Az Európai Gazdasági és Szociális Bizottság véleménye – A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A kritikus informatikai infrastruktúrák védelme – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”

(COM(2009) 149 végleges)

(2010/C 255/18)

Előadó: **Thomas McDONOGH**

2009. március 30-án az Európai Bizottság úgy határozott, hogy az Európai Közösséget létrehozó szerződés 262. cikke alapján kikéri az Európai Gazdasági és Szociális Bizottság véleményét a következő tárgyban:

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”

COM(2009) 149 végleges.

A bizottsági munka előkészítésével megbízott „Közlekedés, energia, infrastruktúra és információs társadalom” szekció 2009. november 12-én elfogadta véleményét. (Előadó: Thomas MCDONOGH.)

Az Európai Gazdasági és Szociális Bizottság 2009. december 16–17-én tartott, 458. plenáris ülésén (a december 16-i ülésnapon) 179 szavazattal, 4 tartózkodás mellett elfogadta az alábbi véleményt.

1. Következtetések és ajánlások

1.1 Az EGSZB üdvözli az Európai Bizottság által az európai kritikus informatikai infrastruktúrák (CII-k) védelmére irányuló cselekvési tervről kiadott közleményt. Ami Európa sérülékenységét illeti a nagyszabású kibertámadásokkal, a műszaki hibákkal, a szándékos támadásokkal, a természeti csapásokkal szemben, illetve ami a gazdaságát és polgárai jólétét fenyegető óriási károkat illeti, az EGSZB osztozik az Európai Bizottság aggodalmában. Egyetértünk az Európai Bizottsággal abban, hogy sürgős fellépésre van szükség az Unión belüli koordináció és együttműködés növeléséhez ennek a kritikus problémának a kezelése érdekében. Abban is egyetértünk, hogy rövid időn belül átfogó politikai keretet kell kialakítani a kritikus informatikai infrastruktúrák védelmére.

1.2 Az EGSZB tudomásul veszi a kritikus informatikai infrastruktúrák védelméről tartott uniós miniszteri konferencia következtetéseit, és riasztónak tartja, hogy Európa nincs kellően felkészülve arra, hogy helyt tudjon állni a nagyszabású kibertámadásokkal, illetve a kritikus informatikai infrastruktúrák üzemzavaraival szemben, mivel az egyes tagállamoknak a kritikus informatikai infrastruktúrák védelmére alkalmazott megközelítései gyakran nem egységesek, és nincsenek megfelelően összehangolva. Nem szorul magyarázatra, hogy az internet fejlődése és az informatikai infrastruktúrák biztonságát és ellenálló képességét illetően a nagy kiterjedésű rendszerekben való gondolkodás szemléletmódjának hiánya hogyan vezetett a mostani súlyos helyzethez. Most azonban, amikor nyilvánvalóvá vált, hogy cselekedni kell, az EGSZB arra szólítja fel az Európai Bizottságot, hogy határozottan és késedelem nélkül lépjen fel a probléma kezelése érdekében.

1.3 Az EGSZB támogatja a közleményben felvázolt, öt pillérre épülő cselekvési tervet, és gratulál az Európai Bizottság munkájához. Rendkívül nehéz ugyanis integrált, több érdekelt felet figyelembe vevő, többszintű megközelítést kialakítani a kritikus informatikai infrastruktúrák biztonságának és ellenálló képességének javítására, különösen akkor, ha az érdekelt felek körének széttagoltságát és az európai informatikai infrastruktúrák bonyolultságát is figyelembe vesszük. Az EGSZB ezenkívül elismeri az ENISA támogató szerepét és hozzájárulását a közlemény céljainak elérése érdekében.

1.4 Az EGSZB megjegyzi, hogy az érdekeltek nem tettek eleget annak érdekében, hogy megvalósítsák a 2007/C 68/01. sz. tanácsi állásfoglalásnak az IKT-infrastruktúrák biztonságáról és ellenálló képességéről szóló elemeit. [1] Az, hogy nem könnyű hatékony politikát kialakítani Európa legkritikusabb informatikai infrastruktúráinak védelmére, kapóra jön azoknak, akik politikai vagy pénzügyi okokból meg akarják támadni az ilyen kritikus infrastruktúrákat. Ezért az EGSZB azt szeretné, hogy a Európai Bizottság határozottabban vállalja azt az erős vezetői szerepet, amely az összes érdekelt fél összefogásához, valamint Európának a kritikus informatikai infrastruktúrákat fenyegető lehetséges veszélyekkel szembeni védelmére irányuló hatékony intézkedések végrehajtásához szükséges. Az EGSZB szerint a közleményben felvázolt cselekvési terv nem fogja meghozni a kívánt eredményeket, hacsak a végrehajtásának felelősségi körét rá nem bízzák egy megfelelő szabályozó hatóságra.

