EURÓPAI PARLAMENT 2009 - 2014

Plenárisülés-dokumentum

A7-0167/2012

16.5.2012

JELENTÉS

„A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé” című dokumentumról
(2011/2284(INI))

Ipari, Kutatási és Energiaügyi Bizottság

Előadó: Ivailo Kalfin

PR_INI

TARTALOMJEGYZÉK

Oldalszám

AZ EURÓPAI PARLAMENT ÁLLÁSFOGLALÁSÁRA IRÁNYULÓ INDÍTVÁNY

„A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé” című dokumentumról
(2011/2284(INI))

Az Európai Parlament,

– tekintettel az „Új digitális menetrend kialakítása Európa számára: 2015.eu” című, 2010. május 5-i állásfoglalására[1],

– tekintettel „Az internet szabályozása: a következő lépések” című, 2010. június 15-i állásfoglalására[2],

– tekintettel a „Széles sávú hozzáférés Európában: beruházás a digitális technológia által vezérelt növekedésbe” című, 2011. július 6-i állásfoglalására[3],

– tekintettel eljárási szabályzatának 48. cikkére,

– tekintettel az Ipari, Kutatási és Energiaügyi Bizottság jelentésére és az Állampolgári Jogi, Bel- és Igazságügyi Bizottság véleményére (A7-0167/2012),

A. mivel az információs és kommunikációs technológiákban (ikt) rejlő lehetőségek csak akkor szolgálhatnak teljes mértékben a gazdaság és a társadalom fejlesztésére, ha a felhasználók hisznek és bíznak azok biztonságában és ellenálló képességében, valamint ha az internetes környezetben ténylegesen érvényesülnek az olyan témákkal kapcsolatos hatályos jogszabályok, mint a személyes adatok védelme és a szellemitulajdon-jogok;

B. mivel az internet, valamint az információs és kommunikációs technológiák (ikt) által a polgárok életének különféle vonatkozásaira gyakorolt hatás gyorsan nő, minthogy azok társadalmi kapcsolattartásunk, kulturális gazdagodásunk és gazdasági növekedésünk kulcsfontosságú hajtóerőivé váltak;

C. mivel az ikt- és az internetbiztonság a gazdasági, társadalmi, technológiai és katonai vonatkozásoknak globálisan részét alkotó, átfogó koncepció, amely a feladatok egyértelmű megfogalmazását és differenciálását igényli, továbbá szilárd nemzetközi együttműködési mechanizmusokat követel meg;

D. mivel az uniós digitális menetrend kiemelt kezdeményezés célja Európa versenyképességének megerősítése az ikt megerősítése révén, illetve az erős és biztos növekedés, valamint a technológia alapú munkahelyek feltételeinek megteremtése;

E. mivel az információbiztonsági termékek, szolgáltatások, alkalmazások és infrastruktúra területén továbbra is a magánszektor az elsődleges beruházó, tulajdonos és irányító, amely az elmúlt évtized során eurómilliárdokat fektetett be; mivel ezt a részvételt a köz-, a

[1] HL C 81. E, 2011.3.15., 45. o.
[2] HL C 236. E, 2011.8.12., 33. o.
[3] Elfogadott szövegek, P7_TA(2011)0322.

magán vagy vegyesen köz- és magántulajdonban álló vagy ekként üzemeltetett infrastruktúrák ellenálló képességét előmozdító megfelelő politikai stratégiákkal kell erősíteni;

F. mivel az ikt-hálózatok, -szolgáltatások és -technológiák magas szintű biztonságának és rugalmasságának kialakítása fokozza az uniós gazdaság versenyképességét, mind azáltal, hogy javítja a kiberkockázatok értékelését és kezelését, mind pedig azáltal, hogy az innovációt és a növekedést támogató, kikezdhetetlenebb informatikai infrastruktúrákkal látja el az uniós gazdaság egészét, új lehetőségeket teremtve ezzel a vállalatok számára, hogy még termelékenyebbé váljanak;

G. mivel a – kibertámadásokat, de más típusú internetes bűncselekményeket is magukban foglaló – kiberbűncselekmények vonatkozásában elérhető bűnüldözési adatok a különböző európai országokban a bűncselekmények számának erőteljes növekedésére utalnak; mivel azonban mind a bűnüldöző szervek, mind a számítástechnikai szükséghelyzeteket kezelő csoportok (CERT) közössége továbbra is csak elvétve bocsát rendelkezésre a kibertámadásokra vonatkozó, statisztikailag reprezentatív adatokat, amelyeket a jövőben megfelelőbben kell összesíteni, ami Unió-szerte lehetővé fogja tenni a bűnüldöző szervek részéről a határozottabb válaszlépéseket, és több információt fog szolgáltatni az egyre növekvő kiberfenyegetésekre adott jogalkotási válaszlépésekhez;

H. mivel az információbiztonság megfelelő szintje kulcsfontosságú az internetalapú szolgáltatások erőteljes elterjedéséhez;

I. mivel a legutóbbi kiberbiztonsági események, hálózati zavarok, valamint az uniós intézmények, az ipar és a tagállamok információs infrastruktúrája elleni számítógépes támadások is azt igazolják, hogy teljes körű nemzetközi együttműködés és a tagállamokra érvényes rugalmassági minimumszabványok alapján kell létrehozni a kritikus informatikai infrastruktúrák védelmének szilárd, innovatív és hatékony rendszerét;

J. mivel az ikt új fejlődési irányvonalai, mint például a számítási felhő formájában történő távoli adattárolás, az internetbiztonság erőteljes középpontba állítását igénylik annak érdekében, hogy teljes mértékben ki lehessen aknázni a technológiai fejlődés előnyeit;

K. mivel az Európai Parlament ismételten megerősítette, hogy kitart a magánélet védelme és az adatvédelem, a hálózatsemlegesség és a szellemitulajdon-jogok védelme magas szintű normáinak alkalmazása mellett;

