AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA

Brüsszel, 22.5.2007
COM(2007) 267 végleges

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé

{SEC(2007) 641}
{SEC(2007) 642}

A BIZOTTSÁG KÖZLEMÉNYE
AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé

1. BEVEZETÉS

1.1. Mi a számítógépes bűnözés?

A társadalmunkban egyre nagyobb jelentőséggel bíró információs rendszerek biztonságának számos vonatkozása van, amelyek közül az egyik legfontosabb a számítógépes bűnözés elleni küzdelem. A számítógépes bűnözés közösen elfogadott fogalommeghatározása hiányában a „számítógépes bűnözés", „számítástechnikai bűnözés", „számítógéppel kapcsolatos bűnözés" vagy „csúcstechnológiás bűnözés" kifejezéseket gyakran használják szinonimaként. E közlemény alkalmazásában „számítógépes bűnözés" alatt „olyan bűncselekmények értendők, amelyeket elektronikus kommunikációs hálózatok és információs rendszerek felhasználásával vagy ilyen hálózatokkal és rendszerekkel szemben követnek el".

A gyakorlatban a számítógépes bűnözés kifejezést a bűncselekmények három kategóriájára használják. Az első kategóriába a **bűncselekmények hagyományos formái** tartoznak, úgymint csalás vagy hamisítás, a számítógépes bűnözéssel összefüggésben azonban mindenekelőtt az elektronikus kommunikációs hálózatokon és információs rendszereken (a továbbiakban: elektronikus hálózatok) keresztül elkövetett bűncselekmények sorolandók ide. A második kategória az **illegális tartalom** elektronikus médián keresztüli közzétételére vonatkozik (többek között gyermekek szexuális kizsákmányolásával kapcsolatos anyagok vagy faji gyűlölet keltése). A harmadik kategóriába az **elektronikus hálózatokkal kapcsolatos bűncselekmények** tartoznak, úgymint az információs rendszerekkel szembeni támadások, a hozzáférés megtagadása és a hackertevékenység. Az ilyen típusú támadások a döntő jelentőségű európai létfontosságú infrastruktúrák ellen is irányulhatnak, és számos területen kihathatnak a fennálló sürgősségi riasztórendszerekre, ami az egész társadalomra nézve végzetes következményekkel járhat. Mindhárom bűncselekmény-kategória közös jellemzője, hogy az elkövetés terjedelme, valamint az adott bűncselekmény és hatásai közötti földrajzi távolság igen jelentős lehet. Következésképpen az alkalmazott nyomozási módszerek technikai szempontjai gyakran ugyanazok. E közlemény ezen közös jellemzőkre összpontosít.

1.2. A számítógépes bűnözéssel kapcsolatos legújabb fejlemények

1.2.1. Általános megjegyzések

A bűnözés folyamatosan változó jellege és a megbízható információk hiánya miatt nehéz pontos képet alkotni a jelenlegi helyzetről. Megfigyelhető azonban néhány általános tendencia:

- A számítógépes bűncselekmények száma növekszik, és a bűnözés egyre kifinomultabbá és nemzetközibbé válik[1]

- Egyértelmű jelek utalnak arra, hogy a számítógépes bűnözésben egyre inkább részt vesznek a szervezett bűnözői csoportok

- A határokon átnyúló bűnüldözési együttműködés alapján folytatott európai büntetőeljárások száma azonban nem növekszik

1.2.2. Az elektronikus hálózatokkal kapcsolatos hagyományos bűncselekmények

A legtöbb bűncselekmény elkövethető elektronikus hálózatok felhasználásával; az elektronikus hálózatokkal kapcsolatos bűnözés különösen elterjedt és egyre gyakoribb formáit a csalás és a megkísérelt csalás különböző típusai jelentik. Az olyan eszközök, mint a személyazonossággal való visszaélés, az adathalászat[2], a kéretlen elektronikus levelek és a rosszindulatú kódok felhasználásával széles körben követhető el csalás. Egyre nagyobb problémát jelent az illegális nemzeti és nemzetközi internetes kereskedelem is. Ide tartozik többek között a kábítószerekkel, veszélyeztetett fajokkal és fegyverekkel való kereskedelem.

