez a platform konkrét operatív hozzáadott értékkel fog rendelkezni, különösen a digitális elemeket tartalmazó termékek biztonságát érintő, aktívan kihasznált sebezhetőségek és súlyos események vonatkozásában. Tekintettel e horizontális jogszabály tág hatályára, az egységes jelentéstételi platformnak hatékony és biztonságos eszköznek kell lennie a nemzeti CSIRT-ek és az ENISA közötti információmegosztás elősegítése tekintetében. Következésképpen SÜRGETI az ENISA-t, hogy – elegendő emberi erőforrás allokálása mellett – kulcsfontosságú prioritásként gyorsítsa fel a platform létrehozását annak biztosítása érdekében, hogy az a kiberrezilienciáról szóló jogszabályban meghatározott határidőre elkészüljön;

10. ELISMERI az ENISA-nak az **európai biztonságirés-adatbázis** létrehozásában játszott szerepét, amely adatbázis célja, hogy jobb átláthatóságot biztosítson a sebezhetőségek feltárása tekintetében, biztosítva egyúttal az érzékeny adatok megfelelő kezelését. Figyelemmel a NIS 2 irányelv átültetési időszakának végére, SÜRGETI az ENISA-t, hogy gyorsítsa fel az említett adatbázis zökkenőmentes működésének biztosításához szükséges valamennyi munkát. Ezzel párhuzamosan FELKÉRI a Kiberbiztonsági Együttműködési Csoportot, hogy az ENISA segítségével tegye ismertebbé a sebezhetőségek feltárására vonatkozó iránymutatásokat, politikákat és eljárásokat;

11. TISZTÁBAN VAN az ENISA által végzett **kiberbiztonsági támogatási fellépés** előnyeivel, amely fellépés a tagállamok rendelkezésére álló, erőfeszítéseik kiegészítését célzó kiberbiztonsági szolgáltatások összességeként működik, továbbá az ENISA-nak az e fellépés végrehajtása során szerzett tapasztalataival is. E tekintetben KIEMELI, hogy az ENISA-nak központi szerepet kell betöltenie az uniós kiberbiztonsági tartalék igazgatásában és működtetésében. FELKÉRI az ENISA-t, hogy a kiberszolidaritásról szóló jogszabály hatálybalépését követően haladéktalanul kezdje meg a szükséges szolgáltatásoknak és azok rendelkezésre állásának a feltérképezését annak érdekében, hogy az uniós kiberbiztonsági tartalék ezáltal minden tagállamban a lehető leghasznosabb legyen, valamint a lehető legnagyobb mértékben igazodjon a felhasználói igényekhez. FELKÉRI az ENISA-t, hogy – amint az erre vonatkozó megbízását megkapta – az uniós kiberbiztonsági tartalék létrehozásának korai szakaszában vonja be a tagállamokat, különösen azáltal, hogy információkat gyűjt az előírt kritériumokról, valamint tájékoztatást nyújt a közelgő pályázatokról. FELKÉRI az ENISA-t, hogy – amint az erre vonatkozó megbízását megkapta – gondoskodjon arról, hogy az irányított biztonsági szolgáltatók kiválasztásának folyamata átlátható, nyitott és tisztességes legyen, továbbá tegye lehetővé, hogy abban – mérettől függetlenül – minden tagállamból származó szolgáltatók részt vehessenek. Ezen túlmenően EMLÉKEZTET arra, hogy az ENISA indokolatlan késedelem nélkül köteles kiadni a határokon átnyúló kiberközpontokra vonatkozó interoperabilitási iránymutatásokat;

