2021. október 7., csütörtök

P9_TA(2021)0412

Az Unió kibervédelmi képességeinek állapota

Az Európai Parlament 2021. október 7-i állásfoglalása az Unió kibervédelmi képességeinek állapotáról (2020/2256(INI))

(2022/C 132/09)

Az Európai Parlament

— tekintettel az Európai Unióról szóló szerződésre (EUSZ) és az Európai Unió működéséről szóló szerződésre (EUMSZ),

— tekintettel a Bizottság alelnöke/az Unió külügyi és biztonságpolitikai főképviselője (alelnök/főképviselő) által 2016. június 28-án ismertetett, „Közös jövőkép, közös fellépés: Erősebb Európa – Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan" című dokumentumra,

— tekintettel az Európai Tanács 2013. december 20-i, 2015. június 26-i, 2016. december 15-i, 2017. március 9-i, 2017. június 22-i, 2017. november 20-i és 2017. december 15-i következtetéseire,

— tekintettel a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelvre ([1]),

— tekintettel a Tanács rosszhiszemű kibertevékenységekkel szembeni közös uniós diplomáciai fellépés keretéről („kiberdiplomáciai eszköztár") szóló, 2017. június 19-i következtetéseire,

— tekintettel a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének az „Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése" című, 2017. szeptember 13-i közös közleményére (JOIN(2017) 0450),

— tekintettel az EU és a NATO közötti együttműködésről szóló, 2018 júliusában aláírt együttes nyilatkozatra,

— tekintettel az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló, 2019. május 17-i (KKBP) 2019/797 tanácsi határozatra,

— tekintettel a Tanácsnak a reziliencia megerősítésére és a hibrid fenyegetések elleni küzdelemre irányuló kiegészítő jellegű erőfeszítésekről szóló, 2019. december 10-i következtetéseire,

— tekintettel az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletre (kiberbiztonsági jogszabály) ([2]),

— tekintettel a Tanács az Uniónak a terrorizmus és az erőszakos szélsőségesség megelőzését és az azok elleni küzdelmet célzó külső tevékenységéről szóló, 2020. június 16-i következtetéseire,

— tekintettel a Tanács és a tagállamok kormányainak a Tanács keretében ülésező képviselői által elfogadott, a polgári KBVP területére vonatkozó paktum létrehozásáról szóló következtetésekre,

— tekintettel az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról szóló, 2020. július 30-i (KKBP) 2020/1127 tanácsi határozatra ([3]),

([1]) HL L 194., 2016.7.19., 1. o.
([2]) HL L 151., 2019.6.7., 15. o.
([3]) HL L 246., 2020.7.30., 12. o.

— tekintettel az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról szóló, 2020. október 22-i (KKBP) 2020/1537 tanácsi határozatra ([4]),

— tekintettel a Bizottság biztonsági unióra vonatkozó stratégiáról szóló, 2020. július 24-i közleményére (COM(2020)0605),

— tekintettel az Unió külügyi és biztonságpolitikai főképviselőjének és a Bizottságnak „Az EU kiberbiztonsági stratégiája a digitális évtizedre" című, 2020. december 16-i közös közleményére (JOIN(2020)0018),

— tekintettel a Bizttság az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló európai parlamenti és tanácsi irányelvre irányuló, 2020. december 16-i javaslatára (COM(2020)0823),

— tekintettel a Bizottság kritikus fontosságú szervezetek rezilienciájáról szóló európai parlamenti és tanácsi irányelvre irányuló, 2020. december 16-i javaslatára (COM(2020)0829),

— tekintettel a Tanács a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló, 2021. március 9-i következtetéseire,

— tekintettel a 2021. március 25-i európai tanácsi nyilatkozatra,

— tekintettel a nyitott munkacsoport 2021. március 10-i jelentésére,

— tekintettel az ENSZ „Közös jövőnk biztosítása" című leszerelési programjára,

— tekintettel az ENSZ fenntartható fejlődési céljaira, különösen a 16. célra, amelynek konkrét célkitűzése a békés és befogadó társadalmak támogatása a fenntartható fejlődés érdekében,

— tekintettel az Európai Számvevőszék európai védelemről szóló 09/2019. sz. áttekintésére,

— tekintettel a kibervédelemről szóló, 2018. június 13-i állásfoglalására ([5]),

— tekintettel eljárási szabályzatának 54. cikkére,

— tekintettel a Külügyi Bizottság jelentésére (A9-0234/2021),

A. mivel az Uniónak és tagállamainak folytatniuk kell egy olyan kiberbiztonsági stratégia kidolgozását, amely reális, pontos és ambiciózus célokat tűz ki, és egyértelműen meghatározza a szakpolitikákat mind a katonai, mind a polgári területen, és ott is, ahol a két ágazat között átfedés van; mivel valamennyi uniós intézménynek és uniós tagállamnak minden szinten kooperatívabban kell dolgoznia e stratégia kialakítása érdekében, melynek elsődleges célként a reziliencia további erősítését, és következésképpen közös, de egyben jobb nemzeti, szilárd polgári és katonai kiberképességek kifejlesztését kell kitűznie a tartós biztonsági kihívásokra való reagálás érdekében;

B. mivel az Unió elkötelezett a hatályos nemzetközi jog kibertérben történő alkalmazása mellett, különös tekintettel az ENSZ Alapokmányára, amely felszólítja az államokat, hogy a nemzetközi viszályaikat békés eszközökkel rendezzék, és nemzetközi érintkezéseik során tartózkodjanak más állam területi integritása, vagy politikai függetlensége ellen irányuló vagy az Egyesült Nemzetek céljaival össze nem férő bármely más módon megnyilvánuló erőszakkal való fenyegetéstől vagy erőszak alkalmazásától;

C. mivel az elmúlt években folyamatosan nőtt az Unió és tagállamai ellen irányuló, állami és nem állami szereplők által végzett olyan rosszindulatú kiberműveletek száma, amelyek biztonsági réseket tártak fel az európai biztonsághoz nélkülözhetetlen hálózatokban; mivel az offenzív kiberszereplők egyre sokfélébbek, kfinomultabbak és számuk növekszik; mivel e támadások következtében kiemelten szükség van a védelmi képességek megerősítésére, valamint az európai kiberképességek fejlesztésére; mivel a kárt okozó kibertámadások bármikor előfordulhatnak, és mind az uniós, mind a nemzeti szintű szereplőket arra kell ösztönözni, hogy hozzák meg a szükséges intézkedéseket annak érdekében, hogy békeidőben is fenntartsák a hatékony kibervédelmi képességeket;

([4]) HL L 351. I, 2020.10.22., 5. o.
([5]) HL C 28., 2020.1.27., 57. o.