1.2.3. Illegális tartalom

Európában egyre növekszik az illegális tartalmú honlapok száma, ideértve a gyermekek szexuális kizsákmányolásával kapcsolatos anyagokat, a terrorcselekményekre való izgatást, valamint az erőszak, a terrorizmus, a rasszizmus és az idegengyűlölet illegális dicsőítését is. Ilyen honlapokkal szemben különösen nehéz a bűnüldözésnek fellépnie, mivel a honlaptulajdonosok és -kezelők gyakran a célországtól eltérő országokban vannak, gyakran az EU-n kívül. A honlapok nagyon gyorsan mozgathatók akár az EU területén kívülre is, és a jogellenesség fogalmának meghatározása államonként jelentősen változik.

1.2.4. Az elektronikus hálózatokkal kapcsolatos bűncselekmények

Egyre gyakoribbá válnak az információs rendszerekkel vagy szervezetekkel és egyénekkel szembeni kiterjedt támadások (gyakran az úgynevezett botneteken[3] keresztül). Az utóbbi időben megfigyelhetők voltak egy állam létfontosságú információs infrastruktúrájával szembeni szisztematikus, jól szervezett és kiterjedt közvetlen támadások is. Ez összefügg a technológiák összeolvasztásával és az információs rendszerek egyre gyakoribb összekapcsolásával, ami e rendszereket sérülékenyebbé tette. A támadások gyakran jól szervezettek, és zsarolási célokat szolgálnak. Feltételezhető, hogy e támadások csak csekély részét jelentik be például azért, mert hátrányokkal járhat egy vállalkozás számára, ha nyilvánosságra kerül, hogy biztonsági problémái vannak.

---

1 Az e közleményben foglalt megállapítások többségét a Bizottság által 2006-ben elrendelt, a számítógépes bűnözésről szóló közlemény hatását értékelő tanulmányból vették át (szerződésszám: JLS/2006/A1/003).

2 Az adathalászat érzékeny információk – úgymint jelszavak és hitelkártyaadatok – elektronikus kommunikáció keretében történő jogellenes megszerzésének megkísérlését jelenti, amely során az elkövető a jogosult személynek adja ki magát.

3 A botnet olyan fertőzött számítógépek összességét jelenti, amelyeken a programok közös irányítás alapján működnek.

1.3. Célkitűzések

E változó körülményekre tekintettel sürgősen intézkedéseket kell hozni – nemzeti és európai szinten egyaránt – a számítógépes bűnözés minden formájával szemben, amelyek egyre nagyobb veszélyt jelentenek a létfontosságú infrastruktúrák, a társadalom, a vállalkozások és a polgárok számára. Az egyének számítógépes bűnözéssel szembeni védelmét gyakran megnehezítik olyan kérdések, mint az illetékes bíróság és az alkalmazandó jog meghatározása, a határokon átnyúló végrehajtás vagy az elektronikus bizonyítékok elismerése és felhasználása, mivel a számítógépes bűnözést lényegében határokon átnyúlóan követik el. E veszélyek kezelése érdekében a Bizottság általános politikai kezdeményezést indít, hogy javuljon az európai és nemzetközi szintű összehangolás a számítógépes bűnözés elleni küzdelemben.

A célkitűzés a számítógépes bűnözés elleni küzdelem erősítése nemzeti, európai és nemzetközi szinten egyaránt. A tagállamok és a Bizottság már régóta prioritásként kezelik egy külön uniós politika kidolgozását. A kezdeményezés a bűnüldözésre és e küzdelem büntetőjogi dimenzióira összpontosít majd, és e politika egyéb uniós fellépéseket is kiegészít a számítógépes biztonság általános javítása érdekében. A politika a következőkre terjed majd ki: az operatív bűnüldözési együttműködés javítása; a tagállamok közötti jobb politikai együttműködés és összehangolás; politikai és jogi együttműködés harmadik országokkal; tudatosságnövelés; képzés; kutatás; az iparral folytatott szoros párbeszéd és esetleges jogalkotási fellépés.

A számítógépes bűnözés elleni küzdelemmel és annak üldözésével kapcsolatos politika meghatározása és végrehajtása során teljes mértékben tiszteletben tartják majd az alapvető jogokat, különösen a véleménynyilvánítás szabadságához való jogot, a magán- és a családi élet tiszteletben tartásához való jogot, valamint a személyes adatok védelmét. Az e politika keretében hozott minden jogalkotási intézkedést először is alaposan megvizsgálnak a tekintetben, hogy összeegyeztethetőek-e e jogokkal és különösen az EU Alapjogi Chartájával. Megjegyzendő továbbá, hogy valamennyi ilyen politikai kezdeményezés végrehajtására az úgynevezett elektronikus kereskedelemről szóló irányelv[4] 12–15. cikkének teljes mértékű figyelembevételével kerül sor, amennyiben e jogi eszköz alkalmazandó.

