Az Európai Unió
Tanácsa

Brüsszel, 2023. május 22.
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Címzett:	a delegációk
Előző dok. sz.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Tárgy:	A Tanács következtetései az EU kibervédelmi politikájáról

Mellékelten továbbítjuk a delegációknak az EU kibervédelmi politikájáról szóló tanácsi következtetéseket, amelyeket a Tanács a 2023. május 22-i ülésén jóváhagyott.

A Tanács következtetései az EU kibervédelmi politikájáról

1. A 2014-ben elfogadott és 2018-ban naprakésszé tett uniós kibervédelmi szakpolitikai keretre építve a Tanács üdvözli az EU kibervédelmi politikájáról szóló ambiciózus közös közleményt, amelynek célja a modern és interoperábilis fegyveres erőinkbe, az élvonalbeli technológiákba és a legkorszerűbb kibervédelmi képességekbe való további beruházás, valamint a közös kihívások kezelését célzó partnerségek megerősítése. Most, hogy egyre nagyobb mértékben függünk a digitális technológiáktól, a kibertér a stratégiai verseny színterévé vált. Ezért rendkívül fontos, hogy a kibertér nyitott, szabad, stabil és biztonságos maradjon. Az Oroszország által Ukrajnával szemben provokáció nélkül indított és indokolatlan agresszív háborút kiberműveletek előzték meg és kísérik, mindez pedig hatással van a globális stabilitásra és biztonságra, az eszkalálódás jelentős kockázatát hordozza magában, és tovább növeli a nem fegyveres konfliktusok összefüggésében az elmúlt években már nagy számban tapasztalható rossz szándékú kibertevékenységek volumenét.

2. Az ukrajnai háború új stratégiai környezetet teremtett, és rámutatott mind arra, hogy az EU-nak, a tagállamainak és a partnereiknek tovább kell erősíteniük az EU kiberfenyegetésekkel szembeni rezilienciáját, mind pedig arra, hogy javítanunk kell a közös kiberbiztonságunkat és kibervédelmünket a kibertérben tanúsított rosszindulatú magatartással és agresszióval szemben. Az EU kibervédelmi politikájáról szóló közös közlemény jelzi azon elhatározásunkat, hogy azonnali és hosszú távú intézkedéseket hozzunk a kibertérben való tevékenységek szabadságának biztosítása érdekében, és reagáljunk azon, fenyegetést jelentő szereplők fellépéseire, akik kísérletet tesznek többek között az EU és partnerei hálózati és információs rendszereibe való behatolásra, illetve e rendszerek megzavarására vagy megsemmisítésére. Az EU kiberbiztonsági stratégiájának kiegészítéseként és a stratégiai iránytűvel összhangban ez a közös közlemény jelentős lépést jelent egy teljes körű, a rezilienciára, a reagálásra, a konfliktusmegelőzésre, a kibertérbeli együttműködésre és stabilitásra egyaránt vonatkozó uniós megközelítés felé. Ezzel összefüggésben a Tanács egyrészről hangsúlyozza, hogy az EU-nak, a tagállamoknak és partnereiknek megfelelő és koherens válaszokat kell adniuk, másrészről várakozással tekint az uniós kiberdiplomáciai eszköztár végrehajtási iránymutatásainak felülvizsgálata elé, amely újabb fontos lépés az EU kiberbiztonsági helyzetének alakítása terén.

3. A Tanács hangsúlyozza, hogy az európai kritikus infrastruktúrák elleni közelmúltbeli kibertámadások, a kiberfenyegetések gyorsan változó környezete és a technológiai fejlődés gyors üteme szintén rámutat arra, hogy fokozott polgári-katonai koordinációra és együttműködésre van szükség, ugyanakkor kiemeli azt is, hogy nincs hierarchia a polgári és a katonai közösségek között.
   Az EU kibervédelmi politikája lehetővé teszi az EU és tagállamai számára, hogy a nemzetközi joggal, többek között az emberi jogok nemzetközi jogával és a nemzetközi humanitárius joggal összhangban megerősítsék a védelemre, a felderítésre, az elhárításra és az elrettentésre irányuló képességeiket, megfelelően kihasználva a polgári és katonai közösségek rendelkezésére álló valamennyi védelmi lehetőséget az EU szélesebb körű biztonsága és védelme érdekében.

