EUROOPA ÜHENDUSTE KOMISJON

Brüssel 22.5.2007
KOM(2007) 267 lõplik

KOMISJONI TEATIS
EUROOPA PARLAMENDILE, NÕUKOGULE
JA REGIOONIDE KOMITEELE

Küberkuritegevuse vastase võitluse üldise poliitika kujundamine

{SEK(2007) 641}
{SEK(2007) 642}

KOMISJONI TEATIS
EUROOPA PARLAMENDILE, NÕUKOGULE
JA REGIOONIDE KOMITEELE

Küberkuritegevuse vastase võitluse üldise poliitika kujundamine

1. SISSEJUHATUS

1.1. Mis on küberkuritegevus?

Järjest mahukamate infosüsteemide turvalisus kätkeb endas mitmeid aspekte, mille puhul küberkuritegevuse vastane võitlus on kesksel kohal. Kuna küberkuritegevuse määratluses ei ole kokku lepitud, kasutatakse sageli läbisegamini mõisteid „küberkuritegevus", „arvutikuriteod" või „kõrgtehnoloogiline kuritegevus". Käesolevas teatises mõistetakse küberkuritegevuse all kuritegusid, mis on pandud toime elektrooniliste sidevõrkude ja infosüsteemide abil või selliste võrkude või süsteemide vastu.

Üldjuhul kasutatakse mõistet „küberkuritegevus" kolme kuritegevusliigi puhul. Esimene neist hõlmab selliseid **traditsioonilisi kuriteovorme** nagu pettus või võltsimine, kuigi küberkuritegevuse puhul on see eelkõige seotud kuritegudega, mis on pandud toime elektrooniliste sidevõrkude ja infosüsteemide abil (edaspidi „elektroonilised võrgud"). Teine liik hõlmab elektroonilises meedias **ebaseadusliku materjali** avaldamist (nt laste seksuaalset kuritarvitamist kajastavad pildid või rassilisele vihkamisele õhutamine). Kolmas liik on seotud **kuritegudega, mis on suunatud elektrooniliste võrkude vastu**, nt infosüsteemide vastu suunatud ründed, teenuste keelamine või häkkerlus. Sellised ründed võivad olla suunatud ka oluliste kriitiliste infrastruktuuride vastu Euroopas ja mõjutada kiirhoiatussüsteeme mitmes valdkonnas, tuues kaasa katastroofilisi tagajärgi kogu ühiskonnale. Kõigil neil vormidel on ühine joon: neid saab panna toime suures ulatuses ja geograafiline kaugus kuriteo toimepanemiskoha ja selle tagajärgede vahel võib olla suur. Seepärast on nende suhtes kohaldatavate uurimismeetodite tehnilised aspektid sarnased. Käesolevas teatises keskendutaksegi nendele ühistele joontele.

1.2. Viimased suundumused küberkuritegevuses

1.2.1. Üldteave

Pidevalt muutuva kuritegevuse ja puuduliku usaldusväärse teabe tõttu on praegusest olukorrast täpset ülevaadet keeruline saada. Siiski on võimalik tuua välja üldsuundumused.

- Küberkuritegude arv kasvab ja küberkuritegevus muutub järjest komplekssemaks ja rahvusvahelisemaks[1].

[1] Enamik käesolevas teatises esitatud väidetest praeguste suundumuste kohta on võetud 2006. aastal komisjoni tellitud küberkuritegevust käsitleva teatise mõju hindamise uuringust (leping nr JLS/2006/A1/003).

- On selgeid märke selle kohta, et organiseeritud kuritegevusrühmitused osalevad küberkuritegevuses järjest rohkem.

- Samas aga ei ole piiriülese õiguskaitse koostöö raames vastutuselevõtmiste arv Euroopas suurenenud.

1.2.2. Traditsiooniline kuritegevus elektrooniliste võrkude abil

Enamik kuritegudest on võimalik panna toime elektrooniliste võrkude abil: eriti levinud on kõiksugu pettused või pettusekatsed ning nende osa elektrooniliste võrkudega seotud kuritegevuses kasvab. Laiaulatuslike pettuste toimepanemiseks võidakse kasutada selliseid vahendeid nagu identiteedivargus, andmepüük[2], rämpspost või pahatahtlikud koodid. Samuti on kasvav probleem ebaseaduslik riigisisene ja rahvusvaheline Internetipõhine kaubandus. See hõlmab nii narkootikume, eriti ohustatud liike kui ka relvi.