1.5 Az EGSZB felhívja az Európai Bizottság figyelmét korábbi véleményeire, amelyekben egy biztonságos információs társadalom szükségességéről, az internet biztonságával kapcsolatos aggályokról és a kritikus infrastruktúrák védelméről fejtette ki álláspontját.

[1] COM(2006) 251.

2. **Ajánlások**

2.1 Az Európai Uniónak egy megfelelő, az Alapjogi Ügynökség munkatársait is magában foglaló szabályozó hatóságot kellene megbíznia a kritikus informatikai infrastruktúrák hatékony védelemmel való ellátásának feladatával.

2.2 Minden tagállamnak nemzeti stratégiát kellene kidolgoznia, szilárd alapokon álló politikát és szabályozási környezetet kellene kialakítania, továbbá holisztikus nemzeti kockázatkezelési folyamatokat, valamint megfelelő felkészülési intézkedéseket és mechanizmusokat kellene bevezetnie. E tekintetben minden egyes tagállamnak számítástechnikai katasztrófaelhárító csoportot (CERT) kellene kialakítania, és azt fel kellene vetetnie az Európai Kormányzati CERT-ek Csoportjába (EGC). ([2])

2.3 Az Európai Bizottságnak fel kellene gyorsítania az ellenálló képesség javításáért felelős köz-magán partnerség (EP3R) létrehozásával kapcsolatos munkáját, és azt be kellene építenie az Európai Hálózat- és Információbiztonsági Ügynökségnek (ENISA), illetve az Európai Kormányzati CERT-ek Csoportjának (EGC) a munkájába.

2.4 A kockázatkezelés terén bevált legjobb gyakorlatoknak minden szinten jelen kellene lenniük a kritikus informatikai infrastruktúrák védelmére irányuló (CIIP-) politikában. Különösen igaz ez arra, hogy a biztonsági és ellenálló képességi hibák potenciális költségeit számszerűsíteni kellene és közölni az érintett felelősökkel.

2.5 Azokra az érintettekre, akik nem teljesítik a CIIP-politika által rájuk rótt feladataikat, a mulasztásuk miatt esetleg bekövetkező rendszerhiba kockázati szintjével és költségeivel arányos pénzbírságot és egyéb büntetéseket kellene kivetni.

2.6 A kritikus informatikai infrastruktúrák biztonságáért és ellenálló képességéért a legnagyobb felelősséget a legfontosabb érdekelt feleknek – a kormányoknak, az infrastruktúra üzemeltetőinek és a technológia szolgáltatóinak – kellene viselniük, és ők nem bújhatnának ki a felelősség alól azáltal, hogy azt a vállalati és magánfogyasztókra hárítják.

2.7 Minden, az EU-ban kivitelezett információs és kommunikációs technológiai (IKT-) rendszerbe már a tervezéskor kötelezően be kell építeni a biztonság és az ellenálló képesség szempontjait. Arra szeretnénk biztatni a kritikus informatikai infrastruktúrák védelmében érintett magánszférabeli feleket, hogy szüntelenül egyre nagyobb tökéletességre törekedjenek az ellenálló képességhez kötődő egyes konkrét területeken – pl. a hálózatkezelés, a kockázatkezelés, illetve az üzleti folytonosság területén.

2.7.1 A legjobb gyakorlatok és szabványok kialakításának és politikai meghatározásának a hibamegelőzéssel, a helyzeti reagálási intézkedésekkel és a kritikus informatikai infrastruktúrák helyreállításával foglalkozó valamennyi politika szerves részét kellene képeznie.

2.7.2 Az internet biztonságának javítása érdekében az EU internethálózatában mindenütt elsődleges figyelmet kellene fordítani az IPv6 (az internetcímek legkorszerűbb protokollja) és a DNSSEC (az internetes tartománynév-rendszer biztonsági javításainak csomagja) megvalósítására.

2.8 Arra biztatjuk az állami és magánszférabeli érdekelteket, hogy rendszeresen működjenek együtt és tartsanak közös gyakorlatokat a felkészültségük és a reagálási intézkedéseik tesztelése érdekében. Teljes mértékben támogatjuk az Európai Bizottság közleményében foglalt, 2010 végéig egy egész Európára kiterjedő gyakorlat lebonyolítására irányuló javaslatot.