2021. október 7., csütörtök

D. mivel a Covid19-világjárvány és a kiberbiztonság hiányának növekedése bizonyította, hogy nemzetközi megállapodásokra van szükség; mivel a Covid19-világjárvány során jelentősen fokozódtak a kibertámadások, és mivel az Unió és tagállamai észlelték az alapvető szereplőkre irányuló kiberfenyegetéseket és rossz szándékú kibertevékenységeket, többek között a kritikus infrastruktúrák – például az energia, a közlekedés és az egészségügy – megzavarására irányuló támadásokat, valamint a kibertérben elkövetett, jelentős külföldi beavatkozásokat, amelyek elmosták a béke és az ellenségeskedés közötti határvonalat; mivel az európai helyreállítási terv további kiberbiztonsági beruházásokat irányoz elő;

E. mivel a kibertér ma már elismert műveleti terület; mivel a kiberfenyegetések alkalmasak arra, hogy veszélyeztessenek minden hagyományos katonai területet, és mivel a hagyományos területek függnek a kibertér funkcionalitásától, nem pedig fordítva; mivel a konfliktusok megvalósulhatnak bármelyik fizikai (szárazföldi, légi, tengeri és űrbeli) és virtuális (kiber) térben, és ezeket erősíthetik a hibrid hadviselés elemei, mint például az internetes dezinformációs kampányok, a helyettesítő erők által vívott háborúk, a kiberképességek offenzív és defenzív használata, valamint a digitális szolgáltatók elleni, a kritikus infrastruktúrák és a demokratikus intézményeink működésének megzavarására irányuló stratégiai támadások, mindezek pedig jelentős pénzügyi veszteséget is okoznak;

F. mivel az Európai Külügyi Szolgálatnak (EKSZ), a Bizottságnak és az Európai Védelmi Ügynökségnek (EDA) támogatnia kell a tagállamokat kibervédelmi képességek és technológiák biztosítására irányuló erőfeszítéseik összehangolásában és fokozásában, ideértve a képességfejlesztés valamennyi szempontját, többek között a katonai doktrínát és vezetést, a szervezést, a személyzetet, a képzést, az ipart, a technológiát, az infrastruktúrát, a logisztikát, az interoperabilitást és az erőforrásokat;

G. mivel a 2017. évi követelménykatalógus kidolgozása során – amelyet arra használnak, hogy számos szemléltető forgatókönyvön keresztül meghatározzák a közös biztonság- és védelempolitika (KBVP) katonai követelményeinek teljes körét – a kibervédelmi képességek szükségessége kiemelt prioritásként fogalmazódott meg;

H. mivel az uniós missziók és műveletek sikeres végrehajtása egyre inkább a biztonságos kibertérhez való zavartalan hozzáféréstől függ, és ezért reziliens kiberműveleti képességekre van szükség;

I. mivel a 2018-ban aktualizált uniós kibervédelmi szakpolitikai keret prioritásokat határozott meg, többek között a kibervédelmi képességek fejlesztését, valamint a KBVP kommunikációs és információs hálózatainak védelmét;

J. mivel az Unió helyzetéről szóló, 2021. évi beszédében a Bizottság elnöke hangsúlyozta az uniós kibervédelmi politika szükségességét;

K. mivel a mesterséges intelligencia (MI) a védelmi erők kiberképességeibe (kiberfizikai rendszerekbe, többek között a járművek közötti kommunikációs és adatkapcsolatok hálózatba kapcsolt rendszerébe) történő, egyre növekvő integrációja az elektronikai hadviselési támadásoknak (zavarásnak, spoofingnak, hackelésnek) való nagyobb kiszolgáltatottságot eredményez;

L. mivel az uniós kiberbiztonság és kibervédelem szintjének emelése szükséges Európa digitális és geopolitikai törekvéseinek sikerre viteléhez, ami nagyobb rezilienciát eredményez, lépést tartva az egyre kifinomultabb kibertámadások veszélyével; mivel az erős kiberbiztonsági kultúrával és erős kiberbiztonsági technológiával rendelkező Unió, beleértve a rossz szándékú cselekvések időben történő és hatékony azonosítására és hozzárendelésére, valamint a megfelelő reagálásra való képességet, képes lenne megvédeni polgárait és tagállamai biztonságát;

M. mivel a nemzetközi terrorista szervezetek szakértelme egyre nő, és egyre gyakrabban alkalmazzák a kiberhadviselést, a kibertámadások elkövetői pedig a legkorszerűbb technológiát használják a rendszerek és eszközök biztonsági réseinek feltárására, valamint a nagy- és megaméretű kibertámadások végrehajtására;

N. mivel a Pegasus kémprogrammal kapcsolatos botrány nyomán kiderült, hogy sok újságíró, emberi jogi aktivista, választott képviselő és más uniós polgár után kémkedtek; mivel a védelmi és az űripar példa nélküli globális versennyel és a fejlett kibertechnológiák megjelenésével járó jelentős technológiai változásokkal néz szembe; mivel az Európai Számvevőszék rámutatott az infokommunikációs technológiák, a kiberhadviselés és a MI területén mutatkozó képességbeli hiányosságokra; mivel az Unió a kiberbiztonsági termékek és szolgáltatások nettó importőre, ami növeli a nem uniós szereplőkkel szembeni technológiai függőség és kiszolgáltatottság kockázatát; mivel egy sor közös uniós Mi-képességgel kellene áthidalni a műszaki hiányosságokat, és biztosítani kellene, hogy azok a tagállamok, amelyek nem rendelkeznek megfelelő technológiai-ipari szakértelemmel vagy képességekkel ahhoz, hogy védelmi minisztériumaikban MI-rendszereket vezessenek be, ne maradjanak le;

O. mivel különböző állami szereplők – például Oroszország, Kína és Észak-Korea – politikai, gazdasági vagy biztonsági célkitűzések megvalósítása érdekében rossz szándékú kibertevékenységeket folytattak, amelyek többek között a kritikus infrastruktúrák elleni támadásokat, kiberkémkedést és az uniós polgárok tömeges megfigyelését foglalták magukban, dezinformációs kampányokat elősegítve, valamint az internet-hozzáférést és az informatikai rendszerek működését korlátozó kártékony szoftvereket terjesztve; mivel az ilyen tevékenységek figyelmen kívül hagyják és sértik a nemzetközi jogot, az emberi jogokat és az alapvető uniós jogokat, miközben veszélyeztetik a demokráciát, a biztonságot, a közrendet és az Unió stratégiai autonómiáját, és ezért közös uniós fellépéssel kell rájuk válaszolni, mint amilyen a közös uniós diplomáciai fellépés keretének alkalmazása, ideértve az uniós kiberdiplomáciai eszköztár tekintetében tervezett korlátozó intézkedések alkalmazását is;

P. mivel a Tanács első alkalommal 2020. július 30-án határozott úgy, hogy korlátozó intézkedéseket vezet be kibertámadásokért felelős vagy azokban részt vevő személyekkel, szervezetekkel és szervekkel szemben a kibertérben előforduló rossz szándékú viselkedés hatékonyabb megelőzése, az attól való eltérítés és elrettentés és az arra való reagálás érdekében; mivel az uniós kiberbiztonsági szankciórendszerre vonatkozó jogi keretet 2019 májusában fogadták el;

Q. mivel az attribúciós formák a kiberdiplomácia és az elrettentési stratégiák központi elemei;

R. mivel az Unió és a NATO közötti együttműködés számos területen fokozódott, beleértve a kiberbiztonságot és -védelmet is, a 2016. évi EU–NATO együttes nyilatkozattal összhangban;

S. mivel az ENSZ kormányzati szakértői csoportjának (UN GGE) 2010., 2013. és 2015. évi konszenzusos jelentései, amelyeket az ENSZ Közgyűlése is jóváhagyott, a kiberstabilitás egyetemes normatív keretét képezik, e keret pedig annak elismeréséből áll, hogy a meglévő nemzetközi jog, beleértve teljes egészében az ENSZ Alapokmányát is, alkalmazandó a kibertérben, amint alkalmazandó a felelős állami magatartásra vonatkozó 11 önkéntes, nem kötelező erejű norma, valamint a bizalomépítő intézkedések és a kapacitásépítés;

