Az Európai Unió
Tanácsa

Brüsszel, 2022. május 23.
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2022. május 23.
Címzett:	a delegációk
Tárgy:	A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról – A Tanács által a 2022. május 23-i ülésén jóváhagyott következtetések

Mellékelten továbbítjuk a delegációknak az Európai Unió kiberbiztonsági helyzetének javításáról szóló következtetéseket, melyet a Tanács a 2022. május 23-i ülésén jóváhagyott.

MELLÉKLET

A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról

AZ EURÓPAI UNIÓ TANÁCSA,

EMLÉKEZTETVE:

– „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér” című, az Európai Parlamentnek és a Tanácsnak címzett, 2013. június 25-i közös közleményről szóló tanácsi következtetésekre[1],

– az uniós kibervédelmi szakpolitikai keretre[2],

– az internetirányításról szóló következtetésekre[3],

– a kiberdiplomáciáról szóló tanácsi következtetésekre[4],

– Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatásáról szóló tanácsi következtetésekre[5],

– az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamentnek és a Tanácsnak címzett, 2017. november 20-i közös közleményről szóló tanácsi következtetésekre[6],

– a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”) szóló tanácsi következtetésekre[7],

– a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról szóló tanácsi következtetésekre[8],

– a külső kiberkapacitás-építésre vonatkozó uniós iránymutatásokról szóló tanácsi következtetésekre[9],

– az uniós politikai szintű integrált válságelhárítási mechanizmusról szóló, 2018. december 11-i (EU) 2018/1993 tanácsi végrehajtási határozatra[10],

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.
10 HL L 320., 2018.12.17., 28. o.

– az uniós kiberbiztonsági kapacitás és képességek megerősítéséről szóló tanácsi következtetésekre[11],

– „Az 5G jelentősége az európai gazdaság számára és az 5G-hez kapcsolódó biztonsági kockázatok enyhítésének szükségessége” című tanácsi következtetésekre[12],

– „A nagymértékben digitalizált Európa jövője 2020 után: A digitális és gazdasági versenyképesség fokozása Unió-szerte és a digitális kohézió” című tanácsi következtetésekre[13],

– a reziliencia megerősítésére és a hibrid fenyegetések elleni küzdelemre irányuló kiegészítő jellegű erőfeszítésekről szóló tanácsi következtetésekre[14],

– az „Európa digitális jövőjének alakítása” című tanácsi következtetésekre[15],

– a csatlakoztatott eszközök kiberbiztonságáról szóló tanácsi következtetésekre[16],

– a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló tanácsi következtetésekre[17],

– a biztonságról és a védelemről szóló tanácsi következtetésekre[18],

– a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás kiegészítéseként szolgáló, a közös kiberbiztonsági egységre vonatkozó kezdeményezésben rejlő lehetőségek feltárásáról szóló tanácsi következtetésekre[19],

– „A biztonság és a védelem területére vonatkozó stratégiai iránytű – Egy, a polgárait, az értékeit és az érdekeit megvédő Európai Unióért, amely hozzájárul a nemzetközi béke és biztonság megvalósításához” című dokumentumra[20],

---

11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. HANGSÚLYOZZA, hogy az elmúlt években egyre többször szembesülünk a kibertérben – úgy állami, mint nem állami szereplők által – tanúsított rossz szándékú magatartással, így az EU és a tagállamok kritikus infrastruktúrája, ellátási láncai és szellemi tulajdona ellen irányuló, rossz szándékú tevékenységek számának jelentős és folyamatos emelkedésével, az átgyűrűző hatások növekvő kockázatával, valamint a vállalkozásaink, szervezeteink és polgáraink ellen irányuló zsarolóvírus-támadások egyre gyakoribbá válásával. MEGÁLLAPÍTJA, hogy néhány ország az erőpolitika visszatérésével párhuzamosan egyre többször és egyre erősebben próbálja a kibertérben megzavarni és aláásni a szabályokon alapuló nemzetközi rendet azzal, hogy a kiberteret, csakúgy mint a nyílt tengert, a levegőt és a világűrt, egyre vitatottabb területté teszi. TISZTÁBAN VAN AZZAL, hogy a nagyszabású kibertámadások, illetve a hálózati és információs rendszerekbe való behatolásra, e rendszerek megzavarására vagy megsemmisítésére tett, rendszerszintű hatással járó kísérletek egyre általánosabbá válnak, és aláásható gazdaságunk biztonságát, valamint érinthetik demokratikus intézményeinket és folyamatainkat, mindemellett pedig jól demonstrálják, hogy néhány szereplő kész veszélybe sodorni a nemzetközi biztonságot és stabilitást. RÁMUTAT ARRA, hogy az Ukrajna ellen irányuló orosz katonai agresszió is bizonyította: a támadó jellegű kibertevékenységek a megfélemlítést, a destabilizációt és a gazdasági zavarokat egyaránt célzó hibrid stratégia szerves részét képezhetik.

2. ISMÉTELTEN KIEMELI, hogy napjaink geopolitikai változásaival szembesülve Uniónk ereje az egységben, a szolidaritásban és az elszántságban rejlik, valamint hogy a stratégiai iránytű végrehajtása meg fogja erősíteni az EU stratégiai autonómiáját és abbéli képességét, hogy együttműködjön partnereivel értékei és érdekei megőrzése érdekében, a kiberbiztonság területén is. HAGSÚLYOZZA, hogy egy a biztonság és a védelem területén erősebb és szélesebb körű képességekkel rendelkező EU kedvező módon fog hozzájárulni a globális és a transzatlanti biztonsághoz, valamint kiegészíti a NATO-t, amely továbbra is a kollektív védelem alapját képezi tagjai számára. ÚJÓLAG MEGERŐSÍTI az EU azon szándékát, hogy még erőteljesebben támogassa a szabályokon alapuló világrendet, amelynek középpontjában az Egyesült Nemzetek Szervezete áll.

