EURÓPAI PARLAMENT 2009 - 2014

Plenárisülés-dokumentum

6.9.2013 B7-0386/2013

ÁLLÁSFOGLALÁSRA IRÁNYULÓ INDÍTVÁNY

benyújtva a Bizottság nyilatkozatát követően

az eljárási szabályzat 110. cikkének (2) bekezdése alapján

az Európai Unió kiberbiztonsági stratégiájáról: nyílt, megbízható és biztonságos kibertér
(2013/2606(RSP))

Malcolm Harbour, Andreas Schwab
a Belső Piaci és Fogyasztóvédelmi Bizottság nevében
Elmar Brok, Tunne Kelam
a Külügyi Bizottság nevében

B7-0386/2013

Az Európai Parlament állásfoglalása az Európai Unió kiberbiztonsági stratégiájáról: nyílt, megbízható és biztonságos kibertér
(2013/2606(RSP))

Az Európai Parlament,

– tekintettel az Európai Bizottság és az Európai Unió külügyi és biztonságpolitikai főképviselője „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér” című, 2013. február 7-i közös közleményére (JOIN(2013)0001),

– tekintettel a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvre irányuló 2013. február 7-i bizottsági javaslatra (COM(2013)0048),

– tekintettel „Az európai digitális menetrend” című 2010. május 19-i (COM (2010)0245) és „Az európai digitális menetrend – európai növekedés digitális alapokon” című 2012. december 18-i (COM(2012)0784) bizottsági közleményekre,

– tekintettel „A számítási felhőben rejlő potenciál felszabadítása Európában” című bizottsági közleményre (COM(2012)0529),

– tekintettel a „Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása” című 2013. március 28-i bizottsági közleményre (COM(2012)0140) és a témával kapcsolatos 2012. június 7-i tanácsi következtetésekre,

– tekintettel az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló, 2013. augusztus 12-i 2013/40/EU európai parlamenti és tanácsi irányelvre[1],

– tekintettel az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvre[2],

– tekintettel a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról szóló, 2011. december 13-i 2011/92/EU európai parlamenti és a tanácsi irányelvre[3],

– tekintettel a szabadság, a biztonság és a jog érvényesülése európai térségének megerősítését célzó stockholmi programra[4], „A szabadság, a biztonság és a jog érvényesülésén alapuló térség megvalósítása a polgárok szolgálatában – A Stockholmi Program végrehajtásáról szóló cselekvési terv” című bizottsági közleményre

[1] HL L 218., 2013.8.14., 8. o.
[2] HL L 345., 2008.12.23., 75. o.
[3] HL L 335., 2011.12.17., 1. o.
[4] HL C 115., 2010.5.4., 1. o.

(COM(2010)0171), „Az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé” című bizottsági közleményre (COM(2010)0673), valamint az Európai Unió belső biztonsági stratégiájáról szóló 2012. május 22-i állásfoglalására[1],

– tekintettel a szolidaritási klauzula Unió által történő végrehajtására vonatkozó részletes szabályokról szóló tanácsi határozatra irányuló, a Bizottság és a főképviselő által benyújtott együttes javaslatra (JOIN(2012)0039),

– tekintettel a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló, 2001. május 28-i 2001/413/IB tanácsi kerethatározatra[2],

– tekintettel „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé” című 2012. június 12-i állásfoglalására[3] és „a kritikus informatikai infrastruktúrák védelméről – Eredmények és következő lépések: a globális kiberbiztonság felé” című bizottsági közleményről (COM(2011)0163) szóló 2011. május 27-i tanácsi következtetésekre,

– tekintettel a digitális egységes piac kiteljesítéséről szóló 2012. december 11-i állásfoglalására[4],

– tekintettel a kiberbiztonságról és -védelemről szóló 2012. november 22-i állásfoglalására[5],

– tekintettel az Európai Hálózat- és Információbiztonsági Ügynökségre (ENISA) vonatkozó európai parlamenti és tanácsi rendeletre irányuló javaslatról (COM(2010)0521) szóló 2013. április 16-i jogalkotási állásfoglalására, amellyel kapcsolatban első olvasatban kialakította álláspontját[6],

– tekintettel az uniós külpolitika digitális szabadságra vonatkozó stratégiájáról szóló 2012. december 11-i állásfoglalására[7],

– tekintettel az Európa Tanács kiberbűnözésről szóló, 2001. november 23-i egyezményére,

– tekintettel az Unió nemzetközi, különösen a szolgáltatások kereskedelméről szóló általános egyezmény (GATS) szerinti kötelezettségeire,

– tekintettel az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkére és az Európai Unió Alapjogi Chartájára[8], különösen annak 6., 8. és 11. cikkeire,