Az Unió kibervédelmi képességeinek állapota

1. hangsúlyozza, hogy a mélyebb és erősebb európai védelmi unió fejlesztésében központi szerepet játszik a közös kibervédelmi politika és a közös és jobb kibervédelmi kapacitások létrehozásának uniós szintű jelentős koordinációja, ami a technikai, stratégiai és operatív képességek komplex együttesét igényli; kijelenti, hogy a kibervédelem olyan intézkedéseket, eszközöket és eljárásokat jelent, amelyek arányosak és összhangban állnak a nemzetközi joggal, amelyek katonai és polgári elemeket egyaránt tartalmaznak, és amelyek célja többek között a KBVP-vel kapcsolatos kommunikációs és információs hálózatok, valamint a KBVP-missziók és -műveletek védelme, valamint a tagállamok segítése; hangsúlyozza, hogy sürgősen fejleszteni kell és meg kell erősíteni mind a közös, mind a tagállami katonai kibervédelmi képességeket;

2. emlékeztet rá, hogy a kibertér határok nélküli jellege, valamint a kibertámadások jelentős száma és növekvő összetettsége miatt összehangolt uniós szintű reagálásra van szükség, beleértve a közös tagállami támogatási képességeket és az EU kiberdiplomáciai eszköztárának intézkedéseihez nyújtott tagállami támogatást is, szükség van továbbá a kiberbiztonsági eseményekre reagáló csoportok közötti információmegosztáson, a bevált gyakorlatok cseréjén, megerősített képzésen, kutatáson és gyakorlatokon alapuló fokozott EU–NATO együttműködésre;

3. üdvözli az uniós kibervédelmi szakpolitikai keretet mint a tagállamok kibervédelmi képességeinek fejlesztését támogató eszközt; hangsúlyozza, hogy az uniós kibervédelmi szakpolitikai keret felülvizsgálatának mindenekelőtt a meglévő hiányosságokra és biztonsági résekre kell rávilágítania az uniós és nemzeti katonai struktúrák tekintetében; hangsúlyozza, hogy fokozni kell a koordinációt az uniós intézmények, ügynökségek és szervek között, a tagállamokkal és a tagállamok között, valamint az Európai Parlamenttel annak biztosítása érdekében, hogy az uniós kibervédelmi szakpolitikai keret teljesítse az Unió kibervédelmi célkitűzéseit;

4. felhívja az EKSZ-t és a Bizottságot, hogy a tagállamokkal együttműködve fejlessze tovább az átfogó intézkedéscsomagot és a koherens informatikai biztonsági politikát a reziliencia és a katonai kibervédelmi koordináció megerősítése érdekében; sürgeti az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportjával (CERT-EU) való együttműködés megerősítését az összes uniós intézmény, szerv és ügynökség által használt hálózatok védelme érdekében, szoros együttműködésben az érintett szervezetek informatikai igazgatóival, valamint az uniós intézmények, szervek és ügynökségek tagállamokkal folytatott kommunikációjának megerősítését; felhívja a Parlamentet, hogy biztosítsa saját részvételét a CERT-EU eredményeiben olyan informatikai biztonsági szint elérése

érdekében, amely lehetővé teszi számára, hogy megkapja a Szerződések szerinti feladatainak ellátásához szükséges összes minősített és nem minősített adatot, többek között a biztonság és védelem területén az információkhoz való hozzáférésről szóló, 2002. évi intézményközi megállapodás felváltására irányuló jelenlegi folyamat eredményeként; felszólítja az EKSZ-t, hogy biztosítsa eszközeinek, helyiségeinek és tevékenységeinek megfelelő kiberbiztonsági szintjét, ideértve a központjait, az uniós küldöttségeket, valamint a KBVP-missziókat és -műveleteket is;

5. tudomásul veszi a 2018-as kibervédelmi szakpolitikai keret azon célkitűzését, hogy létrehozza az Unió katonai CERT-hálózatát; felhívja a tagállamokat, hogy jelentősen növeljék a minősített információk megosztására irányuló kapacitásokat, hogy amennyiben szükséges és hasznos, megkönnyítsék az információmegosztást, és hozzanak létre gyors és biztonságos európai hálózatot a kibertámadások felderítésére, értékelésére és megakadályozására;

6. emlékeztet rá, hogy a képességfejlesztési terv keretében meghatározott, 2018. évi uniós képességfejlesztési prioritások tükrözték annak szükségességét, hogy a képességek teljes spektrumát ki kell fejleszteni, és a kibervédelmet fő prioritássá emelték; emlékeztet rá, hogy a képességfejlesztési terv hangsúlyozta, hogy a kiber-helyzetismereti technológiák és a defenzív kibertechnológiák alapvető fontosságúak a biztonsági veszélyek elleni fellépéshez; üdvözli, hogy az EDA támogatja a tagállamokat a kiberreziliencia javítására szolgáló képességeik, vagyis a kibertámadások felderítésére, az azoknak való megbirkózásra és az azokat követő újbóli talpra állásra szolgáló képesség fejlesztésében; tudomásul veszi a tagállamok által az EDA keretében indított különböző tevékenységeket, többek között az EDA „Kibervédelmi követelmények megtervezése" (CyDRE) elnevezésű projektjét, amelynek célja szervezeti architektúra kifejlesztése kibertérbeli műveletekhez, beleértve a hatókört, a funkciókat és a követelményeket, nemzeti és uniós jogszabályok alapján;

7. felhívja a tagállamokat, hogy a gyors fellépés fokozása és a kibertámadások elleni biztonságos hálózat biztosítása érdekében határozzanak meg a minősített és nem minősített adatokra alkalmazható közös kommunikációs szabványt;

8. üdvözli a koordinált éves védelmi szemlét (CARD) – az első teljes jogú, uniós szintű védelmi szemlét – , amely az egyik olyan kulcsfontosságú eszköz, amely támogatja a tagállamok védelmi kiadásaiban, védelmi terveiben és védelmi együttműködésében érvényesülő általános koherenciát, és amelynek hozzá kell járulnia a kibervédelmi képességek fejlesztésébe történő beruházások előmozdításához;

9. üdvözli az európai védelmi ipari fejlesztési program keretében a hírszerzéssel, a biztonságos kommunikációval és a kibervédelemmel kapcsolatos számos releváns projekt formájában már elért eredményeket; üdvözli különösen a védelemre szolgáló, könnyen telepíthető és összekapcsolt kibereszköztár létrehozására irányuló felhívást, valamint azt a tényt, hogy az EDF hozzá fog járulni a reziliencia megerősítéséhez, valamint a felkészültség, a reagálási képesség és az együttműködés javításához a kiberterületen, feltéve, hogy ezt prioritássá teszik az EDF vonatkozó munkaprogramjairól folytatott tárgyalások során; hangsúlyozza, hogy az Unió kibervédelmi projektek kidolgozására való képessége a technológiák, berendezések, szolgáltatások, adatok és adatfeldolgozás irányításától függ, és megbízható ágazati érdekelti bázisra van hozzá szükség, ugyanakkor felszólít a védelmi beszerzésekről szóló irányelv ([6]) teljes körű végrehajtására és érvényesítésére; felszólítja a tagállamokat, hogy használják ki az EDF-et a kibervédelmi képességek közös fejlesztése érdekében;