2.9 Európában elő kellene segíteni egy erős információbiztonsági iparág kialakítását, hogy felzárkózhassunk az Egyesült Államok gazdagon finanszírozott iparágának kompetenciája mellé. A kritikus informatikai infrastruktúrák védelmével kapcsolatos kutatási és fejlesztési beruházásokat jelentősen fokozni kellene.

2.10 A kiberbiztonság területén a készségfejlesztési, valamint a tudás- és tudatossági programok finanszírozását növelni kellene.

2.11 Információs és támogatási ügynökségeket kellene létrehozni minden tagállamban, hogy a kkv-k és a polgárok megérthessék és teljesíthessék a CIIP-politika terén rájuk háruló feladatokat.

2.12 A biztonság érdekében az EU-nak tovább kellene erősítenie az internet jövőbeli szabályozására vonatkozó álláspontját, ([3]) mely szerint olyan, még több oldalú megközelítésre van szükség, amely az Egyesült Államok nemzeti prioritásait is tiszteletben tartja, ám egyben az Európai Unió érdekeit is tükrözi. Az Uniónak a kérdéssel kapcsolatos fellépése során alaposan tanulmányoznia kell a kiberbiztonság, valamint a polgári és az egyéni szabadságjogok tiszteletben tartása közti kapcsolatokat.

3. **Háttér**

3.1 A kritikus informatikai infrastruktúrákat fenyegető nagyszabású kibertámadások veszélye

3.1.1 Kritikus informatikai infrastruktúrák (CII) alatt azokat az információs és kommunikációs technológiákat (IKT) értjük, amelyek az alapvető áruk és szolgáltatások – ideértve a létfontosságú társadalmi szükségleteket: az áram- és vízellátást, a közlekedést, a banki, az egészségügyi és a segélykérési szolgáltatásokat is – biztosításához szükséges információs és kommunikációs alapot nyújtják.

3.1.2 A CII-ket magas fokú, komplex rendszerintegráció, más infrastruktúráktól (például az elektromos hálózattól) való kölcsönös függés, valamint a hálózatok határokat átszelő kiterjedése jellemzi. Ezek az aprólékosan kidolgozott infrastruktúrák számos veszélynek vannak kitéve, amelyek olyan katasztrofális rendszerhibákhoz vezethetnek, amelyek több tagállamban is kihathatnak a kritikus társadalmi szükségletek ellátására. Veszélyforrás lehet az emberi tévedés, a műszaki hiba, a szándékos támadás (ideértve a bűnelkövetési és a politikai szándékú támadásokat is), valamint a természeti csapások. A kockázatelemzés rávilágít az ilyen rendszerek hiányosságaira, és egyben feltárja, hogy a rendszer felett a polgári és az egyéni szabadságjogokat sértő gyakorlatokkal át lehet venni az irányítást – függetlenül attól, hogy ezek szándékosak-e. Az Európai Bizottságnak kötelessége biztosítani, hogy a közösségi jogszabályok kidolgozása során tiszteletben tartsák az alapvető jogokat.

([2]) http://www.egc-group.org.

([3]) COM(2009) 277 végleges.

3.1.3 A kormányok és a létfontosságú szolgáltatások nyújtói nem hozzák nyilvánosságra a biztonság és az ellenálló képesség terén felmerülő hibákat, hacsak nem kényszerülnek rá. Még így is számos nyilvánosságra került példát találhatunk a kritikus informatikai infrastruktúrák biztonsági és ellenálló képességi hibáiból eredő veszélyekre:

– Észtországban, Litvániában és Grúziában 2007-ben és 2008-ban nagyszabású kibertámadások történtek.

– A földközi-tengeri és a Perzsa-öbölben található, földrészeket összekötő mélytengeri adatkábelek elszakadása 2008-ban több országban is fennakadásokat eredményezett az internetes forgalomban.

– 2009 áprilisában az Egyesült Államok nemzetbiztonsági tisztviselői arról számoltak be, hogy „kiberkémek" hatoltak be az ország elektromos hálózatába, és olyan szoftvereket hagytak hátra, amelyekkel zavart kelthetnek a rendszerben.

– Júliusban az Egyesült Államoknak és Dél-Koreának igen széles körű „szolgáltatásbénító" (*Denial of Service*) támadással kellett szembenézniük (a támadók 100-200 ezer személyi számítógépet használtak „zombiként"), amely számos kormányzati weboldal ellen irányult.

