41. megismétli, hogy a nők fontos szerepet játszanak a közös biztonság- és védelempolitika és a NATO misszióiban, különösen azáltal, hogy a konfliktusok által érintett térségekben foglalkoznak a nőkkel és gyermekekkel; üdvözli, hogy az EU és a NATO egyaránt elismerte ezt a fontos szerepet; javasolja az EU-nak és a NATO-nak, hogy proaktívan támogassák a nemi sokszínűséget struktúrájukban és műveleteikben;

42. hangsúlyozza, hogy az EU-nak biztosítania kell a brexit utáni szoros biztonsági és védelmi kapcsolat fenntartását az Egyesült Királysággal, elismerve, hogy az Egyesült Királyság NATO-tagként és európai országként továbbra is főszerepet játszik az európai védelemben annak ellenére, hogy már nem tagja az EU-nak;

o

o o

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

2018. június 13., szerda

P8_TA(2018)0258

Kibervédelem

Az Európai Parlament 2018. június 13-i állásfoglalása a kibervédelemről (2018/2004(INI))

(2020/C 898/07)

Az Európai Parlament,

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

— tekintettel a Federica Mogherini, a Bizottság alelnöke, az Unió külügyi és biztonságpolitikai főképviselője (alelnök/főképviselő) által 2016. június 28-án bemutatott, „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 „Vitaanyag az európai védelem jövőjéről"című, 2017. június 7-i bizottsági közleményre (COM(2017)0315),

— tekintettel „Az Európai Védelmi Alap felállítása"című, 2017. június 7-i bizottsági közleményre (COM(2017)0295),

— tekintettel az európai védelmi cselekvési tervről szóló, 2016. november 30-i bizottsági közleményre (COM(2016)0950),

— tekintettel a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének Európai Parlamenthez és a Tanácshoz intézett, „Az Európai Unió kiberbiztonsági stratégiája: nyílt, megbízható és biztonságos kibertér"című, 2013. február 7-i közös közleményére (JOIN(2013)0001),

— tekintettel „Az Európai Unió kiberbiztonsági stratégiájának értékelése"című, 2017. szeptember 13-i bizottsági szolgálati munkadokumentumra (SWD(2017)0295),

— tekintettel az EU 2014. november 18-i kiberbiztonsági politikai keretére,

— tekintettel a Tanács kiberdiplomáciáról szóló, 2015. február 10-i következtetéseire,

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

— tekintettel a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének Európai Parlamenthez és a Tanácshoz intézett, „Ellenálló képesség, elrettentés és védelem – erős kiberbiztonság kialakítása az EU-ban"című, 2017. szeptember 13-i közös közleményére (JOIN(2017)0450),

— tekintettel a kiberműveletekre alkalmazandó nemzetközi jogról szóló tallinni kézikönyv második kiadására ([1]),

— 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 ([2]),

— tekintettel a kibertér stabilitásával foglalkozó globális bizottság munkájára,

— tekintettel az európai biztonsági stratégiáról szóló, 2015. április 28-i bizottsági közleményre (COM(2015)0185),

— tekintettel a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének Európai Parlamenthez és a Tanácshoz intézett, „A hibrid fenyegetésekkel szembeni fellépés kerete – európai uniós válasz"című, 2016. április 6-i közös közleményére (JOIN(2016)0018),

— tekintettel a kiberbűnözés elleni küzdelemről szóló, 2017. október 3-i állásfoglalására ([3]),

— tekintettel az Európai Tanács és az Európai Bizottság elnökei és a NATO főtitkára 2016. július 8-i együttes nyilatkozatára, az EU és a NATO Tanácsa által 2016. december 6-án és 2017. december 5-én helybenhagyott, az együttes nyilatkozat végrehajtására vonatkozó közös javaslatokra, valamint az azok végrehajtásáról szóló, 2017. június 14-i és december 5-i helyzetjelentésekre,

— tekintettel a kiberbiztonságról és -védelemről szóló, 2012. november 22-i állásfoglalására ([4]),

— tekintettel az európai védelmi unióról szóló, 2016. november 22-i állásfoglalására ([5]),

— tekintettel az ENISA-ról, az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály") szóló európai parlamenti és tanácsi rendeletre irányuló, 2017. szeptember 13-i bizottsági javaslatra (COM(2017)0477),

— tekintettel a közös kül- és biztonságpolitika (KKBP) végrehajtásáról szóló éves jelentésről szóló, 2017. december 13-i állásfoglalására ([6]),

— tekintettel a közös biztonság- és védelempolitika végrehajtásáról (KBVP) szóló éves jelentésről szóló, 2017. december 13-i állásfoglalására ([7]),

— tekintettel eljárási szabályzatának 52. cikkére,

— tekintettel a Külügyi Bizottság jelentésére (A8-0189/2018),

A. mivel a számítástechnikai és hibrid kihívások, fenyegetések és támadások komoly veszélyt jelentenek az Unió, annak tagállamai és polgárai biztonságára, védelmére, stabilitására és versenyképességére; mivel a kibervédelembe egyértelműen beletartozik a katonai és a polgári dimenzió is;

([1]) Cambridge University Press, 2017. február, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
([2]) HL L 194., 2016.7.19., 1. o.
([3]) Elfogadott szövegek, P8_TA(2017)0366.
([4]) HL C 419., 2015.12.16., 145. o.
([5]) Elfogadott szövegek, P8_TA(2016)0435.
([6]) Elfogadott szövegek, P8_TA(2017)0493.
([7]) Elfogadott szövegek, P8_TA(2017)0492.

2018. június 13., szerda

B. mivel az Unió és tagállamai korábban soha nem tapasztalt fenyegetéssel néznek szembe a politikai indíttatású, államilag támogatott kibertámadások, valamint a kiberbűnözés és terrorizmus formájában;

C. mivel a kiberteret széles körben a katonaság ötödik műveleti területének tekintik, ami lehetővé teszi a kibervédelmi képességek fejlesztését; mivel viták folynak arról, hogy elismerjék-e a kiberteret ötödik hadszíntérként;

D. mivel az EUSZ 42. cikkének (7) bekezdésében foglalt kölcsönös védelmi záradék előírja, hogy az uniós tagállamok valamelyikének a területe elleni fegyveres támadás esetén a többi uniós ország köteles minden rendelkezésére álló segítséget és támogatást megadni ennek az országnak; mivel ez nem érinti az egyes tagállamok biztonság- és védelempolitikájának egyedi jellegét; mivel a kölcsönös védelmi záradékot az EUMSZ 222. cikkében foglalt szolidaritási klauzula egészíti ki, amely előírja, hogy az uniós országok kötelesek együttesen fellépni, ha valamely uniós országot terrortámadás ér, illetve természeti vagy ember okozta katasztrófa áldozatává válik; mivel a szolidaritási klauzula polgári és katonai struktúrák alkalmazását is magában foglalja;

E. mivel ugyan a kibervédelem továbbra is a tagállamok alapvető hatásköre, az Unió kulcsfontosságú szerepet játszik abban, hogy platformot szolgáltasson az európai együttműködéshez, valamint annak biztosításában, hogy a számos hagyományos védelmi erőfeszítésre oly jellemző hatékonyságbeli hiányosságok elkerülése érdekében ezek az új törekvések a kezdetektől fogva nemzetközi szinten és a transzatlanti biztonsági struktúra keretén belül szorosan össze legyenek hangolva; mivel többet kell tennünk együttműködésünk és koordináltságunk fokozásánál; mivel az Unió felderítési, védelmi és elhárítási képességének növelése révén hatékony megelőzést kell biztosítanunk; mivel az Unió hatékony kiberbiztonságának megvalósításához hiteles kibervédelemre és kibertámadás-elhárításra van szükség, biztosítva egyben azt is, hogy a legkevésbé felkészült államok nehogy kibertámadások könnyű célpontjaivá váljanak, és mivel a komoly kibervédelem a KBVP és az európai védelmi unió kialakulásának szükséges részét képezi; mivel a kibervédelem terén tartós a magasan képzett szakemberek hiánya; mivel a fegyveres erők kibertámadásokkal szembeni védelmével kapcsolatos szoros koordináció a hatékony KBVP kialakulásának szükséges részét képezi;