12. ALÁHÚZZA, hogy egy olyan gyorsan fejlődő területen, mint a kibertér, kulcsfontosságú **a kialakulóban lévő technológiákkal kapcsolatos tendenciák nyomon követése** a kiberbiztonsági helyzetünk megőrzéséhez és további megerősítéséhez. ELISMERI az ENISA által arra irányulóan végzett munkát, hogy felhívja a nyilvánosság figyelmét az olyan technológiák által előidézett kockázatokra és kínált lehetőségekre, mint például a mesterséges intelligencia és a kvantuminformatika, ezáltal elősegítve a jelenlegi kihívások jobb megértését. BUZDÍTJA az ENISA-t, hogy továbbra is járuljon hozzá e feladatokhoz, ösztönözze aktívan az ajánlásainak a végrehajtását, valamint adott esetben nyújtson tanácsot az Európai Kiberbiztonsági Kompetenciaközpont részére, és működjön együtt azzal;

AZ ENISA ÁLTAL A KIBERREZILIENCIA ÉS AZ OPERATÍV EGYÜTTMŰKÖDÉS JAVÍTÁSA TERÉN A TAGÁLLAMOKNAK NYÚJTOTT TÁMOGATÁS

13. NYOMATÉKOSÍTJA, hogy az ENISA **a két uniós szintű, a tagállamok által irányított kiberegyüttműködési hálózatnak, a CSIRT-ek hálózatának és az EU-CyCLONe-nak a titkárságaként** fontos szerepet tölt be. HANGSÚLYOZZA az ENISA-nak a Kiberbiztonsági Együttműködési Csoportban való, különösen a különböző munkaágakban történő aktív részvétele és technikai hozzájárulásai révén megvalósuló értékes részvételét. ÖSZTÖNZI az ENISA-t, hogy a jövőben is támogassa e hálózatok működését és együttműködését, mivel azok alapvető csatornákat biztosítanak a tagállamok számára a különböző szinteken történő együttműködés céljából;

14. ISMÉTELTEN HANGSÚLYOZZA, hogy szükség van a **közös helyzetismeret** javítására uniós szinten, ami hozzájárul az EU kiberbiztonsági helyzetéhez, összefüggésben a kiberbiztonsági események észlelésével, valamint az azokra való felkészüléssel és reagálással. E tekintetben NYOMATÉKOSÍTJA, hogy milyen fontosak az ENISA előrejelzési tevékenységei, rendszeres jelentései és fenyegetésértékelései, amelyek mindegyike hozzájárul a helyzetismeret javításához. ÖSZTÖNZI az ENISA-t arra, hogy az uniós szintű helyzetismeret fejlesztéséhez való hozzájárulás során szorosan működjön együtt a tagállamokkal. Ezzel összefüggésben ELISMERI, hogy az ENISA – a CERT-EU-val és az Europollal együtt – fontos szerepet játszik abban, hogy a kiberdiplomáciai eszköztár keretében készített, az egységes információelemzési kapacitás (SIAC) által biztosított helyzetismeretet kiegészítő helyzetismertetők révén támogatja a Tanácsot, valamint NYOMATÉKOSÍTJA, hogy átfogó fenyegetettségi képet kell kialakítani különböző forrásokból, beleértve a magánszektort is. ÖSZTÖNZI e tekintetben az ENISA által az EKSZ-szel – és különösen az INTCEN-nel – folytatott együttműködés továbbfejlesztését, a megbízatásuk teljes körű tiszteletben tartása mellett;

15. KIEMELI, hogy a Bizottság kiberbiztonsági helyzetfeltáró és elemző központja a Bizottságon belüli, belső funkciót tölt be, és azt az ENISA-val és a CERT-EU-val folytatott együttműködése segíti. Annak érdekében, hogy létrejöjjön a szinergiák maximális lehetősége, és csökkenjen az összetettség az uniós kiberbiztonsági ökoszisztémán belül, FELKÉRI a Bizottságot, hogy vegye figyelembe a kiberbiztonsági jogszabály értékelésének eredményeit és a kiberbiztonsági terv értékeléséről folytatott megbeszéléseket annak érdekében, hogy észszerűsíteni lehessen a Bizottság kiberbiztonsági helyzetfeltáró és elemző központjának feladatait, valamint az ENISA kapcsolódó feladatait. ÖSZTÖNZI a Bizottságot, hogy kerülje el a feladatok szükségtelen megkettőzését, egyidejűleg megőrizve az ENISA-nak az uniós szintű közös helyzetismeret kialakításához való hozzájárulásban betöltött központi szerepét, amellyel támogatja a tagállamokat, kellően tiszteletben tartva azok nemzeti hatásköreit;