3.1.4 A problémát csak súlyosbítja a bűnbandák ártó szándéka és a politikai célú kiberhadviselés.

– A bűnbandák az internethez kapcsolt személyi számítógépek operációs rendszereiben felfedezett biztonsági rések kihasználásával úgynevezett *botneteket* (robothálózatot) alakítanak ki, azaz az egyes számítógépeket rosszindulatú szoftverek (*malware*) segítségével egyetlen, a bűnözők irányítása alatt álló hatalmas virtuális számítógéppé szervezik (akárcsak egy „zombi-" vagy távirányításúrobot-hadsereget). Az ilyen *botneteket* azután különböző illegális tevékenységekre használják, illetve a kiberhadviselést folytató terroristák és kormányok „bérbe veszik" a *botneteket* a bűnözőktől, hogy segítségükkel indítsanak nagyszabású kibertámadásokat. Sejtések szerint egy „Conficker" nevű *botnet* már több mint 5 millió személyi számítógépet vont irányítása alá.

3.1.5 A kritikus informatikai infrastruktúrák hibáinak gazdasági költsége rendkívül magas lehet. A Világgazdasági Fórum becslése szerint 10-20 % az esélye annak, hogy az elkövetkező tíz évben jelentős üzemzavar keletkezik a kritikus informatikai infrastruktúrákban, amely – ha bekövetkezik – világszinten körülbelül 250 milliárd dollár kárt okozna a gazdaságnak, és több ezer emberéletet követelne.

3.2 A felkészültség, a biztonság és az ellenálló képesség problémája

3.2.1 Európa kritikus informatikai infrastruktúráinak jelentős része elsősorban az internetre támaszkodik. Az internet architektúrájának alapja az, hogy több millió számítógép kapcsolódik össze, és ebben a hálózatban a feldolgozás, a kommunikáció és a vezérlés világszerte eloszlik. Ez az elosztott architektúra kulcsfontosságú ahhoz, hogy az internet stabil és ellenálló legyen, és probléma esetén gyorsan helyre tudjon állni az adatforgalom. Azonban ez azzal is jár, hogy bármely huligán, akinek szándékában áll és rendelkezik a megfelelő alapismeretekkel, nagyszabású virtuális támadást indíthat a hálózat széléről, például *botnetek* segítségével.

3.2.2 A globális kommunikációs hálózatok és a kritikus informatikai infrastruktúrák igen sok országot kapcsolnak össze. Ez azt jelenti, hogy ha egy országban alacsony a hálózati biztonság és ellenálló képesség szintje, az a vele összekapcsolt összes országban a kritikus informatikai infrastruktúrák biztonságát és ellenálló képességét hátrányosan érintheti. Emiatt a kölcsönös nemzetközi függés miatt az EU-ra hárul az a feladat, hogy integrált politikát dolgozzon ki a kritikus informatikai infrastruktúrák biztonságának és ellenálló képességének kezelésére Unió-szerte.

3.2.3 A kritikus informatikai infrastruktúrákat fenyegető veszélyekről a legtöbb érdekelt fél és számos tagállam igen keveset tud, és nincs is velük tisztában. Az effajta veszélyek kezelésére csak igen kevés ország alkalmaz átfogó politikát.

3.2.4 Az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások keretszabályozásának javasolt átalakítása fokozná a hálózatüzemeltetők azon felelősségét, hogy tegyék meg a szükséges lépéseket a kockázatok feltárására, a szolgáltatásnyújtás folytonosságának biztosítására és a biztonság megsértésének eseteiről való értesítésre. [4]

3.2.5 A kritikus informatikai infrastruktúrák alapját képező technológiák túlnyomó többségét a magánszféra biztosítja, emiatt a CII-k hatékony védelmének biztosítására szolgáló megfelelő együttműködés minden érdekelt fél – kormányok, üzleti vállalkozások és fogyasztók – részéről magas szintű hozzáértést, bizalmat, átláthatóságot és kommunikációt kíván meg.