E közlemény célkitűzése három fő operatív alcélra osztható, amelyek a következőképpen foglalhatók össze:

- A számítógépes bűnözéssel foglalkozó szolgálatok, valamint az Európai Unió egyéb illetékes hatóságai és szakértői közötti összehangolás és együttműködés javítása és megkönnyítése

- A tagállamokkal, az illetékes uniós és nemzetközi szervezetekkel és egyéb érintett szereplőkkel együttműködve a számítógépes bűnözés elleni küzdelemre vonatkozó koherens uniós politikai keret létrehozása

- A számítógépes bűnözés által okozott költségekkel és veszélyekkel kapcsolatos tudatosság növelése

[4] Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (HL L 178, 2000.7.17, 1. o.).

2. A SZÁMÍTÓGÉPES BŰNÖZÉS ELLENI KÜZDELEM TERÜLETÉRE VONATKOZÓ JOGI ESZKÖZÖK

2.1. Uniós szintű hatályos jogi eszközök és fellépések

A számítógépes bűnözésre vonatkozó politikáról szóló e közlemény összefoglalja és továbbfejleszti az információs infrastruktúrák biztonságának növelése és a számítógépes bűnözés elleni küzdelem révén biztonságosabb információs társadalom létrehozásáról szóló 2001-es közleményt[5] (a továbbiakban: a 2001-es közlemény). A 2001-es közlemény megfelelő anyagi és eljárásjogi jogalkotási rendelkezéseket javasolt mind a belföldi, mind pedig a transznacionális bűnözéssel szembeni fellépés érdekében. A közleményt számos jelentős javaslat követte. Ezek közé tartozik különösen az információs rendszerek elleni támadásokról szóló 2005/222/IB kerethatározat[6] elfogadásához vezető javaslat. Ezzel összefüggésben megjegyzendő továbbá, hogy elfogadtak egyéb általánosabb, a számítógépes bűnözés elleni küzdelem vonatkozásait is lefedő jogszabályokat is, mint például a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló 2001/413/IB kerethatározatot[7].

A gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2004/68/IB kerethatározat[8] jó példa arra, hogy a Bizottság milyen nagy hangsúlyt fektet a **gyermekek védelmére** és különösen az információs rendszerek felhasználásával jogellenesen közzétett, a gyermekek szexuális kizsákmányolásával kapcsolatos bármilyen formájú anyagok elleni küzdelemre, amely horizontális célkitűzést a Bizottság a jövőben is követi.

Az információs társadalmat érintő biztonsági kihívások kezelése érdekében az Európai Bizottság hármas megközelítést dolgozott ki a hálózat- és információbiztonsággal kapcsolatosan: különleges hálózat- és információbiztonsági intézkedések, az elektronikus kommunikáció keretszabályozása és a számítógépes bűnözés elleni küzdelem. Noha e három aspektussal bizonyos mértékig egymástól függetlenül is lehet foglalkozni, a közöttük fennálló számos kapcsolat miatt szoros összehangolás szükséges. Ezzel összefüggésben a hálózat- és információbiztonság területén a Bizottság 2001-ben a számítógépes bűnözésről szóló 2001-es közleménnyel párhuzamosan közleményt fogadott el „Hálózat- és információbiztonság: uniós politikai megközelítésre irányuló javaslat” címmel[9]. A 2002/58/EK elektronikus hírközlési adatvédelmi irányelv arra kötelezi a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, hogy biztosítsák szolgáltatásaik biztonságát. Az irányelv rendelkezéseket tartalmaz a kéretlen levelek és a kémprogramok ellen is. A hálózat- és információbiztonsági politikát azóta számos fellépéssel fejlesztették tovább, legutóbb a biztonságos információs társadalomra irányuló stratégiáról szóló közleménnyel[10] – amely megújított stratégiát dolgoz ki és keretet nyújt a hálózat- és információbiztonsággal kapcsolatos koherens megközelítés folytatására és finomítására –, valamint a kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről szóló közleménnyel[11] és az

---

5 COM(2000) 890, 2001.1.26.
6 HL L 69, 2005.3.16, 67. o.
7 HL L 149, 2001.6.2, 1. o.
8 HL L 13, 2004.1.20, 44. o.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.

