Európai Gazdasági és Szociális Bizottság vélemény – Tárgy: „A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A biztonságos információs társadalomra irányuló stratégia: »párbeszéd, partnerség, felvértezés és felelősségvállalás«"

COM(2006) 251 final

(2007/C 97/09)

2006. május 31-én az Európai Bizottság úgy határozott, hogy az Európai Közösséget létrehozó szerződés 262. cikke alapján kikéri az Európai Gazdasági és Szociális Bizottság véleményét a fenti tárgyban.

A bizottsági munka előkészítésével megbízott „Közlekedés, energia, infrastruktúra és információs társadalom" szekció véleményét 2007. január 11-én elfogadta. (Előadó: Antonello PEZZINI)

Az Európai Gazdasági és Szociális Bizottság 2007. február 16-án tartott 433. plenáris ülésén 132 szavazattal, ellenszavazat nélkül, 2 tartózkodás mellett elfogadta az alábbi véleményt.

1. **Következtetések és ajánlások**

1.1 Az Európai Gazdasági és Szociális Bizottság meg van győződve arról, hogy az információs biztonság kérdése egyre inkább aggasztóvá válik a vállalatok, a közigazgatás, az állami és a magánszervek, valamint a polgárok számára.

1.2 Az Európai Gazdasági és Szociális Bizottság általánosságban egyetért a helyzet elemzésével, valamint azon érvekkel, amelyek szerint a hálózati és az információs biztonságot növelni hivatott új stratégia kialakítása szükséges. Mindezt a rendszerek elleni támadások és az azokba való behatolások indokolják, amelyek a földrajzi helyzettől függetlenül bekövetkeznek.

1.3 Az EGSZB úgy véli, hogy – tekintettel a jelenség elterjedtségére és gazdasági téren, valamint a magánéletben megnyilvánuló következményeire – az Európai Bizottságnak további erőfeszítéseket kellene tennie egy innovatív és jól kidolgozott stratégia kialakítása érdekében.

1.3.1 Az EGSZB kiemeli, hogy az Európai Bizottság a közelmúltban új közleményt bocsátott ki az informatikai biztonságról, és rövid időn belül ugyanezen tárgyban újabb dokumentum közlése várható. Az EGSZB fenntartja magának a jogot, hogy a jövőben részletesebb, a hírközlés egészét szem előtt tartó véleményben fejtse ki álláspontját.

1.4 Az EGSZB hangsúlyozza: az informatikai biztonság szempontja semmiféleképp nem választható el a személyi adatok védelmének megerősítésétől és az Emberi Jogok Európai Egyezményében rögzített szabadságjogok védelmétől.

1.5 Az EGSZB felveti a kérdést: mi a jelenlegi helyzetben a javaslat hozzáadott értéke a 2001-ben elfogadott megközelítéshez képest, amelynek célja megegyezett a jelen közleményben szereplő célkitűzéssel ([1]).

1.5.1 A javaslathoz csatolt hatástanulmány ([2]) tartalmaz néhány figyelemreméltó újszerű szempontot a 2001-es állásponthoz képest, de mivel mindössze egy nyelven áll rendelkezésre, nem hozzáférhető sok európai polgár számára, akik véleményüket a minden hivatalos nyelven rendelkezésre álló dokumentum alapján alakítják ki.

1.6 Az EGSZB utal a 2005-ben Tuniszban az információs társadalommal kapcsolatosan megrendezett nemzetközi csúcsértekezleten elfogadott és az ENSZ-közgyűlés által 2006. március 27-én aláírt alábbi következtetésekre:

– megkülönböztetésmentes hozzáférés,

– az IKT népszerűsítése a béke megteremtésének/fenntartásának eszközeként,

– a demokrácia, a kohézió és a jó kormányzás erősítését szolgáló eszközök meghatározása,

– a visszaélések megelőzése, az emberi jogok tiszteletben tartásával ([3]).

1.7 Az EGSZB kiemeli, hogy a lendületes és integrált közösségi stratégiának a párbeszéden, a partnerségen és a felelősségvállaláson túl a következőkre is ki kell terjednie:

– megelőző intézkedések,

– az informatikai biztonságról az informatikai biztosításra való átmenet ([4]),

– közösségi szintű, biztos és elismert jogszabályi keret létrehozása, amely szankciókról is rendelkezik,

– a műszaki szabványosítás megerősítése,

([1]) Lásd az EGSZB véleményét a következő tárgyban: „A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a hálózatok és az információ biztonságáról – Javaslat európai politikai megközelítésre" (HL C 48., 2002.2.21., 33. o.).