F. mivel az uniós tagállamokat gyakran érik állami és nem állami szereplők által végrehajtott, polgári vagy katonai célpontok ellen indított kibertámadások; mivel a jelenlegi kiszolgáltatottság oka elsősorban az európai védelmi stratégiák és kapacitások széttagoltsága, ami lehetővé teszi a külföldi hírszerző ügynökségek számára, hogy több ízben kihasználják az európai biztonság szempontjából elengedhetetlen informatikai rendszerek és hálózatok biztonsági sebezhetőségeit; mivel gyakran előfordul, hogy a tagállami kormányok nem tájékoztatják kellő időben az érintetteket, pedig az ilyen tájékoztatás lehetővé tenné a számukra, hogy kezeljék termékeik és szolgáltatásaik sebezhetőségeit; mivel az ilyen támadások szükségessé teszik az európai támadó és védelmi kapacitások sürgős, polgári és katonai szintű megerősítését és védelmét, megelőzendő, hogy a kiberbiztonsági eseményeknek határokon átnyúló gazdasági és társadalmi hatásai legyenek;

G. mivel a kibertérben elmosódnak a polgári és katonai beavatkozás közötti vonalak;

H. mivel számos kiberbiztonsági eseményt a magán- és állami infrastruktúra ellenállóképességének és szilárdságának hiánya, az adatbázisok elégtelen védelme vagy biztonsága, illetve a kritikus fontosságú információs infrastruktúra más hiányosságai tesznek lehetővé; mivel csupán néhány tagállam vállal felelősséget hálózatainak és információs rendszereinek, valamint az ezekkel kapcsolatos adatainak védelméért, saját gondossági kötelezettsége részeként, ami megmagyarázza a képzésbe és a biztonsági csúcstechnológiába való beruházás, valamint a megfelelő iránymutatások kidolgozásának általános hiányát;

I. mivel az Európai Unió Alapjogi Chartája és az EUMSZ 16. cikke rögzíti a magánélet tiszteletben tartásához és az adatok védelméhez való jogokat, amelyeket a 2018. május 25-én hatályba lépett általános adatvédelmi rendelet szabályoz;

J. mivel a hatékony és eredményes kiberpolitika olyan, amely képes az ellenség elrettentésére, képességeik megzavarására, valamint támadásra való képességük megakadályozására és csökkentésére;

K. mivel számos terrorista csoport és szervezet toborzásra, radikalizálásra és a terrorista propaganda terjesztésére szolgáló olcsó eszközként használja a kiberteret; mivel terrorista csoportok, nem állami szereplők és nemzetközi bűnszövetkezetek arra használják a kiberműveleteket, hogy a névtelenség leple alatt szerezzenek pénzforrásokat, hírszerzési információkat gyűjtsenek és kiberterror-kampányok indításához kiberfegyvereket fejlesszenek ki, kritikus infrastruktúrákat romboljanak szét, tegyenek tönkre vagy semmisítsenek meg, pénzügyi rendszereket támadjanak meg és egyéb illegális tevékenységeket folytassanak, amelyek kihatással járnak az európai polgárok biztonságára nézve;

L. mivel az európai fegyveres erők és kritikus infrastruktúrák elleni kibertámadások elhárítása és az ezekkel kapcsolatos kibervédelem a védelem korszerűsítéséről, Európa közös védelmi erőfeszítéseiről, a fegyveres erők jövőbeli fejlesztéséről és műveleteiről, valamint az Unió stratégiai autonómiájáról szóló viták egyik rendkívül fontos kérdése lett;

M. mivel az ezen új kihívásoknak való megfelelés és kiberreziliencájuk javítása érdekében számos tagállam jelentős beruházásokat tett az elegendő személyzettel ellátott „kiberparancsnokságok"létrehozása terén, de ennél sokkal több még a tennivaló, mivel egyre nehezebb tagállami szinten felvenni a küzdelmet a kibertámadások ellen; mivel a tagállamok „kiberparancsnokságai"offenzív vagy defenzív megbízatásuk tekintetében különböznek; mivel az egyéb kibervédelmi struktúrák tagállamonként nagymértékben eltérőek, és gyakran továbbra is széttagoltak; mivel a kibervédelem és a kibertámadás-elhárítás olyan tevékenységek, amelyeket leginkább európai szintű együttműködéssel, valamint a partnereinkkel és szövetségeseinkkel együttműködve lehet végezni, mivel működési területe nem ismer sem nemzeti, sem szervezeti határokat; mivel a katonai és polgári kiberbiztonság szorosan összefügg, és ezért több szinergiára van szükség a polgári és katonai szektorban tevékenykedő szakemberek között; mivel a magánvállalkozások jelentős szakértelemmel rendelkeznek ezen a területen, ami alapvető irányítási és biztonsági, valamint azzal kapcsolatos kérdéseket vet fel, hogy az államok képesek-e megvédeni állampolgáraikat;

N. mivel a változó kiberbiztonsági fenyegetésekre való kellően gyors válaszadás hiánya miatt sürgős szükség van az uniós kibervédelmi képesség fejlesztésére; mivel a biztonság e téren való fenntartása érdekében kulcsonfontosságú a válaszadás gyorsasága és a készenlét megfelelő szintje;

O. mivel mind az állandó strukturált együttműködés (PESCO), mind az Európai Védelmi Alap (EDA) olyan új kezdeményezés, amely a kkv-k és az induló vállalkozások számára lehetőségeket biztosító környezet létrehozásának támogatásához és a kibervédelem terén folyó kooperációs projektek előmozdításához szükséges hatáskörrel rendelkezik, és mindkettő hozzá fog járulni a szabályozási és intézményi keret kialakításához;

P. mivel a PESCO-ban részt vevő tagállamok elkötelezték magukat annak biztosítása mellett, hogy a kibervédelmi együttműködésre irányuló erőfeszítések – például az információcsere, a képzés és az operatív támogatás terén – tovább növekedjenek;

Q. mivel az állandó strukturált együttműködéshez kiválasztott 17 projektből 2 kapcsolódik a kibervédelem területéhez;

R. mivel az Európai Védelmi Alapnak támogatnia kell az európai védelmi ipar globális versenyképességét és innovativitását azáltal, hogy beruházásokat hajt végre a digitális és kibertechnológiákba, valamint elő kell segítenie az okos megoldások kidolgozását azáltal, hogy részvételi lehetőségeket biztosít a kkv-k és induló vállalkozások számára ebben az erőfeszítésben;

S. mivel az Európai Védelmi Ügynökség (EDA) számos projektet indított a tagállamok kibervédelmi kapacitásaik fejlesztésére irányuló igényeinek kielégítése érdekében, beleértve az oktatási és képzési projekteket, például a kibervédelemre vonatkozó képzést és gyakorlatot koordináló fórumot (CD TEXP), a magánszektor kibervédelmi képzésekkel és gyakorlattal kapcsolatos támogatás iránti igényeinek összevonását (DePoCyTE) és a Cyber Ranges projektet;

T. mivel más uniós projektek is folyamatban vannak a helyzetismeret, a rosszindulatú számítógépes programok észlelése és az információmegosztás terén (a rosszindulatú számítógépes programokkal kapcsolatos információmegosztásra szolgáló platform (MISP), a tartós fenyegetések fejlett észlelésére szolgáló többágenses rendszerek (MASFAD));

U. mivel a kibervédelem területén jelentős és egyre növekvő kapacitásépítési és képzési igények jelentkeznek, amelyeket uniós és NATO-szintű együttműködéssel lehet a leghatékonyabban kielégíteni;

V. mivel az összes modern szervezet műveleteihez hasonlóan a KBVP-missziók és -műveletek is erősen függnek az informatikai rendszerek működésétől; mivel a KBVP-missziókat és -műveleteket érintő kiberfenyegetések különböző rétegekben jelenhetnek meg, a taktikai rétegtől kezdve (KBVP-missziók és -műveletek) a műveleti rétegen át (uniós hálózatok) egészen a globális informatikai infrastruktúra átfogóbb rétegéig;