ENISA 2004-es létrehozásával[12]. Az ENISA fő célkitűzése a szaktudás fejlesztése a köz- és magánszektor közötti együttműködés ösztönzése érdekében, valamint segítségnyújtás a Bizottság és a tagállamok számára. A számítógépes bűnözés elleni küzdelemben fontos szerepet játszanak majd az információs rendszerek biztonságát célzó technológiák területén elért **kutatási eredmények** is. Ennek megfelelően az EU 2007–2013-as időszakra vonatkozó hetedik kutatási keretprogramja[13] (7. KP) célkitűzésként említi az információs és kommunikációs technológiákat, valamint a biztonságot. Az elektronikus kommunikáció keretszabályozásának felülvizsgálata az elektronikus hírközlési adatvédelmi irányelv és a 2002/22/EK egyetemes szolgáltatási irányelv biztonsággal kapcsolatos rendelkezéseinek módosítását eredményezheti[14] a hatékonyság növelése érdekében.

2.2. Fennálló nemzetközi jogi eszközök

Az információs hálózatok átfogó jellege miatt a számítógépes bűnözéssel kapcsolatos politika nem lehet hatékony, ha az erőfeszítések kizárólag az EU-n belülre korlátozódnak. A bűnözők nem csak egyik tagállamból a másikba irányulóan tudják az információs rendszereket megtámadni, illetve bűncselekményeket elkövetni, hanem ezt az EU joghatóságán kívülről is könnyen meg tudják tenni. Ennek megfelelően a Bizottság aktívan részt vesz nemzetközi tárgyalásokon és együttműködési struktúrákban, többek között a G8-ak csúcstechnológiás bűnözéssel foglalkozó Lyon-Róma munkacsoportjában és az Interpol által irányított projektekben. A Bizottság szorosan figyelemmel kíséri a nemzetközi csúcstechnológiás bűnözéssel kapcsolatos, napi 24 órában elérhető hálózat[15] (a 24/7 hálózat) munkáját, amelynek tagja a világ számos állama, ideértve az EU tagállamainak többségét is. A G8-ak hálózata a nap 24 órájában elérhető kapcsolattartó pontokon keresztül lehetővé teszi a részt vevő államok közötti gyors kapcsolatfelvételt elektronikus bizonyítékok összegyűjtésével kapcsolatos esetekben, illetve amikor külföldi bűnüldöző hatóságok azonnali segítségére van szükség.

E területen a legfontosabb európai és nemzetközi jogi eszköz kétségtelenül az Európa Tanács számítástechnikai bűnözésről szóló 2001-es egyezménye[16]. A 2004-ben elfogadott és hatályba lépett egyezmény közös fogalommeghatározásokat tartalmaz a számítógépes bűnözés különböző típusaira, és lefekteti a szerződő államok közötti hatékony igazságügyi együttműködés alapjait. Az egyezményt számos állam, többek között az Amerikai Egyesült Államok és más nem európai államok, valamint az összes tagállam is aláírta. Néhány tagállam azonban még nem ratifikálta az egyezményt vagy az ahhoz csatolt kiegészítő jegyzőkönyvet, amely a számítógépes rendszereken keresztül elkövetett rasszista és idegengyűlölő cselekményekkel foglalkozik. Az egyezmény általánosan elismert jelentőségére tekintettel a Bizottság az egyezmény ratifikálására ösztönzi a tagállamokat és az érintett harmadik országokat, valamint megvizsgálja az Európai Közösség egyezményhez való csatlakozásának lehetőségét.

---

12 A 460/2004/EK rendelet az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, (HL L 77, 2004.3.13, 1. o.).

13 Az Európai Unió már a 6. kutatási és technológiafejlesztési keretprogramban támogatott számos e területre vonatkozó sikeres kutatási projektet.