4. Bár a nemzetbiztonság – többek között a kibertérben is – továbbra is az egyes tagállamok kizárólagos felelőssége, amint azt az EUSZ 4. cikkének (2) bekezdése is megállapítja, a Tanács hangsúlyozza, hogy úgy egyénileg, mint közösen érdemben be kell ruházni a reziliencia megerősítésébe és a teljes spektrumú defenzív kibervédelmi képességek telepítésébe, valamint mozgósítani kell az uniós együttműködési kereteket és pénzügyi ösztönzőket. A Tanács hangsúlyozza, hogy az Unió, a polgáraink, az uniós intézmények, szervek és hivatalok, valamint a kibertérben folytatott KBVP-missziók és -műveletek védelme érdekében tovább kell erősíteni a tagállamok, valamint az uniós intézmények, szervek és hivatalok intézkedéseit. Ezenfelül hangsúlyozza, hogy meg kell erősíteni az EU kibertérben való rezilienciáját a kibervédelmi képességek fejlesztése és a megbízható magánökoszisztémával való együttműködés fokozása révén.

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

5. A Tanács újólag hangsúlyozza, hogy a bizalom növelése a záloga annak, hogy folytatni lehessen egy uniós kiberbiztonsági válságkezelési keret kialakítását a Tanács által kidolgozott kiberválság-kezelési ütemtervvel összhangban, a bizalom növeléséhez pedig elengedhetetlen egy fokozatos, átlátható és inkluzív folyamat. A Tanács ismételten rámutat arra, hogy tovább kell javítanunk kell kibertámadásokkal szembeni védelemre, e támadások észlelésére, elhárítására, illetve az azoktól való elrettentésre irányuló képességünket, amit jobb helyzetismerettel, kapacitásépítéssel, képességfejlesztéssel, képzéssel, gyakorlatokkal, és a reziliencia megerősítésével valósíthatunk meg, valamint azzal, hogy valamennyi rendelkezésre álló uniós eszközzel határozott választ adunk az EU és tagállamai, illetve az uniós intézmények, szervek és hivatalok, továbbá a KBVP-missziók és -műveletek ellen irányuló kibertámadásokra. Ezzel összefüggésben a Tanács arra ösztönzi a főképviselőt és a Bizottságot, hogy a kiberterületen tegyék egyszerűbbé az eljárásokat, kerüljék el a szükségtelen átfedéseket, és biztosítsák a meglévő kezdeményezésekkel való együttműködést és szinergiákat. Meg kell erősíteni az együttműködést és a koordinációt az EU-n és a tagállamokon belüli és az azokhoz tartozó kibervédelmi szereplők, a katonai és polgári kiberközösségek, valamint a köz- és a megbízható magánökoszisztéma között. Ezzel összefüggésben a Tanács arra ösztönzi a tagállamokat, hogy tárják fel polgári-katonai nemzeti koordinációs mechanizmusok lehetőségét, illetve erősítsék meg azokat, segítsék elő a közös önkéntes információmegosztást, osszák meg a levont tanulságokat, járuljanak hozzá interoperábilis szabványok kidolgozásához, végezzenek kockázatértékeléseket és készítsenek kockázati forgatókönyveket, valamint végezzenek – különösen európai szinten – közös gyakorlatokat, teljes mértékben tiszteletben tartva az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelv (NIS2) rendelkezéseit.

6. A Tanács – elismerve az Unió rezilienciájának a NIS 2 irányelv és a kritikus szervezetek rezilienciájáról szóló irányelv révén történő további fokozására irányuló erőfeszítéseket – megismétli a kritikus infrastruktúrák rezilienciájának megerősítését célzó, uniós szintű összehangolt megközelítésre vonatkozó ajánlását[1]. Intézkedéseket szorgalmaz a kritikus szervezetek, az infrastruktúra és a digitális termékek és szolgáltatások rezilienciájának további fokozása érdekében, ugyanakkor megjegyzi, hogy továbbra is a NIS 2 irányelv megfelelő végrehajtása a legfontosabb lépés. Ez – bár túlnyomórészt a polgári területet érintő felelősség – hozzájárul az erősebb kibervédelemhez is. Ezzel összefüggésben a Tanács arra ösztönzi az Unió intézményeit, szerveit és hivatalait, valamint a tagállamokat, hogy támogassák az új és a meglévő uniós koordinációs mechanizmusok, kockázatértékelések, értékelések és forgatókönyvek, valamint a közös önkéntes információmegosztás és gyakorlatok továbbfejlesztését és alkalmazását oly módon, amely hozzáadott értéket teremt, és amely által elkerülhetők a meglévő kezdeményezésekkel való szükségtelen átfedések.

7. A bizalom további erősítése, az együttműködés megszilárdítása és a védelmi rendszereket érintő jelentős és nagyszabású kiberbiztonsági eseményekkel kapcsolatos információk időben történő megosztásának megkönnyítése érdekében a Tanács üdvözli az arra irányuló kezdeményezést, hogy továbbfejlesszék az Európai Unió Tanácsának elnökségei által – az Európai Védelmi Ügynökség (EDA) támogatásával és az Európai Külügyi Szolgálat (EKSZ) részvételével – megrendezendő uniós kibervédelmi parancsnoki konferenciát. A Tanács arra ösztönzi az összes tagállamot, hogy vegyenek részt ezeken a megbeszéléseken. A Tanács az EU nagyszabású kiberbiztonsági eseményekkel szembeni rezilienciájának megerősítése érdekében felkéri az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe) és az uniós kiberparancsnokok konferenciáját, hogy határozzák meg az együttműködésnek, valamint a közös katonai és polgári perspektíva kiaknázásának a lehetséges módjait.