I. A kritikus informatikai infrastruktúrák megerősítésére szolgáló nemzeti és uniós intézkedések

1. örvendetesnek tartja, hogy a tagállamok végrehajtják a kritikus informatikai infrastruktúrák védelmére vonatkozó európai programot, beleértve a kritikus infrastruktúrák figyelmeztető információs hálózatának (CIWIN) létrehozását is;

2. úgy véli, hogy a kritikus információs infrastruktúra védelme terén tett erőfeszítések nemcsak a polgárok általános biztonságát, hanem a polgárok biztonságérzetét is erősítik, továbbá fokozzák a polgároknak a védelmük érdekében tett kormányzati intézkedésekbe vetett bizalmát is;

3. tudomásul veszi, hogy a Bizottság mérlegeli a 2008/114/EK tanácsi irányelv[1] felülvizsgálatát, és kéri, hogy mielőtt további lépéseket tennének, szolgáljanak bizonyítékokkal az irányelv eredményessége és hatása tekintetében; az irányelv hatályának különösen az ikt- és a pénzügyi szolgáltatási ágazat bevonásával történő kiterjesztésére hív fel; felhív továbbá olyan területek figyelembevételére, mint például az egészségügy, élelmiszer- és vízellátási rendszerek, nukleáris kutatás és ipar (amennyiben ezekre nem vonatkoznak egyedi rendelkezések); az a véleménye, hogy ezeknek az ágazatoknak a CIWIN által alkalmazott, horizontális megközelítés hozadékait (amely együttműködésből, egy riasztási rendszerből és a legjobb gyakorlatok cseréjéből áll) szintén élvezniük kellene;

4. a kritikus információs infrastruktúra védelme terén elért európai kiválóság fenntartása és erősítése érdekében hangsúlyozza az európai kutatás tartós integrációja kialakításának és fenntartásának fontosságát;

5. tekintettel arra, hogy a kritikus informatikai infrastruktúrák nemzeti és uniós védelme szorosan összekapcsolódik és nagymértékben függ egymástól, kényes, stratégiai és bizonytalan téma, a szolgáltatás megzavarásával, a biztonsági incidensekkel, a megsemmisítésre irányuló kísérletekkel vagy támadásokkal, például a nem kellően erős infrastruktúrából vagy nem kellően védett végterminálokból eredő eseményekkel szembeni készültség és védelem érdekében az ellenállóképességre vonatkozó minimumszabványok rendszeres frissítésére szólít fel;

6. hangsúlyozza az információbiztonsági szabványok és protokollok fontosságát, és üdvözli, hogy 2011-ben a CEN, CENELEC és ETSI biztonsági szabványok meghatározására kapott megbízást;

7. elvárja, hogy a kritikus informatikai infrastruktúrák tulajdonosai és üzemeltetői tegyék lehetővé a felhasználók számára a rosszindulatú támadások és/vagy kiesések elleni védelemre szolgáló megfelelő eszközök felhasználását, és szükség esetén támogassák őket ebben, szükség szerint humán- vagy automatizált felügyelet révén;

8. támogatja az állami és magánérdekeltek közötti, uniós szintű együttműködést, és ösztönzi a nemzeti és európai polgári – állami, magán vagy állami-magán – kritikus informatikai infrastruktúrák biztonságára és rugalmasságára vonatkozó szabványok kidolgozására és elterjesztésére irányuló erőfeszítéseiket;

9. hangsúlyozza a hálózatbiztonságot veszélyeztető nagyszabású eseményekre felkészítő páneurópai gyakorlatok fontosságát, valamint a fenyegetésértékelésre vonatkozó egységes normák meghatározásának jelentőségét;

10. felhívja a Bizottságot, hogy a tagállamokkal együttműködve értékelje a CIIP cselekvési terv végrehajtását; sürgeti a tagállamokat, hogy hozzanak létre jól működő nemzeti/kormányzati CERT-eket, alakítsanak ki nemzeti kiberbiztonsági stratégiákat, szervezzenek rendszeres, a kibereseményekkel kapcsolatos nemzeti és páneurópai gyakorlatokat, dolgozzanak ki nemzeti kiberincidens vészhelyzeti terveket, és járuljanak hozzá az európai kiberincidens vészhelyzeti terv 2012 végéig történő kidolgozásához;

[1] HL L 345., 2008.12.23., 75. o.

11. javasolja, hogy minden európai kritikus informatikai infrastruktúrára vonatkozóan üzemeltetői biztonsági tervet vagy azzal egyenértékű intézkedést vezessenek be, és hogy biztonsági összekötő tisztviselőket nevezzenek ki;

12. üdvözli az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat[1] aktuális felülvizsgálatát; megállapítja, hogy szükség van a nagyléptékű kibertámadások leküzdésére szolgáló uniós erőfeszítések koordinálására, az ENISA, a tagállami CERT-ek és a jövőbeni európai CERT-kompetenciák bevonásával;

13. úgy véli, hogy az ENISA kulcsfontosságú szerepet tölthet be európai szinten a kritikus információs infrastruktúrák védelme terén azzal, hogy technikai szakértelmet nyújt a tagállamoknak és az Európai Unió intézményeinek, valamint jelentéseket és elemzéseket készít az információs rendszerek biztonságáról európai és globális szinten;

II. A szilárd internetbiztonságot szolgáló további uniós tevékenységek

14. szorgalmazza, hogy az ENISA évente koordináljon és valósítson meg uniós szinten internetbiztonsági figyelemfelkeltő hónapot, hogy a tagállamok és az uniós polgárok különösen figyeljenek oda a kiberbiztonsággal kapcsolatos kérdésekre;