W. mivel az ellenőrző-irányító rendszerek, az információcsere és a logisztika minősített és nem minősített informatikai infrastruktúrára támaszkodik, különösen taktikai és operatív szinten; mivel ezek a rendszerek vonzó célpontokat jelentenek a missziók megtámadását tervező rosszhiszemű szereplők számára; mivel a kibertámadások súlyos következményekkel járhatnak az Unión belüli infrastruktúrára nézve; mivel különösen az uniós energiainfrastruktúrát célzó kibertámadásoknak súlyos következményei lennének, és ezért ezek ellen védekezni kell;

X. mivel egyértelmű, hogy a kibervédelemet a KBVP-missziók és -műveletek tervezési folyamatának minden szakaszában kellőképpen figyelembe kell venni, valamint állandó ellenőrzést igényel, és hogy a missziótervekbe való maradéktalan beépítése és a szükséges kritikus támogatás folyamatos nyújtása érdekében megfelelő kapacitásokat kell ehhez rendelkezésre bocsátani;

Y. mivel az Európai Biztonsági és Védelmi Főiskola (EBVF) hálózata az egyetlen európai képzésszolgáltató a KBVP-struktúrák, missziók és műveletek számára; mivel az európai kibervédelmi képzési kapacitások összevonásában játszott szerepe a jelenlegi tervek szerint jelentősen növekedni fog;

Z. mivel a 2016. évi varsói NATO-csúcstalálkozón kiadott nyilatkozat műveleti területnek ismeri el a kiberteret, amelyben a NATO-nak ugyanolyan hatékonyan kell megvédenie magát, mint a légtérben, a szárazföldön és a tengeren;

AA. mivel az EDA és a NATO által koordinált kettős felhasználású kutatási projektek révén az EU és a NATO hozzájárult a tagállamok kibervédelmi kapacitásainak javításához, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) által nyújtott támogatás révén pedig a tagállamok kiberrezilienciájának fejlesztéséhez;

AB. mivel a NATO 2014-ben a kiberbiztonsági műveleteket a kollektív védelem részeként határozta meg, és 2016-ban a föld, levegő és tenger mellett a virtuális teret is műveleti területként azonosította; mivel az EU és a NATO egymást kiegészítő partnerek kiberrezilienciájuk és kivervédelmi kapacitásuk kiépítésében; mivel a kiberbiztonság és -védelem már most a két szervezet közötti együttműködés egyik legerősebb pillére, és olyan kritikus terület, ahol mindkét szervezetnek egyedülálló kapacitásai vannak; mivel a 2016. július 8-i együttes EU–NATO-nyilatkozatban az EU és a NATO megállapodtak az együttműködés széles körű ütemtervében; mivel a szorosabb együttműködésre vonatkozó 42 javaslatból négy a kiberbiztonságot és -védelmet érinti, amelyek általánosságban a hibrid fenyegetésekre vonatkozó további javaslatokat tartalmaznak; mivel ezt a kiberbiztonsággal és -védelemmel kapcsolatos újabb, 2017. december 5-én előterjesztett javaslat egészítette ki;

AC. mivel az ENSZ információbiztonsággal foglalkozó kormányzati szakértői csoportja (UN GGE) befejezte a tanácskozás utolsó körét; mivel – még ha 2017-ben nem is volt képes konszenzusos jelentést felmutatni – a 2015-ös és a 2013-as jelentések érvényben vannak, többek között annak elismerése is, hogy a béke és a stabilitás fenntartásához, valamint egy nyílt, biztonságos, békés és hozzáférhető ikt-környezet előmozdításához elengedhetetlen a már meglévő nemzetközi jog, különösen az Egyesült Nemzetek Alapokmánya alkalmazása;

AD. mivel a rosszhiszemű kibertevékenységekre vonatkozó közös uniós diplomáciai reagálás közelmúltban kialakított kerete, az EU kiberdiplomáciai eszköztára – amelynek célja az EU és a tagállamok kapacitásainak fejlesztése a potenciális agresszorok magatartásának befolyásolása érdekében – arányos intézkedések, köztük korlátozó intézkedések alkalmazását irányozza elő a KKBP-n belül;

AE. mivel különböző állami szereplők – többek között Oroszország, Kína és Észak-Korea, valamint bizonyos államok, biztonsági ügynökségek vagy magánvállalatok által inspirált, felbérelt vagy szponzorált nem állami szereplők (például bűnszervezetek) – politikai, gazdasági vagy biztonsági célok elérése érdekében rosszhiszemű kibertevékenységeket folytattak, például létfontosságú infrastruktúrákra irányuló támadások, kiberkémkedés, az uniós polgárok tömeges megfigyelése, félretájékoztatási kampányok és az internetes hozzáférést és az informatikai rendszerek működését korlátozó rosszindulatú szoftverek (Wannacry, NotPetya stb.) terjesztése formájában; mivel az ilyen tevékenységek figyelmen kívül hagyják és sértik a nemzetközi jogot, az emberi jogokat és az alapvető uniós jogokat, és mindeközben veszélyeztetik a demokráciát, a biztonságot, a közrendet és az Unió stratégiai autonómiáját, és ezért az Uniónak közös választ kellene adnia ezekre, például a közös uniós diplomáciai intézkedések keretét alkalmazva, többek között az EU kiberdiplomáciai eszköztára számára előírt korlátozó intézkedések révén, például – magánvállalkozások esetében – bírságok és a belső piachoz való korlátozott hozzáférés használatával;

AF. mivel korábban számos alkalommal hajtottak végre ilyen nagyszabású támadásokataz ikt-infrastruktúrák ellen, többek között 2007-ben Észtországban, 2008-ban Grúziában, jelenleg pedig szinte naponta alkalmaznak ilyen támadásokat Ukrajna ellen; mivel jelenleg az EU és a NATO tagállamai ellen is példátlan mértékben vetnek be offenzív kiberképességeket;

AG. mivel a polgári és katonai célokra is felhasználható kiberbiztonsági technológiák olyan „kettős felhasználású"technológiák, amelyek számtalan lehetőséget kínálnak arra, hogy a polgári és katonai szereplők között szinergiák alakuljanak ki számos területen, például a titkosítás, a biztonsági és a sebezhetőség kezelésére szolgáló eszközök, valamint a behatolásérzékelő és -elhárító rendszerek terén;

AH. mivel a következő években a kibertechnológiák fejlesztése olyan új területeket fog érinteni, mint a mesterséges intelligencia, a dolgok internete, robotika és mobileszközök, és mindezen tényezőknek a védelem szempontjából is számos biztonsági vonatkozása lehet;

AI. mivel a több tagállam által létrehozott „kiberparancsnokságok"jelentősen hozzájárulhatnak a létfontosságú polgári infrastruktúrák védelméhez, és mivel gyakori, hogy a kibervédelemmel kapcsolatos ismeretek a polgári területen egyaránt hasznosak;

A kibervédelmi és kibertámadás-elhárítási képességek fejlesztése

1. hangsúlyozza, hogy az európai védelmi unió kialakulásában központi szerepet kell játszania a közös kibervédelmi politikának és a komoly kibervédelmi kapacitásnak;

2. üdvözli a Bizottság kiberbiztonsági csomagra vonatkozó kezdeményezését, melynek célja, hogy előmozdítsa az Unió kibertámadásokkal szembeni ellenálló képességét, továbbá az elrettentést és a védelmet;

3. emlékeztet arra, hogy a kibervédelemnek katonai és polgári vonatkozásai is vannak, és hogy emiatt integrált szakpolitikai megközelítésre, valamint a katonai és polgári érdekelt felek közötti szoros együttműködésre van szükség;

4. felhív a kibervédelmi kapacitások összes uniós intézménynél és szervnél, valamint tagállamban történő koherens fejlesztésére, továbbá a kibervédelem terén való együttműködést még mindig gátló politikai, jogi és szervezeti akadályok felszámolásához szükséges politikai és gyakorlati megoldások biztosítására; rendkívül fontosnak tartja a közszférabeli érdekelt felek közötti, kibervédelemmel kapcsolatos uniós és nemzeti szintű, rendszeres és megerősített információcserét és együttműködést;