1.2.3. Ebaseaduslik materjal

Ebaseaduslikku materjali levitavate veebisaitide arv, millele pääseb juurde Euroopas, järjest kasvab: nendel saitidel võib näha laste seksuaalset kuritarvitamist kajastavaid pilte, õhutamist terrorismiaktidele või vägivalla, terrorismi, rassismi ja ksenofoobia ebaseaduslikku ülistamist. Karistusmeetmeid selliste veebisaitide vastu võtta on väga raske, sest nende omanikud või haldajad ei asu sageli Euroopa Liiduski. Veebisaidi asukoha saab väga kiiresti viia ka väljapoole Euroopa Liidu territooriumi ning ebaseaduslikkuse mõiste on riigiti väga erinev.

1.2.4. Ainult elektroonilistes võrkudes toimepandavad kuriteod

Tundub, et järjest rohkem esineb infosüsteemide või organisatsioonide või eraisikute vastu (sageli nn botnettide[3] kaudu) suunatud ulatuslikke ründeid. Samuti on täheldatud hiljuti juhtumeid, kus järjekindlad, hästi kooskõlastatud ja laiaulatuslikud otseründed on suunatud kriitiliste infoinfrastruktuuride vastu. Olukorda on süvendanud tehnoloogiate põimumine ja infosüsteemide omavaheline kiire ühendatus, muutes nimetatud süsteemid veelgi haavatamateks. Ründed on sageli hästi organiseeritud ja neid kasutatakse väljapressimiseks. Tõenäoliselt teatatakse sellistest juhtumitest võimalikult vähe: see on tingitud eelkõige kahjust, mis selline avalikukstulek võib ettevõttele tuua.

1.3. Eesmärgid

Võttes arvesse seda keskkonna muutust, on vaja võtta nii riikide kui ka Euroopa tasandil kiiresti meetmed mis tahes kuriteoliikide vastu, mis kujutavad endast järjest suuremat ohtu kriitilistele infrastruktuuridele, ühiskonnale, ettevõtlusele ja kodanikele. Isikute kaitse küberkuritegevuse eest muudavad tihti keeruliseks probleemid, mis on seotud pädeva kohtu, kohaldatava õiguse, piiriülese õiguskaitse või elektroonilise tõendusmaterjali tunnustamise ja kasutamisega. Küberkuritegevus on valdavalt piiriülene ja see võimendab nimetatud probleeme veelgi. Nimetatud ohtudega tegelemiseks käivitab komisjon üldise poliitikaalgatuse, et paremini kooskõlastada küberkuritegevuse vastast võitlust Euroopa ja rahvusvahelisel tasandil.

---

[2] Andmepüügi puhul püütakse pettuse teel saada tundlikku teavet, nt paroole või krediitkaardi andmeid, saates petusõnumeid, mis on maskeeritud usaldusväärse isiku saadetiseks.

[3] Botnet tähendab hõivatud arvutivõrku, mida saab ühe käsklusega panna tegema teatavaid toiminguid.

Eesmärk on tõhustada küberkuritegevuse vastast võitlust riikide, Euroopa ja rahvusvahelisel tasandil. Liikmesriigid ja komisjon on tunnistanud juba pikemat aega ELi poliitika edasiarendamist selles valdkonnas prioriteedina. Algatuses keskendutakse selle võitluse kahele mõõtmele ─ õiguskaitse ja kriminaalõigus ─ ning täiendatakse teisi ELi meetmeid, et tõsta turvalisust küberruumis üldiselt. Nimetatud poliitika raames käsitletakse järgmisi küsimusi: operatiivse õiguskaitsekoostöö tõhustamine, parem koostöö ja kooskõlastamine liikmesriikide vahel poliitikaküsimustes, koostöö kolmandate riikidega poliitika- ja õigusküsimustes, teadlikkuse tõstmine, koolitus, teadustegevus, tihedam dialoog tööstusettevõtjatega ning võimalikud õigusmeetmed.