15. támogatja az ENISA-t – a digitális menetrend célkitűzéseinek megfelelően – a hálózati információbiztonsággal kapcsolatos feladatainak ellátásában, és különösen azáltal, hogy útmutatással és tanáccsal látja el a tagállamokat azzal kapcsolatban, hogy miként érjék el CERT-jeik tekintetében az alapvető képességeket, illetőleg hogyan támogassák a bevált gyakorlatok bizalmon alapuló környezet kialakítása révén történő cseréjét; felhívja az ügynökséget, hogy folytasson konzultációt az érdekeltekkel annak érdekében, hogy a magánhálózat- és infrastruktúra-tulajdonosok és üzemeltetők tekintetében hasonló kiberbiztonsági intézkedéseket határozzon meg, illetve a Bizottság és a tagállamok abban való támogatása érdekében, hogy hozzájárulhassanak az információbiztonsági tanúsítási rendszerek, magatartási normák, illetve a nemzeti és európai CERT-ek és infrastruktúra-tulajdonosok és üzemeltetők közötti együttműködési gyakorlat kialakításához és elterjesztéséhez, szükség szerint technológiasemleges közös minimumkövetelmények meghatározása révén;

16. üdvözli az ENISA feladatmeghatározásának felülvizsgálatára irányuló aktuális javaslatot, különösen a feladatmeghatározás kibővítését és az ügynökség feladatainak kiterjesztését; meggyőződése, hogy az ENISA-t – amellett, hogy szakértelem és elemzések biztosításával segíti a tagállamot – fel kell jogosítani arra, hogy uniós szinten és a megfelelő USA-beli partnerekkel együttműködésben a hálózat- és információbiztonsági események megelőzéséhez és kimutatásához, valamint a tagállamok közötti együttműködés erősítéséhez kapcsolódó irányítási feladatokat lásson el; rámutat, hogy az ENISA rendelet értelmében az ügynökség megbízható további, az internetes támadásokra való reagálással kapcsolatos feladatokkal is, amennyiben ez egyértelmű hozzáadott értéket jelent a létező nemzeti válaszadási mechanizmusokhoz képest;

17. üdvözli a 2010-es és 2011-es páneurópai kiberbiztonsági gyakorlatok eredményeit, amelyekre az Unió egészében, az ENISA felügyelete mellett került sor, és amelyek célja a

[1] HL L 69., 2005.3.16., 67. o.

tagállamok páneurópai vészhelyzeti terv kialakításában, karbantartásában és tesztelésében való támogatása volt; felhívja az ENISA-t, hogy tartsa napirenden ezeket a gyakorlatokat, és Európa átfogó internetbiztonsági kapacitásainak növelése érdekében szükség szerint fokozatosan vonja be az érintett magánszereplőket; várakozással tekint a hasonló felfogású partnerekkel való további nemzetközi bővítés elé;

18. felhívja a tagállamokat, hogy hozzanak létre kiberbiztonsági vészhelyzeti terveket, amelyeknek olyan kulcsfontosságú elemeket kell tartalmazniuk, mint például megfelelő kapcsolattartó pontok, valamint segítségnyújtásra, elszigetelésre és javításra vonatkozó rendelkezések a regionális, országos vagy határokon átnyúló jelentőségű hálózati zavarok vagy számítógépes támadások esetén; megjegyzi, hogy a tagállamoknak megfelelő nemzeti szintű koordinációs mechanizmusokat és struktúrákat is be kell vezetniük, amelyek elősegítik az illetékes nemzeti hatóságok közötti hatékonyabb koordináció biztosítását, és intézkedéseiket következetesebbé teszik;

19. az európai kiberincidens vészhelyzeti terv keretében javasolja, hogy a Bizottság tegyen javaslatot a nemzeti és kormányzati CERT-ek között a műszaki és irányítási funkciók jobb uniós szintű összehangolását szolgáló, kötelező erejű intézkedésekre;

20. felhívja a Bizottságot és a tagállamokat, hogy tegyék meg a szükséges intézkedéseket a kritikus infrastruktúrák kibertámadásoktól való védelme érdekében, és határozzanak meg eszközöket a kritikus infrastruktúrákhoz való hozzáférés hermetikus lezárására arra az esetre, ha egy súlyos kibertámadás azok megfelelő működését súlyosan veszélyezteti;

21. várakozással tekint a CERT-EU teljes körű végrehajtása elé, amely kulcsfontosságú tényező lesz az uniós intézményekre irányuló szándékos és rosszindulatú kibertámadások megelőzésében, észlelésében, az azokra való reagálásban és az azokat követő helyreállításban;

22. javasolja, hogy a Bizottság indítványozzon kötelező intézkedéseket a biztonságra és ellenálló képességre vonatkozó minimumszabványok előírására és a nemzeti számítógépes vészhelyzeteket elhárító csoportok (CERT-ek) közötti koordináció javítására;

23. felhívja a tagállamokat és az uniós intézményeket, hogy biztosítsák olyan jól működő CERT-ek létezését, amelyek rendelkeznek az egyeztetett bevált gyakorlatokon alapuló minimális biztonsági és ellenálló képességekkel; rámutat, hogy a nemzeti CERT-eknek egy hatékony hálózat részét kell alkotniuk, amelyben a lényeges információk cseréje a szükséges titoktartási előírásoknak megfelelően zajlik; minden tagállamban kéri a kritikus informatikai infrastruktúrák éjjel-nappal működő védelmi szolgálatának létrehozását, illetve a nemzeti kapcsolattartó pontok között alkalmazandó közös európai vészhelyzeti protokoll meghatározását;

24. hangsúlyozza, hogy tagállamok közötti bizalom kiépítése és együttműködés előmozdítása kulcsfontosságú az adatok, a nemzeti hálózatok és infrastruktúrák védelmében; felhívja a Bizottságot, hogy tegyen javaslatot a határokon átnyúló ikt-fenyegetések elleni küzdelem közös megközelítésének azonosítására és kijelölésére szolgáló közös eljárásra, és elvárja, hogy a tagállamok megadják a Bizottságnak a kritikus informatikai infrastruktúráik kockázataival, fenyegetéseivel és sérülékenységével kapcsolatos általános információkat;