3. Az EU kiberbiztonsági stratégiájáról és a stratégiai iránytűről szóló tanácsi következtetésekkel összhangban ISMÉTELTEN RÁMUTAT arra, hogy javítanunk kell az Unió kiberbiztonsági helyzetét, mégpedig a kibertámadások megelőzésére vonatkozó képességünk megerősítése révén, amit kapacitásépítéssel, képességfejlesztéssel, kiképzéssel, gyakorlatokkal, és a reziliencia megerősítésével valósíthatunk meg, valamint azzal, hogy valamennyi rendelkezésre álló uniós eszközzel határozott választ adunk az EU és tagállamai ellen irányuló kibertámadásokra. Ez egyúttal azt is magában foglalja, hogy a jövőben is demonstráljuk az EU elszántságát aziránt, hogy azonnali és hosszú távra szóló válaszokat adjon azoknak a fenyegető szereplőknek, akik meg kívánják tagadni a kibertérhez való biztonságos és nyílt hozzáférésünket, és sértik stratégiai érdekeinket, például partnereink biztonságát. Ezzel összefüggésben HANGSÚLYOZZA, hogy a kiberbiztonsági helyzet javításának célja egyrészről összefogni azokat az uniós kezdeményezéseket, amelyek a kibertérben való béke és stabilitás megszilárdítására, és egy nyílt, szabad, globális, stabil és biztonságos kibertér megteremtésére irányulnak, másrészről jobban koordinálni azokat a rövid-, közép- és hosszú távú intézkedéseket, amelyek a kiberfenyegetések és kibertámadások megakadályozását, az azoktól való elrettentést, és az azokra való reagálást, illetve a kiberképességek kiaknázását szolgálják. HANGSÚLYOZZA, hogy ezeket az elemeket be kell építeni az EU kiberbiztonsági helyzetének javítását célzó intézkedésekbe, mégpedig az EU kiberterületen betöltött öt funkciójának megfelelően, amelyek a következők: megerősíteni kiberrezilienciánkat és védelmi kapacitásainkat; megerősíteni a szolidaritást és az átfogó válságkezelést; előmozdítani a kibertérre vonatkozó jövőképünket; megerősíteni együttműködésünket a partnerországokkal és nemzetközi szervezetekkel; megelőzni a kibertámadásokat, védekezni azokkal szemben, illetve reagálni azokra.

I. KIBERREZILIENCIÁNK ÉS VÉDELMI KAPACITÁSAINK MEGERŐSÍTÉSE

4. ÚJÓLAG HANGSÚLYOZZA, hogy az EU kiberbiztonságának általános szintjét emelni kell, VÁRAKOZÁSSAL TEKINT az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvtervezet (NIS), a pénzügyi ágazat digitális működési rezilienciájáról szóló rendelettervezet (DORA) és a kritikus fontosságú szervezetek rezilienciájáról szóló irányelvtervezet (CER) gyors elfogadása elé, valamint NYUGTÁZZA az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról szóló rendeletjavaslatot, azzal a céllal, hogy mindezeknek köszönhetően olyan Európai Unióban élhessünk, amely védi a kibertérben a polgárait, a közszolgálatokat és a vállalkozásokat. ÖSZTÖNZI a Bizottságot, hogy annak érdekében, hogy egyértelmű jelzést küldjön az EU ezen területekkel kapcsolatos ambíciójáról, vigye végig a kulcsfontosságú javaslatok elfogadását, hogy biztosított legyen a digitális infrastruktúrák, technológiák, termékek és szolgáltatások védelme, valamint támogatni lehessen a vállalkozásokat abban, hogy meg tudjanak felelni a kihívásnak. FELSZÓLÍTJA a Bizottságot, hogy a kiberrezilienciáról szóló – 2022 vége előtt benyújtandó – jogszabály keretében tegyen javaslatot a csatlakoztatott eszközök, valamint a kapcsolódó eljárások és szolgáltatások tekintetében alkalmazandó közös uniós kiberbiztonsági követelményekre, figyelemmel arra, hogy egy olyan horizontális és holisztikus megközelítést kell létrehozni, amely a digitális termékek teljes életciklusát lefedi, továbbá figyelemmel a meglévő jogszabályokra, különösen a kiberbiztonság területén.

5. FELKÉRI az érintett hatóságokat, így például az Európai Elektronikus Hírközlési Szabályozók Testületét (BEREC), az Európai Uniós Kiberbiztonsági Ügynökséget (ENISA) és a hálózat- és információbiztonsággal foglalkozó együttműködési csoportot, hogy az Európai Bizottsággal együtt tegyenek – kockázatértékelésen nyugvó – ajánlásokat a tagállamok és az Európai Bizottság részére arra vonatkozóan, hogy miként lehet megerősíteni a kommunikációs hálózatok és infrastruktúrák rezilienciáját az Európai Unióban, ideértve az 5G kiberbiztonsággal kapcsolatos uniós eszköztár alkalmazásának folytatását is.

6. FELSZÓLÍTJA az Uniót és annak tagállamait, hogy fokozzák a kiberbiztonság általános szintjének javítását célzó erőfeszítéseiket, például a megbízható kiberbiztonsági szolgáltatók megjelenésének elősegítésével, továbbá HANGSÚLYOZZA, hogy az EU kiberbiztonsági ágazati politikájában kiemelt helyen kell kezelni az ilyen szolgáltatók kiépülésének ösztönzését. A potenciálisan rendszerszintű hatást gyakorló kibertámadásokkal szembeni reziliencia és azok kivédésének javítása érdekében és tanulva a Solarwinds, a Microsoft Exchange és az Apache Log4J sebezhetőségeinek kezelése során levont tanulságokból, FELKÉRI a Bizottságot, hogy tegyen javaslatot arra, hogy milyen módokon lehetne ösztönözni a megbízható kiberbiztonsági szolgáltatások iparágának megjelenését, megerősíteni az IKT-ellátási lánc kiberbiztonságát, kezelni a szoftverek sebezhetőségéből eredő, az Uniót és a tagállamokat érintő potenciális hatásokat, többek között a kiberrezilienciáról szóló közelgő jogszabály fényében is, továbbá javítani a kiberfenyegetések észlelését, illetve a képességek tagállamokon belüli és azok közötti megosztását.