Poliitika, mis käsitleb küberkuritegevuse vastast võitlust ja sellise tegevuse eest vastutuselevõtmist, kujundatakse ja viiakse ellu, järgides põhiõigusi, eelkõige neid õigusi, mis on seotud sõnavabaduse, era- ja perekonnaelu puutumatuse ning isikuandmete kaitsega. Enne selle poliitika raames meetmete võtmist analüüsitakse kõigepealt selle kokkusobivust nimetatud õigustega, eriti Euroopa Liidu põhiõiguste hartaga. Samuti tuleb märkida, et kõikide sellist laadi poliitiliste algatuste käivitamisel võetakse nõuetekohaselt arvesse nn e-kaubanduse direktiivi[4] artikleid 12−15 küsimustes, mille suhtes seda õigusakti kohaldatakse.

Käesoleva teatise eesmärgid võib jagada kolmeks oluliseks osaks, mis saab kokku võtta järgmiselt:

- parandada ja hõlbustada kooskõlastamist ja koostööd küberkuritegevuse üksuste, muude pädevate asutuste ja teiste ekspertide vahel Euroopa Liidus;

- töötada välja koos liikmesriikide, pädevate ELi ja rahvusvaheliste organisatsioonidega ja muude sidusrühmadega küberkuritegevuse vastase võitluse ELi ühtne poliitiline raamistik;

- tõsta teadlikkust küberkuritegevuse maksumusest ja ohtudest.

2. OLEMASOLEVAD ÕIGUSAKTID VÕITLUSEKS KÜBERKURITEGEVUSE VASTU

2.1. Euroopa Liidu olemasolevad vahendid ja meetmed

Käesolev teatis, mis käsitleb poliitikat küberkuritegevuse valdkonnas, toetab ja arendab edasi 2001. aasta teatist pealkirjaga „Turvalisema infoühiskonna poole, parandades infoinfrastruktuuride turvalisust ja võideldes arvutikuritegevuse vastu”[5] (edaspidi „2001. aasta teatis”). 2001. aasta teatises esitati nii riigisisese kui ka piiriülese kuritegevuse vastu võitlemiseks asjakohased sätted, mis hõlmavad nii materiaal- kui menetlusõigust. Nende põhjal tehti mitu olulist ettepanekut, eelkõige ettepanek, mille alusel sündis raamotsus 2005/222/JSK infosüsteemide vastu suunatud rünnete kohta[6]. Siinkohal tuleb ka märkida teisi vastuvõetud õigusakte, mis on küll üldisemad, kuid milles käsitletakse küberkuritegevuse vastase võitluse aspekte, nt raamotsus 2001/413/JSK mittesularahaliste maksevahenditega seotud pettuste ja võltsimiste vastase võitluse kohta[7].

---

4 Euroopa Parlamendi ja nõukogu direktiiv 2000/31/EÜ, 8. juuni 2000, infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (EÜT C 178, 17.7.2000, lk 1).

5 KOM(2000) 890, 26.1.2001.

6 ELT L 69, 16.3.2005, lk 67.

7 EÜT L 149, 2.6.2001, lk 1.

Laste seksuaae ekspluateerimise vastane raamotsus 2004/68/JSK[8] on hea näide selle kohta, et komisjon pöörab erilist tähelepanu **lastekaitsele**, eriti seoses laste seksuaalset kuritarvitamist kujutava materjali avaldamisega infosüsteemide kaudu. See jääb valdkondlikuks prioriteediks ka tulevikus.