25. üdvözli a Bizottságnak az európai információmegosztási és figyelmeztető rendszer 2013-ig történő kiépítésére vonatkozó kezdeményezését;

26. örvendetesnek tartja, hogy több, a Bizottság által kezdeményezett konzultációra került sor az érdekeltekkel az internetbiztonságról és a kritikus informatikai infrastruktúrák védelméről, úgymint az európai ellenálló képesség javításáért felelős állami-magán partnerség; elismeri az ikt-eladók ezen erőfeszítésekben való máris jelentős részvételét és azok iránti elkötelezettségét, és arra ösztönzi a Bizottságot, hogy tegyen további erőfeszítéseket az egyetemek és az ikt-felhasználók szervezetei vonatkozásában annak szorgalmazására, hogy vállaljanak aktívabb szerepet, valamint hogy segítse elő a kiberbiztonsági kérdésekkel kapcsolatos konstruktív, többoldalú párbeszédet; támogatja a digitális közgyűlés továbbfejlesztését a kritikus informatikai infrastruktúrák védelmének irányítási keretévé;

27. üdvözli a tagállamok európai fóruma által az európai kritikus infrastruktúra – középpontban a vezetékes és a mobiltávközléssel – meghatározására szolgáló ágazatspecifikus kritériumok meghatározása, valamint az internet ellenálló képességével és stabilitásával kapcsolatos uniós alapelvek és iránymutatások megvitatása kapcsán végzett munkát; várakozással tekint a tagállamok közötti konszenzus kiépítésének folytatása elé, és ezzel összefüggésben ösztönzi a fórumot, hogy egészítse ki a jelenlegi, fizikai eszközöket középpontba állító megközelítést a logikai infrastrukturális eszközök felölelésére tett erőfeszítésekkel, amelyek a virtualizáció és a számítási felhő technológiájának fejlődésével párhuzamosan egyre fontosabbá válnak a kritikus informatikai infrastruktúrák védelmének eredményessége szempontjából;

28. javasolja, hogy a Bizottság indítson el egy nyilvános páneurópai oktatási kezdeményezést, amely a magán és üzleti végfelhasználók oktatására és figyelmüknek az interneten és a vezetékes, illetve mobil ikt-eszközökön, minden használati szinten egyaránt fenyegető veszélyekre történő felhívására, valamint a biztonságosabb egyéni online viselkedés népszerűsítésére irányul; emlékeztet e tekintetben az idejétmúlt számítástechnikai berendezésekhez és szoftverekhez társuló kockázatokra;

29. felhívja a tagállamokat, hogy a Bizottság támogatásával erősítsék a nemzeti bűnüldöző és igazságügyi hatóságoknak és a megfelelő uniós ügynökségeknek szóló, információbiztonsági témájú képzési és oktatási programokat;

30. támogatja, hogy hozzanak létre a tudományos szakértők számára az információbiztonság terén európai tantervet, mivel ennek kedvező hatása lenne az EU egyre fejlődő kibertérrel és annak fenyegetéseivel kapcsolatos szakértelmére és felkészültségére;

31. javasolja a kiberbiztonsági oktatás támogatását (PhD-hallgatói gyakorlatok, egyetemi kurzusok, munkaértekezletek, hallgatói képzések stb.) és a szakképzési gyakorlatokat a kritikus információs infrastruktúrák védelme terén;

32. felkéri a Bizottságot, hogy legkésőbb 2012 végéig javasoljon egyértelmű terminológián alapuló, átfogó internetbiztonsági uniós stratégiát; véleménye szerint az internetbiztonsági stratégiának egy olyan kibertér létrehozására kell törekednie, amely – egy biztonságos és ellenálló képességgel rendelkező infrastruktúrával és nyílt szabványokkal a háttérben – elősegíti az információ szabad áramlása révén az innovációt és a prosperitást, valamint

biztosítja a magánélet és más polgári szabadságjogok kikezdhetetlen védelmét; fenntartja, hogy a stratégiának részletesen meg kell határoznia az alapelveket, célokat, módszereket, eszközöket és politikákat (belső és külső szinten is), amelyek szükségesek a biztonságos, folyamatos, szilárd és ellenállóképes – akár kritikus infrastruktúrával, akár általános internethasználattal kapcsolatos – szolgáltatás biztosítására irányuló nemzeti és uniós erőfeszítések ésszerűsítéséhez és a tagállamok körében a rugalmassági minimumszabványok létrehozásához;

33. hangsúlyozza, hogy a Bizottság készülő internetbiztonsági stratégiájának központi hivatkozási pontnak kell vennie a kritikus informatikai infrastruktúra védelmével kapcsolatos munkát, továbbá holisztikus és rendszerszemléletű megközelítést kell követnie a kiberbiztonság terén azzal, hogy lefedi mind a megelőző intézkedéseket – ilyen például a biztonsági intézkedések minimumszabványainak bevezetése vagy az egyéni felhasználók, a vállalkozások és az állami intézmények oktatása –, mind a válaszintézkedéseket – ilyenek például a büntetőjogi, polgári jogi és közigazgatási szankciók;

34. sürgeti a Bizottságot, hogy tegyen javaslatot az internetbiztonsági stratégia végrehajtásának és rendszeres frissítésének koordinálására szolgáló szilárd mechanizmusra; úgy véli, hogy ezt a mechanizmust megfelelő igazgatási, szakértői és pénzügyi erőforrásokkal kell támogatni, és hatáskörébe kell tartoznia annak, hogy elősegítse a belső és nemzetközi érdekeltekkel szemben az internetbiztonsággal kapcsolatban képviselt uniós álláspont kidolgozását;