7. ÚJÓLAG HANGSÚLYOZVA, hogy az innovációba való beruházás és a polgári technológia jobb felhasználása alapvető fontosságú technológiai szuverenitásunk fokozásához, a kiberterületen is, FELSZÓLÍTJA a Bizottságot, hogy mihamarabb tegye működőképessé az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontot annak érdekében, hogy erős európai kiberkutatási, -ipari és technológiai ökoszisztéma jöjjön létre, HANGSÚLYOZZA, hogy az európai védelmi technológiai és ipari bázis (EDTIB) megerősítése érdekében fel kell lendíteni a kutatást és az innovációt, fokozni kell a polgári és védelmi területekre áramló beruházásokat, továbbá fejleszteni kell az Uniónak és tagállamainak a kiberképességeit, a stratégiai támogatási képességeket is beleértve. KIEMELI, hogy fontos intenzíven alkalmazni az új technológiákat – mindenekelőtt a kvantum-számítástechnikát, a mesterséges intelligenciát és a big data technológiát – annak érdekében, hogy az EU komparatív előnyökre tegyen szert, többek között a kiberbiztonsági eseményekkel kapcsolatos reagálási műveletek tekintetében.

8. TUDATÁBAN ANNAK, hogy kiberbiztonságunk fokozásával hozzájárulunk a szárazföldön, a levegőben, a tengereken és a világűrben tett erőfeszítéseink eredményességének és biztonságosságának a növeléséhez, HANGSÚLYOZZA annak fontosságát, hogy a kiberbiztonsági megfontolások minden uniós közpolitikában – többek között a NIS 2 irányelvet kiegészítő ágazati jogszabályokban is – érvényre jussanak, továbbá FELKÉRI a Bizottságot annak feltérképezésére, hogy milyen lehetőségek nyílnak a kiberbiztonság megerősítésére az európai védelmi technológiai és ipari bázis (EDTIB) teljes értéklánca mentén.

9. ELISMERI, hogy az EU kiberbiztonsági helyzetének megerősítéséhez elengedhetetlen, hogy megfelelő pénzügyi és humán erőforrásokat biztosítsunk a kiberbiztonság területén, valamint a magánszektor versenyképességét elősegítő környezet megteremtését célzó intézkedésekhez, továbbá hogy a kiberbiztonság stabil, hosszú távú finanszírozásának kérdésével uniós szinten is foglalkozni kell egy olyan horizontális mechanizmus kialakításával és bevezetésével, amely többféle finanszírozási forrást ötvöz, a magasan képzett humán erőforrások költségének a finanszírozását is ideértve. FELSZÓLÍTJA ezért a Bizottságot, hogy 2022 vége előtt térképezze fel az említett mechanizmus kialakításának lehetséges módjait, és munkája eredményét megvitatásra terjessze az érintett tanácsi szervek elé.

10. HANGSÚLYOZZA, hogy fokoznunk kell erőfeszítéseinket és erősítenünk kell az együttműködést a nemzetközi kiberbűnözés – különösen a zsarolóvírusok – elleni küzdelem terén, az EMPACT (Európai Multidiszciplináris Platform a Bűnügyi Fenyegetettség Ellen) mechanizmus keretében, a kiberbiztonsági, bűnüldözési és diplomáciai terület közötti cserék révén, valamint a kiberbűnözéssel kapcsolatos nyomozások és büntetőeljárások lefolytatására való képességek megerősítése útján. ÚJÓLAG MEGERŐSÍTI aziránti elkötelezettségét, hogy tájékoztassa a nyilvánosságot a kiberbiztonsági fenyegetésekről és az azok ellen hozott nemzeti és uniós szintű intézkedésekről, mégpedig a civil társadalom, a magánszektor és a tudományos világ bevonásával, annak érdekében, hogy felhívja a figyelmet a kibervédelem és a kiberhigiénia megfelelő szintjére, illetve ösztönözze annak alkalmazását. HANGSÚLYOZZA, hogy középpontba kell állítani a polgárok kiberbiztonsági készségeit és képességeit uniós és tagállami szinten egyaránt, valamint hogy aktívan be kell vonni a felhasználókat a saját védelmükbe.

II. A SZOLIDÁRIS ÉS ÁTFOGÓ VÁLSÁGKEZELÉS ELŐMOZDÍTÁSA

11. Az éves kibervédelmi gyakorlatokra, egyéb, kiberbiztonsági dimenzióval bíró gyakorlatokra és az EU CyCLES 2022 gyakorlatra alapozva HANGSÚLYOZZA annak fontosságát, hogy a nagyszabású kiberbiztonsági eseményekre adott belső és külső uniós válasz tesztelése és fejlesztése céljából létrejöjjön egy olyan program, amelynek keretében rendszeresen szerveznek közösségek közötti és többszintű kibervédelmi gyakorlatokat a Tanács, az EKSZ, a Bizottság és az érintett érdekelt felek – például az ENISA és a magánszektor – bevonásával, és amely a gyakorlatokra vonatkozó politika keretében kerül kidolgozásra, hozzájárulva annak alakításához. KIEMELI, hogy fontos továbbfejleszteni a Cyber Europe és a BlueOLEx gyakorlatokat, a különböző szinteken adott válaszintézkedések ötvözése mellett. ELISMERI, hogy értékelni kell és meg kell szilárdítani a meglévő gyakorlatokat, valamint hogy meg kell vizsgálni további, a kiberterület specifikus szegmenseire irányuló gyakorlatok szervezésének a lehetőségét, mindenekelőtt egy katonai CERT-gyakorlatot és az uniós intézmények, szervek és hivatalok közötti válsághelyzeti együttműködésre fókuszáló gyakorlatot tűzve ki célul. ELISMERI, hogy az Unió kiberbiztonsági helyzete meg fogja erősíteni a kibertámadások megelőzésére szolgáló képességünket különböző intézkedések, például képzések révén, és ezért FELKÉRI a tagállamokat, hogy fokozzák a kiberbiztonsági képzések és közös gyakorlatok terén folytatott polgári-katonai együttműködést.