10. üdvözli a tagállamok közötti fokozott együttműködést a kibervédelem, valamint a vezetés, irányítás, kommunikáció, informatika, hírszerzés, megfigyelés és felderítés (C4ISR) területén, valamint az állandó strukturált együttműködés (PESCO) keretében elért előrelépést, ideértve az olyan konkrét projektek végrehajtásán keresztül elért előrelépést, mint a „Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén"; emlékeztet rá, hogy az EDF és a PESCO kiváló lehetőségeket kínál a kbervédelmi képességek fejlesztésére és a kiberbiztonsági kezdeményezések felgyorsítására, például a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platformon és a Kiber- és az Információs Terület Koordinációs Központján keresztül; felszólítja a tagállamokat, hogy a prioritásokkal kapcsolatos közös stratégiai megközelítés kidolgozása révén biztosítsák a koherenciát, és összpontosítsanak a kiberkapacitásra; felszólít a kutatás és innováció és a szakmai tapasztalatcsere előmozdítására a PESCO és az EDF teljes potenciáljának kiaknázása érdekében; üdvözli a Tanács 2020. november 5-i határozatát, amely lehetővé teszi a harmadik országok számára, hogy egyes konkrét esetekben csatlakozzanak

([6]) Az Európai Parlament és a Tanács 2009/81/EK irányelve (2009. július 13.) a honvédelem és biztonság területén egyes építési beruházásra, árubeszerzésre és szolgáltatásnyújtásra irányuló, ajánlatkérő szervek vagy ajánlatkérők által odaítélt szerződések odaítélési eljárásainak összehangolásáról (HL L 216., 2009.8.20., 76. o.).

az egyes PESCO-projektekhez, mivel ezek az országok hozzáadott értéket teremthetnek, technikai szakértelmet és további képességeket biztosíthatnak, feltéve, hogy megfelelnek az elfogadott politikai, anyagi és jogi feltételeknek; hangsúlyozza, hogy kivételes és eseti alapon az Unió stratégiai érdeke lehet, hogy a tagállamok és harmadik országok részt vegyenek a kiberterülethez kapcsolódó PESCO-projektekben annak érdekében, hogy a tényleges viszonosság alapján ambiciózusabb kötelezettségvállalásokat tegyenek;

11. hangsúlyozza, hogy a kibervédelem valamennyi KBVP-misszió operatív feladatának tekintendő, és hogy a kiberrezilienciát és a kapcsolódó képességeket a KBVP tervezési folyamatainak megkezdése előtt ki kell alakítani, tesztelni és telepíteni kell; emlékeztet rá, hogy az uniós missziók és műveletek sikeres végrehajtása egyre inkább a biztonságos kibertérhez való zavartalan hozzáféréstől függ, és ezért szilárd és reziliens kiberműveleti képességeket, valamint a katonai létesítmények, missziók és műveletek elleni támadásokra adott megfelelő válaszlépéseket igényel; hangsúlyozza, hogy a polgári KBVP területére vonatkozó paktummal összhangban a polgári KBVP-misszióknak reziliensnek kell lenniük a kibertámadásokkal szemben, és adott esetben támogatniuk kell a fogadó országokat, többek között nyomon követés, mentorálás és tanácsadás révén; javasolja, hogy vizsgálják meg, hogy milyen lehetőségek vannak a partnereink kiberkapacitás-építésének előmozdítására, így például az uniós képzési missziók megbízatásának kibővítését, hogy abba a kibervédelmi szempontok is beletartozzanak, illetve a polgári kibermissziók indítását;

12. üdvözli az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló, 2019. május 14-i tanácsi határozatot, amely célzott korlátozó intézkedéseket tesz lehetővé az Unióra vagy tagállamaira fenyegetést jelentő kibertámadások – ideértve a harmadik országok vagy nemzetközi szervezetek elleni kibertámadásokat – megakadályozása és az ezekre való reagálás érdekében; üdvözli, hogy 2020 júliusában és 2020 októberében ilyen korlátozó intézkedéseket vezettek be, ami hiteles lépés az Unió kiberdiplomáciai eszköztárának, többek között a korlátozó intézkedések, alkalmazása és az Unió kiberelrettentéssel kapcsolatos uniós megközelítés megerősítése felé; felszólít a kibertámadások megfékezését célzó arányos korlátozó intézkedések rendszerének továbbfejlesztésére és szigorú végrehajtására, tiszteletben tartva az internetre vonatkozó európai elképzelést, amely szerint az internet egységes, nyitott, semleges, szabad, biztonságos és nem széttagolt hálózat;

13. emlékeztet rá, hogy a kibertechnológiák kettős felhasználást lehetővé tevő jellege miatt a biztonságos polgári termékek és szolgáltatások kulcsfontosságúak a katonai terület számára is, és így hozzájárulnak a jobb kibervédelemhez; üdvözli ezért az ENISA vezetésével zajló, a tagállamok és az érdekelt felek által együttesen folytatott munkát, amelynek célja, hogy az IKT-termékekre, -szolgáltatásokra és -folyamatokra alkalmazandó tanúsítási rendszereket bocsássanak az Unió rendelkezésére, hogy növeljék a kiberbiztonság általános szintjét a digitális egységes piacon; hangsúlyozza, hogy az Unió központi, úttörő szerepet tölt be olyan szabványok kidolgozásában, amelyek formálják a kiberbiztonsági környezetet, hozzájárulnak a tisztességes versenyhez az Unión belül és a globális színtéren, valamint reagálnak a területen kívüli intézkedésekre és a harmadik országokból eredő biztonsági kockázatokra; elismeri továbbá, hogy az ENISA fontos szerepet játszik a kutatási kezdeményezések és a kiberbiztonság fokozását célzó más együttműködési formák támogatásában; hangsúlyozza a kibervédelmi és kiberbiztonsági képességekbe történő beruházások fontosságát az Unió és a tagállamok rezilienciájának és stratégiai kapacitásainak fokozása céljából; e tekintetben kiemeli a Digitális Európa program és a Horizont Európa, különösen annak „A társadalmat szolgáló polgári biztonság” elnevezésű 3. klaszterének fontosságát; megállapítja, hogy a 2021–2027-re szóló többéves pénzügyi keretben (MFF), valamint a Helyreállítási és Rezilienciaépítési Eszközben jelentős pénzügyi eszközök állnak rendelkezésre;

14. üdvözli azokat az eredményeket, amelyeket néhány uniós tagállam ért el a hadseregükön belüli kiberparancsnokságok létrehozása terén;

Stratégiai jövőkép – a kibervédelmi reziliencia megvalósítása

15. megjegyzi, hogy a stratégiai iránytű fokozni és irányítani fogja az Unió biztonság- és védelempolitikai ambíciószintjének végrehajtását, és az ambíciót képességigényekre fogja lefordítani, többek között prioritásként a kibervédelem terén is, növelve ezáltal az Unió és a tagállamok képességét arra, hogy felderítsék, hozzárendeljék, megelőzzék, elbizonytalanítsák és elrettentsék a rossz szándékú kibertevékenységeket, és megbirkózzanak velük azáltal, hogy megerősíti helyzetüket, helyzetismeretüket, jogi és etikai keretüket, eszközeiket, eljárásaikat és partnerségeiket;

16. kitart amellett, hogy a stratégiai iránytűnek meg kell erősítenie a stratégiai kultúrát a kiberterületen, és meg kell szüntetnie a képességek és megbízatások közötti átfedéseket; hangsúlyozza, hogy meg kell szüntetni az Unión belüli átfogó kiberarchitektúra jelenlegi széttagoltságát és összetettségét, és közös elképzelést kell kialakítani arra vonatkozóan, hogy hogyan lehet elérni a kibertér biztonságát és stabilitását;