– tekintettel az Európai Unió és az Amerikai Egyesült Államok közötti transzatlanti kereskedelmi és beruházási partnerségről jelenleg zajló tárgyalásokra,

– tekintettel eljárási szabályzata 110. cikkének (2) bekezdésére,

---

[1] Elfogadott szövegek, P7_TA(2012)0207
[2] HL L 149., 2001.6.2., 1. o.
[3] Elfogadott szövegek, P7_TA(2012)0237
[4] Elfogadott szövegek, P7_TA(2012)0468
[5] Elfogadott szövegek, P7_TA(2012)0457
[6] Elfogadott szövegek, P7_TA(2013)0103
[7] Elfogadott szövegek, P7_TA(2012)0470
[8] HL C 83., 2010.3.30., 389. o.

A. mivel az egyre kifinomultabb fenyegetések és támadások formáját öltő és egyre nagyobb mértékű számítástechnikai kihívások komoly veszélyt jelentenek a tagállamok, illetve a magánszektor és a tágabb közösség biztonságára, védelmére és gazdasági jólétére; mivel ily módon társadalmunk és gazdaságunk védelme egy folyamatosan formálódó kihívást fog jelenteni;

B. mivel a kibertérnek és a kiberbiztonságnak az Unió és az egyes tagállamok biztonsági és védelmi politikája egyik stratégiai pillérét kellene képezniük; mivel feltétlenül biztosítani kell, hogy a kibertér továbbra is nyitva álljon az eszmék és információk szabad áramlása és a szabad véleménynyilvánítás előtt;

C. mivel az e-kereskedelem és az online szolgáltatások jelentik az internet egyik létfontosságú erősségét, és kulcsfontosságúak az EU 2020 stratégia a polgárok és a magánszektor számára egyaránt előnyös céljainak eléréséhez; mivel az Uniónak teljes mértékben tisztában kell lennie azzal, hogy az internet milyen lehetőségeket rejt és kínál az egységes piac továbbfejlesztéséhez, ideértve az egységes digitális piacot is;

D. mivel az uniós kiberbiztonsági stratégiáról szóló közös közleményben vázolt stratégiai prioritások közé tartozik a számítógépes támadásokkal szembeni ellenálló képesség növelése, a számítástechnikai bűnözés csökkentése, egy kibervédelmi politika kidolgozása, a közös biztonság- és védelempolitikához (KBVP) kapcsolódó kiberképességek kiépítése, valamint a kibertérre vonatkozó koherens nemzetközi szakpolitika létrehozása az Unió számára;

E. mivel az Unión belül a hálózati és információs rendszerek nagy mértékben összekapcsoltak; mivel az internet globális jellegének köszönhetően a hálózati és információs rendszerek biztonságát érintő incidensek közül számos átterjed a nemzeti határokon, és veszélyeztetheti a belső piac működését és a fogyasztóknak az egységes digitális piacba vetett bizalmát;

F. mivel az Unió – és a világ többi része – kiberbiztonságának ereje a leggyengébb láncszem erősségétől függ, és a valamely ágazatban vagy tagállamban felmerülő zavarok hatással vannak a többi ágazatra vagy tagállamra is, ami a tovagyűrűző hatás révén az uniós gazdaság egészére nézve következményekkel jár;

G. mivel 2013 áprilisáig csupán 13 tagállam fogadott el hivatalosan nemzeti kiberbiztonsági stratégiát; mivel továbbra is alapvető különbségek állnak fenn a tagállamok között azzal kapcsolatban, hogy mennyire felkészültek, biztonságosak, illetve milyen stratégiai kultúrával és milyen kapacitásokkal rendelkeznek nemzeti kiberbiztonsági stratégia kidolgozására és végrehajtására, és mivel felmérést kellene készíteni ezekről a különbségekről;

H. mivel az eltérő biztonsági kultúrák és a jogi keretek hiánya az egységes digitális piac tekintetében töredezettséghez vezet, és jelentős aggodalomra ad okot; mivel a kiberbiztonsággal kapcsolatos harmonizált megközelítés hiánya komolyan veszélyezteti a gazdasági jólétet és a tranzakciók biztonságát, és mivel ezért összehangolt erőfeszítésekre és szorosabb együttműködésre van szükség a kormányok, a magánszektor, valamint a bűnüldöző és a hírszerző ügynökségek között;

I. mivel a kiberbiztonság egyre nagyobb költségekkel járó nemzetközi kérdés, amely – az ENSZ Kábítószer- és Bűnügyi Hivatala szerint – jelenleg évente közel 295 milliárd eurót von el a globális gazdaságtól;