12. HANGSÚLYOZZA, hogy a nagyszabású kiberbiztonsági eseményekre való uniós felkészültség javítása érdekében folytatni kell a tagállamok közötti operatív együttműködésnek, valamint az egymással megosztott helyzetismeretnek a tesztelését és megerősítését, többek között az olyan létező hálózatokon keresztül, mint a CSIRT-ek hálózata és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe). ALÁHÚZZA, hogy fontos egy olyan közös nyelv kidolgozásán munkálkodni, amelyet a tagállamok egymás között, illetve az uniós intézményekkel, szervekkel és hivatalokkal használnak a politikai szintű megbeszélések céljára, és amely elősegíti a releváns kiberbiztonsági események súlyosságára és hatására vonatkozó egységes értékelés kialakítását, az események további alakulására vonatkozó lehetséges forgatókönyvek kidolgozását, és adott esetben az azokból eredő igények megállapítását. ALÁHÚZZA e tekintetben annak szükségességét, hogy az egymással megosztott helyzetismeret-értékelő jelentések – például az EU-CyCLONe-nak az uniós tagállamokban előfordult nagyszabású kiberbiztonsági események hatásáról és súlyosságáról készített jelentései, valamint az EU INTCEN által az EU kiberdiplomáciai eszköztára keretében kiadott fenyegetésértékelések – jobban kiegészítsék egymást, FELKÉRI a Bizottságot, a főképviselőt és a Kiberbiztonsági Együttműködési Csoportot, hogy az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – többek között az EU CyCLONe-nal – koordinációban végezzenek el 2022 végéig egy kockázatértékelést, és dolgozzanak ki kiberbiztonsági szempontú kockázati forgatókönyveket egy olyan helyzetre, amikor a tagállamokkal vagy partnerországokkal szemben fenyegetés, vagy támadás lehetősége áll fenn, és ezeket terjesszék az érintett tanácsi szervek elé. HANGSÚLYOZZA, hogy a nagyszabású kiberbiztonsági eseményekre adott uniós válaszról megfelelő és koordinált módon tájékoztatni kell a nyilvánosságot.

13. Nagyszabású kiberbiztonsági események esetére HANGSÚLYOZZA, hogy meg kell erősíteni a koordinációt, és adott esetben építeni kell az elért eredményekre és a PESCO kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok által végzett munkára, valamint – a CSIRT-ek hálózatának és az EU-CyCLONe-nak a munkájából kiindulva – a biztonsági eseményekre való reagálási képességeink tagállamok közötti önkéntes összevonására. ELISMERI, hogy a magánszektorral való kapcsolatok kiépítése révén megerősödhetnek az állami kapacitások, különösen az EU-ban tapasztalható szakemberhiánnyal összefüggésben, valamint hogy a megfelelő magánszektorbeli partnerek megtalálása és koordinálása jelentős különbséget jelenthet nagyszabású kiberbiztonsági események esetén. A nagyszabású kiberbiztonsági eseményekre való teljes körű felkészültség érdekében FELKÉRI a Bizottságot, hogy 2022 harmadik negyedévének végéig nyújtson be javaslatot egy új kiberbiztonsági veszélyhelyzeti reagálási alapra vonatkozóan.

14. A stratégiai iránytűvel összhangban ÚJÓLAG HANGSÚLYOZZA, hogy aktívan hozzá kell járulnunk az Európai Unióról szóló szerződés 42. cikkének (7) bekezdése szerinti kölcsönös segítségnyújtáshoz és az Európai Unió működéséről szóló szerződés 222. cikke szerinti szolidaritáshoz, mindenekelőtt gyakran megrendezésre kerülő gyakorlatok révén. Ezzel összefüggésben HANGSÚLYOZZA, hogy tovább kell munkálkodni a kétoldalú polgári és/vagy katonai támogatás biztosítása és koordinálása területén – többek között a tagállamok kifejezett kérésére az EU által nyújtandó esetleges támogatás lehetőségeinek feltérképezésével –, valamint a 42. cikk (7) bekezdésének végrehajtásával összefüggésben a megfelelő válaszintézkedések meghatározása területén, többek között koordinált kommunikációs stratégia kidolgozásán keresztül. MEGJEGYZI, hogy ennek magában kell foglalnia a már létező uniós válságkezelési mechanizmusokkal és az uniós polgári védelmi mechanizmussal való lehetséges kapcsolódások feltárását is.

15. HANGSÚLYOZZA, hogy az EU kiberbiztonsági helyzetének megerősítéséhez a biztonságos kommunikáció megerősítésére is szükség lesz. E célból ÚJÓLAG HANGSÚLYOZZA a stratégiai iránytű által e tekintetben adott iránymutatásokat, és FELKÉRI a Bizottságot és más releváns intézményeket, szerveket és hivatalokat, hogy 2022 végéig térképezzék fel a kiberterületen történő biztonságos kommunikáció már létező eszközeit, a releváns tanácsi szervekben és a releváns együttműködési csoportokkal – így a CSIRT-ek hálózatával és az EU-CyCLONe-nal – való megvitatás céljából.