([2]) A „hatástanulmány" nem bír ugyanolyan értékkel, mint egy „stratégiai dokumentum".

([3]) Az ENSZ 2006.3.27-i 57. és 58. számú ajánlása. Tunis Final Document, 15. szám.

([4]) Lásd: „*Emerging technologies in the context of security*", Közösségi Kutatóközpont (JRC) – Állampolgár-védelmi és Biztonsági Intézet (IPSC), stratégiai kutatási füzet, 2005. szeptember, Európai Bizottság, http://serac.jrc.it.

– a felhasználók digitális azonosítása,

– az informatikai biztonságra irányuló európai elemzési és előrejelzési (*Foresight*) gyakorlatok létrehozása, multimodális technológiai konvergenciafeltételek között,

– az európai és a nemzeti kockázatértékelési mechanizmusok megerősítése,

– az informatikai monokultúrák kialakulásának megakadályozását célzó intézkedések,

– a közösségi koordináció megerősítése európai és nemzetközi szinten egyaránt,

– a Főigazgatóságok között működő IKT *Security Focal Point* létrehozása,

– a *European Network and Information Security Network* létrehozása,

– az informatikai biztonságra irányuló európai kutatás szerepének optimalizálása,

– az „Informatikai Biztonság Európai Napjának" létrehozása,

– a különböző szintű oktatási intézményekben közösségi kísérleti projektek beindítása az informatikai biztonsággal összefüggő témákról.

1.8 Végezetül az EGSZB úgy véli, hogy a lendületes és integrált közösségi stratégiához megfelelő költségvetési forrásokat kell előirányozni, egy ilyen stratégiához pedig közösségi szintű kezdeményezések és megerősített koordinációs intézkedések kell, hogy társuljanak: ezek teszik lehetővé Európa egységes fellépését a nemzetközi környezetben.

2. **Indokolás**

2.1 Az információs társadalom biztonsága alapvető kihívás, amikor a kommunikációs hálózatokba és szolgáltatásokba vetett bizalomról, illetve azok megbízhatóságának biztosításáról van szó, ezek ugyanis kritikus tényezőt jelentenek a gazdaság és a társadalom fejlődése szempontjából.

2.2 Az informatikai rendszereknek és hálózatoknak védelemre van szükségük versenyképességük és kereskedelmi potenciáljuk fenntartásához, az elektronikus hírközlés integritásának és folytonosságának biztosításához, valamint a csalások megelőzéséhez és a magánélet törvényes védelméhez.

2.3 Az elektronikus hírközlés és a hozzá kapcsolódó szolgáltatások a távközlési ágazat legnagyobb szegmensét képviselik: 2004-ben az európai vállalatok körülbelül 90 %-a használta aktívan az internetet, 65 %-uk pedig saját weboldalt alakított ki, míg becslések szerint az európai népesség körülbelül fele használja rendszeresen az internetet, a családok 25 %-a pedig állandó jelleggel használja a széles sávú hozzáférést ([5]).

2.4 A beruházások gyors fejlődéséhez képest a biztonságra fordított kiadások az információs technológiákba való összes befektetés mindössze 5-13 %-át képviselik. Ez az arány túlságosan csekély. A közelmúltban készült tanulmányok kimutatták, hogy abból a 30 protokollból, amelyen a kulcsstruktúrák osztoznak, 23 érzékeny a „multiprotokoll" jellegű támadásokkal szemben ([6]). Ezenkívül a becslések szerint naponta átlagosan 25 millió kéretlen elektronikus üzenet (*spam*) ([7]) küldésére kerül sor. Ezért az EGSZB üdvözli az Európai Bizottság nemrégiben benyújtott javaslatát e tárggyal kapcsolatosan.