35. felkéri a Bizottságot, hogy javasoljon a kritikus ágazatokban, nevezetesen az ikt-ágazatban és a pénzügyi szolgáltatások, de egyben az energiaellátás, a közlekedés, a víz- és élelmiszer-ellátás ágazatában is a biztonsági visszaélések bejelentésére vonatkozó uniós keretet, a tagállamok és a felhasználók kiberbiztonsági eseményekről, számítógépes támadásokról és hálózati zavarokról történő értesítése céljából;

36. sürgeti a Bizottságot, hogy javítsa az Unióban, a tagállamokban és az iparban (különösen a pénzügyi szolgáltatásokban és az ikt-ágazatban) előforduló kibertámadások költségére vonatkozó, statisztikailag reprezentatív adatok elérhetőségét azáltal, hogy erősíti a 2013-ra létrehozni tervezett számítógépes bűnözés elleni küzdelem európai központjának, a CERT-eknek, továbbá a Bizottság más kezdeményezéseinek – így az európai információmegosztási és figyelmeztető rendszernek – az adatgyűjtési kapacitását, biztosítva az európai ipart és a tagállamokat érintő kibertámadásokra és a kiberbűnözés más formáira vonatkozó módszeres jelentéstételt és adatmegosztást, és ezáltal erősítve a bűnüldözést;

37. támogatja a nemzeti magánszektorok és az ENISA közötti szoros kapcsolatot és kölcsönhatást annak érdekében, hogy a nemzeti/kormányzati CERT-ek bekapcsolódjanak az európai információmegosztási és figyelmeztető rendszer (EISAS) fejlesztésébe;

38. rámutat arra, hogy az internetbiztonság növelésére szolgáló technológiák kifejlesztésének és alkalmazásának elsődleges hajtóereje az ikt-ágazat; emlékeztet arra, hogy az uniós szakpolitikáknak el kell kerülniük, hogy akadályozzák az európai internetes gazdaság növekedését, és be kell építeniük a szükséges ösztönzőket az üzleti, illetve a köz- és magánszféra közötti partnerségekben rejlő lehetőségek teljes mértékű kiaknázása

érdekében; ajánlja annak megvizsgálását, hogy milyen további ösztönzőkkel lehetne az ipart a 2008/114/EK irányelv szerinti kikezdhetetlenebb üzemeltetői biztonsági tervek kidolgozására késztetni;

39. felhívja a Bizottságot, hogy terjesszen elő jogalkotási javaslatot a kibertámadások (azaz a célzott adathalászat, az online csalás stb.) további kriminalizálására;

III. Nemzetközi együttműködés

40. emlékeztet arra, hogy a nemzetközi együttműködés a hatásos kiberbiztonsági intézkedések bevezetésének alapvető eszköze; elismeri, hogy jelenleg az EU nem vesz részt folyamatosan a kiberbiztonsággal kapcsolatos nemzetközi együttműködési folyamatokban és párbeszédekben; felkéri a Bizottságot és az Európai Külügyi Szolgálatot (EKSZ), hogy valamennyi hasonló gondolkodású országgal kezdjen konstruktív párbeszédet az internet és a kritikus infrastruktúra ellenálló képességének növelésére szolgáló, egységes értelmezés és politikák kialakítása céljából; fenntartja ugyanakkor, hogy az EU-nak állandó jelleggel bele kell foglalnia az internetbiztonsági kérdéseket külkapcsolatainak körébe, többek között a különböző finanszírozási eszközök tervezésekor vagy pedig olyan nemzetközi megállapodások megkötésekor, amelyek érzékeny adatok cseréjét és tárolását vonják maguk után;

41. tudomásul veszi az Európa Tanács 2001. évi, a kiberbűnözésről szóló budapesti egyezményének kedvező eredményeit; rámutat ugyanakkor hogy annak ösztönzése mellett, hogy még több ország írja alá és ratifikálja az egyezményt, az EKSZ-nek kétoldalú és többoldalú megállapodásokat is ki kell alakítania a hasonló felfogású nemzetközi partnerekkel az internetbiztonságról és ellenálló képességről;

42. rámutat arra, hogy a párhuzamos erőfeszítések elkerülése érdekében össze kell hangolni a különböző nemzetközi és uniós intézmények, szervek és hivatalok, valamint a tagállamok által jelenleg folytatott számos tevékenységet, és e célból érdemes megfontolni egy, a koordinációért felelős tisztviselő kijelölését, ami egy európai uniós kiberbiztonsági koordinátor kinevezését is jelentheti;

43. kiemeli az Unió és az Egyesült Államok CIIP-ben érintett legjelentősebb szereplői és jogalkotói közötti strukturált párbeszéd különös fontosságát a jogi és a kormányzati keretek egységes felfogása, értelmezése és közös álláspontja érdekében;

44. örvendetesnek tartja, hogy a 2010. novemberi EU–USA csúcstalálkozón létrejött az EU–USA kiberbiztonsági és kiberbűnözési munkacsoport, valamint támogatja a munkacsoport arra irányuló törekvéseit, hogy a transzatlanti politikai párbeszéd részévé tegye az internetbiztonsággal kapcsolatos kérdéseket; üdvözli, hogy a Bizottság az Egyesült Államok kormányával közösen az EU–USA munkacsoport égisze alatt közös programot és útitervet dolgoz ki a 2012–2013-ban közösen/szinkronizáltan tartandó transzkontinentális kibergyakorlatokhoz;

45. indítványozza az Unió és az Egyesült Államok jogalkotói közötti strukturált párbeszéd létrehozását az internettel kapcsolatos kérdéseknek az egységes felfogás, értelmezés és álláspontok kialakítása részeként történő megvitatása érdekében;

46. szorgalmazza az EKSZ-nél és a Bizottságnál, hogy a tagállamok európai fóruma által végzett munka alapján biztosítson magának aktív pozíciót a vonatkozó nemzetközi fórumokon, többek között a tagállami álláspontok összehangolásával az Unió alapvető értékeinek, céljainak és politikáinak az internet biztonsága és ellenálló képessége terén történő előmozdítása céljából; megjegyzi, hogy az említett fórumok körébe tartozik a NATO, az ENSZ (elsősorban a Nemzetközi Távközlési Egyesület és az Internetirányítási Fórum révén), a Bejegyzett Nevek és Számok Internetszervezete, az internetes számkiosztó hatóság, az EBESZ, az OECD és a Világbank;

47. ösztönzi a Bizottságot és az ENISA-t, hogy vegyenek részt a főbb érdekeltek azt célzó párbeszédében, hogy nemzetközi szinten meghatározzák a kibertér műszaki és jogi normáit;

48. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást a Tanácsnak és a Bizottságnak.