17. hangsúlyozza, hogy a széttagoltságot komoly aggodalmak kísérik az uniós szintű források és a személyzet hiánya miatt, ami akadályozza a legbiztonságosabb digitális környezet megteremtésére irányuló törekvést, és ezért hangsúlyozza, hogy mindkettőt növelni kell; sürgeti az alelnököt/főképviselőt és/vagy a tagállamokat, hogy növeljék a pénzügyi és

kibervédelmi személyzeti erőforrásokat, különösen a kiberhírszerzési elemzőket és a kiberkriminalisztikai szakértőket, valamint képzésüket a döntéshozatal és a szakpolitikai döntéshozatal, a szakpolitikai végrehajtás, a kiberbiztonsági eseményekre való reagálás és nyomozás területén, beleértve a kiberkészségek fejlesztését, hogy megerősítsék EU azon képességét, hogy a kibertámadásokat jellemezni és azonosítani tudja, és ezáltal rövid időn belül megfelelő politikai, polgári és katonai választ adjon; felszólít a CERT-EU és az Európai Unió Helyzetelemző Központja (INTCEN) további finanszírozására, valamint a tagállamok támogatására a biztonsági műveleti központok (SOC-ok) létrehozásában és megerősítésében, annak érdekében, hogy EU-szerte létrejöjjön a SOC-ok hálózata, amely fokozhatná a polgári-katonai együttműködést, hogy időben ki lehessen adni a kiberbiztonsági eseményekkel kapcsolatos figyelmeztetéseket;

18. megjegyzi, hogy a kiberterületet érintő korszerűbb uniós katonai képzés és oktatás jelentősen javítaná a tagállamok közötti bizalom szintjét, növelve a szabványműveleti eljárásokat, egyértelműbb szabályokat kialakítva, valamint javítva a végrehajtást; e tekintetben megjegyzi, hogy az Európai Biztonsági és Védelmi Főiskola (EBVF) fontos képzési munkát végez a kibervédelem területén, és üdvözli e tekintetben a kiberoktatással, -képzéssel, -értékeléssel és -gyakorlattal kapcsolatos platform létrehozását, amelynek célja a polgári és katonai személyzet kiberbiztonsági és -védelmi képzése, valamint a kiberterülettel kapcsolatos képzés szükséges harmonizációjának és szabványosításának megvalósítása; hangsúlyozza, hogy az EBVF-nek több uniós strukturális finanszírozást kell kapnia, hogy fokozni tudja az uniós kibervédelmi készségek fejlesztéséhez való hozzájárulását, különös tekintettel arra, hogy egyre nagyobb szükség van a legmagasabb szintű kiberszakértőkre; felszólítja a tagállamokat, hogy támogassák a tudományos körökkel való partnerségeket, amelyek célja a kiberbiztonsági kutatási-fejlesztési program előmozdítása a polgári és a védelmi ágazatban egyaránt alkalmazható új közös technológiák, eszközök és készségek kifejlesztése érdekében; hangsúlyozza az oktatás fontosságát, melynek célja a közvélemény tudatosságának növelése és a polgárok készségeinek fejlesztése, hogy meg tudják védeni magukat a kibertámadásokkal szemben;

19. hangsúlyozza, hogy az uniós kibervédelmi szakpolitikáknak figyelembe kell venniük a nemek közötti egyenlőség szempontjait, és ambiciózusnak kell lenniük a nemek közötti szakadéknak a kibervédelmi szakemberek körében történő megszüntetése terén, különösen aktív, nemi szempontból semleges szakpolitikák és a nők igényeihez igazított képzési programok révén;

20. emlékeztet arra, hogy a kibervédelemnek katonai és polgári dimenziója egyaránt van, és ezért az eszközök közötti szorosabb együttműködésre, szinergiákra és koherenciára van szükség; hangsúlyozza, hogy először elemezni kell és meg kell vitatni az együttműködéssel és a koordinációval kapcsolatos problémákat, valamint a humán és technikai erőforrásokat illető hiányosságokat mind nemzeti, mind uniós szinten; megjegyzi, hogy mind a katonai, mind a polgári erőforrások sikeres integrációja csak az összes érdekelt fél részvételével zajló képzések és gyakorlatok révén biztosítható; kiemeli e tekintetben a NATO „Locked Shields" elnevezésű gyakorlatát, amely a polgári és katonai kibervédelmi képességek tesztelésének és javításának egyik legjobb példája; felhívja ezért az alelnököt/főképviselőt és a Bizottságot, hogy dolgozzon ki integrált politikai megközelítést és mozdítsa elő a szinergiákat és a szoros együttműködést a katonai CERT-hálózat, a CERT-EU és a CSIRT-ek hálózata között;

21. üdvözli az alelnök/főképviselő és a Bizottság „Az EU kiberbiztonsági stratégiája a digitális évtizedre" című közös közleményét, amelynek célja a polgári, védelmi és űrbeli kibertevékenység közötti szinergiák és együttműködés fokozása; úgy véli, hogy a stratégia mérföldkő az Unió és a tagállamok kiberrezilienciájának megerősítése szempontjából, megerősítve ezáltal az EU digitális vezető szerepét és stratégiai kapacitásait;

22. javasolja egy közös kiberbiztonsági egység létrehozását az együttműködés fokozására, hogy ezáltal egy biztonságos és gyors információs hálózatot garantálva reagálni lehessen az uniós intézmények, szervek és hivatalok közötti információmegosztás hiányára, és hogy lehetővé váljon a meglévő struktúrák, erőforrások és képességek teljes mértékű kihasználása; megjegyzi, hogy a közös kiberbiztonsági egység fontos szerepet játszhat az EU súlyos, határokon átnyúló kibertámadásokkal szembeni védelmében, ami az ágazatok közötti információmegosztás koncepcióján alapul; hangsúlyozza a koordináció fontosságát, hogy a fejlesztés során elkerülhető legyen a struktúrák és a felelősségi körök megkettőzése; üdvözli e tekintetben a Bizottság 2021. június 23-i ajánlását, amely előírja, hogy a kibervédelmi közösséggel való információmegosztás lehetővé tétele érdekében egyedi interfészeket kell kiépíteni a közös kiberbiztonsági egységgel, konkrétan az EKSZ képviseletén keresztül; hangsúlyozza továbbá, hogy a releváns PESCO-projektek képviselőinek támogatniuk kell a közös kiberbiztonsági egység munkáját, különösen a helyzetismeret és a felkészültség tekintetében;

23. emlékeztet rá, hogy a kibervédelmi képességek javításához – tekintettel azok gyakran kettős felhasználást lehetővé tevő jellegére – polgári hálózat- és információbiztonsági szakértelemre is szükség van; hangsúlyozza, hogy a kettős felhasználású, készen kapható rendszerek elterjedése kihívásokat jelenthet abból a szempontból, hogy a rendszereket egyre

több állami és nem állami ellenséges szereplő is hasznosítja; felszólítja a Bizottságot és a tagállamokat, hogy vezessenek be számos kulcsfontosságú eszközt, például tanúsítást, valamint a magánszereplők felelősségének felügyeletét; hangsúlyozza, hogy a technológiai innovációt főként a magánvállalkozások mozgatják, és ezért kulcsfontosságú a magánszektorral és a civil szereplőkkel – köztük a kritikus infrastruktúrák kezelésében részt vevő iparágakkal és szervezetekkel, valamint a kkv-kkal, a civil társadalommal, a szervezetekkel és a tudományos körökkel – való együttműködés, amelyet meg kell erősíteni; megjegyzi, hogy a hálózati és információs rendszerek biztonságáról szóló irányelv és a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv javasolt felülvizsgálatát, amelynek célja a kritikus infrastruktúrák védelme, az ellátási lánc biztonságának fokozása és a szabályozott szereplők digitális ökoszisztémába való bevonása; emlékeztet arra, hogy minden tagállamnak külön politikával kell rendelkeznie az ellátási lánc kiberbiztonsági kockázatainak kezelésére vonatkozóan, amely különösen a megbízható beszállítók kérdésével foglalkozik; emlékeztet továbbá arra, hogy a kiberbiztonsági irányelvnek tiszteletben kell tartania a tagállamok hatásköreit, és hivatkozik a Biztonság- és Védelempolitikai Albizottság e két javaslatról megfogalmazott véleményeire;