[1] Javaslat – A Tanács ajánlása a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről, COM(2022) 551.

8. A határozottabb és koordináltabb uniós szintű reagálás előmozdítása céljából a Tanács üdvözli a katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok uniós operatív hálózatának (MICNET) létrehozását, és várakozással tekint a hálózat kezdeti műveleti képességének 2024 közepéig történő elérése elé, amely hálózat célja, hogy a részt vevő tagállamok között javuljon a védelmi rendszereket érintő kiberbiztonsági eseményekkel kapcsolatos technikai információmegosztás. A Tanács minden tagállamot arra ösztönöz, hogy a hálózat hatékonyságának biztosítása érdekében vegyen részt a MICNET-ben. A Tanács felkéri továbbá a tagállamokat, hogy építsenek a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) hálózata tekintetében levont tanulságokra, és határozottan sürgeti, hogy kellő időben hozzanak létre hatékony együttműködési és koordinációs mechanizmust a két hálózat között, teljes mértékben tiszteletben tartva az egyes szervezetek irányítási mechanizmusait és felhasználóit.

9. Tekintettel arra, hogy állami és nem állami szereplők egyre több rossz szándékú kibertevékenységet folytatnak az EU KBVP-missziói és -műveletei ellen, a Tanács felkéri az EU-t és tagállamait, hogy erősítsék meg a KBVP-missziók és -műveletek védelmét és biztonságát célzó képességeiket. E tekintetben a Tanács üdvözli azokat a célkitűzéseket, amelyek az uniós katonai hálózatok és struktúrák védelmének – többek között az EU kibertérrel mint műveleti területtel kapcsolatos katonai koncepciójával és stratégiájával[2] összhangban történő – további előmozdítására irányulnak.

[2] EEAS(2021) 706 REV4.

10. A Tanács újólag hangsúlyozza a 2022. májusi tanácsi következtetésekben[3] foglaltakat, valamint azt, hogy aktívan hozzá kell járulnunk az EUSZ 42. cikkének (7) bekezdése szerinti kölcsönös segítségnyújtáshoz, valamint az EUMSZ 222. cikke szerinti szolidaritáshoz. A Tanács hangsúlyozza, hogy fontos tovább mélyíteni a 42. cikk (7) bekezdése végrehajtásának az EU és tagállamai általi közös értelmezését, többek között a kibertámadást is magában foglaló, összetettebb helyzeteket illetően, a nemzetközi jog vonatkozó alapelveinek megfelelően. Üdvözli annak lehetőségét, hogy az érintett tagállam(ok) kifejezett kérésére az EU – az egyes tagállamok biztonság- és védelempolitikája sajátos jellegének sérelme nélkül – támogatást nyújtson kibertámadás esetén.

11. A Tanács hangsúlyozza a „kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok (CRRT-k), valamint kölcsönös segítségnyújtás a kiberbiztonság területén” elnevezésű PESCO-projekt keretében elért eredményeket, valamint azt, hogy a projekt készen áll arra, hogy kérésre a tagállamok és az EU igényeinek megfelelő képességként lépjen fel a KBVP-missziók és -műveletek támogatása, valamint az EU partnereinek való segítségnyújtás terén. A Tanács üdvözli a PESCO-projekt keretébe tartozó CRRT-k képességeinek, a kiberbiztonsági eseményekre való reagálással foglalkozó nemzeti csoportoknak és adott esetben a biztonsági eseményekre való reagálásra irányuló további képességeknek – például a stratégiai iránytűben előirányzott jövőbeli, hibrid fenyegetéseket kezelő gyorsreagálású csapatoknak – a továbbfejlesztését, amely többek között mindezek uniós szintű koordinációjának és együttműködésének az előmozdítása révén valósul meg.

[3] A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról, 2022. május 23., 9364/22.