16. NYOMATÉKOSÍTJA, hogy a közös helyzetismeret kialakítása előfeltétele az Unió egészében, időben történő és hatékony válságkezelésnek. ALÁHÚZZA, hogy uniós szinten számos különböző kulcsfontosságú szereplő vesz részt **a nagyszabású kiberbiztonsági eseményekre való reagálásban**, továbbá hogy ilyen események bekövetkezése esetén a tagállamok közötti hatékony együttműködés sarokkövét a CSIRT-ek hálózata és az EU-CyCLONe képezi. Az ENISA a CSIRT-ek hálózatának és az EU-CyCLONe-nak a titkárságaként fontos szerepet játszik a kiberválságok kezelésében. FELKÉRI a Bizottságot, hogy a kiberbiztonsági terv értékelését használja fel arra, hogy megfelelő módon reflektáljon a nagy kiterjedésű, határokon átnyúló biztonsági eseményekre és válságokra való, együttműködésen alapuló válasz kidolgozásához történő hozzájárulással kapcsolatos további feladatokra és felelősségi körökre, valamint az ENISA-ra mint a CSIRT-ek hálózatának és az EU-CyCLONe-nak a titkárságára háruló, továbbá a közelmúltbeli kiberbiztonsági jogszabályok által ráruházott szerepre;

17. ALÁHÚZZA a rendszeres **kiberbiztonsági gyakorlatok** szervezésének jelentőségét, amelyek jelentősen növelik az EU felkészültségét az eseményekre és válságokra való reagálás terén. TUDATÁBAN VAN annak, hogy az ENISA értékes és széles körű tapasztalatokra tett szert ezen a területen, támogatva a tagállamokat. TISZTÁBAN VAN azzal, hogy az ENISA fontos szerepet játszik a kiberbiztonsági gyakorlatok tervezési, előkészítő, végrehajtási és értékelési szakaszában, továbbá HANGSÚLYOZZA, hogy annak továbbra is az egyik központi szereplőnek kell maradnia uniós szinten, szem előtt tartva azt, hogy az említett gyakorlatokat strukturált keretekre és közös terminológiákra alapozva kell végrehajtani. FELKÉRI az ENISA-t, a CSIRT-ek hálózatát és az EU-CyCLONe-t, hogy a lehető leghatékonyabban használják ki a meglévő rendszeres gyakorlatokat az uniós válságreagálási keret tesztelése és javítása céljából, valamint biztosítsák a levont tanulságok maximális hasznosítását;

AZ ENISA EGYÜTTMŰKÖDÉSE A KIBERBIZTONSÁGI ÖKOSZISZTÉMA EGYÉB SZEREPLŐIVEL

18. ÚJÓLAG HANGSÚLYOZZA, hogy a kiberbiztonság horizontális jellege miatt létfontosságú **az összes szereplő közötti együttműködés tagállami és uniós szinten** egyaránt, valamint RÁMUTAT arra, hogy az általános kiberreziliencia európai szintű növeléséhez az ENISA és a kiberterület egyéb releváns szervezetei közötti közös munkára is szükség van;

19. ALÁHÚZZA, hogy az uniós intézmények, szervek és hivatalok azon képessége, hogy megőrizzék kiberbiztonságukat, fontos az általános uniós szintű kiberreziliencia szempontjából, amelyben a CERT-EU szerepe felbecsülhetetlen értékű. E tekintetben ÜDVÖZLI a CERT-EU és az ENISA között kialakult strukturált együttműködést, továbbá ÖSZTÖNZI őket arra, hogy a jövőben is folytassák szoros együttműködésüket;