INDOKOLÁS

Mindennapi életünk valamennyi területén egyre nagyobb szerepet kap a technológia – kezdve a kommunikációtól a pénzügyekig és banki szolgáltatásokig, a közlekedéstől az energiaellátásig, a kultúrától és szórakozástól az egészségügyig.

Napjainkban az internet és a számítógépes technológiák növekvő használata következtében az internetbiztonság az Európai Unióban és a világ többi részén is a legfontosabb politikai prioritások közé tartozik. A 2010-ben elindított EU 2020 stratégiának kiemelt politikaként része az Unió digitális menetrendje, amely ambiciózus célokat tűzött ki az Európai Unió technológiai fejlődésére vonatkozóan. Az innovatív ikt-technológiák – például a nagy sebességű és szupergyors vezetékes és mobilinternet, valamint a mobiltelefon-hálózatok, az intelligens hálózatok, sőt az olyan internetszolgálatások, mint a számítási felhő és a tárgyak internete – egyre növekvő felhasználása és alkalmazása minden esetben egyetlen egyszerű, de döntő fontosságú tényezőre hagyatkozik – a biztonságra, ellenálló képességre és bizalomra.

A Bizottság 2006 decemberében elfogadta a kritikus infrastruktúrák védelmére vonatkozó európai programról szóló közleményt. A közlemény meghatározza a kritikus infrastruktúrák védelmére vonatkozó uniós szintű tevékenységek átfogó keretét. Két évvel később a Tanács elfogadta az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008/114/EK irányelvet. Az első szakaszban az irányelv az energia- és közlekedési ágazatra helyezte a hangsúlyt. Kizárólag azokkal az infrastruktúrákkal foglalkozik, amelyek kiesése legalább két uniós tagállamot érintene.

A 2008/114/EK irányelv – jóllehet nem sorolta a kritikus infrastruktúrák közé – jövőbeni kiemelt fontosságú ágazatként azonosította az ikt-ágazatot. Mindazonáltal a Bizottság 2005-től kezdve hangsúlyozza, hogy össze kell hangolni az elektronikus kommunikáció iránti bizalom kiépítésére irányuló törekvéseket[1]. E célból 2006-ban elfogadták a biztonságos információs társadalomra irányuló stratégiát[2], amelynek legfontosabb részeit jóváhagyta a 2007/068/01 tanácsi állásfoglalás.

A Bizottság 2009-ben elfogadta az „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása” című közleményt[3]. Ebben a Bizottság meghatározta a kritikus informatikai infrastruktúrák védelmére vonatkozó cselekvési tervet azzal a céllal, hogy ösztönözze és támogassa a kritikus informatikai infrastruktúrák nemzeti és uniós szintű biztonságát. A terv megállapítja a Bizottság, az ENISA, a tagállamok és az ipar konkrét feladatait. Az ikt-infrastruktúrák növekvő biztonságával és ellenálló képességével kapcsolatos kérdés volt a témája a továbbiakban az európai digitális menetrendnek[4] és a kapcsolódó tanácsi következtetéseknek[5], az információs rendszerek elleni támadásokról szóló irányelvjavaslatnak[6], valamint az

1 COM(2005)0229
2 COM(2006)0251
3 COM(2009)0149
4 COM(2010)0245
5 A Tanács 2010. május 31-i következtetései.
6 COM(2010)0517

Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítését és modernizálását szolgáló új mandátumra vonatkozó bizottsági javaslatnak[1].

A Bizottság 2011 márciusában közzétett egy közleményt a kritikus informatikai infrastruktúrák védelméről: Eredmények és következő lépések: a globális kiberbiztonság felé" című dokumentumról[2]. E dokumentumban a Bizottság áttekinti a kritikus informatikai infrastruktúrák védelmére vonatkozó cselekvési terv végrehajtásának 2009 óta elért eredményeit, és kijelöli a következő lépéseket, fokozott hangsúlyt helyezve az Unió határain túli nemzetközi együttműködésre.

Mindezen, néhány év alatt bekövetkezett fejlemények – amelyekkel nem merül ki a kibertér biztonságának növelésére irányuló uniós erőfeszítések tárháza – bizonyítják, hogy az internetbiztonság aktuális probléma. Nyilvánvaló, hogy az internet a kritikus infrastruktúrák egyike, és hogy az internetszolgáltatással kapcsolatos zavarok jelentős veszteségeket és biztonsági kockázatokat idézhetnek elő, amelyek rendkívül sok európai polgárt és vállalkozást érintenének. Ezen túlmenően a technológia gyors fejlődése szükségessé teszi, hogy az internet elleni támadások megelőzése, a helyreállítási intézkedések és a világháló ellenálló képessége átfogó, reakcióra alkalmas, rugalmas, innovatív és hosszú távú kereten alapuljon. E keretnek biztosítania kell, hogy a kormányok, vállalkozások, magánszemélyek és minden más érdekelt között tényleges kölcsönös kapcsolat legyen. Végül, de nem utolsósorban, az internet ellenálló képességének növelése csak abban az esetben lehetséges, ha megvalósul a nemzetközi együttműködés és a nemzetközi szabványok hatékony rendszere.