3.2.6 Több érdekelt felet figyelembe vevő, többszintű, nemzetközi megközelítésre van tehát mindenképpen szükség.

3.3 Öt pillérre épülő cselekvési terv

A kihívások leküzdésére az Európai Bizottság egy öt pillérre épülő cselekvési tervet javasol:

1. felkészülés és megelőzés: készültség biztosítása minden szinten;

2. észlelés és reagálás: megfelelő korai figyelmeztető mechanizmusok felállítása;

3. a hatások enyhítése és helyreállítás: a kritikus informatikai infrastruktúrák védelmére szolgáló uniós védekező mechanizmusok megerősítése;

4. nemzetközi együttműködés: a közösségi prioritások nemzetközi szinten való képviselete;

5. az IKT-ágazatra vonatkozó kritériumok: támogatás nyújtása az európai kritikus infrastruktúrák azonosításáról és kijelöléséről szóló irányelv [5] végrehajtásához.

[4] A COM(2007) 697 (végleges) sz. dokumentum 13a. és 13b. cikke a 2002/21/EK irányelv módosítására tesz javaslatot.

[5] A Tanács 2008/114/EK irányelve.

A fenti címek mindegyikéhez külön célkitűzések és céldátumok tartoznak; némelyik feladat egészen 2011 végéig eltart majd.

4. **Észrevételek**

4.1 A közleményben felvázolt erősen konzultatív, önkéntes alapú és együttműködésre épülő megközelítés alapján nagyon nehéz lesz hatékony stratégiát kialakítani és megvalósítani a kritikus informatikai infrastruktúrák védelmére. A feladat komolyságára és sürgősségére való tekintettel az EGSZB azt ajánlja, hogy az Európai Bizottság vizsgálja meg az Egyesült Királyságban és az Egyesült Államokban alkalmazott politikát, amely egy megfelelő szabályozó hatóságot ruház fel felelősségi és jogkörökkel.

4.2 Az EGSZB egyetért az ENSZ Közgyűlésének 58/199. sz. határozatában foglalt felhívással, amely szerint szükséges *A kibervédelem globális kultúrájának megteremtése és a kritikus informatikai infrastruktúrák védelme*. Tekintettel arra, hogy a kritikus informatikai infrastruktúrák biztonsága és ellenálló képessége szempontjából az országok kölcsönösen függnek egymástól – ahogyan egy lánc is csak annyira erős, amennyire a leggyengébb láncszeme –, aggodalomra adhat okot, hogy mindeddig csupán 9 tagállam alakított ki számítástechnikai katasztrófaelhárító csoportot (CERT) és lépett be az Európai Kormányzati CERT-ek Csoportjába (EGC). Ezeknek a csoportoknak a létrehozásával kiemeltebb helyen kell foglalkozni a kormányközi napirendben.

4.3 Az EU hálózati biztonsága minden olyan polgárt érint, akinek az élete esetleg a létfontosságú szolgáltatásoktól függhet. Ugyanezekre a polgárokra hárul annak felelőssége, hogy képességükhöz mérten a lehető legjobban megvédjék internetkapcsolatukat a támadásoktól. Még nagyobb felelősség nehezedik a kritikus informatikai infrastruktúrák alapját képező információs és kommunikációs technológiák és szolgáltatások nyújtóira. Elengedhetetlenül fontos, hogy minden érintett fél kellően tájékozott legyen a kiberbiztonsággal kapcsolatban. Az is fontos, hogy Európa kellő számú szakemberrel rendelkezzen a biztonság és az IKT-k ellenálló képessége terén.

4.4 Az EGSZB azt ajánlja, hogy minden tagállamban állítsanak fel egy olyan szervezetet, amelynek az lenne a feladata, hogy tájékoztassa, oktassa és támogassa a kis- és középvállalkozói szektort a hálózati biztonság területén. A nagy vállalatok könnyen hozzájuthatnak a szükséges ismeretekhez, de a kkv-k támogatásra szorulnak.

4.5 Mivel a kritikus informatikai infrastruktúrák biztosítása többnyire a magánszektor kezében van, fontos, hogy a kritikus informatikai infrastruktúrákért felelős minden cég hozzájáruljon a bizalom és az együttműködés magas szintjének eléréséhez. Az Európai Bizottság által júniusban útnak indított EP3R kezdeményezés dicséretes és ösztönzendő. Az EGSZB azonban úgy véli, hogy a kezdeményezést jogszabályokkal is támogatni kell annak érdekében, hogy azokat az érdekelt feleket is együttműködésre lehessen bírni, akik nem látják el felelősségteljesen az ezzel járó feladataikat.