J. mivel a nemzetközi szervezett bűnözés, kihasználva a technológiai előnyöket, műveleti területét egyre inkább a kibertérbe helyezi át, és a számítástechnikai bűnözés radikálisan megváltoztatja a bűnszervezetek hagyományos szerkezetét; mivel ennek következtében a szervezett bűnözés kevésbé helyhez kötött, és nagyobb a valószínűsége annak, hogy globális szinten kihasználja a területi különbségeket és az eltérő nemzeti joghatóságokat;

K. mivel a kiberbűnözés illetékes hatóságok általi kivizsgálását továbbra is számos akadály nehezíti, ideértve például a kibertérben lebonyolított ügyletek során alkalmazott, pénzmosásra használható „virtuális fizetőeszközöket”, a területi különbségek és a joghatósági határok kérdéseit, a hírszerzési információk megosztásával kapcsolatos képességek elégtelen voltát, a képzett személyzet hiányát, valamint a többi érintettel folytatott együttműködés következetlenségeit;

L. mivel a kibertér fejlesztésének alapját a technológia képezi, és mivel ahhoz, hogy fejleszteni tudjuk az uniós kibertér ellenálló képességét és biztonságát, folyamatosan alkalmazkodni kell a technológiai változásokhoz; mivel intézkedéseket kell tenni annak biztosítása érdekében, hogy a jogszabályok mindig figyelembe vegyék a technológiák legújabb fejleményeit, lehetővé téve ezzel a számítógépes bűnözők hatékony azonosítását és bíróság elé állítását, valamint a számítástechnikai bűnözés áldozatainak védelmét;

1. üdvözli az európai uniós kiberbiztonsági stratégiáról szóló közös közleményt és a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvre irányuló javaslatot;

2. hangsúlyozza az internet és a kibertér kiemelkedő és egyre növekvő jelentőségét a politikai, gazdasági és társadalmi tranzakciók tekintetében, nemcsak az Unión belül, hanem a világ egyéb szereplői tekintetében is;

3. hangsúlyozza, hogy stratégiai kommunikációs politikát kell kidolgozni az Unió kiberbiztonságával, a kiberválsághelyzetekkel, a stratégiai felülvizsgálatokkal, a köz- és a magánszféra együttműködésével és a készültséggel kapcsolatban, valamint ajánlásokat kell kidolgozni a nyilvánosság számára;

4. emlékeztet arra, hogy a magas szintű hálózati és információs biztonságra nem csupán azért van szükség, hogy fenn lehessen tartani a társadalom és a gazdaság zökkenőmentes működéséhez elengedhetetlen szolgáltatásokat, hanem ahhoz is, hogy a kritikus infrastruktúrák hatékonyságának, alkalmasságának és biztonságos működésének fokozásával meg lehessen óvni a polgárok testi épségét; hangsúlyozza, hogy miközben kezelni kell a hálózati és információs biztonság kérdéseit, fontos feladat a fizikai biztonság javítása is; hangsúlyozza, hogy az infrastruktúrának a szándékos és a nem szándékos zavarokkal szemben egyaránt ellenállónak kell lennie; hangsúlyozza, hogy ennek kapcsán a kiberbiztonsági stratégiának nagyobb hangsúlyt kellene fektetnie a nem szándékos rendszerhibák főbb okaira;

5. ismételten felszólítja a tagállamokat, hogy indokolatlan késedelem nélkül fogadjanak el

nemzeti kiberbiztonsági stratégiákat, amelyek kitérnek a technikai és koordinációs kérdésekre, valamint az emberi erőforrásokkal és a pénzeszközök elosztásával kapcsolatos szempontokra is, és amelyek a magánszektor részvételének garantálása érdekében külön szabályokat tartalmaznak a magánszektorra vonatkozó előnyökről és felelősségéről, valamint hogy gondoskodjanak átfogó kockázatkezelési eljárásokról, illetve óvják a szabályozási környezetet;

6. megállapítja, hogy kizárólag az uniós intézmények és a tagállamok együttes vezetése és politikai szerepvállalása segíthet a hálózati és információs biztonság magas szintjének megvalósításához az Unióban, és járulhat hozzá az egységes piac biztonságos és zökkenőmentes működéséhez;

7. hangsúlyozza, hogy az Unió kiberbiztonsági politikájának biztonságos és megbízható digitális környezetet kellene nyújtania, amely az uniós alapjogi chartában és az EUMSZ 16. cikkében meghatározottak szerint a szabadságok online védelmén és megőrzésén és az alapvető jogok online tiszteletben tartásán alapul és ezek garantálására hivatott, különös tekintettel a magánélethez való jogra és az adatvédelemre; úgy véli, hogy külön figyelmet kell fordítani a gyermekek online védelmére;