5. nyomatékosítja, hogy a kialakulóban lévő európai védelmi unió keretében a tagállamok kibervédelmi képességeit előtérbe kell helyezni, és a kezdetektől fogva a lehető legnagyobb mértékben integrálni kell a maximális hatékonyság biztosítása érdekében; sürgeti ezért a tagállamokat, hogy világos ütemtervet használva, szorosan működjenek együtt a saját kibervédelmük kialakítása során, ezáltal hozzájárulva a Bizottság, az Európai Külügyi Szolgálat (EKSZ) és az EDA által koordinált, arra irányuló folyamathoz, hogy a tagállamokban hatékonyabbá váljanak a kibervédelmi struktúrák, sürgősen végrehajtva a rövid távú intézkedéseket és előmozdítva a szakértelem megosztását; úgy véli, hogy ki kell fejlesztenünk a kritikus információk és infrastruktúrák biztonságos európai hálózatát; elismeri, hogy a támadások eredetének meghatározására irányuló erős képességek a hatékony kibervédelem és kibertámadás-elhárítás nélkülözhetetlen alkotóelemei, valamint hogy a hatékony megelőzéshez további alapvető technológiai szakértelem kifejlesztésére lenne szükség; sürgeti a tagállamokat, hogy növeljék pénzügyi és emberi erőforrásaikat, különös tekintettel a kiberkriminalisztikai szakértőkre, hogy hatékonyabban meg tudják állapítani a kibertámadások elkövetőinek kilétét; hangsúlyozza, hogy az együttműködés megvalósításához az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA) is meg kell erősíteni;

6. elismeri, hogy számos tagállam úgy ítéli meg, hogy a saját kibervédelmi képességgel való rendelkezés nemzeti biztonsági stratégiájuk középpontjában áll, és nemzeti szuverenitásuk lényeges részét képezi; hangsúlyozza azonban, hogy a kibertér határok nélküli jellege miatt az EU kibertérbeli stratégiai autonómiáját biztosító, valóban átfogó és hatékony erőkhöz olyan dimenzióra és tudásra van szükség, amely túlmutat az egyes tagállamok lehetőségein, és ehhez uniós szinten valamennyi tagállam részéről intenzívebb és összehangolt reagálásra van szükség; mindezekre figyelemmel megjegyzi, hogy az Uniót és tagállamait szorítja az idő az említett erők kifejlesztése tekintetében, és haladéktalanul cselekedniük kell; megjegyzi, hogy az uniós kezdeményezéseknek, például a digitális egységes piacnak köszönhetően az EU jó helyzetben van ahhoz, hogy vezető szerepet vállaljon az európai kibervédelmi stratégiák kidolgozásában; emlékeztet arra, hogy az uniós szintű kibervédelem kialakításának hozzá kell járulnia az Unió azon képességéhez, hogy megvédje magát; üdvözli ezzel kapcsolatban az ENISA állandó megbízással való felruházására és megerősített szerepére vonatkozó javaslatot;

7. ebben az összefüggésben sürgeti a tagállamokat, hogy a lehető legjobban használják ki PESCO és az Európai Védelmi Alap nyújtotta keretet az együttműködési projektek előterjesztéséhez;

8. tudomásul veszi az EU és tagállamai által a kibervédelem területén végzett kemény munkát; tudomásul veszi konkrétabban a virtuális gyakorlótérre (Cyber Ranges) irányuló EDA-projekteket, a kibervédelmi stratégia kutatási menetrendjét és a telepíthető kiberhelyzet-felismerő csomagok kialakítását a parancsnokságokban;

9. üdvözli a PESCO keretében indítandó két kiberprojektet, nevezetesen a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platformot, valamint a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportokat és a kiberbiztonság területén megvalósuló kölcsönös segítségnyújtást; hangsúlyozza, hogy ez a két projekt egy olyan defenzív kiberpolitikára összpontosít, amely a kiberfenyegetéssel kapcsolatos információknak a hálózatba kapcsolt tagállamok platformja segítségével történő megosztásán, valamint a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok felállításán alapul, lehetővé téve a tagállamok számára, hogy segítsenek egymásnak a nagyobb mértékű kiberreziliencia biztosításában, valamint a kiberfenyegetések közös észlelésében, felismerésében és csökkentésében; felhívja a Bizottságot és a tagállamokat, hogy a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású nemzeti csoportokkal, valamint a kiberbiztonság területén megvalósuló kölcsönös segítségnyújtással kapcsolatos PESCO-projektek alapján hozzanak létre kiberbiztonsági eseményekkel foglalkozó gyorsreagálású európai csoportot, hogy a részt vevő tagállamok erőfeszítéseit támogatva hangolja össze az erőfeszítéseket, derítse fel a kollektív kiberfenyegetéseket és tegyen ellenintézkedéseket;

10. megjegyzi, hogy a kibervédelmi projektek kialakítására irányuló európai kapacitás a technológiák, berendezdések, szolgáltatások és adatok, valamint azok kezelésének ismeretén alapul, és megbízható ipari szereplők csoportjára kell alapozni;

11. emlékeztet arra, hogy az irányítási rendszerek homogenitásának javítására irányuló erőfeszítések egyik célja annak biztosítása, hogy a rendelkezésre álló irányítási eszközök interoperábilisak legyenek a nem uniós NATO-tagállamokéival és az alkalmi partnerekéivel, valamint a döntéshozatal felgyorsítása és az információk irányításának kiberkockázat esetén történő megőrzése céljából az információcsere zökkenőmentességének garantálása;

12. javasolja, hogy találjanak módot a NATO intelligens védelmi projektjeinek kiegészítésére (például: multinacionális kibervédelmi kapacitásfejlesztés, a rosszindulatú számítógépes programokkal kapcsolatos információmegosztásra szolgáló platform (MISP) és multinacionális kibervédelmi oktatás és képzés (MNCDE&T));

13. elismeri az olyan területeken tapasztalható fejlődést, mint a nanotechnológia, a mesterséges intelligencia, a nagy adathalmazok, az elektromos és elektronikus berendezések hulladékai és a fejlett robotika; sürgeti a tagállamokat és az Uniót, hogy fordítsanak különös figyelmet arra, hogy e területek előnyeit ellenséges állami szereplők és bűnszervezetek is kihasználhatják; szorgalmazza a képzések és a kapacitások fejlesztését az olyan szofisztikált bűncselekmények elleni védelem érdekében, mint a személyazonossággal való komplex visszaélés és az áruhamisítás;

14. hangsúlyozza, hogy a kibertérbeli biztonsággal kapcsolatban nagyobb terminológiai egyértelműségre van szükség, valamint átfogó és integrált megközelítésre és közös erőfeszítésekre a kiber- és hibrid fenyegetések elleni küzdelemhez, a szélsőségesek és bűnözők online menedékének felderítéséhez és felszámolásához, az EU és az uniós ügynökségek, úgymint Europol, Eurojust, EDA és ENISA közötti információmegosztás erősítése és fokozása révén;

15. hangsúlyozza, hogy a mesterséges intelligencia a kibertámadások és a kibervédelem terén is egyre nagyobb a szerephez jut; sürgeti az Uniót és a tagállamokat, hogy a kibervédelmi képességeikkel kapcsolatos kutatás és gyakorlati fejlesztés során is fordítsanak különös figyelmet erre a területre;

16. nyomatékosítja, hogy a pilóta nélküli – fegyveres vagy nem fegyveres – légi járművek alkalmazása miatt külön intézkedéseket kell tenni potenciális kibersebezhetőségeik csökkentése érdekében;

A KBVP-missziók és -műveletek kibervédelme

17. hangsúlyozza, hogy a kibervédelmet a KBVP-missziók és -műveletek operatív feladatának kell tekinteni, és azt fel kell venni a KBVP-vel kapcsolatos valamennyi tervezési folyamatba, biztosítva, hogy a tervezési folyamat során végig figyelembe veszik a kiberbiztonságot, ezáltal csökkentve kibersebezhetőségekkel kapcsolatos hiányosságokat;