20. Az elért pénzügyi autonómia révén az Európai Kiberbiztonsági Kompetenciaközpont jelentősen hozzá fog járulni egy erőteljes európai kiberbiztonsági kutatási, ipari és technológiai ökoszisztéma kialakításához, magában foglalva a munkaerő-fejlesztéshez szükséges készségeket, a megbízatásával összhangban. ÖSZTÖNZI az ENISA-t és az Európai Kiberbiztonsági Kompetenciaközpontot, hogy az uniós kiberbiztonsági ipar versenyképességének növelése érdekében folytassák szoros együttműködésüket, különösen a kutatási és innovációs igényekkel és prioritásokkal, valamint a kiberkészségekkel kapcsolatosan. FELKÉRI a Bizottságot annak megvizsgálására, hogy az ENISA és az Európai Kiberbiztonsági Kompetenciaközpont működését illetően hogyan lehet még nagyobb mértékben optimalizálni a szinergiákat és még jobban észszerűsíteni a tevékenységeket, a megbízatásuknak megfelelően;

21. ALÁHÚZZA, hogy a fenyegetettségi helyzettel kapcsolatos, rendszeres és naprakész tájékoztatás nyújtása hozzájárul a kiberbűnözés elleni hatékony küzdelemhez szükséges intézkedések és eszközök jobb azonosításához. HANGSÚLYOZZA azt a hozzáadott értéket, amelyet az EU közös kiberértékelési jelentései (J-CAR) képviselnek, amelyek az ENISA, az Europol Kiberbűnözés Elleni Európai Központja (EC3) és a CERT-EU közötti közös együttműködés eredményei, és már eddig is értékes hozzájárulást nyújtottak a különböző kihívások kezeléséhez, beleértve a kiberbűnözés elleni küzdelmet is. FELKÉRI az ENISA-t és az Europolt, hogy a jövőben is folytassanak strukturált módon történő együttműködést;

22. NYOMATÉKOSÍTJA, hogy a kibervédelem a kibertérből származó fenyegetések kezelésének fontos és folyamatosan fejlődő részét képezi. KIEMELI annak szükségességét, hogy az ENISA működjön együtt az EKSZ-szel és a Bizottsággal azokban az esetekben, amelyekben az ENISA szerepet játszik az uniós kibervédelmi politika végrehajtásának támogatásában, szoros együttműködésben az EDA-val, az Európai Kiberbiztonsági Kompetenciaközponttal és a kibervédelmi közösséggel. HANGSÚLYOZZA az ENISA polgári ügynökségként betöltött szerepét. ALÁHÚZZA, hogy fontos a polgári-katonai együttműködés elmélyítése és észszerűsítése a kiberterületen az EU-n belül, ideértve a szerep- és feladatkörök egyértelmű megosztását a két közösség között, valamint az EU és a NATO között, teljes mértékben tiszteletben tartva az inkluzivitás, a kölcsönösség, a kölcsönös nyitottság és az átláthatóság elvét, valamint a két szervezet döntéshozatali autonómiáját. ÖSZTÖNZI az ENISA-t, hogy továbbra is törekedjen munkamegállapodásokra a NATO Kommunikációs és Információs Ügynökségével;