Selleks et lahendada infoühiskonna ees seisvaid turvalisuse küsimusi, on Euroopa Komisjon töötanud välja võrgu- ja infoturbeks kolmetasandilise lähenemisviisi: võrgu- ja infoturbe erimeetmed, elektroonilist sidet reguleeriv raamistik, küberkuritegevuse vastane võitlus. Kuigi neid kolme tahku on teatud määral võimalik arendada iseseisvalt, on arvukate vastastikuste mõjude tõttu parem kasutada kooskõlastatud strateegiat. Võrgu- ja infoturbega seotud valdkonnas võeti 2001. aasta küberkuritegevust käsitleva teatisega samal ajal vastu komisjoni 2001. aasta teatis võrgu- ja infoturbe kohta: Ettepanek ELi lähenemisviisi kohta[9] E-puutumatuse direktiivis 2002/58/EÜ on sätestatud, et üldkasutatavate elektrooniliste sideteenuste osutajad peavad tagama oma teenuste turvalisuse. Direktiiv hõlmab ka rämpsposti ja nuhkvara vastaseid sätteid. Võrgu- ja infoturbe poliitikat on sellest ajast saadik arendatud mitme meetme kaudu: viimane teatis „Turvalise infoühiskonna strateegia – dialoog, partnerlus ja aktiivne osalemine"[10], milles on sätestatud ajakohastatud strateegia ning raamistik võrgu- ja infoturbele ühtse lähenemise arendamiseks ja täpsustamiseks, teatis rämpsposti, nuhkvara ja õelvara vastu võitlemise kohta[11] ning Euroopa Võrgu- ja Infoturbeameti loomine[12] 2004. aastal. Euroopa Võrgu- ja Infoturbeameti peamine ülesanne on arendada eriteadmisi ja edendada avaliku- ja erasektori osalejate ulatuslikku koostööd ning abistada komisjoni ja liikmesriike. Küberkuritegevuse vastases võitluses mängivad olulist osa ka infosüsteemide turvalisusega seotud tehnoloogia alase **teadustegevuse** tulemused. Info- ja sidetehnoloogiat ning turvet on nimetatud ka ELi teadustegevuse seitsmendas raamprogrammis, mis hõlmab ajavahemikku 2007−2013[13]. Elektroonilist sidet käsitleva raamistiku läbivaatamine võib tuua kaasa turbesätete muudatusi ja muuta need tõhusamaks e-puutumatuse direktiivis ja universaalteenust käsitlevas direktiivis 2002/22/EÜ[14].

2.2. Olemasolevad rahvusvahelised õigusaktid

Kuna infovõrgustikke iseloomustab globaalsus, ei saa küberkuritegevust käsitlev poliitika olla tõhus, kui selle raames tehtavad jõupingutused piirduvad vaid ELiga. Kurjategijad võivad rünnata infosüsteeme ja panna toime kuritegusid mitte ainult ühest liikmesriigist teise, vaid saavad neid teha hõlpsasti ka väljaspool ELi jurisdiktsiooni. Seepärast on komisjon aktiivselt osalenud rahvusvahelistes aruteludes ja koostööstruktuurides, nt G8 Lyon-Roma rühm, mis tegeleb kõrgtehnoloogia kuritegevusega, ja Interpoli juhitavad projektid. Komisjon jälgib eriti tähelepanelikult kõrgtehnoloogiaga seotud kuritegevust käsitleva, ööpäevaringselt töötava kontaktpunktidest koosneva võrgustiku tööd (24/7 võrgustik[15]), kuhu kuulub liikmeid kõikjalt maailmast, sealhulgas suurem osa ELi liikmesriikidest. G8 võrgu kaudu on võimalik kiirendada kontakte osalisriikide vahel, ööpäevaringselt töötavad kontaktpunktid on loodud

---

8 ELT L 13, 20.1.2004, lk 44.
9 KOM(2001) 298.
10 KOM(2006) 251.
11 KOM(2006) 688.
12 Määrus 460/2004, millega luuakse Euroopa Võrgu- ja Infoturbeamet, (ELT L 77, 13.3.2004, lk 1).
13 Euroopa Liit on juba teadusuuringute ja tehnoloogiaarenduse kuuenda raamprogrammi raames toetanud mitmeid asjakohaseid ja edukaid teadusprojekte.
14 KOM(2006) 334, SEK(2006) 816, SEK(2006) 817.
15 Vt Euroopa Nõukogu küberkuritegevuse konventsiooni artikkel 35.

elektrooniliste tõendusmaterjalidega seotud juhtumite ning välisriigi õiguskaitseasutuste kiiret abi vajavate juhtumite jaoks.

Nii Euroopa kui ka rahvusvahelisel tasandil on selles valdkonnas peamine õigusakt vaieldamatult Euroopa Nõukogu 2001. aasta küberkuritegevuse konventsioon[16]. Nimetatud konventsioon võeti vastu ja see jõustus 2004. aastal ning selles on määratletud erinevate küberkuritegude liigid ja sätestatud alus õigusalase koostöö toimimiseks osalisriikide vahel. Sellele on alla kirjutanud mitmed riigid, kaasa arvatud Ameerika Ühendriigid ja teised väljaspool Euroopat asuvad riigid ning kõik ELi liikmesriigid. Siiski ei ole kõik liikmesriigid veel ratifitseerinud konventsiooni või selle lisaprotokolle, mis käsitlevad arvutisüsteemide kaudu toimepandud rassistlike või ksenofoobilisi akte. Võttes arvesse selle konventsiooni olulisust, julgustab komisjon liikmesriike ja asjaomaseid kolmandaid riike seda tegema ning kaaluma Euroopa Ühenduse võimalust saada konventsiooniosaliseks.