2.5 A számítógépes vírusok területén ([8]) a „*worms*" ([9]) és a „*spyware*" ([10]) kategóriájába tartozó vírusok egész világon való gyors terjedése párhuzamosan haladt az elektronikus hírközlési rendszerek és hálózatok egyre intenzívebb fejlődésével. E rendszerek és hálózatok egyre összetettebbé, ugyanakkor egyre sérülékenyebbé váltak, többek között a multimédia és a mobiltelefon-hálózatok, valamint a *GRID infoware* rendszerek ([11]) konvergenciája miatt: a zsarolási esetek, a DdoS (*Distributed denials of service*), az online személyazonosság-lopás, a *phishing* ([12]), a *piracy* ([13]) stb. hasonló kihívást jelentenek az információs társadalom számára. Az Európai Közösség már foglalkozott ezzel a problémával egy 2001-es közleményében ([14]), amivel kapcsolatban az EGSZB már kifejtette véleményét ([15]), most pedig egy három intézkedéssorozaton nyugvó stratégiát javasol:

– specifikus biztonsági intézkedések,

([5]) *i2010: Stratégia a biztonságos információs társadalomért*. Információs Társadalom és Média Főigazgatóság, „Factsheet 8" (2006. június) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-en.pdf.

([6]) *Proceedings of the First International Conference on Availability, Reliability and Security* (ARES'06) – Kötet: 00 ARES 2006, Kiadó: IEEE Computer Society.

([7]) *Spam* = Kéretlen, kereskedelmi jellegű elektronikus levél. A *spam* szó eredeti jelentése „spiced pork and ham" (fűszeres sertéshús és sonka), ami a második világháború idején közkedvelt húskonzerv volt. Ebben az időben ez az étel jelentette az USA hadserege és az angolok egyik fő élelmiszerforrását, mivel nem élelmiszerjegyre adták. Miután az emberek hosszú évekig ezen az ételen éltek, elegük lett a „spamból" – a szó negatív jelentéstartalmat kapott.

([8]) *Számítógépes vírus*: a rosszindulatú szoftverekhez (malware) tartozó szoftvertípus, amely – általában anélkül, hogy a felhasználó felfedezné – képes megfertőzni a fájlokat, oly módon, hogy önmagáról készített másolatok révén reprodukálódik. A vírusok kisebb-nagyobb mértékben károsíthatják azt az operációs rendszert, amelybe behatoltak, de még a legjobb esetben is az erőforrások bizonyos mértékű pazarlásához vezetnek a RAM, a CPU és a merevlemez tárterülete vonatkozásában.
http://hu.wikipedia.org/wiki/Sz %C3 %A1m %C3 %ADt %C3 % B3g %C3 %A9pes_v %C3 %ADrus.

([9]) *Worm* (féreg) = önmaga másolására képes rosszindulatú szoftver. Az „*email worm*" a hálózatot megbénító támadás, amely abban áll, hogy összegyűjti egy helyi programban (például MS Outlook) szereplő valamennyi e-mail címet, majd e címekre százával küldi a láthatatlan mellékletként csatolt, ugyanezen „férget" tartalmazó e-maileket.

([10]) *Spyware* (kémprogram) = a felhasználó által látogatott oldalak nyomát követő szoftverprogramok, amelyek saját magukat installálják, a felhasználó értesítése, tudta, beleegyezése és ellenőrzése nélkül.

([11]) *GRID infoware* = lehetővé teszi számos, földrajzilag különböző helyen lévő számítógép-erőforrás megosztását, kiválasztását és összefogását (például szuperkomputerek, számítógép-klaszterek, tárolórendszerek, adatforrások, eszközök és emberi erőforrások), és mindezt egyetlen, egységes erőforrásként jeleníti meg, amely képes rendkívül bonyolult számítások megoldására, valamint rendkívül adatintenzív alkalmazásokra.

([12]) *Phishing* = informatikai berkekben „*phishing*"-nek (adathalászat) nevezik azt a *cracking* technikát, amely a személyi és titkos adatokhoz való hozzáférés megszerzésére irányul, célja pedig a személyazonosság-lopás. Mindez hamis elektronikus levelek küldésével történik, amelyeket úgy alakítanak ki, hogy hitelesnek tűnjenek.

([13]) *Piracy* = a számítógépes „kalózok" által használt fogalom egy olyan szoftver megnevezésére, amelyből eltávolították a másolásvédelmet, és amely az interneten való letöltés révén bárki rendelkezésére áll.

([14]) COM(2001) 298 final.