III. A KIBERTÉRRE VONATKOZÓ JÖVŐKÉPÜNK ELŐMOZDÍTÁSA

16. EMLÉKEZTET arra, hogy a kiberdiplomácia közös és átfogó uniós megközelítésének célja, hogy hozzájáruljon a konfliktusmegelőzéshez, a kiberbiztonsági fenyegetések mérsékléséhez és a nemzetközi kapcsolatok stabilitásának növeléséhez. Ezzel összefüggésben ÚJÓLAG MEGERŐSÍTI az EU-nak a kibertérben felmerülő nemzetközi jogviták békés eszközökkel történő rendezése iránti elkötelezettségét, valamint az arra vonatkozó elkötelezettségét, hogy az államoknak a kibertérben végrehajtott fellépéseire a nemzetközi jogot – többek között az emberi jogok nemzetközi jogát és a nemzetközi humanitárius jogot – alkalmazzák. HANGSÚLYOZZA, hogy az EU és tagállamai elkötelezettek amellett, hogy a kibertérben tanúsított felelősségteljes állami magatartásnak – az ENSZ valamennyi tagállama által elfogadott – önkéntes, nem kötelező normáival összhangban cselekedjenek. HANGSÚLYOZZA a nyitott, szabad, globális, stabil és biztonságos kibertér fontosságát, amelyben maradéktalanul érvényesülnek az emberi jogok, az alapvető szabadságok és a jogállamiság, támogatva szabad és demokratikus társadalmaink társadalmi jóllétét, gazdasági növekedését, jólétét és integritását, továbbá ÚJÓLAG MEGERŐSÍTI, hogy az EU és tagállamai elkötelezettek ezen értékek és elvek további előmozdítása mellett. A kibertér kulcsfontosságú érdekelt feleivel folytatandó konstruktív, őszinte és nyitott párbeszéd csatornáinak kialakítását szem előtt tartva HANGSÚLYOZZA annak fontosságát, hogy az uniós csatlakozási tárgyalásoknak, valamint az EU nemzetközi partnerekkel és versenytársakkal folytatott stratégiai és politikai párbeszédeinek szerves részét képezzék a kiberkérdések, többek között az EU kiberdiplomáciai eszköztára, és ezzel egyidejűleg FELHÍVJA a főképviselőt a már létező kétoldalú kiberpárbeszédek áttekintésére és arra, hogy szükség esetén tegyen javaslatot hasonló együttműködés elindítására további országokkal, illetve releváns nemzetközi szervezetekkel.

17. EMLÉKEZTET a több érdekelt felet érintő együttműködés fontosságára, mivel más érdekelt felek is felelősséget viselnek a kiberbiztonságért, nevezetesen a nemzetközi és regionális fórumokon elfogadott ajánlások és határozatok végrehajtását illetően. FELHÍVJA az EU-t és tagállamait, hogy továbbra is mozdítsák elő a kibertér- és internetmodellünket a több érdekelt felet érintő megközelítésre építve és olyan kezdeményezéseken keresztül, mint például a Párizsi felhívás a kibertérbeli bizalom és biztonság érdekében, valamint az internet jövőjéről szóló nyilatkozat, hangsúlyozva a kibertérbeli stabilitás közös előnyeit, és világszerte növelve a tájékozottságot az internetre vonatkozó államközpontú, autoriter jövőkép veszélyeivel kapcsolatban, továbbá FELHÍVJA az EU-t és tagállamait, hogy erősítsék tovább az együttműködést a több érdekelt felet tömörítő közösséggel, többek között olyan releváns projekteken keresztül, mint például az EU külpolitikai eszközének uniós kiberdiplomáciai kezdeményezése.

18. ELKÖTELEZI MAGÁT a releváns nemzetközi szervezetek munkájában – különösen az ENSZ Első és Harmadik Bizottságának vonatkozó folyamataiban – való folyamatos részvétel mellett, hangsúlyozva ugyanakkor, hogy a jelenleg hatályos nemzetközi jogot fenntartások nélkül alkalmazni kell a kibertérben és a kibertérre vonatkozóan. HANGSÚLYOZZA a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-keretének fenntartására és előmozdítására irányuló folytatódó erőfeszítések fontosságát, valamint KIEMELI, hogy az EU és tagállamai aktívan fognak munkálkodni e keret végrehajtásának megerősítésén, többek között a kibertérben tanúsított felelősségteljes állami magatartás előmozdítására irányuló cselekvési program létrehozása révén. HANGSÚLYOZZA, hogy az EU és tagállamai tevékenyen részt fognak venni azokban a tárgyalásokban, amelyek célja egy olyan ENSZ-egyezmény kidolgozása, amely a bűnüldöző és igazságügyi hatóságok hatékony eszköze lesz a jövőben a kiberbűnözés elleni globális küzdelemben, teljeskörűen figyelembe véve az e területre vonatkozó nemzetközi és regionális eszközök jelenleg meglévő keretét, különösen a Számítástechnikai Bűnözésről szóló Budapesti Egyezményt. HANGSÚLYOZZA a bizalomépítő intézkedések regionális és nemzetközi szintű továbbfejlesztése és működőképessé tétele további támogatásának fontosságát, valamint a kibertérre vonatkozó, már létező bizalomépítő intézkedéseknek az EBESZ keretében történő alkalmazása további ösztönzésének fontosságát, többek között nemzetközi feszültségek idején is.