24. üdvözli, hogy 2020. szeptember 29-én elindult az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (CyCLONe), amely az EU technikai és politikai szintjei közötti szakadék megszüntetésével tovább javította az időben történő információmegosztást és helyzetismeretet; megjegyzi, hogy a hatékony kibervédelmi képességek szükségessé teszik a szükséges ismeret elvén alapuló információmegosztási kultúráról a megosztás szükségességén alapuló információmegosztási kultúrára való átállást;

25. üdvözli a polgári, a védelmi és az űripar közötti szinergiákról szóló bizottsági cselekvési tervet, és emlékeztet e három ágazat szoros egymásrautaltságára a kibervédelem terén; megjegyzi, hogy más katonai területektől eltérően a kibertér „létrehozásához” használt infrastruktúrát elsősorban az EU-n kívüli kereskedelmi szervezetek működtetik, ami harmadik felektől való ipari és technológiai függőségekhez vezet; határozottan úgy véli, hogy az EU-nak fokoznia kell technológiai szuverenitását és az innovációt, és be kell ruháznia az olyan új technológiák biztonsági és védelmi célú felhasználásába, mint a mesterséges intelligencia és a kvantuminformatika; határozottan ösztönzi a mesterséges intelligenciára összpontosító kutatási-fejlesztési menetrend kidolgozását a tagállamokban; hangsúlyozza azonban, hogy a mesterséges intelligencia katonai alkalmazása során tiszteletben kell tartani a nemzetközi emberi jogi jogszabályokat és a nemzetközi humanitárius jogot, és hogy az EU-nak vezető szerepet kell vállalnia egy, a mesterséges intelligenciára vonatkozó globális szabályozási keret előmozdításában, amely demokratikus értékeken és az „emberi beavatkozás” megközelítésen alapul;

26. megjegyzi az Európai Unió Műholdközpontja (Satcen) által végzett fontos munkát, és hangsúlyozza, hogy az Uniónak megfelelő erőforrásokkal kell rendelkeznie a műholdas képek és információgyűjtés területén; kéri az ügynökséget, hogy elemezze és készítsen jelentést az uniós és tagállami műholdak űrszeméttel és kibertámadásokkal szembeni biztonságáról és/vagy sebezhetőségéről; hangsúlyozza, hogy az EU Satcennek strukturálisabb uniós finanszírozásban kell részesülnie annak érdekében, hogy fenntarthassa az uniós fellépésekhez való hozzájárulását; hangsúlyozza, hogy a kibervédelmi képességek alapvető fontosságúak a Satcennel való biztonságos és reziliens információcsere biztosításához mind az űrből biztosított biztonság, mind az űrbiztonság terén, hogy az EU megőrizze és fokozza a helyzetismerethez szükséges stratégiai autonómiáját; hangsúlyozza, hogy az EU-nak törekednie kell arra, hogy megakadályozza a világűr hadviselésre való felhasználását;

27. üdvözli az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont bukaresti létrehozásáról szóló tanácsi határozatot, amely az Európai horizont programból és a Digitális Európa programból fogja biztosítani a kiberbiztonsággal kapcsolatos finanszírozást, és ösztönzi a nemzeti koordinációs központok hálózatával való zökkenőmentes együttműködést; hangsúlyozza, hogy a Központ fontos szerepet játszik a vonatkozó kiberbiztonsági projektek és kezdeményezések végrehajtásában, amelyek hozzájárulnak az Unió rezilienciájának támogatásához nélkülözhetetlen új képességek létrehozásához, valamint a polgári és a védelmi kiberbiztonsági ágazat közötti koordináció fokozásához; hangsúlyozza, hogy a Kiberbiztonsági Kompetenciaközpontnak emellett össze kell fognia a főbb európai érdekelt feleket, köztük az ipar képviselőit, a tudományos és kutatási szervezeteket, valamint más releváns civil társadalmi szervezeteket is a kiberbiztonsági szaktudás Unió-szerte történő megerősítése és terjesztése céljából;

28. hangsúlyozza a titkosítás és a titkosított adatokhoz való jogszerű hozzáférés fontosságát; emlékeztet arra, hogy az adattitkosítás, valamint az ilyen képességek megerősítése és lehető legszélesebb körű használata jelentős mértékben hozzájárulhat az államok, a társadalmak és az ipar kiberbiztonságához; bátorítja egy, az „európai digitális szuverenitásra” vonatkozó programot a jelenlegi képességeknek az alapvető európai jogok és értékek, mint például a magánélethez való jog, a véleménynyilvánítás szabadsága és a demokrácia által motivált kiber- és titkosítási eszközök tekintetében történő megerősítése és fejlesztése érdekében, hogy a kiberbiztonsági piacon fokozni lehessen az európai versenyképességet és növelni lehessen a belső keresletet;

2021. október 7., csütörtök

29. üdvözli a kibertérrel mint műveleti területtel kapcsolatos, hamarosan bemutatandó katonai koncepciót és stratégiát, amely az uniós KBVP műveleti területeként határozza meg a kiberteret; felszólít a KBVP-missziók információs infrastruktúrái sebezhetőségének folyamatos értékelésére, valamint a közös harmonizált előírások végrehajtására a kibervédelmi oktatás, képzés és gyakorlatok terén a KBVP-missziók támogatása érdekében;

30. sajnálatát fejezi ki amiatt, hogy az EU Katonai Tervezési és Végrehajtási Szolgálata (MPCC) minősített rendszereinek jelenlegi korlátai akadályozzák annak képességeit; felszólítja ezért az EKSZ-t, hogy gyorsan biztosítsa az MPCC számára a legkorszerűbb, autonóm és biztonságos kommunikációs és információs rendszert (CIS), amely akár a KBVP-misszióinak és -műveleteinek minősített uniós adatait is képes kezelni, megfelelő szintű védelemmel és rezilienciával, valamint egy telepített kötelékparancsnoksággal együtt;