([15]) Lásd az 1. lábjegyzetet.

– jogszabályi keret, beleértve a személyi adatok és a magánélet védelmét,

– a számítógépes bűnözés elleni küzdelem.

2.6 Az információs technológiára (IT) irányuló támadások észlelése, azonosítása és megelőzése egy hálózati rendszeren belül kihívás a megfelelő megoldások felkutatása szempontjából, mivel a konfigurációk szüntelenül változnak, a hálózati protokollok, valamint a kínált és a kifejlesztett szolgáltatások sokszínűek, az aszinkron támadási formák pedig rendkívül összetettek ([16]).

2.7 Sajnos azonban a biztonságot szolgáló beruházások megtérülése aligha szemmel látható, a polgárok (felhasználók) magatartása pedig nem elég felelősségteljes. Mindez a kockázatok alábecsüléséhez és a biztonsági kultúra fejlesztésére fordított figyelem csökkenéséhez vezetett.

3. **Az európai bizottsági javaslat**

3.1 A biztonságos információs társadalomra irányuló stratégiáról szóló közleménnyel ([17]) az Európai Bizottság célja az informatikai biztonság javítása volt. Ehhez lendületes és integrált stratégiát alakított ki, amely az alábbiakra épül:

a) a hatóságok és az Európai Bizottság közötti párbeszéd javítása, a nemzeti szakpolitikák összehasonlító értékelésével, valamint az elektronikus kommunikáció biztonsági területen leghatékonyabb eljárásainak azonosításával;

b) a polgárok és a kkv-k tudatosságának fokozása a hatékony biztonsági rendszerek vonatkozásában. Ennek során ösztönző, aktív szerep jut az Európai Bizottságnak, és fokozottabban be kell vonni az Európai Hálózati és Információs Biztonsági Ügynökséget (ENISA);

c) párbeszéd az eszközök és a normák vonatkozásában, a biztonság és az alapjogok (beleértve a magánélet védelmét) közötti kiegyensúlyozott viszony érdekében.

3.2 A közlemény ezenkívül – tekintettel a biztonság megsértésével, a felhasználók bizalmi szintjével és az IKT biztonsági ipar fejleményeivel kapcsolatos adatgyűjtés megfelelő keretének tervezett kialakítására – bizalmi partnerség kialakítását irányozta elő az ENISA és az alábbiak között:

a) a tagállamok,

b) a fogyasztók és a felhasználók,

c) az informatikai biztonsági ipar,

d) a magánszektor.

Mindehhez többnyelvű közösségi portált hoznak létre, amely tájékoztat és figyelmeztet a veszélyekre, a magánszektor, a tagállamok és a kutatók közötti stratégiai partnerség létrehozása céljából.

3.2.1 A közleményben szerepel továbbá az érdekeltek felelősségvállalásának növelése a biztonsággal kapcsolatos szükségleteket és kockázatokat illetően.

3.2.2 A nemzetközi és a harmadik országokkal való együttműködés vonatkozásában a „hálózati és információs biztonság globális dimenziója arra készteti az Európai Bizottságot – mind nemzetközi szinten, mind a tagállamokkal együttműködve –, hogy növelje a globális együttműködés előmozdítására irányuló erőfeszítéseit" ([18]). Ez a javaslat azonban nem jelenik meg ismét a párbeszédre, a partnerségre és a felelősségvállalásra vonatkozó intézkedésekben.

4. **Megjegyzések**

4.1 Az EGSZB egyetért a hálózati és információs biztonság integrált és lendületes európai stratégiájának kialakítását indokoló elemzésekkel és érvekkel, mivel alapvető jelentőségűnek tartja a biztonság kérdését az információs technológiák alkalmazásának ösztönzése, valamint a beléjük vetett bizalom növelése vonatkozásában. Az EGSZB egyébként már számos véleményben ([19]) kifejtette ezzel kapcsolatos álláspontját.

4.1.1 Az EGSZB ismételten felhívja a figyelmet ([20]) arra, hogy „az Internet és az on-line kommunikáció új technológiái (például a mobiltelefonok és a multimédia-funkcióval bíró, hálózatra csatlakoztatható PDA-készülékek, melyek komoly piaci sikereket érnek el) a tudásalapú gazdaság, az e-gazdaság és az e-közigazgatás fejlődésének alapvető eszközei".