12. A Tanács üdvözli a Kiber- és az Információs Terület Koordinációs Központja (CIDCC) elnevezésű PESCO-projekt keretében végzett munkát, amely projekt célja az, hogy katonai képességet biztosítson a közös műveleti kiberbiztonsági helyzetkép szempontjából releváns információk összegyűjtéséhez és elemzéséhez. A Tanács üdvözli továbbá azt a javaslatot, hogy 2025-től kezdődően a koncepcióigazolást – amennyiben az említett szervezet információs koordinációs központként sikeresnek bizonyul – beépítsék egy uniós kibervédelmi koordinációs központba (EUCDCC), fokozva ezáltal a koordinációt és a helyzetismeretet különösen az uniós KBVP-missziók és -műveletek parancsnokai tekintetében, továbbá megerősítve az EU szélesebb értelemben vett vezetési és irányítási architektúráját. A Tanács felkéri a főképviselőt, hogy terjesszen elő koncepciót és ütemtervet az EUCDCC létrehozására vonatkozóan, a hasonló nemzetközi szervezetek tekintetében levont tanulságokra építve, azonosítva a szükséges erőforrásokat, elkerülve a szükségtelen átfedéseket, és törekedve a tágabb uniós kiberbiztonsági kerettel való kiegészítő jellegre.

13. A Tanács kiemeli a kiberfenyegetésekkel és -tevékenységekkel kapcsolatos stratégiai hírszerzési együttműködés fontosságát, és felkéri a tagállamokat, hogy illetékes hatóságaikon keresztül továbbra is járuljanak hozzá az EU Helyzetelemző Központja, az Európai Unió Katonai Törzsének Hírszerzési Igazgatósága, valamint a tagállamok által az egységes információelemzési kapacitás (SIAC) keretében végzett munkához. A Tanács hangsúlyozza továbbá, hogy meg kell erősítenünk kiberhírszerzési kapacitásainkat a kiberrezilienciánk és a reagálás fokozása, továbbá polgári és katonai KBVP-misszióink és -műveleteink, valamint fegyveres erőink és a SIAC kiberbiztonsági kapacitásainak hatékony támogatása érdekében, a tagállamok önkéntes hírszerzési hozzájárulásai alapján és hatáskörük sérelme nélkül.

14. A Tanács nyugtázza az Európai Bizottság kiberbiztonsági helyzetfeltáró és elemző központját, amelynek célja a Bizottság helyzetismeretének javítása. A Tanács hangsúlyozza, hogy kölcsönösen előnyös együttműködést kell kialakítani e központ és más uniós intézmények, szervek és hivatalok – különösen az ENISA és a CERT-EU – között. A Tanács nyomatékosítja, hogy a helyzetismeret kialakítása során biztosítani kell az uniós együttműködési hálózatokkal való szoros együttműködést, valamint tiszteletben kell tartani az információk bizalmas jellegét. A Tanács megállapítja, hogy uniós szinten meg kell erősíteni a közös helyzetismeretet, és – a szükségtelen párhuzamos erőfeszítések elkerülése mellett – tovább kell fejleszteni az uniós kiberbiztonsági válságreagálási keretet.

15. A Tanács emlékeztet arra, hogy a kiberoktatás, -képzés és -gyakorlatok elengedhetetlenek a felkészültség és a hatékonyság biztosításához, és üdvözli a nemzeti tevékenységeket, valamint az EU által az Európai Biztonsági és Védelmi Főiskola (EBVF), az EDA, az ENISA és a folyamatban lévő PESCO-projektek – például az összevont virtuális gyakorlóterek és az Uniós Kiberakadémia és Innovációs Központ (CAIH) – keretében biztosított tevékenységeket. Ezen erőfeszítések további fokozása szempontjából a Tanács várakozással tekint az EDA CyDef-X keretprojektjének létrehozása elé, amelynek célja a kibervédelmi gyakorlatok összehangolása és támogatása. A Tanács arra ösztönzi az EDA-t, hogy a tagállamokkal és az EKSZ-szel – a polgári gyakorlatok esetében pedig a Bizottsággal és az ENISA-val is – szoros együttműködésben vizsgálja meg, hogy a CyDef-X miként tudná még inkább támogatni az olyan gyakorlatokat, mint a CYBER PHALANX, többek között az EUSZ 42. cikkének (7) bekezdése szerinti kölcsönös támogatás és az EUMSZ 222. cikke szerinti szolidaritási klauzula tekintetében. A Tanács szorgalmazza továbbá, hogy a CyDef-X-en belül használják fel és fejlesszék tovább a meglévő kibervédelmi tesztelési és gyakorlási környezeteket, például az összevont virtuális gyakorlótereket. A Tanács hangsúlyozza, hogy a kiberválságokkal kapcsolatos gyors és hatékony döntéshozatali folyamat biztosítása érdekében fontos, hogy rendszeres döntéshozatali gyakorlatokat tartsanak a tagállami döntéshozatali szinten dolgozó személyek részére.

16. A Tanács nyugtázza a kiberbiztonsági szolidaritásról szóló jogszabályra vonatkozó javaslatot, valamint az EU-ban a kiberbiztonsági veszélyek és események felderítéséhez és az azokra való reagáláshoz szükséges képességek megerősítésére irányuló szándékot. A Tanács hangsúlyozza, hogy az e területre vonatkozó javaslatok csak akkor lehetnek eredményesek, ha összhangban vannak a tagállamok válságelhárítási kereteivel és szükségleteivel. A Tanács kiemeli annak fontosságát, hogy a rendelkezésre álló uniós kockázatértékelések figyelembevételével – nemzeti hatáskörben – teszteljék a kritikus infrastruktúrákat a potenciális sebezhetőségek szempontjából, amennyiben a tesztelést hasznosnak ítélik.