8. felszólítja a tagállamokat és a Bizottságot, hogy tegyenek meg minden szükséges lépést az európai polgárok tudatosságának, képességeinek és oktatásának előmozdítását és javítását célzó, a digitális ismeretekre vonatkozó tantervek részét képező, kora gyermekkortól kezdve alkalmazható képzési programok kidolgozására, különös tekintettel a személyes biztonságra; üdvözli az ENISA támogatásával, valamint az állami hatóságokkal és a magánszektorral együttműködésben megrendezendő európai kiberbiztonsági hónapra irányuló kezdeményezést, melynek célja, hogy felhívja a figyelmet a hálózati és információs rendszerek védelmével kapcsolatos kihívásokra;

9. úgy véli, hogy a kiberbiztonsággal kapcsolatos oktatás növeli az európai társadalomnak a számítógépes fenyegetésekkel kapcsolatos tudatosságát, és ezzel ösztönzi a kibertér felelős használatát, illetve hozzájárul a számítógépes készségek fejlesztéséhez; elismeri az Europol és az annak keretében működő új Számítástechnikai Bűnözés Elleni Európai Központ, valamint az ENISA és az EUROJUST kulcsfontosságú szerepét abban, hogy uniós szintű képzéseket tartanak a nemzetközi igazságügyi együttműködés eszközeinek használatáról, valamint a számítástechnikai bűnözés különböző aspektusaihoz kapcsolódó bűnüldözésről;

10. ismételten hangsúlyozza, hogy szakmai tanácsot és jogi tájékoztatást kell nyújtani, illetve programokat kell létrehozni a számítástechnikai bűnözés megelőzéséről és az ellene folytatott küzdelemről; ösztönzi a kritikus infrastruktúra és az információs rendszerek védelmére szakosodott számítástechnikai mérnökök, valamint az átvitel-ellenőrzési rendszerek és forgalomirányítási központok üzemeltetőinek képzését; hangsúlyozza, hogy az állami szektorban dolgozók számára valamennyi szinten sürgősen rendszeres kiberbiztonsági képzési programokat kell indítani;

11. ismételten óvatosságra int a polgárok kommunikációs és informatikai eszközök alkalmazására irányuló lehetőségeinek korlátozásával kapcsolatban, és hangsúlyozza, hogy a számítógépes fenyegetésekre és támadásokra adott válaszlépések kidolgozása során a tagállamoknak nem szabad törekedniük állampolgáraik jogainak és

szabadságainak megnyirbálására, és megfelelő jogalkotási eszközökkel kell rendelkezniük ahhoz, hogy meg tudják különböztetni a polgári és a katonai szintű számítógépes incidenseket;

12. úgy véli, hogy a kiberbiztonság területébe történő szabályozói beavatkozásnak kockázatközpontúnak kell lennie, a kritikus infrastruktúrára kell összpontosítania, mivel annak megfelelő működése jelentős közérdeknek minősül, illetve a hálózati ellenálló képesség biztosítása érdekében az ágazat már létező, piacalapú erőfeszítéseire kell építkeznie; hangsúlyozza az operatív szintű együttműködés központi szerepét a számítógépes fenyegetésekkel kapcsolatos információknak az állami hatóságok és a magánszektor közötti hatékonyabb megosztásában, uniós és nemzeti szinten egyaránt, valamint az Unió stratégia partnereivel is, aminek célja a hálózatok és az információk biztonságának biztosítása a kölcsönös bizalom, értékek és elkötelezettség kialakítása, valamint a szakmai ismeretek megosztása révén; hangsúlyozza, hogy a köz- és magánszféra közötti partnerségnek hálózati és technológiai semlegességen kell alapulnia, és a nyilvánosságra jelentős hatást gyakorló problémák kezelésére irányuló erőfeszítésekre kell összpontosítania; felszólítja a Bizottságot, hogy ösztönözze valamennyi érintett piaci résztvevőt fokozottabb éberségre és együttműködésre, hogy megvédjék a többi résztvevőt a szolgáltatásaikat érő károktól;

13. elismeri, hogy a kiberbiztonsági incidensek felderítése és bejelentése elengedhetetlen az Unió számítógépes támadásokkal szembeni ellenálló képességének fokozásához; úgy véli, hogy a biztonság jelentős megsértésével járó incidensek illetékes nemzeti hatóságoknak történő bejelentésének lehetővé tétele érdekében arányos és szükséges jelentéstételi követelményeket kell előírni, ezzel lehetővé téve a kiberbiztonsági incidensek fokozott ellenőrzését és a tudatosság fokozását valamennyi szinten;