18. elismeri, hogy egy sikeres KBVP-misszió vagy -művelet megtervezéséhez mind az operatív központban, mind pedig a misszió területén jelentős kibervédelmi szakértelemre, valamint biztonságos informatikai infrastruktúrára és hálózatokra van szükség, hogy alapos fenyegetésértékelést lehessen végezni és megfelelő védelmet lehessen nyújtani ezen a területen; felszólítja az EKSZ-t és a KBVP-műveletek parancsnokságát ellátó tagállamokat, hogy erősítsék meg az uniós missziónak és műveleteknek biztosítandó kibervédelmi szakértelmet; megjegyzi, hogy van egy határ arra vonatkozóan, hogy a KBVP-missziók mennyire jól készíthetők fel a kibertámadások elleni védelemre;

19. hangsúlyozza, hogy minden KBVP-misszió és -művelet tervezésének a kiberfenyegetések alapos értékelésével kell együtt járnia; megjegyzi, hogy az ENISA által a fenyegetésekkel kapcsolatban összeállított osztályozás megfelelő mintát nyújt ehhez az értékeléshez; javasolja, hogy hogy a KBVP-parancsnokságok számára hozzanak létre a kiberreziliencia értékelésére szolgáló kapacitást;

20. elismeri különösen annak a jelentőségét, hogy a szükséges minimumon tartsák a KBVP-missziók és műveletek digitális lábnyomát és támadási felületét; sürgeti a tervezésben érintetteket, hogy a tervezési folyamat kezdetétől fogva vegyék ezt figyelembe;

21. elismeri az EDA képzési igényekre vonatkozó elemzését, amely feltárta, hogy a döntéshozók körében – nem csupán a tagállamokban – komoly hiányosságok vannak a kibervédelmi készségek és kompetenciák tekintetében, és üdvözli az EDA arra irányuló kezdeményezéseit, hogy a KBVP-missziók és -műveletek tervezésének támogatása érdekében tanfolyamokat tartsanak a tagállamokban a vezető beosztású döntéshozók számára;

Kibervédelmi oktatás és képzés

22. megjegyzi, hogy egy modern uniós kibervédelmi oktatási és képzési rendszer jelentősen csökkentené a fenyegetéseket, és felhívja az Uniót és a tagállamokat, hogy fokozzák együttműködésüket az oktatás, képzés és a gyakorlatok terén;

23. határozottan támogatja a katonai Erasmus programot és a többi, közös képzésre és cserére irányuló kezdeményezést, melyek célja a pályakezdő katonai személyzet fokozottabb cseréje révén a tagállamok fegyveres erői közötti interoperabilitás erősítése és egy közös stratégiai kultúra kialakítása, szem előtt tartva, hogy az összes tagállam és NATO-szövetséges között szükség van erre az interoperabilitásra; úgy véli azonban, hogy a kibervédelem terén a képzési és oktatási célú cseréknek túl kell mutatniuk e kezdeményezésen, és ki kell terjedniük a katonai állomány bármilyen korú és rangú tagjaira és az összes olyan felsőoktatási intézmény diákjaira, amelyek kiberbiztonsági oktatási programokkal rendelkeznek;

24. hangsúlyozza, hogy több szakértőre van szükség a kibervédelem területén; felhívja a tagállamokat, hogy segítsék elő a katonai és nem katonai felsőoktatási intézmények közötti együttműködést a szakértőhiány kezelése érdekében, több lehetőséget teremtve a kibervédelmi oktatás és képzés terén, és fordítsanak több erőforrást a kiberműveletekkel, és többek között a mesterséges intelligenciával kapcsolatos speciális képzésre; felszólítja a katonai akadémiákat, hogy tanterveikbe építsék be a kibervédelmi oktatást, hogy növelni lehessen a KBVP-missziók igényeihez rendelkezésre álló kibertehetség-állományt;

25. felhívja az összes tagállamot, hogy megfelelően és proaktívan tájékoztassák a vállalkozásokat, iskolákat és polgárokat a kiberbiztonságról és a legfontosabb digitális fenyegetésekről, felhívják a figyelmet azokra és tanácsot adjanak; üdvözli ezzel kapcsolatban a kiberbiztonsági útmutatókat, melyek célja, hogy a polgárok és szervezetek hatékonyabb kiberbiztonsági stratégiát kövessenek, növeljék a kiberbiztonsággal kapcsolatos ismereteket és általánosságban javítsák a kiberrezilienciát;

26. megjegyzi, hogy mivel a személyi állományon belül több olyan tagra van szükség, aki speciális képesítéssel rendelkezik, a tagállamoknak nemcsak az alkalmas katonai állomány toborzására, hanem a szükséges szakemberek megtartására is hangsúlyt kell helyezniük;

27. üdvözli, hogy a „Cyber Ranges"elnevezésű virtuális gyakorlótereket összefogó szövetség 11 tagállama (Ausztria, Belgium, Németország, Észtország, Görögország, Finnország, Írország, Lettország, Hollandia, Portugália és Svédország) végrehajtja az EDA összevonásra és megosztásra irányuló menetrendje keretében elindított négy kibervédelmi projekt közül az elsőt; kéri a többi tagállamot, hogy csatlakozzanak ehhez a kezdeményezéshez; felszólítja a tagállamokat, hogy mozdítsák elő a virtuális kibervédelmi képzés és a virtuális gyakorlóterek nagyobb mértékű és kölcsönös elérhetőségét; megjegyzi ezzel kapcsolatban, hogy az ENISA szerepét és szakértelmét is figyelembe kell venni;

28. úgy véli, hogy az ilyen kezdeményezések hozzájárulnak a kibervédelmi oktatás színvonalának uniós szintű javításához, különösen széles körű technikai platformok létrehozásával és az uniós szakértők közösségének kialakításával; úgy véli, hogy növelheti az európai fegyveres erők vonzerejét, ha átfogó kibervédelmi képzést nyújtanak, hogy elérjék és megtartsák a kibertehetségeket; hangsúlyozza annak szükségességét, hogy rámutassanak a számítógépes rendszerek, a tagállamok és az uniós intézmények gyenge pontjaira; elismeri, hogy az emberi hiba egyike a kiberbiztonsági rendszerek leggyakrabban azonosított gyengeségeinek, ezért felszólít a katonai személyzet és az uniós intézményekben dolgozó polgári személyzet rendszeres képzésére;

29. felszólítja az EDA-t, hogy indítsa el a kibervédelemre vonatkozó oktatást, képzést és gyakorlatot koordináló fórumot (CD TEXP) a „Cyber Ranges"szövetség lehető leghamarabbi támogatása érdekében, hangsúlyt helyezve az összehangolt követelményekkel kapcsolatos együttműködés erősítésére, a kibervédelmi kutatás és technológiai innovációk előmozdítására, valamint a harmadik országoknak a kapacitásépítéssel kapcsolatban nyújtandó segítségre, hogy a kibervédelem terén ellenálló képességet tudjanak kiépíteni; felhívja a Bizottságot és a tagállamokat, hogy ezeket a kezdeményezéseket egészítsék ki a kibervédelmi képzés európai kiválósági központjának létrehozásával, hogy a legígéretesebb újoncok szakértői képzésben részesüljenek a részt vevő tagállamok kiberképzésének támogatása érdekében;

30. üdvözli, hogy az EBVF égisze alatt létrejön a kibervédelmi oktatással, képzéssel és gyakorlattal, valamint értékeléssel foglalkozó fórum (ETEE) a tagállami képzési és oktatási lehetőségek növelése céljából;

31. fokozottabb eszmecserére ösztönöz a helyzetismeret terén szimulációs kibergyakorlatok és az egyes kapacitásfejlesztési erőfeszítések összehangolása révén, a nagyobb mértékű interoperabilitás kialakítása, valamint a jövőbeni támadásokra vonatkozó hatékonyabb megelőzés és reagálás megvalósítása érdekében; szorgalmazza az ilyen projektek NATO-szövetségesekkel, az uniós tagállamok fegyveres erőivel és a kibertámadások visszaverésében nagy tapasztalattal rendelkező egyéb partnerekkel történő végrehajtását, a műveleti készültség fejlesztése, valamint a közös eljárások és előírások kialakítása érdekében, hogy átfogóan lehessen kezelni a különböző kiberfenyegetéseket; ebben a tekintetben üdvözli, hogy az EU részt vesz kibergyakorlatokban, például az úgynevezett kibertámadási és -védelmi gyakorlatban (CODE);