17. A Tanács nyugtázza a Bizottság arra irányuló javaslatát, hogy hozzanak létre egy kiberbiztonsági vészhelyzeti mechanizmust, amely elősegíthetné a megbízható magánszolgáltatók kiberbiztonsági szolgáltatásainak rendelkezésre állását, vagyis azt, hogy e szolgáltatók kérésre segítséget nyújtsanak a tagállamoknak nagyszabású kiberbiztonsági események esetén, ugyanakkor hangsúlyozza, hogy e mechanizmus működésének alapvető pilléreként, az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) támogatásával elő kell segíteni az európai kiberbiztonsági ágazat léptékváltását. A Tanács hangsúlyozza, hogy az egyes tagállamokra rendkívül fontos szerep hárul nemzeti szükségleteik nyomon követésében és értékelésében.

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

18. A Tanács újólag hangsúlyozza: ösztönzi kívánja a tagállamokat arra, hogy fejlesszék tovább a kibervédelmi műveletek végrehajtásához szükséges saját képességeiket, ideértve adott esetben a kibertámadások elleni védelemre, azok felderítésére, elhárítására és az azoktól való elrettentésre irányuló proaktív védelmi intézkedéseket is. Tekintettel arra, hogy a NIS 2 irányelv nem vonatkozik azokra a közigazgatási szervekre, amelyek a védelem területén végzik tevékenységüket, a Tanács felkéri az EDA-t, hogy – adott esetben a Bizottság és az EKSZ támogatásával – segítse a tagállamokat olyan, a NIS 2 irányelv által ihletett, jogilag nem kötelező erejű önkéntes ajánlások kidolgozásában, amelyek a védelmi közösség kiberbiztonságának fokozására irányulnak, és felkéri az összes tagállamot, hogy aktívan vegyenek részt ebben a törekvésben. Ezeknek az ajánlásoknak figyelembe kell venniük a más kereteken belül tett hasonló erőfeszítéseket.

19. Ahogyan azt a stratégiai iránytű is elismeri, az EU cselekvőképessége attól függ, hogy képes-e csökkenteni stratégiai függőségeit a kibervédelmi képességeit és ellátási láncait illetően, valamint kifejleszteni és felhasználni az élvonalbeli kibervédelmi technológiákat. Ez magában foglalja az európai védelmi technológiai és ipari bázis (EDTIB) Unió-szerte történő megerősítését, valamint az EU arra való képességének fokozását, hogy a kölcsönös előnyök biztosítása érdekében viszonossági alapon világszerte együttműködjön a hasonló gondolkodású partnerekkel. A Tanács ezért felszólítja a kiberbiztonsági és a kibervédelmi ágazat szereplőit, hogy a teljes spektrumú kibervédelmi képességek kifejlesztése és megvalósítása érdekében szorosan működjenek együtt szinergiák kialakítása céljából. A Tanács felkéri a Bizottságot, hogy – adott esetben az ECCC-vel szoros együttműködésben – további beruházások és szakpolitikai intézkedések révén továbbra is támogassa egy erős, agilis, globálisan versenyképes és innovatív európai kibervédelmi ipari és technológiai bázis kialakítását, beleértve a kis- és középvállalkozásokat (kkv-k) is.

20. Tekintettel a kibervédelmi képességek interoperabilitásának és közös jellegének a fontosságára, beleértve az új generációs kibervédelmi képességek együttműködésen alapuló fejlesztését is, a Tanács felkéri az EDA-t és az Európai Unió Katonai Törzsét, hogy dolgozzanak ki olyan uniós kibervédelmi interoperabilitási követelményeket, amelyek a – különösen az Észak-atlanti Szerződés Szervezete (NATO) keretében meghatározott – meglévő elvekre, folyamatokra és szabványokra épülnek, és összeegyeztethetők azokkal. A Tanács felkéri továbbá a tagállamokat, hogy az Európai Védelmi Szabványügyi Bizottság keretében, szoros együttműködésben valamennyi érdekelt féllel – beleértve adott esetben az európai szabványügyi szervezeteket és a NATO-t is – vizsgálják meg, hogy szükség lehet-e specifikus önkéntes szabványokra a védelmi rendszerekre vonatkozóan.