19. EMLÉKEZTET arra, hogy a kialakulóban lévő technológiák és az alapvető internetes architektúra területére vonatkozó, az uniós értékekkel összhangban lévő nemzetközi szabványok biztosítására irányuló proaktív, emberi jogokon alapuló megközelítés létfontosságú annak biztosításához, hogy az internet továbbra is globális, nem széttagolt és nyitott maradjon, továbbá TÁMOGATJA azt az elvet, hogy a technológiák alkalmazása és fejlesztése során tiszteletben kell tartani az emberi jogokat, a magánélet védelmére kell összpontosítani, és a technológiák alkalmazásának jogszerűnek, biztonságosnak és etikusnak kell lennie. ÖSZTÖNZI a főképviselőt és a Bizottságot, hogy dolgozzanak ki stratégiai jövőképet a digitális területre vonatkozó azon technikai kérdésekkel kapcsolatban, amelyek külpolitikai vonzatokkal rendelkeznek és amelyek hatással lehetnek a kibertér és különösen az internet stabilitására, többek között a releváns szakosodott nemzetközi szervezeteken belül (Nemzetközi Távközlési Egyesület stb.).

IV. A PARTNERORSZÁGOKKAL ÉS NEMZETKÖZI SZERVEZETEKKEL FOLYTATOTT EGYÜTTMŰKÖDÉS FOKOZÁSA

20. HANGSÚLYOZZA, hogy az EU kiberkapacitás-építési stratégiáját jobban össze kell kapcsolni a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-normáival, többek között a harmadik országok végrehajtási erőfeszítéseit támogató, személyre szabott együttműködési és kapacitásépítési programok kidolgozásával, és ennek során folytatni és bővíteni kell az erőfeszítéseinket a kibertérben tanúsított felelősségteljes állami magatartás előmozdítására irányuló ENSZ-cselekvési program előmozdítására. HANGSÚLYOZZA annak fontosságát, hogy az EU mint biztonságszolgáltató ajánlatának szerves részét képezze a kiberkapacitás-építés, az erőfeszítéseknek a tagállamok és az uniós intézmények, szervek és hivatalok közötti megfelelő koordinációja mellett, és különösen ÜDVÖZLI a tagállamok közötti, valamint a köz- és magánszektorbeli partnerekkel való együttműködést, mindenekelőtt az EU CyberNet-en (az uniós kiberkapacitás-építési hálózaton) és a globális kiberszakértői fórumon (GFCE) keresztül, a koordináció biztosítása és az átfedések elkerülése érdekében.

FELHÍVJA a főképviselőt és a Bizottságot, hogy 2022 harmadik negyedévéig hozzanak létre egy *kiberkapacitás-építési testületet*, és tartsanak rendszeres véleménycseréket a kiberkérdésekkel foglalkozó horizontális munkacsoportban. FELHÍVJA a Bizottságot és a főképviselőt a Szomszédsági, Fejlesztési és Nemzetközi Együttműködési Eszköz (NDICI), az Előcsatlakozási Támogatási Eszköz (IPA III) és más pénzügyi eszközök, például az Európai Békekeret és a Global Gateway kezdeményezés további mozgósítására, hogy ezeken keresztül támogassa partnereink rezilienciájának fokozását és a kiberfenyegetések azonosítására és kezelésére, valamint a kiberbűnözés nyomozására és büntetőeljárás alá vonására vonatkozó kapacitásának megerősítését, illetve együttműködési projektek kidolgozását, többek között –

és különösen – válságok összefüggésében, továbbá SZORGALMAZZA az együttműködést a nyugat-balkáni partnerekkel, valamint az EU keleti és déli szomszédságának országaival, illetve uniós és tagállami szakértők kiküldését a kiberválságok során történő támogatás felajánlása érdekében, figyelembe véve a meglévő jogi megbízatásokat.

21. HANGSÚLYOZZA, hogy fokozni kell az erőfeszítéseket egy strukturált és nyitott uniós tájékoztatási megközelítés kidolgozására egyrészt azzal kapcsolatban, hogy miként lehet előmozdítani a nemzetközi jognak a kibertérben való alkalmazására vonatkozó globális közös értelmezést és a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-keretét – ideértve a kibertérben tanúsított felelősségteljes állami magatartás előmozdítására irányuló cselekvési programmal kapcsolatos kezdeményezést is –, másrészt az EU-nak és tagállamainak a kiberbűnözésről szóló ENSZ-egyezményre irányuló, folyamatban lévő tárgyalások során képviselendő álláspontjával kapcsolatban, és ezen erőfeszítések részeként FELKÉRI a főképviselőt, hogy 2022 végéig nyújtson be tájékoztatási tervet a Tanácsnak. ÖSZTÖNZI a főképviselőt és a Bizottság szolgálatait, hogy teljeskörűen és szisztematikusan használják ki a 145 küldöttség kínálta lehetőségeket, és alakítsanak ki rendszeres, gyümölcsöző együttműködést közöttük és a tagállamok harmadik országbeli nagykövetségei között, a tervezett uniós kiberdiplomáciai hálózat égisze alatt. FELHÍVJA a főképviselőt, hogy 2022 harmadik negyedévéig hozza létre az uniós kiberdiplomáciai hálózatot, amely hozzájárul az információcseréhez, az uniós és tagállami személyzet közös képzési tevékenységeihez, a koherens kapacitásépítési erőfeszítésekhez, valamint a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-kerete és a tagállamok közötti bizalomépítő intézkedések végrehajtásának a megerősítéséhez.