23. BUZDÍTJA az EU-t, hogy a szabad, globális, nyitott és biztonságos kibertér megőrzése érdekében továbbra is mozdítsa elő közös értékeinket és közös erőfeszítéseinket a globális fórumokon belül. HANGSÚLYOZZA, hogy a kiberfenyegetések és -események határokon átnyúló jellege erőteljes és hatékony együttműködést tesz szükségessé nem csupán uniós szinten, hanem a **nemzetközi szervezetekkel és partnerekkel** is. MEGÁLLAPÍTJA, hogy az ENISA nemzetközi részvételének a stratégiai partnerekre és az uniós tagjelölt országokra kell fókuszálnia, összhangban az EU közös kül- és biztonságpolitikájával. NYOMATÉKOSÍTJA, hogy az ENISA-nak a nemzetközi részvétele során a megbízatásával és a kiberbiztonsági jogszabály vonatkozó rendelkezéseivel összhangban kell eljárnia. TUDATÁBAN VAN annak, hogy a vonatkozó eljárásokkal összhangban egyértelműsíteni kell az ENISA nemzetközi részvételét, biztosítva különösen azt, hogy az ENISA igazgatótanácsa a kapcsolódó tevékenységekről megfelelő módon és időben tájékoztatást kapjon. ÖSZTÖNZI az ENISA részvételét a releváns nemzetközi kiberbiztonsági együttműködési keretekben, ideértve olyan szervezeteket is, mint a NATO és az EBESZ;

24. ISMÉTELTEN HANGSÚLYOZZA, hogy az EU és annak tagállamai gyakorta rámutattak a **kiberbiztonsági készségek** terén meglévő hiányosságokra. EMLÉKEZTET arra, hogy a Bizottság és az ENISA az összes érdekelt fél számára történő iránymutatás érdekében széles körű és átfogó keretet vezetett be, amelynek részét képezi például az Európai Kiberbiztonsági Készségek Kerete, a Kiberkészségek Akadémiájáról szóló közlemény, valamint a kiberkészségekről szóló, évente megrendezett európai konferencia, továbbá ÖSZTÖNZI a Bizottságot és az ENISA-t, hogy – különös tekintettel az európai digitális infrastruktúra-konzorciumról (EDIC) folyamatban lévő megbeszélésre – építsen e kezdeményezésekre. E célból FELKÉRI a Bizottságot, hogy egyeztessen EDIC létrehozásában érdekelt tagállamokkal. ELISMERI, hogy mind az ENISA, mind pedig az Európai Kiberbiztonsági Kompetenciaközpont megbízatással rendelkezik a készségek Unió-szerte történő előmozdítására. FELKÉRI az ENISA-t, hogy kezelje prioritásként a tagállamok készségfejlesztési és oktatási erőfeszítéseinek támogatását, a közvélemény tudatosságának erősítését, továbbá adott esetben működjön együtt az Európai Kiberbiztonsági Kompetenciaközponttal;

25. TISZTÁBAN VAN azzal, hogy az ENISA az elmúlt években **együttműködést** alakított ki **a magánszektorral**. EMLÉKEZTET arra, hogy mivel a magánszektor folyamatosan figyelemmel kíséri a kiberfenyegetettségi helyzetet, az iparág által gyűjtött információk segíthetnek a közös helyzetismeret javításában. Ezért arra BUZDÍTJA az ENISA-t, hogy a tagállamokkal szoros együttműködésben és az uniós szervezeteken átívelően fokozza a magánszektorral való együttműködést;

26. FELSZÓLÍTJA a Bizottságot és az ENISA-t, hogy vizsgálják meg, miként lehetne fokozni az ENISA és az európai **szabványügyi** szervezetek közötti együttműködést. NYOMATÉKOSÍTJA, hogy az ENISA-nak növelnie kell az európai kiberbiztonsági szabványosítással kapcsolatos szakértelmét, többek között a szabványosítási tevékenységek nyomon követése és az azokban való részvétel útján;

27. SÜRGETI a Bizottságot és az ENISA-t, hogy vizsgálják meg, miként lehet tovább optimalizálni az uniós kiberbiztonsági keret működését, figyelembe véve az e következtetésekben foglalt ajánlásokat és javaslatokat. A folyamatos együttműködés, a feladatok és az erőforrások rangsorolása, valamint az összetett kiberkörnyezet egyszerűsítése a jelenlegi és a jövőbeli kihívások kezelésének kulcsfontosságú elemeit jelentik majd.