3. KÜBERKURITEGEVUSE VASTAST VÕITLUST KÄSITLEVATE ERIVAHENDITE EDASINE ARENG

3.1. Operatiivse õiguskaitsekoostöö ja ELi tasandi koolituse tõhustamine

Õiguse, vabaduse ja turvalisuse valdkonna peamiseks nõrgaks lüliks on **piiriülese operatiivse koostöö** struktuuride puudus või nende alakasutus. Traditsiooniline vastastikune abi on osutunud küberkuritegevusega seotud kiireloomuliste juhtumite puhul aeglaseks ja ebatõhusaks ning uued koostööstruktuurid ei ole veel piisavalt arenenud. Euroopa riikide kohtu- ja õiguskaitseasutused teevad tihedat koostööd Europoli, Eurojusti ja muude struktuuride kaudu, kuid samas on selge vajadus tugevdada ja täpsustada vastutusalasid. Komisjoni korraldatud konsultatsioonide käigus on selgunud, et neid olulisi kanaleid ei ole kasutatud optimaalselt. Paremini kooskõlastatud Euroopa lähenemine peab olema nii operatiivne kui ka strateegiline ning hõlmama ka teabevahetust ja parimat tava.

Komisjon pöörab lähitulevikus erilist tähelepanu **koolitusvajadustele**. On teada tõsiasi, et tehnoloogia areng toob kaasa vajaduse kohtu- ja õiguskaitseasutuste jätkuõppe järele küberkuritegevuse küsimustes. Seepärast on ELi kavandanud rahvusvahelise koolitusprogrammidele oma rahalist toetust suurendada ja seda paremini kooskõlastada. Samuti töötab komisjon koostöös liikmesriikide ja muude pädevate asutustega nagu Europol, Eurojust, Euroopa Politseikolledž (CEPOL) ja Euroopa õigusalase koolituse võrgustik selle nimel, et viia lõpule ELi tasandil asjaomaste koolitusprogrammide kooskõlastamine ja nende omavaheline kokkusobitamine.

Komisjon korraldab **kohtumise** liikmesriikide õiguskaitseasutuste ekspertide ning Europoli, CEPOLi ja Euroopa õigusalase koolituse võrgustiku ekspertidega, et arutada, kuidas parandada strateegilist ja operatiivset koostööd, samuti korraldab ta 2007. aastal küberkuritegevuse teemalise koolituse Euroopas. Muu hulgas kaalutakse ka nii ELi alalise kontaktpunkti loomist teabevahetuseks kui ka ELi küberkuritegevust käsitleva koolitusfoorumi asutamist. 2007. aasta kohtumine on esimene lähitulevikus kavandatud kohtumiste seeriast.

---

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

3.2. Dialoogi tugevdamine tööstusettevõtjatega

Nii era- kui ka avalik sektor on huvitatud sellest, et arendada ühiselt meetodeid, kuidas teha kindlaks ja ennetada kuritegevuse tagajärjel tekkivat kahju. Era- ja avaliku sektori ühine osalemine, mis põhineb usaldusel ja ühisel eesmärgil − kahju vähendamine − tõotab olla tõhus viis turvalisuse parandamiseks ning küberkuritegevuse vastu võitlemiseks. Komisjoni küberkuritegevuse poliitika osad, mis käsitlevad era- ja avaliku sektori aspekte, on kavas kaasata kavandatud ELi üldisesse poliitikasse, mis käsitleb dialoogi era- ja avaliku sektori vahel, hõlmates Euroopa turvalisust tervikuna. Nimetatud poliitikat hakkab eelkõige vedama Euroopa turvalisusuuringute ja innovatsioonifoorum, mille komisjon plaanib peagi luua ning mis koondab asjaomaseid sidusrühmi era- ja avalikust sektorist.