31. felszólít a kiberbiztonság uniós válságreagálási mechanizmusokba való további integrálására, valamint a különböző kiberközösségek meglévő kezdeményezéseinek, struktúráinak és eljárásainak összekapcsolására a tagállamok közötti fokozott kölcsönös segítségnyújtás és operatív együttműködés érdekében, különösen jelentős kibertámadások esetén, az interoperabilitás növelése és a kibervédelem közös értelmezésének kialakítása érdekében; határozottan hangsúlyozza a válságkezeléssel kapcsolatos további, de gyakoribb gyakorlatok és forgatókönyveken alapuló szakpolitikai megbeszélések fontosságát, többek között a kölcsönös segítségnyújtási záradékról (az EUSZ 42. cikkének (7) bekezdése) egy feltételezett jelentős kibertámadási forgatókönyv alapján, amely potenciálisan fegyveres támadásnak minősülhet; kéri, hogy legyen több ilyen kezdeményezés a kölcsönös segítségnyújtásra és/vagy szolidaritásra vonatkozó végrehajtási eljárások közös értelmezésének megerősítése érdekében, összhangban az EUSZ 42. cikkének (7) bekezdésével és az EUMSZ 222. cikkével, többek között azzal a konkrét céllal, hogy a tagállamokat érő kibertámadásokra vonatkozó eljárásokat gyakorlatban is megvalósítsák; üdvözli a NATO 2021. június 14-i brüsszeli csúcstalálkozóján kiadott közleményt, amely megerősíti a NATO elkötelezettségét a képességek teljes skálájának mindenkori alkalmazása mellett a kiberfenyegetések teljes spektrumával szembeni aktív elrettentés, védelem és elhárítás érdekében, beleértve az 5. cikk eseti alapon történő alkalmazására vonatkozó határozatot is; üdvözli az uniós kiberbiztonsági válságreagálási keret és a kiberdiplomáciai eszköztár összehangolásáról szóló további megbeszéléseket;

32. megjegyzi, hogy az EU egyre növekvő mértékben vesz részt a geopolitikai ellenfelekkel való hibrid konfliktusokban; hangsúlyozza, hogy e cselekmények különösen destabilizáló és veszélyes jellegűek, mivel elmossák a háború és a béke közötti határvonalakat, destabilizálják a demokráciákat és kétségeket ébresztenek a célcsoportokban; emlékeztet arra, hogy ezek a támadások önmagukban gyakran nem elég súlyosak ahhoz, hogy kiváltsák a NATO-szerződés 5. cikkének vagy az EUSZ 42. cikke (7) bekezdésének alkalmazását, noha kumulatív stratégiai hatásuk van, és nem kezelhetők hatékonyan a jogsérelmet elszenvedett tagállam által alkalmazott retorziós intézkedésekkel; úgy véli, hogy az EU-nak ezért arra kell törekednie, hogy megoldást találjon e joghézag kitöltésére az EUSZ 42. cikke (7) bekezdésének és az EUMSZ 222. cikkének olyan módon történő újraértelmezésével, amely a kollektív védelemre vonatkozó küszöbérték alatt is fenntartaná a kollektív védelemhez való jogot, és lehetővé tenné az uniós tagállamok önkéntes alapon történő kollektív ellenintézkedéseit, valamint nemzetközi szinten is együtt kell működnie szövetségeseivel egy hasonló, nemzetközi szintű megoldás érdekében; hangsúlyozza, hogy ez az egyetlen hatékony eszköz a hibrid fenyegetésekre való reagálás terén mutatkozó bénultság leküzdésére, és olyan eszköz, amellyel növelhetők az ellenfeleink költségei;

33. megismétli, hogy az erős közös attribúciós képességek az uniós és tagállami képességek megerősítésének kulcsfontosságú eszközei, valamint a hatékony kibervédelem és a kibertámadásoktól való elrettentés alapvető elemét képezik; hangsúlyozza, hogy a technikai információkkal, elemzésekkel és fenyegetettségi információkkal kapcsolatos, tagállamok közötti uniós szintű információmegosztás javítása lehetővé tenné az uniós szintű kollektív attribúciót; elismeri, hogy a kibervédelem bizonyos fokig hatékonyabb, ha bizonyos offenzív eszközöket és intézkedéseket is tartalmaz, feltéve, hogy használatuk megfelel a nemzetközi jognak; hangsúlyozza, hogy a kibertámadások elkövetőinek pontos megnevezése az elrettentés hasznos eszköze; felkér arra, hogy mérlegeljék a rossz szándékú kibertevékenységek elkövetőinek közös állami felderítését, ideértve annak lehetőségét, hogy az EKSZ égisze alatt az egyes szereplők kibertérbeli magatartásáról szóló jelentéseket készítsenek, amelyek uniós szinten összefoglalják a tagállamok ellen irányuló, államilag támogatott rossz szándékú kibertevékenységeket;

34. úgy véli, hogy az Unió és a NATO közötti kiber-együttműködés alapvető fontosságú, amely lehetővé teheti és megerősítheti a rossz szándékú kiberbiztonsági események hivatalos kollektív azonosítását és következésképpen a korlátozó szankciók és intézkedések bevezetését; megjegyzi, hogy a reziliencia funkciója és a hatékony elrettentés akkor érhető el, ha az ellenfelek tisztában lennének (a kibertámadások súlyosságán, nagyságrendjén és célpontján alapuló) lehetséges ellenintézkedések tárházával, valamint azok arányosságával és megfelelőségével, és a nemzetközi jognak, különösen az ENSZ Alapokmányának való megfelelésükkel;

35. üdvözli a főképviselő/alelnök arra irányuló javaslatát, hogy ösztönözzék és segítsék elő az INTCEN-en belül a tagállamok uniós kiberhírszerzési munkacsoportjának létrehozását a kiberfenyegetésekkel és -tevékenységekkel kapcsolatos stratégiai hírszerzési együttműködés előmozdítása érdekében, hogy további támogatást lehessen nyújtani az

uniós helyzetismerethez és a közös diplomáciai fellépésre vonatkozó döntéshozatalhoz; ösztönzi a közös javaslatcsomag további előrehaladását, különösen a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoporttal és a NATO hibrid elemző egységével a helyzetismeret és -elemzés megosztása, valamint a taktikai és operatív együttműködés terén folytatott folyamatos együttműködést;

A partnerségek megerősítése és az Unió szerepének erősítése nemzetközi összefüggésben

36. úgy véli, hogy a NATO-val folytatott kiber-együttműködés fontos szerepet játszik a tagállamok kollektív biztonságának területeit érintő kibertámadások megelőzésében, megakadályozásában és szükség esetén az azokra való reagálásban; felszólítja a tagállamokat, hogy teljeskörűen osszák meg a bizonyítékokat és a hírszerzési értesüléseket, hogy azok felhasználhatók legyenek a kiberbiztonsági szankciólisták létrehozásához; felszólít e témát illetően a NATO-val való fokozott koordinációra a kibergyakorlatokban és közös képzésekben, például a párhuzamos és koordinált gyakorlatokban (PACE) való részvétel révén;

37. elismeri, hogy az EU-nak és a NATO-nak egyeztetnie kell azokban a kérdésekben, amikor ellenséges szereplők az euroatlanti biztonsági érdekeket fenyegetik; aggodalmát fejezi ki különösen Kína, Oroszország és Észak-Korea által a kibertérben tanúsított rendszerszintű agresszív magatartás miatt, beleértve a kormányzati intézmények és magánvállalatok elleni számos kibertámadást; úgy véli, hogy az EU és a NATO közötti együttműködésnek a kibernetika, a hibrid fenyegetések, a kialakulóban lévő és forradalmi technológiák, a világűr, a fegyverzetellenőrzés és a nonproliferáció területén jelentkező kihívásokra kell összpontosítania; sürgeti az EU és a NATO együttműködését az 5G bevezetésének szabályozása terén, hogy betarthatók legyenek azok a szigorú nemzeti biztonsági szabványok, amelyek biztosítják a nemzeti és nemzetközi információs hálózatoknak a kommunikáció titkosítására való alkalmasságát;