([16]) Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* – 2005 USA, Arizona
Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc
Mazin Yousif, Intel Corporation, USA – Részben az Intel Corporation IT R&D Council által finanszírozott munka.

([17]) COM(251) 2006, 2006.5.31.

([18]) Lásd a COM(2006) 251 dokumentum 3. fejezetének utolsó előtti bekezdését.

([19]) Lásd az alábbi dokumentumokat:
– Az EGSZB véleménye a következő tárgyban: *„Javaslat európai parlamenti és tanácsi irányelvre a nyilvános elektronikus hírközlési szolgáltatások nyújtása keretében feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról"* (HL C 69., 2006.3.21., 16. o.),
– Az EGSZB véleménye a következő tárgyban: *„A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának i2010: európai információs társadalom a növekedésért és a foglalkoztatásért"* (HL C 110., 2006.5.9., 83. o.),
– Az EGSZB véleménye a következő tárgyban: *„Javaslat európai parlamenti és tanácsi határozatra az Internet és az új on-line technológiák biztonságosabb használatának előmozdítását célzó többéves közösségi program létrehozásáról"* (HL C 157., 2005.6.28., 136. o.),
– Az EGSZB véleménye a következő tárgyban: *„A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Hálózati és információs biztonság: európai stratégiai megközelítés kialakítására irányuló javaslat"* (HL C 48., 2002.2.21., 33. o.).

([20]) Lásd 19. lábjegyzet, 3. pont.

4.2 *Az ambiciózusabb európai bizottsági javaslatokért*

4.2.1 Az EGSZB úgy véli, hogy az Európai Bizottság által javasolt megközelítésmód – amelynek lényege, hogy ezen integrált és dinamikus stratégiát egy nyílt és befogadó jellegű párbeszédre építi, amelyhez a valamennyi érdekelttel, főként a felhasználókkal való megerősített partnerség és felelősségvállalás társul – tovább bővíthető.

4.2.2 Ezt az álláspontot már korábbi véleményeinkben is kiemeltük: „Ahhoz, hogy hatékony legyen, ennek az összevetésnek valamennyi internethasználót be kell vonnia, akiket ki kell képezni és tájékoztatni kell az alkalmazandó megelőzési intézkedésekről, valamint azon eszközökről, amelyekkel előre fel lehet készülni a káros vagy nem kívánt tartalmak fogadásának elkerülésére, vagy annak megakadályozására, hogy valaki akaratán kívül e tartalmak közvetítőjévé váljon. Az EGSZB véleménye szerint szükséges, hogy a program képzésre és a tájékoztatásra irányuló része abszolút prioritást biztosítson a felhasználók bevonásának” ([21]).

4.2.3 Az EGSZB véleménye szerint azonban a felhasználók és a polgárok bevonásának úgy kell történnie, hogy az információ és a hálózatok szükséges védelme összhangban legyen a polgári szabadságjogokkal, valamint a felhasználók biztonságos és költségkímélő hozzáféréshez való jogával.

4.2.4 Tekintetbe kell venni, hogy az informatikai biztonságra való törekvés költségekkel jár a fogyasztó számára, amiatt is, hogy időt veszít az akadályok eltávolításával vagy megkerülésével. Az EGSZB szerint minden számítógépet kötelező jelleggel automatikusan vírusellenes védőrendszerrel kellene ellátni. A felhasználó szabadon dönthetne e rendszer aktiválásáról, a terméknek azonban gyárilag tartalmaznia kellene azt.

4.3 *A lendületesebb és innovatívabb közösségi stratégiáért*

4.3.1 Mindezen túl az EGSZB szerint az Európai Uniónak ambiciózusabb célokat kellene kitűznie, valamint innovatív, integrált és lendületes stratégiát elfogadnia, amelyhez új kezdeményezéseket kellene társítania, például az alábbiakat:

– a felhasználók digitális azonosítását lehetővé tévő mechanizmusok, a felhasználókat ugyanis túl gyakran kérik a személyi adataik megadására,

– az ETSI-n ([22]) keresztül végrehajtandó intézkedések, amelyek az IKT biztonságos használatának feltételei, és amelyek az egész Unió közös biztonsági küszöbe segítségével meghatározott pontos és gyors megoldásokat kínálhatnak,