22. HANGSÚLYOZZA az elkötelezettségét az iránt, hogy a továbbiakban is együttműködjön a nemzetközi szervezetekkel és a partnerországokkal a kiberfenyegetettségi helyzetre vonatkozó közös értelmezés előmozdítása, valamint az együttműködési mechanizmusok kidolgozása és együttműködésen alapuló diplomáciai válaszintézkedések proaktív azonosítása érdekében. EMLÉKEZTETVE a 2016. évi varsói és a 2018. évi brüsszeli együttes nyilatkozat végrehajtása keretében a kiberbiztonság területén folytatott EU–NATO együttműködés fő eredményeire, teljes mértékben tiszteletben tartva mindkét szervezet döntéshozatali autonómiáját és eljárásait és az átláthatóság, a kölcsönösség és az inkluzivitás elve alapján, HANGSÚLYOZZA, hogy tovább kell erősíteni a NATO-val a kiberkérdések területén folytatott együttműködést egyrészt gyakorlatokon és a szakemberek közötti információmegosztáson és -cserén keresztül, többek között a képességfejlesztéssel, a partnerek kapacitásépítésével, missziókkal és műveletekkel, valamint a nemzetközi jog és a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-normáinak alkalmazhatóságával kapcsolatban, másrészt a rossz szándékú kibertevékenységekre adandó lehetséges koordinált válaszintézkedéseken keresztül.

V. A KIBERTÁMADÁSOK MEGELŐZÉSE, AZ AZOKKAL SZEMBENI VÉDEKEZÉS, ILLETVE AZ AZOKRA VALÓ REAGÁLÁS

23. ELISMERI, hogy a kibertér a geopolitikai verseny színterévé vált, éppen ezért ÚJÓLAG HANGSÚLYOZZA, hogy az EU-nak képesnek kell lennie gyorsan és határozottan reagálni a kibertámadásokra, így például az EU és tagállamai ellen irányuló, államilag támogatott, rossz szándékú kibertevékenységekre, és ennek érdekében meg kell erősítenie az uniós kiberdiplomáciai eszköztárat, és maradéktalanul ki kell használnia az abban rendelkezésre álló összes – politikai, gazdasági, diplomáciai, jogi és stratégiai kommunikációs – eszközt a rossz szándékú kibertevékenységek megakadályozására, az azoktól való elrettentésre és az azokra való reagálásra. HANGSÚLYOZZA, hogy az ellenséges szereplőknek tisztában kell lenniük azzal, hogy a tagállamok és az uniós intézmények elleni kibertámadásokat korai szakaszban észleljük, gyorsan azonosítjuk, és minden szükséges eszközt és szakpolitikát bevetünk ellenünk. FELKÉRI a tagállamokat és a főképviselőt, hogy a Bizottság támogatásával 2023 első negyedévének végéig készítsék el az uniós kiberdiplomáciai eszköztár végrehajtására vonatkozó iránymutatások felülvizsgált változatát, és ennek során támaszkodjanak különösen egyrészt a kiberbiztonsági helyzet elemeire, másrészt az uniós kiberdiplomáciai eszköztár bevezetése óta az annak végrehajtása során és az EU CyCLES kibergyakorlat során levont tanulságokra, és tárják fel mindenekelőtt további reagálási intézkedések lehetőségét.

24. NYOMATÉKOSÍTJA, hogy a Tanács megfelelő szerveiben és bizottságaiban rendszeres eszmecserét kell folytatni a kiberfenyegetettségi helyzetről, és ezzel párhuzamosan rendszeresen együtt kell működni a magánszektorral is, továbbá figyelembe kell venni a közelmúltbeli kiberbiztonsági események súlyosságának és hatásainak értékelését, emellett pedig növelni kell az uniós kiberdiplomáciai eszköztár további alkalmazásaival kapcsolatos tudatosságot és felkészültséget, valamint további eszközöket kell kidolgozni végrehajtásának előmozdítására. Mindamellett, hogy a nemzetbiztonság továbbra is az egyes tagállamok kizárólagos felelőssége marad, MEGÁLLAPÍTJA, hogy meg kell erősíteni a hírszerzési adatok és az információk cseréjét csakúgy, mint a tagállamok közötti, illetve az Európai Unió Helyzetelemző Központjával folytatott együttműködést, hogy a döntéshozatali folyamat kezdeti szakaszában – ideértve az attribúció kérdésével kapcsolatos döntéseket is – meg lehessen osztani a hírszerzési információkat, és ezzel lehetővé lehessen tenni az EU és partnerei ellen irányuló rossz szándékú kibertevékenységekre való gyors, hatékony és érdemi reagálást. ÚJÓLAG HANGSÚLYOZZA, hogy a tagállamok hatásköreinek sérelme nélkül, az általuk a hírszerzés terén nyújtott önkéntes hozzájárulások révén meg kell erősíteni az Európai Helyzetelemző Központ kiberbiztonsági kapacitásait, és meg kell vizsgálni a tagállami kiberhírszerzési munkacsoport lehetséges létrehozására vonatkozó javaslatot.

25. ELISMERVE, hogy az EU a nyilatkozataival és az uniós kiberdiplomáciai eszköztár keretében hozott korlátozó intézkedésekkel határozott üzenetet fogalmazott meg, miszerint az EU-ra, a tagállamaira és a partnereire nézve külső fenyegetést jelentő rossz szándékú kibertevékenységek elfogadhatatlanok, így az említett nyilatkozatok és korlátozó intézkedések hozzájárulnak a rossz szándékú kibertevékenységek megakadályozásához, az azoktól való elrettentéshez, illetve az azokra való reagáláshoz, ÚJFENT HANGSÚLYOZZA elszántságát arra, hogy alkalmazza ezeket az intézkedéseket egy a nemzetközi jognak a kibertérben való alkalmazására vonatkozó közös uniós álláspont további kialakítása és előmozdítása érdekében azzal a céllal, hogy emlékeztessen minden felet a nemzetközi jog, így többek között az ENSZ Alapokmánya értelmében a kibertérre vonatkozó kötelezettségekre, és előmozdítsa a kibertérben tanúsított felelősségteljes állami magatartás ENSZ-keretét, ideértve az államok kellő gondosságra vonatkozó kötelezettségét is, aminek értelmében nem engedhetik meg tudatosan azt, hogy területükön információs és kommunikációs technológiák felhasználásával nemzetközi jogot sértő cselekményeket kövessenek el. Utalva arra, hogy megfelelő, kellő időben megfogalmazott üzenetekkel csökkenteni lehet az eszkaláció kockázatát, és el lehet rettenteni az európai érdekeket célba vevő támadókat, FELKÉRI a főképviselőt, hogy dolgozzon ki egy koherens kommunikációs stratégiát az uniós kiberdiplomáciai eszköztár használatáról, és terjessze azt a tagállamok elé.