1 COM(2010)0521
2 COM(2011)0163

22.3.2012

VÉLEMÉNY AZ ÁLLAMPOLGÁRI JOGI, BEL- ÉS IGAZSÁGÜGYI BIZOTTSÁG RÉSZÉRŐL

az Ipari, Kutatási és Energiaügyi Bizottság részére

A kritikus informatikai infrastruktúra védelme. Eredmények és következő lépések: a globális kiberbiztonság felé
(2011/2284(INI))

Előadó: Hankiss Ágnes

JAVASLATOK

Az Állampolgári Jogi, Bel- és Igazságügyi Bizottság felkéri az Ipari, Kutatási és Energiaügyi Bizottságot mint illetékes bizottságot, hogy állásfoglalásra irányuló javaslatába foglalja bele az alábbi javaslatokat:

1. úgy véli, hogy a kritikus információs infrastruktúra védelme olyan interdiszciplináris megközelítést igényel, amelynek a polgári jogok, az igazságügy és a belügy fontos szempontjait egyaránt magában kell foglalnia, így például a belső biztonságot, a személyes adatok védelmét, valamint az adatok bizalmasságához és a magánélethez való jogot, ezáltal növeli a biztonságot és egyidejűleg tiszteletben tartja az alapvető jogokat;

2. emlékeztet arra, hogy az EU belső biztonsági stratégiája a virtuális tér biztonságának a polgárok és vállalkozások számára való növelésének összefüggésében tartalmazza a kritikus információs infrastruktúra védelmét;

3. sürgeti az európai kritikus infrastruktúrák meghatározásának befejezését és folyamatos naprakésszé tételét a Bizottság felügyelete mellett, a 2008/114/EK irányelvvel összhangban (az európai létfontosságú infrastruktúrák azonosítására és kijelölésére, valamint annak értékelésére vonatkozóan, hogy kell-e fokozni védelmüket); hangsúlyozza azt is, hogy európai szinten a lehető leghamarabb létre kell hozni a kritikus infrastruktúrákkal kapcsolatos figyelmeztető információs hálózatot; kitart amellett, hogy tekintettel a közintézmények, üzleti vállalkozások és magánháztartások információs és kommunikációs technológiáktól (IKT) való komoly függésére, a 2008/114/EK tanácsi irányelvet felül kell vizsgálni annak érdekében, hogy az IKT-t is létfontosságú szektorként ismerjék el;

4. felszólítja a tagállamokat, hogy dolgozzanak ki nemzeti stratégiákat, és biztosítsanak megbízható politikai döntéshozatali és szabályozási környezetet, átfogó kockázatkezelési eljárásokat és megfelelő előkészítő intézkedéseket és mechanizmusokat; sürgeti azokat a tagállamokat, amelyek még nem hozták létre a nemzeti hálózatbiztonsági vészhelyzeteket elhárító csoportjukat (CERT), hogy ezt idejében tegyék meg, és szükség esetén vegyék igénybe az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) segítségét;

5. úgy véli, hogy az érzékeny személyes adatokat kezelő valamennyi nagy kiterjedésű adatbázist – mint az EU, a tagállamok és a pénzügyi és egészségügyi intézmények adatbázisai – a kritikus információs infrastruktúra részének kell tekinteni, és a lehető legmagasabb szintű szabványok szerint biztosítani kell az ilyen adatok védelmét;

6. felszólítja a Bizottságot és a tagállamokat, hogy tegyék meg a szükséges intézkedéseket a kritikus infrastruktúra kibertámadásokkal szembeni védelme érdekében, és biztosítsanak eszközöket a kritikus infrastruktúrához való hozzáférés lezárására arra az esetre, ha egy közvetlen kibertámadás súlyosan veszélyezteti annak megfelelő működését;

7. hangsúlyozza a hálózatbiztonságot veszélyeztető nagyszabású eseményekre felkészítő páneurópai gyakorlatok fontosságát, valamint a fenyegetésértékelésre vonatkozó egységes normák meghatározásának jelentőségét;

8. úgy véli, hogy az ENISA kulcsfontosságú szerepet tölthet be európai szinten a kritikus információs infrastruktúrák védelme terén azzal, hogy technikai szakértelmet nyújt a tagállamoknak és az Európai Unió intézményeinek, valamint jelentéseket és elemzéseket készít az információs rendszerek biztonságáról európai és globális szinten;

9. meggyőződése, hogy az uniós szint feletti nemzetközi együttműködés elengedhetetlen, mivel a számítástechnikai fenyegetések globális természetűek, ezért a nemzetközi jog rendelkezéseinek megfelelő globális válaszokat igényelnek; hangsúlyozza azt is, hogy a különleges adatok cseréjét érintő minden nemzetközi megállapodásnak figyelembe kell vennie az adattovábbítás és -tárolás biztonságosságát;

10. hangsúlyozza, hogy a Bizottság készülő internetbiztonsági stratégiájának központi hivatkozási pontnak kell vennie a kritikus informatikai infrastruktúra védelmével kapcsolatos munkát, továbbá holisztikus és rendszerszemléletű megközelítést kell követnie a kiberbiztonság terén azzal, hogy lefedi mind a megelőző intézkedéseket – ilyen például a biztonsági intézkedések minimumszabványainak bevezetése vagy az egyéni felhasználók, a vállalkozások és az állami intézmények oktatása –, mind a válaszintézkedéseket – ilyenek például a büntetőjogi, polgári jogi és közigazgatási szankciók;

11. meggyőződése, hogy erősíteni és fokozni kell az együttműködést mindenekelőtt a polgári és a katonai szereplők, valamint az igazságügyi és egyéb illetékes hatóságok között az informatikai rendszerek elleni támadások megelőzése, elhárítása és szankcionálása terén, ideértve a tagállamok rendőrségeit és más bűnüldöző hatóságait, valamint az európai szintű szakosodott ügynökségeket is, mint például az Eurojustot, az Europolt és az ENISA-t;