21. A Tanács üdvözli a Bizottságnak egy olyan terv előterjesztésére irányuló erőfeszítéseit, amely a meglévő polgári kiberbiztonsági és kibervédelmi szabványok alkalmazásának az előmozdítását, valamint új önkéntes szabványok kidolgozását célozza. A Tanács hangsúlyozza, hogy adott esetben össze kell hangolni a kiberbiztonsági és a kibervédelmi szabványokat. A Tanács elismeri, hogy az ilyen önkéntes szabványok hasznosak lehetnek az uniós kiberbiztonsági és kibervédelmi ágazatok számára, és szorosabb együttműködést sürget a polgári és a védelmi szabványügyi testületek között.

22. A Tanács szorgalmazza olyan ajánlások gyors kidolgozását, amelyek a kibertérben folytatott biztonságos kommunikáció meglévő eszközeinek a Bizottság és az érintett intézmények általi feltérképezésén alapulnak. Az ajánlásokat lehetőség szerint össze kell hangolni az információmegosztásra vonatkozó meglévő kezdeményezésekkel, és azok kidolgozásakor figyelembe kell venni a kialakulóban lévő és forradalmi technológiák által a jelenlegi titkosítási módszerekre nézve képviselt kockázatokat is.

23. A Tanács üdvözli továbbá a kezdeti munkát azon kockázatértékeléssel és forgatókönyvekkel kapcsolatban, amelyeket – a Tanács kérésére – a Bizottság, a főképviselő és a Kiberbiztonsági Együttműködési Csoport dolgoz ki, és amelyek kezdetben az energetikai és a távközlési ágazatra terjednek ki. A Tanács tisztában van azzal, hogy az uniós kommunikációs infrastruktúrára és hálózatokra vonatkozó célzott kiberbiztonsági kockázatértékelések is kidolgozás alatt állnak. A Tanács újólag hangsúlyozza: rendkívül fontos, hogy a tagállamok, valamint az uniós intézmények, szervek és hivatalok közös képet alakítsanak ki a kiberbiztonsági események lehetséges hatásairól. A Tanács ezért felkéri a fent említett szereplőket: biztosítsák, hogy az uniós és adott esetben nemzeti szintű intézkedések és támogatás meghatározása és priorizálása során kellő figyelmet kapjanak a kockázatértékelések, a forgatókönyvek és az azokat követő ajánlások. A Tanács szorgalmazza továbbá, hogy a kockázatértékelési folyamatok, valamint a kibergyakorlatok kidolgozása során valamennyi érintett szereplő figyelembe vegye a kockázati forgatókönyveket.

III. **Beruházás a kibervédelmi képességekbe**

24. A Tanács arra ösztönzi a tagállamokat, hogy növeljék az interoperábilis kibervédelmi képességek kiépítésére, fenntartására és továbbfejlesztésére irányuló beruházásaikat. A Tanács támogatja azt, hogy az egyéb kereteken belül tett hasonló erőfeszítéseket figyelembe véve önkéntes vállalások kerüljenek kidolgozásra a nemzeti kibervédelmi képességek továbbfejlesztésére vonatkozóan.

25. A Tanács felszólítja a tagállamokat és az EDA-t, hogy használják ki a képességfejlesztési terv felülvizsgálatában rejlő, arra vonatkozó lehetőséget, hogy ambiciózus célokat tűzzenek ki az együttműködésen alapuló kibervédelem uniós szintű fejlesztése tekintetében. A Tanács továbbá arra ösztönzi a tagállamokat, hogy az aktualizált prioritásokra és a PESCO keretében tett vállalásaikra építve növeljék az együttműködésen alapuló uniós kibervédelmi képességfejlesztési projektekben való részvételük szintjét, és ennek kapcsán elismeri, hogy az uniós szintű, együttműködésen alapuló projektek közvetlen előnyökkel járnak a nemzeti kibervédelmi képességek fejlesztése szempontjából.

26. A Tanács üdvözli a kialakulóban lévő és forradalmi technológiák védelmi vonatkozású rendszerekben való lehetséges alkalmazásainak feltérképezésére irányuló, együttműködésen alapuló, uniós szintű kutatási erőfeszítéseket, megjegyezve ugyanakkor, hogy gondoskodni kell arról, hogy ezek a technológiai fejlesztések gyorsan beépüljenek a meglévő és a jövőbeli képességekbe. A Tanács arra ösztönzi a tagállamokat és az uniós ipart, hogy a lehető legjobban használják ki az együttműködésen alapuló, uniós szintű kutatási lehetőségeket, például az EDA keretében, a folyamatban lévő PESCO-projektekben – mint például az Uniós Kiberakadémia és Innovációs Központ (CAIH) –, továbbá az Európai Védelmi Alap, valamint adott esetben a Horizont Európa és a Digitális Európa program keretében a kettős felhasználású projektek esetében. Ezen túlmenően a Tanács üdvözli a célzott kereteknek a polgári területről – különös tekintettel az uniós védelmi innovációs programra és az európai védelmi innovációs központra – történő technológiaátvételt hasznosító védelmi innováció támogatása céljából való kiaknázását. A Tanács továbbá arra ösztönzi az Európai Kiberbiztonsági Kompetenciaközpontot és az EDA-t, hogy szinergiák létrehozása és a párhuzamosságok elkerülése érdekében dolgozzanak ki munkamegállapodást azzal a céllal, hogy megkönnyítsék a két szervezet személyzete közötti információmegosztást a polgári, a kettős felhasználású és a védelmi technológiai prioritásokkal kapcsolatban.