Moodsa infotehnoloogia ja elektroonilise infosüsteemide väljatöötamist kontrollivad peamiselt eraettevõtjad. Nemad teostavad ohuhinnanguid, koostavad kuritegevusevastase võitluse programme ja töötavad välja kuritegevuse ennetamiseks tehnilisi lahendusi. Tööstus on suhtunud väga positiivselt ametiasutuste abistamisse küberkuritegevuse vastases võitluses, eelkõige seoses lastepornograafia[17] ning muu ebaseadusliku materjali avaldamisega Internetis.

Teine teema on seotud ilmse puudusega, mis valitseb teabe, eriteadmiste ja parima tava jagamisel era- ja avaliku sektori vahel. Ärimudelite või -saladuste kaitsmise huvides on eraettevõtjad tihti tõrjuvad või ei ole nende suhtes selgesõnaliselt seaduses sätestatud kohustust õiguskaitseasutuste teavitamiseks või nendega asjaomase kuritegudega seotud teabe jagamiseks. Samas aga oleks sellist teavet vaja, kui ametiasutused koostavad tõhusat ja asjaomast kuritegevusevastast poliitikat. Piiriülese teabevahetuse parandamise võimalusi kaalutakse ka isikuandmete kaitse eeskirjade raames.

Komisjonil on juba praegu oluline osa küberkuritegevusega tegelevates era- ja avalikku sektorit hõlmavates struktuurides, nt pettustevastase võitluse eksperdirühm[18]. Komisjon on veendunud, et tõhus küberkuritegevuse vastane üldine poliitika peab hõlmama strateegiat koostöö kohta avaliku ja erasektori ettevõtjate vahel, sealhulgas kodanikuühiskonna organisatsioonid.

Era- ja avalikku sektori laiemaks kaasamiseks koostöösse korraldab komisjon 2007. aastal õiguskaitseasutuse ekspertide ja erasektori esindajate, eelkõige Interneti-teenuste osutajate jaoks konverentsi, et arutada, kuidas tõhustada era- ja avaliku sektori operatiivset koostööd Euroopas[19]. Konverentsi raames käsitletakse küsimusi, mis on olulised mõlema sektori jaoks, kuid eelkõige järgmisi teemasid:

- operatiivse koostöö parandamine võitlemisel ebaseadusliku tegevusega ja materjalide avaldamisega Internetis, eelkõige seoses terrorismi, laste seksuaalset kuritarvitamist kujutava materjali ja muu ebaseadusliku tegevusega, mis on eriti tundlik lastekaitse seisukohast;

- era- ja avaliku sektori kokkulepete kavandamine eesmärgiga blokeerida kõikjal Euroopas ebaseaduslikku materjali sisaldavad veebisaidid, eelkõige laste seksuaalset kuritarvitamist kujutavat materjali sisaldavad veebisaidid;

---

[17] Üks viimaseid näiteid koostööst selles valdkonnas on õiguskaitseasutuste ja krediitkaardiäriühingute vaheline koostöö, kus viimased aitasid politseid tabada isikuid, kes ostsid veebis lastepornograafiat.

[18] See http://ec.europa.eu/internal_market/payments/fraud/index_en.htm.

[19] Konverentsi võib pidada arvutikuritegusid käsitleva teatise punktis 6.4 esitatud ELi foorumi jätkuks.

- Euroopa mudeli kavandamine vajaliku ja asjaomase teabe jagamiseks era- ja avalikus sektoris, arendades vastastikuse usalduse õhkkonda ja arvestades kõikide huvitatud isikute huvisid;

- õiguskaitseasutuste kontaktpunktidest koosneva võrgustiku loomine nii era- kui ka avalikus sektoris.

3.3. Õigusaktid

Kuriteo mõiste ja riikide karistusseadustike üldine ühtlustamine küberkuritegevuse valdkonnas ei ole veel asjakohane, sest nimetatud mõiste hõlmab väga erinevat liiki süütegusid. Kuna õiguskaitseasutuste vaheliseks tõhusaks koostööks oleks vaja kuriteo mõistete vähemalt osalist ühtlustamist, on liikmesriikide õigusaktide ühtlustamine pikaajaline eesmärk[20]. Teatavate kuriteo põhimääratluste puhul on juba läbitud üks oluline etapp raamotsuse näol infosüsteemide vastu suunatud rünnete kohta. Nagu eespool kirjeldatud, on päevakorda tõusnud uued ohud ja komisjon jälgib tähelepanelikult seda arengut, võttes arvesse korrapärase hindamise olulisust täiendavate õigusaktide vajaduste hindamisel. Nende muutuvate ohtude jälgimisel tehakse tihedat koostööd Euroopa kriitilise infrastruktuuri kaitse programmiga.