14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

15 Lásd az Európa Tanács számítástechnikai bűnözésről szóló egyezményének 35. cikkét.

16 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3. A SZÁMÍTÓGÉPES BŰNÖZÉS ELLENI KÜZDELMET CÉLZÓ KÜLÖNLEGES ESZKÖZÖK TOVÁBBFEJLESZTÉSE

3.1. Az operatív bűnüldözési együttműködés és az uniós szintű képzés erősítése

A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség egyik fő gyenge pontja továbbra is a **határokon átnyúló** közvetlen **operatív együttműködés** struktúráinak hiánya, illetve azok nem kielégítő igénybevétele. A számítógépes bűnözéssel kapcsolatos sürgős esetekben a hagyományos kölcsönös segítségnyújtás lassúnak bizonyult és nem volt hatékony, továbbá még nem dolgozták ki megfelelően az új együttműködési struktúrákat. Noha Európában a nemzeti igazságügyi és bűnüldöző hatóságok szorosan együttműködnek az Europolon, az Eurojuston és más struktúrákon keresztül, nyilvánvalóan szükség van a feladatok erősítésére és egyértelmű meghatározására. A Bizottság által lefolytatott konzultációk rámutattak arra, hogy nem használják ki optimálisan e döntő jelentőségű csatornákat. A koordináltabb európai megközelítésnek egyszerre kell operatívnak és stratégiainak lennie, és ki kell terjednie az információk és bevált gyakorlatok cseréjére is.

A Bizottság a közeljövőben különös hangsúlyt kíván fektetni a **képzési** igényekre. Megállapított tény, hogy a technológiai fejlődés szükségessé teszi a bűnüldöző és igazságügyi hatóságok számítógépes bűnözéssel kapcsolatos folyamatos képzését. A tervek szerint ezért az EU megerősített és jobban összehangolt pénzügyi támogatást nyújt majd a multinacionális képzési programokhoz. A Bizottság továbbá a tagállamokkal és egyéb illetékes szervekkel – úgymint az Europol, az Eurojust, az Európai Rendőrakadémia (CEPOL) és az európai igazságügyi képzési hálózat (EJTN) – szorosan együttműködve azon is dolgozik majd, hogy megvalósuljon valamennyi vonatkozó képzési program uniós szintű koordinációja és összekapcsolása.

A Bizottság **találkozót** szervez a tagállamok, valamint az Europol, a CEPOL és az EJTN bűnüldözéssel foglalkozó szakértői számára annak megvitatása érdekében, hogy 2007-ben Európában hogyan lehetne javítani a stratégiai és operatív együttműködést, valamint a számítógépes bűnözéssel kapcsolatos képzést. Többek között megvizsgálják majd az információcserét segítő állandó uniós kapcsolattartó pont, valamint a számítógépes bűnözéssel foglalkozó uniós képzési platform létrehozását. A 2007-es találkozó lesz a közeljövőben tervezett üléssorozat első ilyen találkozója.

3.2. Az iparral folytatott párbeszéd erősítése

A magán- és a közszektor egyaránt érdekelt abban, hogy közösen dolgozzanak ki módszereket a bűnözésből eredő károk felmérésére és megelőzésére. A magán- és a közszektornak a közös bizalmon és a kárcsökkentés közös célkitűzésén alapuló közös részvétele minden bizonnyal hatékonyan erősíti majd a biztonságot a számítógépes bűnözés elleni küzdelemben is. A Bizottság számítógépes bűnözéssel kapcsolatos politikájának ezen aspektusa idővel a köz- és a magánszektor közötti párbeszéddel kapcsolatosan tervezett átfogó uniós politika részévé válik, amely az európai biztonság teljes területét lefedi majd. E politikát különösen az Európai Biztonságkutatási és Innovációs Fórum viszi majd tovább, amelyet a Bizottság hamarosan létre kíván hozni, és amelyben a köz- és a magánszektor érintett szereplői vesznek majd részt.

A modern információs technológiák és elektronikus kommunikációs rendszerek fejlődését messzemenően a magánszektor szereplői irányítják. A magánvállalkozások veszélyértékeléseket végeznek, programokat dolgoznak ki a bűnözés elleni küzdelem érdekében, és technikai megoldásokat alakítanak ki a bűncselekmények megelőzésére. Az ipar igen pozitív hozzáállásról tett bizonyságot a hatóságok számítógépes bűnözés elleni küzdelemben való segítésében, különösen a gyermekpornográfiával[17] és az egyéb típusú illegális internetes tartalommal szembeni fellépésben.