32. emlékeztet arra, hogy a reziliens kibertér kifogástalan kiberhigiéniát igényel; felhívja a köz- és magánszférabeli érdekelt feleket, hogy tartsanak rendszeres kiberhigiéniai képzéseket a személyzet minden tagja számára;

33. javasolja a szakértelem és a tapasztalatok cseréjének fokozását a fegyveres erők, a rendőrség, valamint a tagállamok kiberfenyegetések elleni küzdelemben aktívan részt vevő egyéb állami szervei között;

Kibervédelmi együttműködés az EU és a NATO között

34. ismételten hangsúlyozza, hogy az EU és a NATO közös értékeik és stratégiai érdekeik alapján különös felelősséggel és képességgel rendelkeznek arra, hogy a növekvő kiberbiztonsági és kibervédelmi kihívásokat hatékonyabban, az esetleges egymást kiegészítő elemeket megkeresve, szoros együttműködésben kezeljék, kerülve a párhuzamos erőfeszítéseket és tiszteletben tartva egymás felelősségi köreit;

35. felhívja a Tanácsot, hogy más uniós intézményekkel és struktúrákkal együttműködve vizsgálja meg annak lehetőségeit, hogy minél korábban uniós szintű támogatást nyújtsanak ahhoz, hogy a kiberterület összehangolt módon és a NATO-val való együttműködésben beépüljön a tagállamok katonai doktrínáiba;

36. felszólít a már elfogadott intézkedések konkrét megvalósítására; felszólít az EU és a NATO közötti együttműködés továbbfejlesztését célzó új kezdeményezések azonosítására, figyelembe véve a NATO együttműködésen alapuló kibervédelmi kiválósági központjával (CCD COE) és a NATO kommunikációs és információs akadémiájával (NCI) való együttműködés lehetőségeit, melyek célja, hogy növeljék az informatikai és kiberbiztonsági rendszerekkel – szoftverekkel és hardverekkel – kapcsolatos képzési kapacitásokat; megjegyzi, hogy ebbe beletartozhat a NATO-val arról a lehetőségről folytatott párbeszéd, hogy az Unió a kiegészítő jelleg és az együttműködés fokozása érdekében csatlakozzon a CCD COE központhoz; üdvözli a hibrid fenyegetések elleni küzdelem európai kiválósági központjának közelmúltbeli felállítását; sürgeti az összes érintett intézményt és szövetségest, hogy tartsanak rendszeresen vitassák meg tevékenységeiket annak érdekében, hogy elkerüljék az átfedéseket és segítsék elő a kibervédelem összehangolt megközelítését; úgy véli, hogy döntő fontosságú a kiberfenyegetéssel kapcsolatos információk tagállamok közötti és a NATO-val való cseréjének a kölcsönös bizalom alapján történő ösztönzése;

37. meg van győződve arról, hogy az EU és a NATO közötti fokozott együttműködés fontos és hasznos a kibervédelem területén a kibertámadásokkal kapcsolatos megelőzéshez, védelemhez és elhárításhoz; ezért felszólítja mindkét szervezetet operatív együttműködésük és koordinációjuk növelésére, valamint közös kapacitásépítési erőfeszítéseik bővítésére, különösen a polgári és katonai kibervédelmi személyzetnek szervezett közös képzések és gyakorlatok formájában, valamint a tagállamoknak a NATO intelligens védelmi projektjeiben való részvétele révén; létfontosságúnak tartja, hogy az EU és a NATO fokozza az információk megosztását annak érdekében, hogy hivatalosan meg lehessen állapítani a kibertámadások elkövetőit, majd korlátozó szankciókat lehessen kivetni a felelősökre; sürgeti a két szervezetet, hogy a válságkezelés kiberbiztonsági vonatkozásai terén is szorosabban működjenek együtt;

38. üdvözli az azzal kapcsolatos elképzelések megosztását, hogy a kibervédelmi követelményeket és előírásokat be kell építeni a missziók és műveletek tervezésébe és végrehajtásába az interoperabilitás előmozdítása érdekében, és reményét fejezi ki azzal kapcsolatban, hogy ezt nagyobb műveleti együttműködés fogja követni az adott missziók kibervédelmének biztosítása és az operatív megközelítések összehangolása terén;

39. üdvözli az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (CERT-EU) és a NATO számítógép-incidenskezelő képessége (NCIRC) közötti megállapodást, amelynek célja az információcsere, a logisztikai támogatás, a közös fenyegetésértékelések, a személyzettoborzás és a bevált gyakorlatok megosztása a fenyegetésekre valós időben történő reagálás érdekében; hangsúlyozza, hogy fontos ösztönözni a CERT-EU és az NCIRC közötti információcserét, illetve törekedni kell a bizalom szintjének növelésére; úgy véli, feltételezhető, hogy a CERT-EU birtokában lévő információk hasznosak lehetnek a kiberbiztonsági kutatás és a NATO számára, és hogy ezért ezeket az információkat meg kell osztani, az uniós adatvédelmi jogszabályok maradéktalan betartása mellett;

40. üdvözli a két szervezet közötti együttműködést a kibervédelmi gyakorlatok terén; tudomásul veszi az EU képviselőinek részvételét az éves kiberkoalíciós gyakorlat keretében; elismeri az előrelépést, amelyet a NATO 2017. évi válságkezelő gyakorlatában a párhuzamos és összehangolt gyakorlatokban (PACE) való uniós részvétel képvisel, és üdvözli különösen egy kibervédelmi elem beépítését a gyakorlatba; sürgeti mindkét szervezetet, hogy fokozza ezeket az erőfeszítéseket;

41. sürgeti az EU-t és a NATO-t, hogy szervezzenek rendszeres stratégiai szintű gyakorlatokat a két fél legmagasabb szintű politikai vezetésének részvétele mellett; üdvözli e tekintetben az EU CYBRID 2017 elnevezésű észt gyakorlatot, amelynek keretében először vett részt egy uniós gyakorlatban a NATO főtitkára;

42. megjegyzi, hogy komoly lehetőség van egy ambiciózusabb és konkrétabb kibervédelmi együttműködési programra, amely túlmutat a konkrét műveletek kapcsán megvalósuló együttműködés elméleti szintjén; sürgeti mindkét szervezetet, hogy a már meglévő intézkedéseket konkrétan és hatékonyan hajtsa végre, és terjesszen elő ambiciózusabb javaslatokat a közös nyilatkozat végrehajtásának következő felülvizsgálatára;

43. üdvözli a 2014-ben létrehozott, a NATO és az ipar közötti kiberpartnerséget (NCIP), és kéri, hogy az EU vegyen részt az együttműködésen alapuló NCIP-erőfeszítésekben, hogy a NATO–EU együttműködéshez csatlakozzanak a kibertechnológiákra szakosodott vezető ipari szereplők, hogy a folyamatos együttműködés révén javuljon a kiberbiztonság, különös figyelmet fordítva a következőkre: képzések, gyakorlatok és oktatás a NATO, az EU és az ipar képviselői számára; az EU és az ipar bevonása a NATO intelligens védelmi projektjeibe; a NATO, az EU és az ipar közötti, együttműködésen alapuló információmegosztás és a felkészültségre és helyreállításra vonatkozó bevált gyakorlatok; közösen kifejlesztett kibervédelmi képességek biztosítása; valamint szükség esetén együttműködésen alapuló reagálás biztosítása a kiberbiztonsági eseményekre;

44. felhívja a figyelmet az ENISA-rendelet (526/2013/EU) felülvizsgálatáról és az információs és kommunikációs technológiák európai kiberbiztonsági tanúsítási és címkézési keretének megállapításáról szóló rendeletre irányuló javaslattal kapcsolatos munkára; felhívja az ENISA-t, hogy írjon alá megállapodást a NATO-val a gyakorlati együttműködésük, többek között az információmegosztás és a kibervédelmi gyakorlatokban való részvétel fokozása érdekében;