– megelőző intézkedések a hálózati és az információs biztonság minimális követelményeinek integrációja, valamint olyan kísérleti projektek révén, amelyek a biztonsághoz kapcsolódó tanfolyamokra irányulnak bármilyen jellegű és szintű oktatási intézményben,

– biztos és elismert, európai szintű jogszabályi keret kialakítása. Ennek az informatikára és a hálózatokra alkalmazott keretnek lehetővé kellene tennie az informatikai biztonságról az informatika biztosítására való áttérést,

– a kockázatértékelés európai és nemzeti mechanizmusainak megerősítése, valamint a törvények és előírások alkalmazhatóságának javítása a magánélet és az adatbankok ellen elkövetett számítógépes bűncselekmények leküzdése érdekében,

– az informatikai monokultúrák kialakulásának megakadályozását célzó intézkedések, mivel az ilyen jellegű termékek és megoldások könnyebb „behatolási” lehetőséget kínálnak. A diverzifikált plurikulturális innovációk támogatása, amelyek célja az egységes európai információs tér (SEIS – *Single European Information Space*) kialakítása.

4.3.2 Az EGSZB szerint ésszerű lenne egy főigazgatóságok közötti *IKT Security Focal Point* ([23]) létrehozása. A Focal Point az alábbi szinteken való cselekvést tenné lehetővé:

– az Európai Bizottság szolgálatai szintjén,

– az egyes tagállamok szintjén, az interoperabilitási szempontokat, a személyazonosság kezelését, a magánélet védelmét, az információhoz és a szolgáltatásokhoz való hozzáférés szabadságát, valamint a biztonság minimumkövetelményeit szolgáló horizontális megoldások révén,

– nemzetközi szinten, hogy ily módon biztosíthatóvá váljon az EU egységes fellépése a különböző nemzetközi fórumokon (ENSZ, G8, OECD, ISO).

4.4 *A megerősített, felelős koordinálást szolgáló EU-intézkedésekért*

4.4.1 Az EGSZB nagy jelentőséget tulajdonít a *European Network and Information Security Network* létrehozásának, amely a biztonsági mechanizmusokkal és azok interoperabilitásával, a fejlett kriptográfiával és a magánélet védelmével kapcsolatos kutatások, tanulmányok és workshopok előmozdítását szolgálja.

4.4.2 Az EGSZB úgy véli, hogy e kényes ágazat vonatkozásában célszerű lenne az európai kutatás szerepét az alábbiak tartalmának összefogása révén optimalizálni:

– az Európai Biztonságkutatási Program (ESRP) ([24]), amely újra megjelenik a 7. K+F keretprogramban,

([21]) Lásd 19. lábjegyzet, 3. pont.

([22]) ETSI, *European Telecomunications Standards Institute*, ld. főként a 2006. január 16-17-én megrendezett workshopot. Az ETSI specifikációkat dolgozott ki többek között az illegális lehallgatással (TS 102 232, 102 233, 102 234), a LAN Wireless internet-hozzáféréssel (TR 102 519), továbbá az elektronikus aláírásokkal kapcsolatban, valamint biztonsági algoritmusokat fejlesztett ki a GPRS és az UMTS mobiltelefonok számára.

([23]) Ez a Főigazgatóságok közötti *Focal Point* finanszírozható lenne a 7. K+F keretprogram „Együttműködés” egyedi programjának információs társadalmi technológiák (IST) prioritása, vagy az Európai Biztonságkutatási Program (ESRP) keretében.

([24]) Lásd 7. Kutatási, Technológiafejlesztési és Demonstrációs keretprogram, „Együttműködés” egyedi program biztonságkutatás tematikus prioritását, amely a 2007-2013 közötti időszakra 1,35 milliárd eurós költségvetéssel rendelkezik.

– a *Safer Internet plus* program

– és a létfontosságú infrastruktúrák védelmére vonatkozó európai program (EPCIP) ([25]).

4.4.3 E javaslatokat ki lehetne egészíteni az „Informatikai Biztonság Európai Napja" bevezetésével, amelyhez az iskolákban nemzeti képzési kampányok, valamint a fogyasztók tájékoztatását szolgáló kampányok társulnának a számítógépen közvetített információk védelmével kapcsolatos eljárásokról. Ennek során nyilvánvalóan terjeszteni kellene a számítógépek széles és rendkívül gyorsan változó területén bekövetkezett technológiai előrelépésekkel kapcsolatos információkat is.