14. arra ösztönzi a Bizottságot és az egyéb szereplőket, hogy vezessenek be a kiberbiztonságra és a számítástechnikai bűnözéssel szembeni ellenálló képességre vonatkozó olyan politikákat, amelyek gazdasági ösztönzőkkel fokozzák a kiberbiztonság és a számítógépes bűnözéssel szembeni ellenálló képesség magas szintjét;

Számítógépes támadásokkal szembeni ellenálló képesség

15. megállapítja, hogy a különböző ágazatok és tagállamok eltérő szintű képességekkel és készségekkel rendelkeznek, és hogy ez akadályozza a kölcsönös bizalmon alapuló együttműködést, és veszélyezteti az egységes piac működését;

16. úgy véli, hogy a kis- és középvállalkozásokra vonatkozó követelményeknek arányos és kockázatalapú megközelítésen kell alapulniuk;

17. kitart amellett, hogy javítani kell a kritikus infrastruktúrák számítógépes támadásokkal szembeni ellenálló képességét, és emlékeztet arra, hogy a szolidaritási záradék (EUMSZ 222. cikk) végrehajtását szolgáló későbbi intézkedések során figyelembe kell venni a tagállamokkal szembeni számítógépes támadások kockázatát is; felhívja a Bizottságot és a főképviselőt, hogy a 2015-től készítendő közös, integrált fenyegetés- és kockázatértékelési jelentésekben vegyék figyelembe e kockázatot;

18. hangsúlyozza, hogy különösen a kritikus szolgáltatások épségének, rendelkezésre

állásának és bizalmas jellegének biztosítása érdekében a kritikus infrastruktúra azonosításának és besorolásának naprakésznek kell lennie, és meg kell határozni a hálózati és információs rendszereikre vonatkozó biztonsági minimumkövetelményeket;

19. elismeri, hogy a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvre irányuló javaslat előirányoz ilyen biztonsági minimumkövetelményeket az információs társadalommal összefüggő szolgáltatást nyújtókra és a kritikus infrastruktúrák üzemeltetőire vonatkozóan;

20. felhívja a tagállamokat és az Uniót, hogy dolgozzanak ki megfelelő kereteket a gyors, kétirányú információmegosztási rendszerek számára, amelyek biztosítják a magánszektor anonimitását, és folyamatosan naprakészen tartják a közszférát, szükség esetén pedig segítséget nyújtanak a magánszektor számára;

21. üdvözli a Bizottság azon elképzelését, hogy a kiberbiztonságra vonatkozóan kockázatkezelési kultúrát alakít ki, és sürgeti a tagállamokat és az uniós intézményeket, hogy a számítástechnikai válságkezelést mielőbb építsék be a válságkezelési terveikbe és kockázatelemzéseikbe; ezenfelül felhívja a tagállamok kormányait és a Bizottságot, hogy a magánszféra szereplőit ösztönözzék arra, hogy a számítástechnikai válságkezelést foglalják bele válságkezelési terveikbe és kockázatelemzéseikbe, személyzetüket pedig részesítsék kiberbiztonsági képzésben;

22. felhívja valamennyi tagállamot és az uniós intézményeket, hogy hozzák létre a jól működő, hálózatbiztonsági veszélyhelyzeteket elhárító csoportok (CERT) hálózatát, amely a hét minden napján, éjjel-nappal üzemel; rámutat, hogy a nemzeti CERT-eknek egy hatékony hálózat részét kell alkotniuk, amelyben a lényeges információk cseréje a szükséges bizalmi és titoktartási normáknak megfelelően zajlik; megállapítja, hogy a CERT-eket összefogó ernyőkezdeményezések és egyéb fontos biztonsági szervek hasznos eszközök lehetnek a bizalom határokon és ágazatokon átnyúló kontextusban való fejlesztése szempontjából; elismeri a CERT-ek és a bűnüldöző szervek közötti, a számítástechnikai bűnözés elleni küzdelem terén folytatott hatékony és eredményes együttműködés jelentőségét;

23. támogatja az ENISA-t a hálózat- és információbiztonsággal kapcsolatos feladatainak ellátásában, különösen azáltal, hogy iránymutatást nyújt és tanácsot ad a tagállamok számára, valamint hogy támogatja a bevált gyakorlatok megosztását és a bizalom légkörének kialakítását;

24. hangsúlyozza, hogy az ágazatnak a kiberbiztonsági teljesítményre vonatkozóan megfelelő követelményeket kell alkalmaznia a közlekedési hálózatokban és az információs rendszerekben használt IKT-termékek értékláncának teljes hosszában, megfelelő kockázatelemzést kell végrehajtania, biztonsági normákat és megoldásokat kell elfogadnia és a számítógépes támadások ellen védett közlekedési rendszerek biztosítása érdekében fejlesztenie kell a bevált gyakorlatok és az információk megosztását;