Problémát jelent az információk, szakismeretek és bevált gyakorlatok köz- és a magánszektor közötti cseréjének egyértelmű hiánya. A magánszektor szereplői az üzleti modellek és titkok védelme érdekében gyakran csak nehezen működnek együtt, illetve nem terheli őket egyértelmű jogi kötelezettség arra vonatkozóan, hogy a bűncselekmények miatt feljelentést tegyenek, vagy az azokra vonatkozó információkat megosszák a bűnüldöző hatóságokkal. Ilyen információkra azonban szükség lehet ahhoz, hogy a hatóságok hatékony és megfelelő bűnmegelőzési politikát dolgozhassanak ki. A személyes adatok védelmére vonatkozó szabályok fényében is megvizsgálják majd a szektorok közötti információcsere javításának lehetőségeit.

A Bizottság már most jelentős szerepet játszik számos, a számítógépes bűnözéssel foglalkozó köz-magán struktúrában, mint például a csalásmegelőzési szakértői csoportban[18]. A Bizottság meggyőződése, hogy a számítógépes bűnözés elleni küzdelemmel kapcsolatos hatékony általános politikának tartalmaznia kell a közszféra és a magánszféra szereplői – ideértve a civil társadalmi szervezeteket is – közötti együttműködésre vonatkozó stratégiát is.

A köz- és a magánszféra e területen való szélesebb körű együttműködése érdekében a Bizottság 2007-ben konferenciát szervez a bűnüldözéssel foglalkozó szakértők és a magánszektor képviselői – különösen az internetszolgáltatók – számára annak megvitatása érdekében, hogyan lehetne javítani a köz- és a magánszféra közötti operatív együttműködést Európában[19]. A konferencián minden olyan témát megvitatnak, amely mindkét szektor számára hasznos lehet, így különösen:

- Az operatív együttműködés javítása az internetes bűncselekmények és jogellenes tartalom elleni küzdelemben, különösen a terrorizmus, a gyermekek szexuális kizsákmányolásával kapcsolatos anyagok és a gyermekek védelme tekintetében különösen súlyos egyéb bűncselekmények területén

- A köz- és a magánszektor közötti megállapodások kezdeményezése jogellenes tartalmú – különösen gyermekek szexuális kizsákmányolásával kapcsolatos anyagokat tartalmazó – honlapok uniós szintű letiltása céljából

- Európai modell kialakítása a szükséges és releváns információk magán- és közszektor közötti megosztására a kölcsönös bizalom kialakítása és valamennyi érintett fél érdekeinek figyelembevétele érdekében

---

17 Az e területen folytatott együttműködés újabb példája a bűnüldöző hatóságok és a hitelkártyákat kibocsátó társaságok közötti együttműködés, amely keretében utóbbiak segítették a rendőrséget internetes gyermekpornográf termékeket vásárló személyek felkutatásában.

18 Lásd http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 A konferencia a számítógépes bűnözésről szóló közlemény 6.4. pontjában bemutatott uniós fórum folytatásának is tekinthető.

- Bűnüldözési kapcsolattartó pontok hálózatának létrehozása a magán- és a közszektorban egyaránt

3.3. Jogalkotás

A számítógépes bűnözés területén még nem célszerű általánosan harmonizálni a bűncselekmények fogalommeghatározásait és a nemzeti büntetőjogi rendelkezéseket, mivel e fogalom számos bűncselekménytípust lefed. Mivel a bűnüldöző hatóságok közötti hatékony együttműködés gyakran attól függ, hogy legalább részben harmonizáltak-e a bűncselekmények fogalommeghatározásai, továbbra is hosszú távú célkitűzés marad a tagállami jogszabályok harmonizálásának folytatása[20]. Néhány bűncselekmény kulcsfontosságú fogalommeghatározására tekintettel fontos lépést jelentett az információs rendszerek elleni támadásokról szóló kerethatározat elfogadása. Ahogyan fentebb már említésre került, azóta új veszélyek merültek fel, és a Bizottság szorosan figyelemmel kíséri e fejlődést, hogy bármikor értékelhesse további jogalkotás szükségességét. A felmerülő veszélyek figyelemmel kísérését szorosan összehangolják a létfontosságú infrastruktúrák védelmére vonatkozó európai programmal.