A kibertérre alkalmazandó nemzetközi normák

45. kéri a kibervédelmi képességek szempontjainak ágazatokon átívelő feladatként történő beépítését a közös kül- és biztonságpolitikába, valamint az EU és tagállamai külső fellépéseibe, és szorosabb együttműködésre szólít fel a kibervédelem terén a tagállamok, az uniós intézmények, az ENSZ, a NATO, az Egyesült Államok és más stratégiai partnerek között, különösen a kibertérrel kapcsolatos szabályok, normák és végrehajtási intézkedések tekintetében;

46. sajnálatát fejezi ki amiatt, hogy több hónapos tárgyalások után az ENSZ kormányzati szakértői csoportja (UN GGE) 2016-ban és 2017-ben képtelen volt képes konszenzusra vonatkozó új jelentést felmutatni; emlékeztet arra, hogy (amint azt a 2013. évi jelentés is elismerte) a hatályos nemzetközi jog és különösen az Egyesült Nemzetek Alapokmánya – amely tiltja bármely állam politikai függetlensége elleni fenyegetést vagy erő alkalmazását, így a részvételen alapuló hivatalos eljárások, többek között a választások lebonyolításához alapvetően szükséges műszaki infrastruktúra megzavarására irányuló kényszerítő erejű kiberműveleteket egy másik államban – alkalmazandó és végrehajtandó a kibertérben; megjegyzi, hogy a UN GGE 2015-ös jelentése felsorolja a felelős állami magatartás normáit, többek között azon tilalmat, hogy az államok nem folytathatnak vagy támogathatnak tudatosan olyan kibertevékenységeket, amelyek sértik a nemzetközi jogban foglalt kötelezettségeiket; felhívja az EU-t, hogy vállaljon vezető szerepet a kibertérben alkalmazandó nemzetközi normákról és azok végrehajtásáról folytatott jelenlegi és jövőbeni vitákban;

47. megjegyzi, hogy a tallinni kézikönyv 2.0 jelentősége alapot teremt ahhoz a vitához és elemzéshez, hogy hogyan alkalmazható a hatályos nemzetközi jog a kibertérre; felszólítja a tagállamokat, hogy kezdjék el elemezni és alkalmazni mindazt, amit a szakértők a tallinni kézikönyvben megfogalmaztak, és állapodjanak meg a nemzetközi magatartás további önkéntes normáiról; megjegyzi különösen azt, hogy a kiberképességek offenzív alkalmazásának a nemzetközi jogon kell alapulnia;

48. megerősíti a nyílt, szabad, stabil és biztonságos kibertér iránti teljes elkötelezettségét, amely tiszteletben tartja a demokrácia, az emberi jogok és a jogállamiság alapvető értékeit, és ahol a nemzetközi vitákat békés eszközökkel rendezik az ENSZ Alapokmánya és a nemzetközi jog alapelvei alapján; felhívja a tagállamokat, hogy támogassák a kiberdiplomácia és a meglévő kibernormák közös és átfogó uniós megközelítésének további végrehajtását és a NATO-val együtt dolgozzanak ki uniós szintű kritériumokat és fogalommeghatározásokat arra vonatkozóan, hogy mi minősül kibertámadásnak, hogy az EU gyorsabban tudjon közös álláspontra jutni a kibertámadás formájában elkövetett, nemzetközi jogot sértő cselekményt követően; határozottan támogatja a UN GGE 2015-ös jelentés önkéntes végrehajtását, jogilag nem kötelező erejű normák alkalmazását a kibertérben (a magánélet és az alapvető polgári jogok tiszteletben tartása mellett), valamint regionális bizalomépítő intézkedések létrehozását; támogatja ezzel összefüggésben a kibertér stabilitásával foglalkozó globális bizottság arra irányuló munkáját, hogy normákra és politikákra vonatkozó javaslatokat dolgozzon ki a nemzetközi biztonság és stabilitás növelése és annak érdekében, hogy iránymutatással szolgáljanak a kibertérbeli felelősségteljes állami és nem állami magatartásra vonatkozóan; helyesli azt a javaslatot, miszerint az állami és nem állami szereplők nem hajthatnak végre, illetve nem engedélyezhetnek tudatosan olyan tevékenységet, amely szándékosan és jelentősen károsítja az internet nyilvános felületét, ennélfogva a kibertér stabilitását;

49. elismeri, hogy a technológiai infrastruktúra nagy részét a magánszféra birtokolja vagy üzemelteti, és hogy a nyitott, szabad, stabil és biztonságos kibertér biztosításához elengedhetetlen, hogy az érdekelt felek közötti többoldalú párbeszéd keretében szoros együttműködésre, konzultációra, valamint a magánszféra és a civil társadalmi csoportok bevonására kerüljön sor;

50. elismeri, hogy a végrehajtás nehézségei miatt az államok közötti kétoldalú megállapodások nem mindig hozták meg a kívánt eredményeket; úgy véli ezért, hogy a hasonló gondolkodású országok konszenzusra hajlandó csoportjain belüli koalíciók kiépítése hatékony eszközt jelent a több érdekelt fél által tett erőfeszítések kiegészítéséhez; hangsúlyozza, hogy a bűnözés és a terrorcselekmények elleni küzdelem fokozása során a helyi hatóságoknak fontos szerepet kell játszaniuk a technológiai innováció és az adatmegosztás folyamatában;

51. üdvözli, hogy a Tanács elfogadta a rosszhiszemű kibertevékenységekkel szembeni közös uniós diplomáciai fellépés keretét, azaz EU kiberdiplomáciai eszköztárát; támogatja, hogy az EU tehessen korlátozó intézkedéseket – esetleg szankciókat vethessen ki – a kibertérben a tagállamok ellen támadást intézőkkel szemben;

52. felhív továbbá világos, proaktív megközelítés követésére a kiberbiztonság és kibervédelem tekintetében, az uniós kiberdiplomácia ágazatokon átívelő feladatként történő megszilárdítására az uniós külpolitikában, valamint az uniós kapacitások és eszközök átfogó megerősítésére annak érdekében, hogy hatékonyan megerősítsék az EU normáit és értékeit, valamint egyengessék az utat a kibertér szabályaira, normáira és végrehajtási intézkedéseire vonatkozó globális konszenzus megteremtése előtt; megjegyzi, hogy a kibertámadásokkal szembeni ellenálló képesség harmadik országokban történő kiépítése hozzájárul a nemzetközi békéhez és biztonsághoz, így végső soron az európai polgárok számára teremt biztonságosabb környezetet;

53. úgy véli, hogy a kibertámadásokra – például a NotPetya és a WannaCry zsarolóvírus-támadásra – vagy állami irányítás mellett, vagy valamely állam tudtával és jóváhagyásával kerül sor; megjegyzi, hogy ezek a kibertámadások – amelyek súlyos és maradandó gazdasági kárt okoznak, valamint az életet is veszélyeztetik – egyértelműen sértik a nemzetközi jogot és jogi normákat; úgy véli ezért, hogy a NotPetya, illetve a WannaCry zsarolóvírus-támadás kimeríti a nemzetközi jog megsértését az Oroszországi Föderáció, illetve Észak-Korea részéről, és hogy e két országgal szemben az EU-nak és a NATO-nak arányos és megfelelő válaszintézkedéseket kell foganatosítania;

54. felszólít arra, hogy az Europol Számítástechnikai Bűnözés Elleni Európai Központja váljon kapcsolattartó ponttá a kiberbűnözéssel foglalkozó bűnüldözési csoportok és kormányzati szervek számára, azzal az elsődleges feladattal, hogy támadás esetén irányítsa mind a „.eu"domain, mind az uniós hálózatok kritikus infrastruktúrájának védelmét; hangsúlyozza, hogy a kapcsolattartó pontot információcserével és azzal is meg kell bízni, hogy segítséget nyújtson a tagállamoknak;