Ipari és technológiai erőforrások

25. úgy véli, hogy a magas szintű hálózat- és információbiztonság központi szerepet játszik az Unión belül mind a biztonsági megoldások szolgáltatói, mind azok felhasználói

versenyképességének javításában; úgy ítéli meg, hogy míg az Unióban az IT-biztonsági ágazat jelentős kihasználatlan potenciállal rendelkezik, a magán-, közszférabeli és üzleti felhasználók ugyanakkor gyakran nincsenek tisztában a kiberbiztonsági befektetések költségeivel és hasznaival, és ennélfogva továbbra is ki vannak szolgáltatva a káros számítógépes fenyegetéseknek; hangsúlyozza, hogy a CERT-ek felállítása e tekintetben jelentős tényezőnek minősül;

26. úgy véli, hogy a kiberbiztonsági megoldások kínálata és az iránt való kereslet bőségéhez az IKT-ügyekkel foglalkozó nemzeti hatóságok részéről a tudományos erőforrásokba, a kutatásba és fejlesztésbe (K+F) való megfelelő beruházások, valamint tudásbővítés és kapacitásépítés szükséges az innováció serkentése és a hálózat- és információbiztonsági kockázatokkal kapcsolatos kellő tudatosság megteremtése érdekében, amelyek együttesen egy összehangolt európai biztonsági ágazat felé mutatnak;

27. felhívja az uniós intézményeket és a tagállamokat, hogy tegyék meg a szükséges intézkedéseket a kiberbiztonság belső piacának létrehozása érdekében, amelyen belül a felhasználók és a szolgáltatók a lehető legjobban kihasználhatják a rendelkezésre álló innovációkat, szinergiákat és együttes szakértelmüket, és amely lehetővé teszi a kkv-k piacra lépését;

28. arra ösztönzi a tagállamokat, hogy a más ágazatokban, például a légi közlekedési ágazatban megvalósult beruházásokhoz hasonlóan vegyék fontolóra az európai kiberbiztonsági ágazatba történő közös beruházások végrehajtását;

Számítástechnikai bűnözés

29. úgy véli, hogy a kibertérben folytatott bűncselekmények ugyanolyan károsak a társadalmak jólétére nézve, mint a fizikai világban megvalósulók, és hogy a bűnözés e formái gyakran egymást erősítik, amint az a gyermekek szexuális kizsákmányolása, valamint a szervezett bűnözés és a pénzmosás területén is megfigyelhető;

30. megállapítja, hogy bizonyos esetekben kapcsolat áll fenn a jogszerű és a jogellenes üzleti tevékenységek között; hangsúlyozza, hogy a terrorizmus finanszírozása és a súlyos szervezett bűnözés között kapcsolat áll fenn, és e kapcsolat fenntartását az internet megkönnyíti; hangsúlyozza, hogy a nyilvánosságban tudatosítani kell a számítástechnikai bűnözésben való érintettség komolyságát és azt, hogy ami első látásra „társadalmilag elfogadott” bűncselekménynek minősül – például a filmek illegális letöltése – gyakran jelentős pénzösszegeket generálhat a nemzetközi bűnszervezetek számára;

31. egyetért a Bizottsággal abban, hogy az interneten kívül érvényes normáknak és elveknek online is érvényesülniük kell, és ezért a számítástechnikai bűnözés elleni küzdelmet naprakész jogszabályokkal és operatív képességekkel fokozni kell;

32. úgy ítéli meg, hogy a számítástechnikai bűnözés határokon átnyúló jellege miatt különösen fontosak a közös erőfeszítések és a tagállami szinten felül, uniós szinten biztosított szakértelem, valamint az, hogy az Eurojust, az Europol Számítástechnikai Bűnözés Elleni Európai Központja, a CERT-ek, valamint az egyetemek és a kutatóközpontok számára megfelelő erőforrásokat és képességeket kell biztosítani ahhoz, hogy a szakértelem, az együttműködés és az információmegosztás csomópontjaiként

működjenek;

33. határozottan üdvözli a Számítástechnikai Bűnözés Elleni Európai Központ létrehozását, és bátorítja, hogy a jövőben fejlesszék ezt az ügynökséget, illetve annak létfontosságú szerepét az információk és a szakértelem határokon átnyúló, időben történő és hatékony megosztásában, a számítástechnikai bűnözés megelőzésére, felderítésére és kivizsgálására irányuló erőfeszítések támogatása céljából;