Siiski tuleks praegu kaaluda ka konkreetselt küberkuritegevuse vastu võitlemist käsitleva õigusakti vastuvõtmist. Eraldi teema, mille puhul võib osutada vajalikuks õigusakti vastuvõtmine, on seotud olukordadega, kus küberkuriteo raames pannakse toime **identiteedivargus**. Tavaliselt mõistetakse identiteedivarguse all isikut tuvastavate andmete kasutamist, nt krediitkaardinumbri kasutamist kuriteo vahendina. Enamik liikmesriikides mõistetakse kurjategija suure tõenäosusega süüdi pigem pettuses või mõnes muus süüteos kui identiteedivarguses: pettust peetakse tõsisemaks õigusrikkumiseks. Identiteedivargust ei käsitleta kõikides liikmesriikides kuriteona. Sageli on identiteedivargust kergem tõestada kui pettust; seepärast oleks õiguskaitsekoostöö EL tasandil tõhusam, kui identiteedivargust käsitletaks kõikides liikmesriikides kuriteona. Komisjon alustab 2007. aasta alguses konsultatsioone, et teha kindlaks, kas selles valdkonnas oleks asjakohane võtta vastu õigusakt.

3.4. Statistika areng

Üldiselt ollakse nõus, et kuritegevuse levikut kajastavad jooksvad andmed ei ole kaugeltki piisavad ning on vaja oluliselt parandada andmete võrdlust liikmesriikide vahel. Komisjoni 7. augusti 2006. aasta teatises pealkirjaga „*Igakülgse ja ühtse ELi kuritegevuse ja kriminaalasjades õigusemõistmise näitajate hindamise strateegia väljatöötamine: ELi tegevuskava 2006–2010*" on selle probleemi lahendamiseks esitatud suurte eesmärkidega viieaastane kava[21]. Selle tegevuskava raames loodud eksperdirühm oleks sobilik foorum, et töötada välja asjakohased näitajad küberkuritegevuse ulatuse mõõtmiseks.

---

[20] Seda pikaajalist eesmärki on juba nimetatud 2001. aasta teatise 3. leheküljel.

[21] KOM(2006) 437, 7.8.2006.

4. TULEVIKUPLAANID

Komisjonil on kavas kehtestada küberkuritegevuse vastast võitlust käsitlev üldine poliitika. Komisjoni piiratud volituste tõttu kriminaalõiguses saab see poliitika vaid täiendada liikmesriikide ja teiste organite võetud meetmeid. Olulisemaid meetmeid, millest igaüks hõlmab kas ühe, mitme või kõikide 3. peatükis esitatud vahendi kasutamist, toetatakse ka rahastamiskava „Kuritegevuse ennetamine ja kuritegevuse vastu võitlemine" raames.

4.1. Küberkuritegevuse vastane võitlus üldiselt

- Luua õiguskaitse- või kohtuasutuste tugevdatud operatiivkoostöö liikmesriikide vahel. Seda alustatakse eksperdikohtumise korraldamisega 2007. aastal ning selle raames võidaks luua ka küberkuritegevuse ELi keskne kontaktpunkt.

- Suurendada rahalist toetust algatustele, mille eesmärk on tõsta õiguskaitse- ja kohtuasutuste küberkuritegevust käsitleva koolituse taset ning kooskõlastada paremini jõupingutusi, mis tehakse rahvusvaheliseks koolitustööks selles valdkonnas, luues ELi koolitusfoorumi.

- Julgustada liikmesriike ja riigiasutusi võtma tõhusaid meetmeid võitlemaks küberkuritegevuse vastu ja eraldama piisavaid vahendeid selliste kuritegude vastu võitlemiseks.

- Toetada teadusuuringuid, millest on kasu küberkuritegevuse vastaseks võitluseks.

- Korraldada koos õiguskaitseasutuste ja eraettevõtjatega vähemalt üks oluline konverents (2007. aastal), eelkõige selleks, et algatada koostööd elektrooniliste võrkude kaudu ja nende vastu toimepandava ebaseadusliku tegevuse vastu Internetis ja edendada mitteisiklike andmete vahetuse tõhustamist, ning esitada 2007. aastal toimuva konverentsi kokkuvõttes konkreetsed era- ja avaliku sektori koostööprojektid.