26. SZORGALMAZZA a rossz szándékú kibertevékenységek tekintetében alkalmazandó lépcsőzetes, célzott és folyamatos megközelítések és reakciók kidolgozását, aminek során használni kell az uniós kiberdiplomáciai eszköztár keretében rendelkezésre álló eszközök széles skáláját, így többek között a kiberbiztonsági szankciórendszert, valamint további intézkedéseket kell fontolóra venni. KIEMELI, hogy növelni kell annak lehetőségét, hogy eseti alapon mobilizálni lehessen minden rendelkezésre álló külső és belső eszközt a kibertámadások megakadályozására, az azoktól való elrettentésre, és az azokra való reagálásra, és hogy ezeket az eszközöket gyorsan, hatékonyan, lépcsőzetesen, célzottan lehessen végrehajtani egy hosszú távú stratégiai szerepvállalás keretében. FELSZÓLÍTJA a főképviselőt, hogy a Bizottsággal együttműködve a lehetőségek széles körére figyelemmel tárja fel, hogy az EU, annak érdekében, hogy készen álljon szükség esetén gyors és hatékony intézkedéseket hozni, milyen közös választ adhat a kibertámadásokra, ideértve a szankciók lehetőségét is, és 2023 első negyedévének végéig terjessze e lehetőségeket a Tanács elé.

27. Megállapítva, hogy a kibervédelem elsősorban nemzeti hatáskörbe tartozik, ARRA ÖSZTÖNZI a tagállamokat, hogy fejlesszék tovább saját képességeiket kibervédelmi műveletek folytatására, és ennek keretében hozzanak proaktív, esetleg a többi tagállam és az EU javát is szolgáló intézkedéseket a kibertámadásokkal szembeni védelem, a kibertámadások észlelése és elhárítása, valamint az azoktól való elrettentés céljából. Minden tagállamot ösztönöz arra, hogy szükség esetén erősítse meg képességeit segítség és támogatás nyújtására és fogadására. HANGSÚLYOZZA, hogy e képességek továbbfejlesztésének az egyik legfontosabb célnak kell lennie a jövőben az EU kibervédelmi szakpolitikájában. MEGÁLLAPÍTJA, hogy az uniós kibervédelmi szakpolitika keretében nagyon figyelmet kell fordítani arra, hogy a releváns uniós intézmények és szervek milyen szerepet tölthetnek be az EU és a tagállamok releváns kibervédelmi szereplői közötti együttműködés fokozásában, illetve e szereplők kapacitásának a megbízatásukkal összhangban lévő fejlesztésében. FELKÉRI a főképviselőt és a Bizottságot, hogy járuljanak hozzá az uniós kiberbiztonsági helyzet javításához azzal, hogy 2022-ben ambiciózus javaslatot nyújtanak be az EU kibervédelmi szakpolitikájára vonatkozóan, aminek alapján a Tanács tovább javíthatja az EU kiberbiztonsági helyzetét.

28. HANGSÚLYOZZA, hogy a katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok (milCERT-ek) közötti együttműködés révén fokozni kell az interoperabilitást és az információmegosztást. FELKÉRI a tagállamokat, hogy az Európai Védelmi Ügynökség munkájára építve hozzák létre a milCERT-ek hálózatát azzal a céllal, hogy fejlesszék az együttműködést és megkönnyítsék az információcserét, ami egyúttal segítene megerősíteni a többi kiberközösséggel való koordinációt is, illetve hozzák létre a katonai kiberparancsnokságok hálózatát, hogy megerősítsék az uniós tagállamok ilyen parancsnokságai vagy más releváns hatóságok közötti strukturált együttműködést. E hálózatok kialakítása a PESCO kiberprojektjei mellett hozzájárulna egy erősebb kibervédelemhez uniós szinten. HANGSÚLYOZZA, hogy a javasolt milCERT-hálózatok és a már meglévő polgári hálózatok (CSIRT-ek hálózata) között fontos az együttműködés az információmegosztás és a helyzetismeret javítása érdekében.

29. A kibertérre mint műveleti területre vonatkozó katonai koncepció és stratégia alapján, és nyugtázva EU által vezetett katonai műveletekhez és missziókhoz kapcsolódó katonai kibervédelmi koncepció jelenleg zajló kidolgozását, ÚJÓLAG HANGSÚLYOZZA, hogy a kiberbiztonsági dimenziót integrálni kell a KKBP-műveletek és -missziók tervezésébe és végrehajtásába, többek között kiberképességeik megerősítése révén, valamint HANGSÚLYOZZA, hogy ez hozzá fog járulni ahhoz, hogy az EU szintjén javuljon a kiberbiztonsággal kapcsolatos helyzetismeret.

30. Végezetül MEGÁLLAPÍTJA, hogy a kiberbiztonsági helyzet javítása egy lépéssel közelebb viszi az EU-t egyrészről ahhoz, hogy doktrínát alakítson ki a kibertérben való tevékenységekre vonatkozóan, amelyek megerősített reziliencián, jobb képességeken és szélesebb körű reagálási lehetőségeken alapulnak majd, másrészről pedig ahhoz, hogy közös álláspontot alakítson ki a nemzetközi jognak a kibertérben való alkalmazásáról. A Tanács 2023-ban ÁTTEKINTI MAJD az e következtetések végrehajtása terén elért haladást annak érdekében, hogy biztosítsa az EU kiberbiztonsági helyzetének további javítását.