55. hangsúlyozza, hogy normákat kell kidolgozni a magánélet védelme és a biztonság, a titkosítás, a gyűlöletbeszéd, a félretájékoztatás és a terrorfenyegetések vonatkozásaiban;

56. ajánlja, hogy minden uniós tagállam vállaljon kötelezettséget arra, hogy segítséget nyújt a kibertámadás alatt álló bármely másik tagállamnak, és hogy a NATO-val való szoros együttműködésben nemzeti kiberbiztonsági elszámoltathatóságot biztosít;

Polgári-katonai együttműködés

57. felszólítja az érdekelt feleket, hogy erősítsék meg a tudásátadási partnerségeket, hajtsanak végre megfelelő üzleti modelleket, és teremtsenek bizalmat a vállalatok, illetve a védelmi és polgári végfelhasználók között, valamint javítsák az elméleti tudás gyakorlati megoldásokba történő átadását annak érdekében, hogy szinergiák és összekapcsolt megoldások jöjjenek létre a polgári és katonai piacokon, átlátható eljárások és az uniós és nemzetközi jog tiszteletben tartásán alapuló egységes európai kiberbiztonsági piacot alkotva az EU stratégiai autonómiájának megőrzése és megerősítése céljából; megjegyzi, hogy a kiberbiztonsági magánvállalkozások kulcsfontosságú szerepet játszanak a kibertámadások korai előrejelzésében és az elkövetők kilétének megállapításában;

58. nyomatékosan hangsúlyozza a kutatás és fejlesztés fontosságát, különösen a védelmi piac magas szintű biztonsági követelményeinek fényében; sürgeti az EU-t és a tagállamokat, hogy nyújtsanak gyakorlatiasabb támogatást az európai kiberbiztonsági ipar és más érdemleges gazdasági szereplők számára, csökkentsék a bürokratikus terheket, különösen a kkv-knak és az induló vállalkozásoknak (a kiberbiztonság területén az innovatív megoldások legfontosabb forrásai), valamint szorosabb együttműködést mozdítsanak elő az egyetemi kutatóintézetekkel és a jelentősebb szereplőkkel annak érdekében, hogy csökkentssék a külső forrásokból származó internetes biztonsági termékektől való függőséget, és a stratégiai önállóságot fokozva stratégiai ellátási láncot hozzanak létre az EU-n belül; ebben az összefüggésben megjegyzi, hogy az EDF és a többéves pénzügyi keretben szereplő egyéb eszközök értékes hozzájárulást tudnak elérni;

59. ösztönzi a Bizottságot, hogy integráljon kibervédelmi elemeket az Európai Kiberbiztonsági Kutatási és Kompetenciaközpontok Hálózatába, tekintettel arra is, hogy a kettős felhasználású kiberképességek és -technológiák számára elegendő erőforrásokat biztosítsanak a következő többéves pénzügyi keretben;

60. megjegyzi, hogy az állami és különböző polgári infrastruktúrális eszközök megóvásaa tagállamok és különösen az információs rendszerek biztonságáért felelős hatóságok létfontosságú védelmi feladata, amelynek vagy nemzeti kiberparancsnokságok, vagy a nevezett hatóságok hatáskörébe kell tartoznia; hangsúlyozza, hogy ehhez magas szintű bizalomra, valamint a lehető legszorosabb együttműködésre van szükség a katonai szereplők, a kibervédelmi ügynökségek, a hatáskörrel rendelkező egyéb hatóságok és az érintett iparágak között, ami csakis a polgári és katonai szereplők feladatainak, szerepeinek és kötelezettségeinek világos meghatározása révén érhető el, továbbá nyomatékosan felkér minden érintett szereplőt, hogy a tervezési folyamataikban vegyék ezt figyelembe; felhív a határon átnyúló együttműködés fokozására (az uniós adatvédelmi jogszabályok maradéktalan betartása mellett) a rosszindulatú kibertevékenységek felszámolásával kapcsolatos bűnüldözés terén;

61. felhívja a tagállamokat, hogy kiberbiztonsággal kapcsolatos nemzeti stratégiájukat összpontosítsák az információs rendszerek és a kapcsolódó adatok védelmére, és tekintsék e kritikus infrastruktúra védelmét a vonatkozó gondossági kötelezettségük részének; sürgeti a tagállamokat, hogy fogadjanak el és hajtsanak végre olyan stratégiákat, iránymutatásokat és eszközöket, amelyek észszerű szintű védelmet biztosítanak a fenyegetések észszerűen azonosítható szintjeivel szemben, oly módon, hogy a védelem költségei és terhei arányosak legyenek a kockázatnak kitett feleket fenyegető lehetséges kárral; felhívja a tagállamokat, hogy tegyenek megfelelő, a joghatóságuk alá tartozó jogi személyeket a kezelésükben lévő személyes adatok védelmére kötelező lépéseket;

62. elismeri, hogy a kiberfenyegetések változó körülményei miatt tanácsos lenne szorosabb és strukturált együttműködést folytatni a rendőrséggel, különösen bizonyos kritikus területeken, úgymint a kiberdzsihádd al, a kiberterrorizmussal, az online radikalizálódással, többek között a szélsőséges és radikális szervezetek finanszírozásával kapcsolatos fenyegetetések nyomon követése terén;

63. bátorítja a szoros együttműködést az uniós ügynökségek – például az EDA és az ENISA, a Számítástechnikai Bűnözés Elleni Európai Központ – között, a szinergiák előmozdítására és az átfedések elkerülésére irányuló, ágazatokon átívelő megközelítés szellemében;

64. felszólítja a Bizottságot, hogy a tagállamokkal, az EDA-val, a Parlamenttel és az EKSZ-szel szoros együttműködésben dolgozza ki az európai kibervédelem koordinált megközelítésének ütemtervét, beleértve az EU kibervédelmi politikai keretének korszerűsítését annak biztosítása érdekében, hogy a szakpolitikai mechanizmus releváns eszközét jelentő keret továbbra is alkalmas legyen az EU kibervédelmi célkitűzéseinek elérésére; megjegyzi, hogy ennek a folyamatnak az uniós közös biztonság- és védelempolitika átfogóbb stratégiai megközelítésének részét kell képeznie;

65. kéri a kiberbiztonsági kapacitás fejlesztési együttműködés keretében történő fejlesztését, valamint szorgalmazza a folyamatos oktatást és kibertudatossági képzést, ezáltal növelve az országok és társadalmak kiber- és hibridfenyegetésekkel szembeni ellenálló képességét, számolva azzal, hogy az elkövetkező években több millió új felhasználó lesz az interneten, többségük a fejlődő országokban;

66. nemzetközi együttműködést és többoldalú kezdeményezéseket szorgalmaz szilárd kibervédelmi és kiberbiztonsági keretek kiépítése céljából, hogy fel lehessen venni a küzdelmet az állam korrupció, pénzügyi csalás, pénzmosás, terrorizmusfinanszírozás általi foglyul ejtése ellen, valamint a kiberterrorizmussal és a kriptovalutákkal és egyéb alternatív fizetési módokkal kapcsolatos kihívások kezelése érdekében;

67. megjegyzi, hogy a kibertámadások – például a NotPetya vírus – gyorsan terjednek, így széles körű globális ellenálló képesség hiányában válogatás nélkül okoznak kárt; úgy véli, hogy a kibervédelmi képzésnek és oktatásnak az Unió külső tevékenységének részét kell képeznie, és hogy a kiberreziliencia kiépítése a harmadik országokban hozzájárul a nemzetközi békéhez és biztonsághoz, végső soron az európai polgárok nagyobb biztonságához;

Intézményi megerősítés

68. felhívja a tagállamokat, hogy a PESCO keretében folytassanak ambiciózusabb együttműködést a kiberterületen; javasolja, hogy a tagállamok a PESCO keretében indítsanak egy új informatikai együttműködési programot a jelenlegi és jövőbeni uniós missziók és műveletek gyors és hatékony tervezésének, irányításának és ellenőrzésének támogatása céljával; megjegyzi, hogy ennek következtében javulnia kell a kibertérbeli műveleti kapacitások koordinációjának, és az Európai Tanács határozata esetén létrejöhet egy közös kibervédelmi parancsnokság;