34. felhívja a tagállamokat annak biztosítására, hogy a polgárok könnyen hozzáférjenek a számítógépes fenyegetésekre és azok leküzdésének módjára vonatkozó információkhoz; úgy véli, hogy ezen iránymutatásnak arra vonatkozó információkat is magában kell foglalnia, hogy a felhasználók hogyan védhetik meg magánéletüket az interneten, milyen módon észleljék és jelentsék a szexuális visszaélés online előkészületének eseteit, hogyan telepítsék a szoftvereket és tűzfalakat, hogyan kezeljék a jelszavakat, illetve milyen módon észleljék a hamis azonosítást (adathalászat), a honlap forgalmának hamis weboldalra történő illegális átirányítását (pharming) és egyéb támadásokat;

35. kitart amellett, hogy azok a tagállamok, amelyek még nem ratifikálták az Európa Tanács kiberbűnözésről szóló budapesti egyezményét, azt haladéktalanul tegyék meg; üdvözli az Európa Tanács arra vonatkozó megbeszéléseit, hogy a technológiai fejlődés nyomán aktualizálni kell az egyezményt annak biztosítása érdekében, hogy a számítástechnikai bűnözés kezelésében továbbra is hatékony maradjon, továbbá felhívja a Bizottságot és a tagállamokat, hogy vegyenek részt ebben a vitában; bátorítja az annak elősegítésére irányuló erőfeszítéseket, hogy az egyezményt más országok is ratifikálják, és felhívja a Bizottságot, hogy ezt az Unión kívül tevékenyen népszerűsítse;

Kibervédelem

36. hangsúlyozza, hogy a számítógépes kihívások, fenyegetések és támadások a tagállamok védelmét és nemzetbiztonsági érdekeit veszélyeztetik, és hogy a kritikus infrastruktúra védelmének feladatával kapcsolatos polgári és katonai megközelítéseknek a szinergiák létrehozására irányuló erőfeszítések révén mindkettő számára a maximális előnnyel kell járniuk;

37. ezért felhívja a tagállamokat, hogy fokozzák együttműködésüket az Európai Védelmi Ügynökséggel (EDA) annak érdekében, hogy a jelenlegi kezdeményezések és projektek alapján javaslatokat és kezdeményezéseket dolgozzanak ki a kibervédelmi képességekre vonatkozóan; hangsúlyozza, hogy növelni kell a K+F arányát, többek között az erőforrások összefogása és megosztása révén;

38. ismételten kifejti, hogy az átfogó uniós kiberbiztonsági stratégiának figyelembe kell vennie a meglévő ügynökségek és szervek hozzáadott értékét, valamint az azon tagállamokban összegyűjtött bevált gyakorlatokat, amelyek már saját nemzeti kiberbiztonsági stratégiákat vezettek be;

39. felhívja az alelnököt/főképviselőt, hogy a válságkezelési tervezésbe építse be a kiber-válságkezelést, továbbá hangsúlyozza, hogy a tagállamoknak az EDA-val együttműködve terveket kell kidolgozniuk a KVBP-missziók és műveletek számítógépes támadások elleni védelmére; felhívja őket, hogy állítsanak fel európai kibervédelmi erőket;

40. hangsúlyozza, hogy a kiberbiztonság területén jó gyakorlati együttműködés folyik a NATO-val, valamint hogy ezt az együttműködést különösen a tervezés, a technológia, a képzés és a felszerelések területén történő szorosabb koordináció révén fokozni kell;

41. arra irányuló erőfeszítéseket vár az Unió részéről, hogy a nemzetközi partnerekkel, többek között a NATO-val párbeszédet indítson, határozza meg az együttműködés területeit, kerülje el a tevékenységek megkettőzését, és lehetőség szerint törekedjen arra, hogy azok kiegészítsék egymást;

Nemzetközi politika

42. úgy véli, hogy a nemzetközi együttműködés és a párbeszéd lényeges szerepet játszik a bizalom és az átláthatóság megteremtésében és a világszintű hálózatosodás és információmegosztás magas szintjének elősegítésében; ezért felhívja a Bizottságot és az Európai Külügyi Szolgálatot, hogy állítson fel egy kiberdiplomáciai csapatot, amelynek feladata többek között a hasonló gondolkodású országokkal és szervezetekkel való párbeszéd előmozdítása lenne; kéri, hogy az EU tevékenyebben vegyen részt a kiberbiztonsággal foglalkozó számos magas szintű nemzetközi konferencián;

43. úgy véli, hogy egyensúlyt kell teremteni az adatok határokon átnyúló továbbítása, az adatvédelem és a kiberbiztonság mint egymással versengő célok között, összhangban az unió nemzetközi – különösen a GATS keretében vállalt – kötelezettségeivel;

44. felhívja az alelnököt/főképviselőt, hogy a kiberbiztonsági dimenziót juttassa érvényre az Unió külső fellépéseiben, különösen a harmadik országokkal fenntartott kapcsolatokban a kiberbiztonság kezelésének módjára vonatkozó együttműködés, tapasztalat- és információcsere fokozása érdekében;