4.4.4 Az EGSZB több ízben kiemelte, hogy a „digitális tranzakciók vélt biztonsága és a beléjük vetett bizalom határozza meg, hogy a vállalatok várhatóan milyen sebességgel vezetik be az IKT-t üzleti tevékenységükben. Hasonlóképpen, a fogyasztói hajlandóság hitelkártya-adatok weboldalakon történő kiszolgáltatására nagymértékben a tranzakció vélt biztonságának függvénye." ([26])

4.4.5 Az EGSZB meg van győződve arról – tekintettel az ágazat hatalmas növekedési potenciáljára –, hogy egyrészről szakpolitikák kialakítására van szükség, másfelől a létező politikákat az új fejleményekhez kell igazítani. Az informatikai biztonság területén kialakított európai kezdeményezéseket integrált stratégia révén kell összekapcsolni; ennek során meg kell szüntetni az ágazatok közötti határokat, és biztosítani kell az IKT homogén és biztos elterjesztését a társadalomban.

4.4.6 Az EGSZB szerint egyes fontos stratégiák – mint például a jelen stratégia – megvalósítása csigalassúsággal halad előre, mivel a tagállamok a közösségi szinten meghozandó fontos döntésekkel szemben bürokratikus és kulturális nehézségeket támasztanak.

4.4.7 Az EGSZB szerint továbbá a közösségi források nem elegendőek sok olyan, halasztást nem tűrő projekt megvalósításához, amelyek csak akkor képesek konkrét válaszokat adni a globalizáció következményeként keletkezett új problémákra, ha közösségi szinten hajtják végre őket.

4.5 *A közösségi fogyasztóvédelem erősítéséért*

4.5.1 Az EGSZB tudatában van annak, hogy a tagállamok a biztonságtechnológiai intézkedéseket és a biztonságmenedzsment eljárásokat a saját igényeiknek megfelelően alakították ki, és ennek során általában különböző szempontokra összpontosítottak. Emiatt is nehéz a biztonsággal összefüggő problémákra egyértelmű és hatékony választ adni. Néhány közigazgatási hálózat kivételével rendszeres formában nem létezik a tagállamok között határokon átnyúló együttműködés, noha nyilvánvaló, hogy a biztonsággal összefüggő kérdések nem kezelhetők az egyes országokban egymástól elszigetelten.

4.5.2 Az EGSZB kiemeli továbbá, hogy a Tanács a 2005/222/IB kerethatározat révén az egyes tagállamok igazságügyi és egyéb felelős hatóságai közötti együttműködési rendszert fogadott el, amelynek célja, hogy biztosítsa ez utóbbiak megközelítésmódjának következetességét, mégpedig az informatikai rendszerek elleni támadások területére vonatkozó büntetőjogi rendelkezéseik harmonizációja révén, konkrétan az alábbi területeken:

– az informatikai rendszerekhez való jogosulatlan hozzáférés,

– jogosulatlan beavatkozás egy informatikai rendszer működésének súlyos akadályozására vagy megszakítására irányuló szándékos cselekmény révén,

– jogosulatlan beavatkozás az adatokra vonatkozóan, egy informatikai rendszer adatainak törlésére, károsítására, megcsonkítására, módosítására, megsemmisítésére vagy hozzáférhetetlenné tételére irányuló szándékos cselekmény révén,

– a fenti bűncselekményekre való felbujtás, az azokhoz kapcsolódó bűnpártolás, illetve az azokban való bűnrészesség.

4.5.3 Ezenkívül a határozatban szerepelnek a jogi személyek felelősségének meghatározására szolgáló kritériumok, valamint a felelősség megállapítása esetén az e személyre alkalmazandó szankciók ([27]).

4.5.4 A tagállami hatóságokkal folytatandó párbeszéd keretében az EGSZB támogatja az Európai Bizottság javaslatát arra vonatkozóan, hogy e hatóságok kezdjék meg a hálózati és az információs biztonság területén alkalmazott nemzeti politikáik összehasonlító értékelését, beleértve a közigazgatási ágazatban kialakított szakpolitikákat is. Ez a javaslat egyébként már szerepelt az EGSZB egyik 2001-ben készült véleményében is.