Már most meg kellene azonban fontolni a számítógépes bűnözés elleni célzott jogalkotást. Egy esetlegesen jogalkotást is szükségessé tevő különleges kérdés azon esetekre vonatkozik, amikor a számítógépes bűncselekményt **személyazonossággal való visszaéléssel** követik el. A „személyazonossággal való visszaélés" alatt általánosan az értendő, hogy valaki személyes azonosító információk, pl. hitelkártyaszám felhasználásával követ el más bűncselekményeket. A legtöbb tagállamban az elkövetőt valószínűleg csalás vagy egyéb esetleges bűncselekmény miatt üldöznék, és nem személyazonossággal való visszaélés miatt, mivel az előbbi súlyosabb bűncselekménynek tekintendő. A személyazonossággal való visszaélést nem minden tagállam minősítette bűncselekménynek. A személyazonossággal való visszaélés bűncselekményét gyakran könnyebb bizonyítani, mint a csalást, így az uniós bűnüldözési együttműködést jobban szolgálná, ha valamennyi tagállam bűncselekménnyé minősítené a személyazonossággal való visszaélést. A Bizottság 2007-ben konzultációt indít annak megvizsgálása érdekében, hogy megfelelő-e a jogi szabályozás.

3.4. A statisztikai adatgyűjtés javítása

Általánosan elismert tény, hogy a bűnözés gyakoriságát illetően jelenleg messzemenően elégtelen információk állnak rendelkezésre, és jelentős fejlődésre van szükség ahhoz, hogy az egyes tagállamok adatai összehasonlíthatók legyenek. A Bizottság e probléma kezelése érdekében ambiciózus ötéves tervet dolgozott ki *„A bűnözéssel és a büntető igazságszolgáltatással kapcsolatos statisztikákra vonatkozó átfogó és koherens EU-stratégia kialakítása: az EU cselekvési terve a 2006–2010-es időszakra"* című, 2006. augusztus 7-i közleményében[21]. Az e cselekvési terv alapján felállított szakértői csoport megfelelő fórumot nyújt majd a számítógépes bűnözés terjedelmének mérését segítő releváns mutatók kidolgozásához.

---

[20] E hosszabb távú célkitűzés már említésre került a 2001-es közlemény 3. oldalán is.

[21] COM(2006) 437, 2006.8.7.

4. TOVÁBBI TEENDŐK

A Bizottság jelenleg tovább kívánja fejleszteni a számítógépes bűnözésre vonatkozó általános politikát. A Bizottságnak a büntetőjog területén fennálló korlátozott hatásköre miatt e politika csak kiegészítheti a tagállamok és más szervek által hozott intézkedéseket. A legfontosabb intézkedések – amelyek mindegyike maga után vonja a 3. fejezetben bemutatott egy, több vagy valamennyi eszköz igénybevételét – a „Bűnmegelőzés és a bűnözés elleni küzdelem" pénzügyi programon keresztül is támogatást kapnak:

4.1. A számítógépes bűnözés elleni küzdelem általában

- Megerősített operatív együttműködés kialakítása a tagállamok bűnüldöző és igazságügyi hatóságai között; ennek első lépéseként 2007-ben különleges szakértői ülést szerveznek, és sor kerülhet a számítógépes bűnözéssel foglalkozó központi uniós kapcsolattartó pont felállítására is

- Nagyobb pénzügyi támogatás nyújtása olyan kezdeményezésekhez, amelyek a számítógépes bűnözéssel kapcsolatos esetek kezelése érdekében a bűnüldöző és igazságügyi hatóságok hatékonyabb képzését célozzák, valamint az e területet érintő multinacionális képzési intézkedések koordinálása uniós képzési platform felállításával

- A tagállamok és valamennyi hatóság határozottabb elkötelezettségének ösztönzése a számítógépes bűnözés elleni hatékony intézkedések meghozatala és az e bűncselekményekkel szembeni fellépéshez szükséges megfelelő források biztosítása érdekében

- A számítógépes bűnözés elleni küzdelmet segítő kutatás támogatása

- Legalább egy nagyobb konferencia szervezése (2007-ben) a bűnüldöző hatóságok és a magánszektor szereplőinek részvételével, különösen az elektronikus hálózatokon keresztül megvalósuló, illetve azok elleni illegális internetes tevékenységek elleni küzdelem érdekében folytatott együttműködés kialakítása és a nem személyes adatok hatékonyabb cseréjének elősegítése érdekében, valamint e 2007-es konferencia következtetéseinek végrehajtása konkrét köz-magán együttműködési projekteken keresztül