38. üdvözli a CERT-EU és a NATO kiberbiztonsági eseményeket kezelő képessége (NCIRC) közötti megállapodást, amely azáltal biztosítja a fenyegetésekre való valós idejű reagálás képességét, hogy mind az EU-ban, mind a NATO-ban javítja a kiberbiztonsági események megelőzését, felderítését és az azokra való reagálást; hangsúlyozza továbbá annak fontosságát, hogy a NATO Kibervédelmi Kiválósági Együttműködési Központjával (CCDCOE) és a NATO Kommunikációs és Információs Akadémiájával (NCI) együttműködésben növeljék az informatikai és kiberrendszerek kibervédelmi képzési képességeit;

39. felszólít az Unió és a NATO közötti további együttműködésre, különösen a kibervédelmi interoperabilitási követelmények tekintetében, a lehetséges komplementaritások keresése és a kapacitások kölcsönösen előnyös erősítése, az érintett KBVP-struktúráknak a NATO Federated Mission Networking (szövetségi misszió hálózatépítése) kezdeményezéséhez történő csatlakozására való törekvés, valamint a párhuzamosságok elkerülése és egymás feladatainak elismerése révén; sürgeti az uniós PESCO és a NATO Smart Defence (intelligens védelem) és Connected Forces (összekapcsolt haderők) kezdeményezése és védelmi beruházási kötelezettségvállalása megerősítését, valamint az összevonás és megosztás előmozdítását a beszállítók és a végfelhasználók közötti kapcsolatokban a szinergiák, a harmonizáció és a hatékonyság javítása érdekében; üdvözli az EU-NATO együttműködés során a kibervédelem területén elért eredményeket, nevezetesen a koncepciók és doktrínák cseréjét, a kibergyakorlatokon való kölcsönös részvételt és a kölcsönös tájékoztatókat illetően, különösen a válságkezelés kiberdimenziójával kapcsolatban; javasolja egy, a kiberfenyegetésekkel kapcsolatos közös EU–NATO információs központ, valamint a kiberbiztonsággal foglalkozó közös munkacsoport létrehozását;

40. felszólít a kibervédelem szorosabb összehangolására a tagállamok, az uniós intézmények, a NATO szövetségesei, az ENSZ és az Európai Biztonsági és Együttműködési Szervezet (EBESZ) között; e tekintetben ösztönzi az EBESZ kibertérrel kapcsolatos bizalomépítő intézkedéseinek további előmozdítását, és hangsúlyozza, hogy hatékony nemzetközi együttműködési eszközöket kell kifejleszteni a partnerek kiberkapacitás-építésének támogatása, valamint bizalomépítő intézkedések kidolgozása és előmozdítása, illetve a civil társadalommal és az érdekelt felekkel folytatott inkluzív együttműködés érdekében; üdvözli az indiai–csendes-óceáni térséggel folytatott együttműködésre vonatkozó, 2021. április 19-i uniós stratégiában hangsúlyozott globális, nyílt, szabad, stabil és biztonságos kibertérnek tulajdonított jelentőséget; felszólít arra, hogy aktívan építsenek ki szorosabb kapcsolatokat az indiai–csendes-óceáni térség hasonlóan gondolkodó demokráciáival, például az Egyesült Államokkal, Dél-Koreával, Japánnal, Indiával, Ausztráliával és Tajvannal a kiberfenyegetéssel szembeni fellépéssel kapcsolatos tudás és tapasztalatok megosztása, valamint információcsere érdekében; hangsúlyozza továbbá a más országokkal – különösen az EU közvetlen szomszédságában fekvő országokkal – való együttműködés fontosságát a kiberbiztonsági fenyegetések elleni védelmi kapacitásuk kiépítésének elősegítése érdekében; üdvözli, hogy a Bizottság támogatja a kiberbiztonsági programokat a Nyugat-Balkánon és a keleti partnerség országaiban; hangsúlyozza, hogy sürgető szükség van a nemzetközi jog – köztük az ENSZ Alapokmánya – tiszteletben tartására és a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó, széles körben elismert nemzetközi normatív keret betartására, valamint a nemzetközi jog kibertérben való alkalmazásának módozatairól az ENSZ keretében folyó vitához való hozzájárulásra;

2021. október 7., csütörtök

41. hangsúlyozza a kiberterületen az Egyesült Királysággal való erős partnerség fontosságát, amely a kibervédelmi arzenálját tekintve vezető nemzet; felszólítja a Bizottságot, hogy vizsgálja meg egy arra irányuló folyamat újraindításának lehetőségét, hogy a jövőben hivatalos és strukturált együttműködési keretet hozzanak létre ezen a területen;

42. hangsúlyozza, hogy a kibertérben biztosítani kell a békét és a stabilitást; felszólítja a tagállamokat és az Uniót, hogy – többek között egy cselekvési program előterjesztésével – vállaljanak vezető szerepet az ENSZ égisze alatt zajló viták és kezdeményezések során annak érdekében, hogy proaktív megközelítést alkalmazzanak egy közös nemzetközi szabályozási keret létrehozása során, valamint az ENSZ kormányzati szakértői csoportjának az ENSZ Közgyűlése által jóváhagyott konszenzusos jelentéseire építve ténylegesen elősegítsék az elszámoltathatóság kialakítását, az új normák betartását, a digitális technológiákkal való visszaélés megelőzését és a kibertérben tanúsított felelősségteljes állami magatartás előmozdítását; üdvözli a nyitott munkacsoport végső jelentésének ajánlásait, különösen egy cselekvési program létrehozását illetően; ösztönzi az ENSZ-t, hogy mozdítsa elő az államok, a kutatók, a tudományos körök, a civil társadalmi szervezetek, a humanitárius szereplők és a magánszektor közötti párbeszédet annak érdekében, hogy az új nemzetközi rendelkezésekkel kapcsolatos szakpolitikai döntéshozatali folyamatok inkluzívak legyenek; kéri valamennyi folyamatban lévő többoldalú erőfeszítés felgyorsítását annak érdekében, hogy a technológiai fejlődés és az új hadviselési módszerek ne haladhassák meg a normatív és szabályozási keretrendszereket; felszólít a fegyverzet-ellenőrzési architektúra korszerűsítésére egy digitális szürke zóna kialakulásának elkerülése érdekében; kéri, hogy megbízatásuk tényleges végrehajtásával összhangban erősítsék meg az ENSZ békefenntartó misszióit kibervédelmi képességekkel;

43. emlékeztet az érdemi emberi beavatkozás nélkül támadások végrehajtására képes, teljesen autonóm módon működő fegyverek fejlesztésének, gyártásának és használatának betiltását szorgalmazó álláspontjára; felhívja az alelnököt/főképviselőt, a tagállamokat és az Európai Tanácsot, hogy fogadjanak el közös álláspontot a fegyverrendszerek kritikus funkciói felett érdemi emberi ellenőrzést biztosító autonóm fegyverrendszerről; követeli nemzetközi tárgyalások megindítását a teljesen önálló módon működő fegyvereket betiltó, jogilag kötelező erejű eszközről;

44. hangsúlyozza a nemzeti parlamentekkel való együttműködés fontosságát a kibervédelem területével kapcsolatos bevált gyakorlatok cseréje érdekében;

o

o o

45. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást az Európai Tanácsnak, a Tanácsnak, a Bizottságnak, a Bizottság alelnökének/az Unió külügyi és biztonságpolitikai főképviselőjének, a védelem és kiberbiztonság területén működő uniós ügynökségeknek, a NATO főtitkárának, valamint a tagállamok kormányainak és parlamentjeinek.