EURÓPAI PARLAMENT 2009 - 2014

Állampolgári Jogi, Bel- és Igazságügyi Bizottság

2011/2284(INI)

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

PA_NonLeg

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 ellenálló képesség 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.