27. A Tanács üdvözli a Bizottság azon szándékát, hogy az EDA-val, az Európai Kiberbiztonsági Kompetenciaközponttal – megbízatásukkal összhangban – és a tagállamokkal együttműködésben, az érdekelt felekkel – például az iparral – konzultálva olyan technológiai ütemtervet dolgozzon ki a kritikus kibertechnológiákra vonatkozóan, amely a kritikus kibertechnológiák azonosítása, továbbá a technológiai fejlődés és a stratégiai függőségek feltérképezése révén lehetőséget nyújt e függőségek csökkentésére, támogatva az EU stratégiai autonómiáját és technológiai szuverenitását, megőrizve ugyanakkor a nyitott gazdaságot. A Tanács megállapítja, hogy a kritikus kibertechnológiákra vonatkozó technológiai ütemterv segítséget nyújthat az uniós finanszírozási eszközök stratégiai prioritásainak kiválasztásában, ugyanakkor összhangban van az ezekre vonatkozó szabályokkal. A Tanács emlékeztet arra, hogy az EU-nak ambiciózus és határozott európai iparpolitikát kell folytatnia egy olyan fenntartható, vonzó és versenyképes üzleti környezet megteremtése érdekében, amely lehetővé teheti a kiberterületen működő európai szervezetek léptékváltását is.

28. A Tanács nagyra értékeli a kiberbiztonsági készséghiánynak az új szakemberek – köztük nők – bevonzásával, továbbképzéssel és átképzéssel, továbbá a sokszínű és inkluzív kibermunkaerő kiépítését célzó képzésekbe és gyakorlatokba való beruházással és ilyen képzések és gyakorlatok szervezésével történő kezelésére irányuló szándékot. A Tanács – miközben tisztában van azokkal a kihívásokkal, amelyekkel az EU-nak a humán tőke tekintetében szembe kell néznie a kiberbiztonság és a kibervédelem terén – üdvözli a Kiberkészségek Akadémiája kezdeményezést, amely a kibervédelmi munkaerő számára is előnyös lehet.

29. A Tanács felkéri a tagállamokat, hogy osszák meg egymással a szakképzett kiberbiztonsági szakemberek kiképzésére vonatkozó bevált gyakorlatokat, kiaknázva a katonai, a polgári és a bűnüldözési kezdeményezések közötti szinergiákat, és felszólítja az EBVF-et, hogy az EDA és az ENISA támogatásával és szakértelmével mérlegelje a bevált gyakorlatok cseréje javításának, valamint a katonai és polgári területek közötti további szinergiák kialakításának lehetőségeit a képzés és a kiberspecifikus védelmi készségek fejlesztése tekintetében.

30. A Tanács hangsúlyozza, hogy ahhoz, hogy azonosítani és kezelni lehessen a kiberbiztonsági munkaerőpiac terén mutatkozó hiányosságokat, közös értelmezést kell kialakítani a kiberbiztonsági munkaerő összetételéről és a kapcsolódó készségekről, továbbá leszögezi, hogy valamennyi érdekelt felet be kell vonni, beleértve a tagállamokat és az ipart is. A Tanács tudatában van annak, hogy a kiberbiztonsági munkaerőpiac nyomon követésére szolgáló mutatók létrehozása segítene a kiberbiztonsági készségigények azonosításában és a források megfelelő elosztásában, és a szakpolitikákkal kapcsolatos – különösen a NIS 2-ből eredő – kötelezettségek teljesítéséhez is hozzájárulna. A Tanács üdvözli a kibervédelmi készségek tanúsítási keretrendszerére vonatkozó javaslatot, és felkéri a főképviselőt, hogy az EBVF vezetőjeként az EKSZ-szel, a Bizottsággal és a tagállamokkal együttműködésben, a polgári kezdeményezések kiaknázásával törekedjen annak előmozdítására.