- Köz-magán fellépések kezdeményezése és az azokban való részvétel mindenekelőtt a fogyasztók tudatosságának növelése érdekében a számítógépes bűnözés által okozott költségek és az általa jelentett veszélyek tekintetében, elkerülve ugyanakkor azt, hogy csökkenjen a fogyasztók bizalma kizárólag a biztonság negatív vonatkozásaira való összpontosítás miatt

- A számítógépes bűnözés elleni küzdelemben átfogó nemzetközi együttműködés elősegítése és az abban való aktív részvétel

- A Bizottság e területre vonatkozó politikájával összhangban álló nemzetközi projektek kezdeményezése, támogatása és az azokhoz való hozzájárulás, például a G8-ak által indított projektek, amelyek összhangban állnak az országos és regionális stratégiai dokumentumokkal (a harmadik országokkal való együttműködés tekintetében)

- Konkrét intézkedésekkel valamennyi tagállam és érintett harmadik ország ösztönzése arra, hogy ratifikálják az Európa Tanács számítástechnikai bűnözésről szóló egyezményét és kiegészítő jegyzőkönyvét, valamint azon lehetőség megvizsgálása, hogy a Közösség csatlakozzon az egyezményhez

- A tagállamok információs infrastruktúrájával szembeni jól szervezett és kiterjedt támadások jelenségének megvizsgálása a tagállamokkal együtt, e támadások megelőzése és az ellenük való küzdelem érdekében, ideértve a válaszadás összehangolását, valamint az információk és bevált gyakorlatok megosztását

4.2. Az elektronikus hálózatokon keresztül elkövetett hagyományos bűncselekmények elleni küzdelem

- Alapos elemzés végzése a személyazonossággal való visszaéléssel szembeni konkrét uniós jogszabályra vonatkozó javaslat kidolgozása érdekében

- Technikai módszerek és eljárások kialakításának elősegítése a csalás és az illegális internetes kereskedelem elleni fellépés érdekében, többek között köz-magán együttműködési projekteken keresztül

- A munka folytatása és továbbfejlesztése konkrét területeken, mint például az elektronikus hálózatokon keresztül készpénz-helyettesítő fizetési eszközökkel elkövetett csalás elleni küzdelemben (csalásmegelőzési szakértői csoport)

4.3. Illegális tartalom

- A meghatározott illegális tartalommal szembeni intézkedések kidolgozásának folytatása, különösen a gyermekek szexuális kizsákmányolásával kapcsolatos anyagok és a terrorcselekményekre való izgatás tekintetében, mindenekelőtt a gyermekek szexuális kizsákmányolásáról szóló kerethatározat végrehajtásának nyomon követése keretében

- A tagállamok ösztönzése, hogy elegendő pénzügyi forrásokat biztosítsanak a bűnüldöző hatóságok munkájának megerősítéséhez, különös tekintettel a szexuális kizsákmányolással kapcsolatos, on-line terjesztett anyagok áldozatainak azonosítására

- Olyan illegális tartalommal szembeni intézkedések meghozatala és támogatása, amely kiskorúakat erőszakra és más súlyos jogellenes magatartásra ösztönözhet; ide tartoznak többek között a különösen erőszakos on-line videojátékok bizonyos típusai

- A tagállamok közötti és harmadik országokkal való párbeszéd kezdeményezése és ösztönzése az illegális tartalommal szembeni fellépés technikai módszereiről és az illegális honlapok letiltásának eljárásairól, a szomszédos országokkal e kérdésben esetlegesen megkötendő hivatalos megállapodások kidolgozása érdekében is

- A hatóságok és a magánszektor szereplői – különösen az internetszolgáltatók – közötti, uniós szintű önkéntes megállapodások és egyezmények kidolgozása az illegális internetes honlapok letiltását célzó eljárások vonatkozásában

4.4. Nyomon követés

E közlemény a közeljövőben megteendő lépésként számos olyan intézkedést megfogalmaz, amelyek az együttműködési struktúrákat kívánják javítani az EU-ban. A Bizottság segíti ezen intézkedések meghozatalát, értékeli a tevékenységek végrehajtása során elért eredményeket, valamint jelentést tesz a Tanács és a Parlament számára.