45. arra irányuló erőfeszítéseket vár az Unió részéről, hogy a nemzetközi partnerekkel párbeszédet indítson, határozza meg az együttműködés területeit, kerülje el a tevékenységek megkettőzését, és lehetőség szerint törekedjen arra, hogy azok kiegészítsék egymást; felhívja az alelnököt/főképviselőt és a Bizottságot, hogy a nemzetközi szervezetekben járjanak el proaktív módon, és hangolják össze a tagállamok arra vonatkozó álláspontját, hogy a kiberbiztonság területén milyen módon mozdíthatók elő hatékonyan a különböző megoldások és a politikák;

46. úgy véli, hogy erőfeszítéseket kell tenni annak biztosítására, hogy a kibertérben érvényre jussanak a meglévő nemzetközi jogi eszközök, többek között az Európa Tanács kiberbűnözésről szóló egyezménye; ezért úgy ítéli meg, hogy nemzetközi szinten jelenleg nincs szükség új jogi eszközök kidolgozására; ugyanakkor üdvözli a kibertérre vonatkozó, a kibertérben való jogkövetést szolgáló magatartási normák kidolgozására irányuló nemzetközi együttműködést; úgy véli, hogy a technológiai fejlemények figyelembevétele céljából fontolóra kell venni a meglévő jogi eszközök aktualizálását; úgy véli, hogy a joghatósági kérdések az igazságügyi együttműködés és a határokon átnyúló bűnesetek elkövetőinek bíróság elé állítása tárgyában alapos vitát tesznek szükségessé;

47. úgy ítéli meg, hogy különösen a kiberbiztonsággal és a számítástechnikai bűnözés kérdésével foglalkozó EU–USA munkacsoport megfelelő eszközül szolgálhat az EU és az Egyesült Államok számára ahhoz, hogy szükség esetén megosszák egymással a

kiberbiztonsági politikákkal kapcsolatos bevált gyakorlatokat; ezzel összefüggésben megállapítja, hogy a kiberbiztonsághoz kapcsolódó területeket, például a hálózati és információs rendszerek biztonságos működésétől függő szolgáltatásokat a transzatlanti kereskedelmi és beruházási partnerség (TTIP) soron következő tárgyalásainak napirendjére fogják tűzni;

48. megállapítja, hogy a kiberbiztonsági készségek és a fenyegetések és rosszindulatú támadások megelőzésére, felderítésére és hatékony leküzdésére irányuló képességek a földgolyó különböző részein nem egyenletesen oszlanak el; hangsúlyozza, hogy a számítógépes támadásokkal szembeni ellenálló képesség növelésére és a számítógépes fenyegetések leküzdésére irányuló erőfeszítések nem szorítkozhatnak a hasonló gondolkodású partnerekre, hanem a kevésbé fejlett képességekkel, technikai infrastruktúrával és jogi kerettel rendelkező térségekre is ki kell terjedniük; úgy véli, hogy a CERT-ek összehangolása e téren alapvető fontosságú; felhívja a Bizottságot, hogy tegye lehetővé – és szükség esetén segítse – a harmadik országok arra irányuló erőfeszítéseit, hogy megfelelő eszközök révén maguk alakítsák ki kiberbiztonsági képességeiket;

Végrehajtás

49. kéri, hogy a nemzeti kiberbiztonsági stratégiák hatékonyságát a legmagasabb politikai szinten rendszeresen értékeljék annak biztosítása érdekében, hogy azokat az új világszintű fenyegetésekhez igazítsák, illetve hogy a különböző tagállamokban azonos kiberbiztonsági szint érvényesüljön;

50. kéri a Bizottságot, hogy dolgozzon ki egyértelmű ütemtervet, amelyben meghatározza az uniós szinten a kiberbiztonsági stratégia értelmében elérendő célkitűzések végrehajtásának és a végrehajtás értékelésének időkeretét; felkéri a tagállamokat, hogy e stratégia keretében a nemzeti tevékenységekre vonatkozóan fogadjanak el hasonló ütemtervet;

51. kéri, hogy a Bizottság, a tagállamok, az Europol és az újonnan létrehozott Számítástechnikai Bűnözés Elleni Európai Központ, az Eurojust és az ENISA rendszeres jelentéseket terjesszenek elő, amelyekben értékelik a kiberbiztonsági stratégiában meghatározott célkitűzések tekintetében elért előrelépéseket, ideértve a végrehajtás haladását mérő főbb teljesítménymutatókat is;

52. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást a Tanácsnak, a Bizottságnak, a tagállamok kormányainak és parlamentjeinek, az Europolnak, az Eurojustnak és az Európa Tanácsnak.