4.6 *A biztonság kultúrájának általánosabbá válásáért*

4.6.1 Az informatikai biztonság iparának ténylegesen biztosítania kell, hogy – a technika állásának megfelelően – használja a saját installációi materiális felügyeletét garantáló rendszereket, valamint kodifikálja a kommunikációkat, hogy védje ügyfelei magánélet védelméhez, valamint a személyi adatok titkosságához való jogát ([28]).

([25]) COM(2005) 576, 2005.11.17.
([26]) Lásd 19. lábjegyzet, 2. pont.
([27]) Lásd 19. lábjegyzet, 4. pont.
([28]) Lásd 97/66/EK irányelvet a személyi adatok kezeléséről a hírközlési ágazatban (HL L 24., 1998.1.30.).

4.6.2 A tudatosításra irányuló intézkedéssel kapcsolatban az EGSZB alapvető jelentőségűnek tartja, hogy valódi „biztonsági kultúra" jöjjön létre, amely teljes mértékben összeegyeztethető a tájékoztatás, a kommunikáció és a véleménynyilvánítás szabadságával. Másrészről emlékeztet arra, hogy számos felhasználó nincsen tudatában a számítógépes kalózkodáshoz kötődő valamennyi kockázatnak, míg számos gazdasági szereplő, szolgáltatásértékesítő vagy -nyújtó nem képes megítélni, hogy a rendszernek vannak-e gyenge pontjai, és ha igen, ezek milyen mértékben veszélyeztetettek.

4.6.3 A magánélet és a személyi adatok védelme elsődleges célkitűzések, a fogyasztóknak azonban arra is joguk van, hogy valóban hatékony védelmet kapjanak a „kémszoftverek" (*spyware* és *web bugs*) vagy más módszerek révén való név szerinti, jogosulatlan azonosítással szemben Vissza kellene szorítani a *spamming* ([29]) gyakorlatát is (azaz a kéretlen üzenetek nagy tömegben való kiküldését), amely gyakran ezen visszaélések eredménye. Ezek a rendszerbe való behatolások ugyanis e cselekmények áldozatai számára költséggel járnak ([30]).

4.7 *Az erősebb és aktívabb EU-Ügynökségért*

4.7.1 Az EGSZB helyesnek tartaná az Európai Hálózati és Információs Biztonsági Ügynökség szerepének megerősítését akár a tudatosítást célzó kampányokkal, főként azonban a szolgáltatók és a felhasználók tájékoztatására és képzésére irányuló intézkedésekkel kapcsolatban. Mindezt egyébként már a nyilvános elektronikus hírközlési szolgáltatások nyújtásáról szóló, nemrégiben készült véleményében ([31]) is kifejtette.

4.7.2 Ami pedig az érdekeltek minden egyes csoportjára irányuló, a felelősségvállalást célzó intézkedéseket illeti, úgy tűnik, hogy ezeknél szigorúan betartották a szubszidiaritási elvet. Hiszen a tagállamok és a magánszektor felelőssége, hogy ezen intézkedéseket specifikus hatásköreiknek megfelelően végrehajtsák.

4.7.3 A közös tevékenységek megszervezéséhez az ENISA-nak részesülnie kellene a *European Network and Information Security Network* európai hálózat által nyújtott hozzájárulásokból; az informatikai biztonság többnyelvű közösségi webportálját pedig arra kellene felhasználnia, hogy személyre szabott és interaktív jellegű információkat nyújtson közérthető formában, különösen a különböző korú egyéni felhasználók, valamint a kis- és középvállalkozások részére.

Kelt Brüsszelben, 2007. február 16-án.

az Európai Gazdasági és Szociális Bizottság
elnöke
Dimitris DIMITRIADIS

([29]) A jelenség neve franciául: pollupostage.

([30]) Lásd az EGSZB véleményeit az elektronikus kommunikációs hálózatokról (HL C 123., 2001.4.25., 50. oldal), az elektronikus kereskedelemről (HL C 169., 1999.6.16., 36. oldal), valamint az elektronikus kereskedelem kihatásairól az egységes piacra (HL C 123., 2001.4.25., 1. oldal).

([31]) Lásd 19. lábjegyzet, 1. pont.