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

31. A Tanács felszólítja a főképviselőt és a Bizottságot, hogy erősítsék meg és tegyék intenzívebbé az együttműködésüket, és vizsgálják meg a kibervédelmi szakpolitikákkal kapcsolatos, kölcsönösen előnyös és az igényekhez igazított partnerségek kialakításának lehetőségeit, többek között az Európai Békekeret révén történő kibervédelmi kapacitásépítés terén. Ennek érdekében a kibervédelemmel is foglalkozni kell az EU által a kiberterület kapcsán folytatott párbeszédek és konzultációk, valamint a partnerekkel folytatott általános biztonsági és védelmi konzultációk során. Emellett intenzívebbé kell tenni a magánszektorral folytatott párbeszédet és együttműködést. A Tanács hangsúlyozza, hogy a kiberbiztonsági szabványokkal és tanúsítással kapcsolatos nemzetközi együttműködés hozzáadott értéket jelentene az európai ipar számára. Üdvözli ezért a Bizottság azon kötelezettségvállalását, hogy ezt fontos részévé teszi a harmadik országokkal és nemzetközi szervezetekkel folytatott uniós kiberpárbeszédeknek.

32. A Tanács hangsúlyozza, hogy a kibertérbeli konfliktusok megelőzése és azok kockázatának csökkentése tekintetében jelentős szerepet tölt be a nemzetközi együttműködés, különösen a bizalomépítő intézkedések regionális és nemzetközi szinten – többek között az ENSZ keretében – történő továbbfejlesztése és működőképessé tétele, valamint a kibertérre vonatkozó, már létező bizalomépítő intézkedéseknek például az Európai Biztonsági és Együttműködési Szervezet (EBESZ) keretében történő alkalmazása további ösztönzése révén, többek között nemzetközi feszültségek idején is.
Az EU és tagállamai hangsúlyozzák, hogy a kibertérben alkalmazni kell a hatályos nemzetközi jogot, és hangsúlyozza a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-keretének fenntartására és előmozdítására irányuló folytatódó erőfeszítések fontosságát, valamint azt, hogy munkálkodni kell annak végrehajtásán, többek között a kibertérben tanúsított felelősségteljes állami magatartás előmozdítására irányuló cselekvési program létrehozása révén.

33. Az EU–NATO együttműködésről szóló együttes nyilatkozatokkal összhangban a Tanács felkéri a főképviselőt – az EDA vezetőjeként is – és a Bizottságot, hogy jobban erősítsék meg, mélyítsék el és szélesítsék ki a NATO-val a kiberterületen kialakított partnerséget, teljes mértékben tiszteletben tartva az inkluzivitás, a viszonosság, a kölcsönös nyitottság és az átláthatóság elvét, valamint a két szervezet döntéshozatali autonómiáját. Figyelembe véve, hogy biztosítani kell az egymást kiegészítő és összehangolt erőfeszítéseket, a lehető legnagyobb mértékben bevonva azokat a tagállamokat is, amelyek nem tagjai a NATO-nak, és el kell kerülni a szükségtelen átfedéseket, a Tanács szorgalmazza, hogy az EU és a NATO között hozzanak létre kapcsolatokat a megfelelő szinteken a képzés, az oktatás, a helyzetismeret, a gyakorlatok és a K+F-platformok terén, és keressenek potenciális szinergiákat a nemzeti kibervédelmi képességek fejlesztésére és a válságkezelési keretekre, a kritikus infrastruktúrák védelmére, a helyzetismerettel kapcsolatos véleménycserék fokozására, a rossz szándékú kibertevékenységekre adandó koordinált válaszintézkedésekre, valamint a harmadik országokban folytatott kapacitásépítési erőfeszítésekre vonatkozó önkéntes kötelezettségvállalások között. Ez magában foglalja a NATO kiberbiztonsági eseményeket kezelő képessége (NCIRC) és az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) közötti technikai megállapodást, valamint a kibervédelmi kérdésekről valamennyi szinten folytatott intenzívebb politikai párbeszédet is.

V. **Konklúzió**

34. Az EU kibervédelmi politikájáról szóló tanácsi következtetésekre építve a Tanács felszólítja a főképviselőt és a Bizottságot, hogy a tagállamok általi jóváhagyás céljából 2023 második negyedévéig dolgozzák ki a szóban forgó politikára vonatkozó végrehajtási tervet. A Tanács felkéri továbbá a tagállamokat, hogy az uniós kibervédelmi politikával összefüggésben önkéntesen nyilatkozzanak a kibervédelemmel kapcsolatos ambícióikról és intézkedéseikről, és teljes mértékben használják ki a jogilag nem kötelező erejű önkéntes ajánlásokat és kötelezettségvállalásokat annak érdekében, hogy fokozzák a nemzeti és multinacionális kibervédelmi erőfeszítéseiket annak érdekében, hogy uniós szinten azok a lehető legnagyobb hatást érjék el. A Tanács felkéri a főképviselőt, a Bizottságot és a tagállamokat, hogy 2024 második negyedévétől kezdődően évente tegyenek jelentést és folytassanak megbeszélést a közös közlemény elemeinek végrehajtása és a végrehajtási terv megvalósítása terén elért eredményekről.