12. hangsúlyozza az állami és a magánszektor közötti szoros együttműködés jelentőségét,

mivel a két szektor által nyújtott különböző előnyök, egymást kölcsönösen kiegészítve hozzájárulhatnak az infrastruktúra és ezáltal az európai polgárok életének és magánéletének védelmét célzó erőfeszítésekhez; felszólítja a Bizottságot, hogy hozzon létre ***az ellenállóképesség javításáért felelős európai állami-magán partnerséget***, amelyet integrálnának az ENISA és az európai kormányzati CERT-ek csoportjának munkájába;

13. rámutat arra, hogy a párhuzamos erőfeszítések elkerülése érdekében össze kell hangolni a különböző nemzetközi és uniós intézmények, szervek és hivatalok, valamint a tagállamok által jelenleg folytatott számos tevékenységet, és e célból érdemes megfontolni egy, a koordinációért felelős tisztviselő kijelölését, ami egy európai uniós kiberbiztonsági koordinátor kinevezését is jelentheti;

14. úgy véli, hogy a kritikus információs infrastruktúra védelme terén tett erőfeszítések nemcsak a polgárok általános biztonságát, hanem a polgárok biztonságérzetét is erősítik, továbbá fokozzák a polgároknak a védelmük érdekében tett kormányzati intézkedésekbe vetett bizalmát is;

15. a kritikus információs infrastruktúra védelme terén elért európai kiválóság fenntartása és erősítése érdekében hangsúlyozza az európai kutatás tartós integrációja kialakításának és fenntartásának fontosságát;

16. hangsúlyozza az aktív kutatási útiterv fontosságát a kiberbiztonság terén;

17. javasolja a kiberbiztonsági oktatás támogatását (PhD-hallgatói gyakorlatok, egyetemi kurzusok, munkaértekezletek, hallgatói képzések stb.) és a szakképzési gyakorlatokat a kritikus információs infrastruktúrák védelme terén;

18. támogatja a nemzeti magánszektorok és az ENISA közötti szoros kapcsolatot és kölcsönhatást annak érdekében, hogy a nemzeti/kormányzati CERT-ek bekapcsolódjanak az európai információmegosztási és figyelmeztető rendszer (EISAS) fejlesztésébe;

19. hangsúlyozza egy közös európai kiberbiztonsági stratégia, valamint az ahhoz kapcsolódó fellépések és szükséges erőforrások meghatározására vonatkozó világos menetrend fontosságát;

20. kiemeli az Unió és az Egyesült Államok CIIP-ben érintett legjelentősebb szereplői és jogalkotói közötti strukturált párbeszéd fontosságát, a jogi és a kormányzati keretek egységes felfogása, értelmezése és közös álláspontja érdekében.

A BIZOTTSÁGI ZÁRÓSZAVAZÁS EREDMÉNYE

Az elfogadás dátuma	21.3.2012
A zárószavazás eredménye	+: 45 –: 0 0: 2
A zárószavazáson jelen lévő tagok	Roberta Angelilli, Edit Bauer, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Rosario Crocetta, Frank Engel, Cornelia Ernst, Tanja Fajon, Kinga Göncz, Nathalie Griesbeck, Sylvie Guillaume, Anna Hedh, Salvatore Iacolino, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu, Anthea McIntyre, Jan Mulder, Antigoni Papadopoulou, Judith Sargentini, Csaba Sógor, Renate Sommer, Rui Tavares, Kyriacos Triantaphyllides, Wim van de Camp, Renate Weber, Josef Weidenholzer, Cecilia Wikström
A zárószavazáson jelen lévő póttag(ok)	Vilija Blinkevičiūtė, Andrew Henry William Brons, Michael Cashman, Anna Maria Corazza Bildt, Ana Gomes, Nadja Hirsch, Stanimir Ilchev, Iliana Malinova Iotova, Franziska Keller, Wolfgang Kreissl-Dörfler, Mariya Nedelcheva, Hubert Pirker, Zuzana Roithová, Kārlis Šadurskis
A zárószavazáson jelen lévő póttag(ok) (187. cikk (2) bekezdés)	Luis de Grandes Pascual

A BIZOTTSÁGI ZÁRÓSZAVAZÁS EREDMÉNYE

Az elfogadás dátuma	8.5.2012
A zárószavazás eredménye	+: 51 –: 7 0: 0
A zárószavazáson jelen lévő tagok	Amelia Andersdotter, Josefa Andrés Barea, Jean-Pierre Audy, Zigmantas Balčytis, Ivo Belet, Bendt Bendtsen, Jan Březina, Maria Da Graça Carvalho, Giles Chichester, Jürgen Creutzmann, Pilar del Castillo Vera, Dimitrios Droutsas, Adam Gierek, Norbert Glante, Robert Goebbels, András Gyürk, Fiona Hall, Edit Herczog, Kent Johansson, Romana Jordan, Krišjānis Kariņš, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Paul Rübig, Salvador Sedó i Alabart, Francisco Sosa Wagner, Konrad Szymański, Britta Thomsen, Evžen Tošenovský, Ioannis A. Tsoukalas, Claude Turmes, Marita Ulvskog, Vladimir Urutchev, Kathleen Van Brempt, Alejo Vidal-Quadras, Henri Weber
A zárószavazáson jelen lévő póttag(ok)	Ioan Enciu, Françoise Grossetête, Takis Hadjigeorgiou, Roger Helmer, Jolanta Emilia Hibner, Bernd Lange, Werner Langen, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Inês Cristina Zuber
A zárószavazáson jelen lévő póttag(ok) (187. cikk (2) bekezdés)	Anne E. Jensen, Nicole Kiil-Nielsen, Norica Nicolai