- Algatada selliseid era- ja avalikku sektorit hõlmavaid meetmeid ja neis osaleda, mille eesmärk on tõsta teadlikkust küberkuritegevuse maksumusest ja sellise tegevusega seotud ohtudest, eriti tarbijate hulgas, püüdes samal ajal jätta kahjustamata tarbijate ja kasutajate usaldust, keskendudes ka turvalisuse muudele kui vaid negatiivsetele aspektidele.

- Osaleda aktiivselt küberkuritegevuse vastast võitlust hõlmavas laiemas koostöös ja seda edendada.

- Algatada, täiendada ja toetada rahvusvahelisi projekte, mis vastavad komisjoni poliitikale selles valdkonnas, nt projektid, mida teostatakse G8 raames ja mis on kooskõlas riiklike ja piirkondlike strateegiadokumentidega (koostöö suhtes kolmandate riikidega).

- Võtta konkreetseid meetmeid, et julgustada kõiki liikmesriike ja asjaomaseid kolmandaid riike ratifitseerima Euroopa Nõukogu küberkuritegevuse konventsiooni ja selle lisaprotokolle ning kaaluma ühenduse saamist konventsiooniosaliseks.

- Uurida koos liikmesriikidega nende infoinfrastruktuuri vastu suunatud kooskõlastatud ja laiaulatuslikke ründeid, et neid ennetada ja nende vastu võidelda, hõlmates ka nendele reageerimise kooskõlastamist ning teabe ja parima tava jagamist.

4.2. Võitlus elektrooniliste võrkude kaudu toimuva traditsioonilise kuritegevuse vastu

- Algatada põhjalik analüüs, et valmistada ette identiteedivarguse vastast võitlust käsitlev konkreetne ettepanek ELi õigusakti vastuvõtmiseks.

- Edendada tehniliste meetodite ja menetluste arendamist, et võidelda pettuste ja ebaseadusliku kaubanduse vastu Internetis ning seda ka era- ja avaliku sektori koostööprojektide raames.

- Jätkata ja arendada edasi tööd konkreetsetes sihtvaldkondades, nt pettustevastase võitluse eksperdirühma raames seoses elektrooniliste võrkudes kasutatavate mittesularahaliste maksevahendiga.

4.3. Ebaseaduslik materjal

- Jätkata konkreetset ebaseaduslikku materjali käsitlevate meetmete väljatöötamist, eriti seksuaalset kuritarvitamist kujutavat materjali ja terrorismile õhutamist käsitlevad meetmed, ning raamotsuse laste seksuaalse ekspluateerimise ja lastepornograafia vastu võitlemise kohta rakendamise järelevalvet.

- Kutsuda liikmesriike üles eraldama piisavaid rahalisi vahendeid, et tugevdada õiguskaitseasutuste tööd, milles pööratakse erilist tähelepanu isikutele, kes on veebis levitatava seksuaalset kuritarvitamist käsitleva materjalide ohvrid.

- Algatada ja toetada meetmeid, milles võideldakse sellise ebaseadusliku materjali vastu, milles õhutatakse alaealisi vägivallale ja muule tõsisele ebaseaduslikule käitumisele, eelkõige teatavat liiki äärmiselt vägivaldsed veebipõhised videomängud.

- Algatada ja edendada liikmesriikide ja kolmandate riikide vahelist dialoogi ebaseadusliku materjali vastast võitlust käsitlevat tehniliste meetodite küsimuses ning ebaseaduslike veebisaitide sulgemismenetluste suhtes, et võimaluse korral töötada välja koos naaberriikidega selles küsimuses ametlik kokkulepe.

- Töötada ELi tasandil välja vabatahtlikud kokkulepped ja konventsioonid riigiasutuste ja eraettevõtjate vahel, eriti Interneti-teenuse osutajatega, ebaseaduslike veebisaitide blokeerimise ja sulgemise menetluste kohta.

4.4. Järelmeetmed

Käesolevas teatises on järgmise sammuna kirjeldatud mitmeid meetmeid, mille eesmärk on koostööstruktuuride tõhustamine ELis. Komisjon viib need meetmed ellu, hindab meetmete rakendamisel tehtud edusamme ja esitab nõukogule ja Euroopa Parlamendile aruande.