4.6 A kockázatkezelés tudományága segít választ adni az ebben a dokumentumban tárgyalt problémafajtákra. Az Európai Bizottságnak meg kellene követelnie, hogy ahol csak lehetséges, a cselekvési tervben kövessék a kockázatkezelés terén bevált legjobb gyakorlatokat. Különösen hasznos a hibák veszélyforrásait és költségeit számszerűsíteni a kritikus informatikai infrastruktúrák minden szintjén. Ha ismerjük a hiba valószínűségét és várható költségeit, könnyebben lehet cselekvésre ösztönözni az érintett feleket. Könnyebb továbbá pénzügyi felelősséget róni rájuk arra az esetre nézve, ha elmulasztják kötelességeik teljesítését.

4.7 A befolyásos érdekeltek igyekeznek jogi felelősségüket oly módon korlátozni, hogy piaci erejük kihasználásával arra kényszerítik fogyasztóikat, illetve beszállítóikat, hogy olyan feltételeket fogadjanak el, amelyek a nagyvállalatot mentesítik saját felelősségeik alól – példaként említhetjük az olyan szoftverlicenc-megállapodásokat vagy internetszolgáltatói hálózat-összekapcsolási megállapodásokat, amelyek biztonsági ügyekben korlátozzák a cég jogi felelősségét. Az ilyen megállapodásokat jogszerűtlennek kellene minősíteni, és a felelősség terhét a nagyvállalatnak kellene viselnie.

4.8 A biztonság és az ellenálló képesség szempontjait minden IKT-hálózat esetében figyelembe lehet és kell is venni a tervezéskor. Elsősorban a hálózati architektúrák topológiáját kellene szemügyre venni a tagállamokban és az EU egészében, és megállapítani, hogy hol koncentrálódik elfogadhatatlan mértékben a kommunikációs forgalom, és a hálózat mely pontjain a legnagyobb a hiba esélye. Például egyes tagállamokban igen kevés internetcsatlakozási pontban (*Internet Exchange Point, IXP*) sűrűsödik az internetforgalom, ami elfogadhatatlan veszélyforrást jelent.

4.9 Az EGSZB felhívja az Európai Bizottság figyelmét a COM(2008) 313 végleges jelű dokumentumról – Az *internet fejlesztése: cselekvési terv az internetprotokoll 6-os verziójának (IPv6) európai alkalmazására* – készített véleményében [6] megfogalmazott megjegyzésekre is, amelyek az IPv6 protokollnak az EU teljes internethálózatán való alkalmazásával járó biztonsági előnyöket emelik ki. Azt ajánljuk továbbá, hogy az internet biztonságának növelése érdekében, ahol csak lehetséges, alkalmazzák a DNSSEC-technológiákat.

4.10 Az Egyesült Államok útnak indította a kibertér biztonságára irányuló politikáját, amelynek révén a költségvetés 2009-ben és 2010-ben 40 milliárd dollárt különített el hálózatbiztonsági célokra. Ez a biztonsági ágazat számára óriási mennyiségű forrást jelent, emiatt valószínűleg számos, az informatikai biztonság terén tevékenykedő cég – köztük európaiak is – az Egyesült Államokra összpontosítják majd erőfeszítéseiket. Ez ahhoz is hozzájárul majd, hogy az Egyesült Államok biztonsági vállalatai világelsők legyenek. Nagyon nagy előnyt jelentene, ha Európának is olyan élvonalbeli ipara lenne, amely versenyre kelhet az amerikai cégekkel, valamint ha a biztonsági ágazat kellő erőfeszítést befektetve megfelelően összpontosítana Európa infrastrukturális szükségleteire. Az EGSZB arra kéri az Európai Bizottságot, hogy gondolkodjon el azon, miként tudna az Egyesült Államok által biztosított hatalmas mennyiségű anyagi forrással egyenértékű ösztönzést nyújtani.

[6] HL C 175., 2009.7.28., 92. o.,

4.11 Az EGSZB támogatja az Európai Bizottság nemrégiben közzétett, az internet szabályozásának következő lépéseiről szóló közleményét. (7) Az EGSZB úgy véli, hogy az EU-nak közvetlenebb befolyása kellene, hogy legyen az ICANN (a kijelölt internetes neveket és azonosítószámokat nyilvántartó vállalat) és az IANA (a kijelölt internetes azonosítószámokat felügyelő hatóság) politikájára és gyakorlataira, és az Egyesült Államok által gyakorolt jelenlegi egyoldalú felügyeletet többoldalú, nemzetközi felelősségi köröket létrehozó megállapodásokkal kellene felváltani.

Kelt Brüsszelben, 2009. december 16-án.

az Európai Gazdasági és Szociális Bizottság elnöke

Mario SEPI

(7) COM(2009) 277 végleges.