EIROPAS KOPIENU KOMISIJA

Briselē, 22.5.2007
COM(2007) 267 galīgā redakcija

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI UN EIROPAS REĢIONU KOMITEJAI

Vispārīgā politika cīņai ar kibernoziedzību

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

KOMISIJAS PAZIŅOJUMS
EIROPAS PARLAMENTAM, PADOMEI
UN EIROPAS REĢIONU KOMITEJAI

Vispārīgā politika cīņai ar kibernoziedzību

1. IEVADS

1.1. Kas ir kibernoziedzība?

Mūsdienu sabiedrībai arvien nozīmīgāko informācijas sistēmu drošība aptver daudzus aspektus, kuru būtiskākā sastāvdaļa ir cīņa ar kibernoziedzību. Ņemot vērā, ka neeksistē vienota kibernoziedzības definīcija, bieži tiek lietoti savstarpēji aizvietojami termini „kibernoziedzība", „datornoziedzība", „ar datoriem saistīta noziedzība" vai „augsto tehnoloģiju noziedzība". Šajā paziņojumā ar terminu „kibernoziedzība" saprot „noziedzīgas darbības, ko veic, izmantojot elektroniskos sakaru tīklus un informācijas sistēmas, vai kas ir vērstas pret šādiem tīkliem un sistēmām."

Praksē terminu kibernoziedzība lieto attiecībā uz trīs noziedzīgu darbību kategorijām. Pirmā ietver **noziedzīgo nodarījumu tradicionālās formas**, kā piemēram, krāpšana vai viltošana, taču saistībā ar kibernoziedzību tā īpaši attiecas uz nodarījumiem, ko veic ar elektronisko sakaru tīklu un informācijas sistēmu (turpmāk – elektroniskie tīkli) palīdzību. Otrā attiecas uz **nelegāla satura** informācijas publiskošanu elektroniskajos medijos (piemēram, materiāli, kuros atspoguļota seksuāla vardarbība pret bērniem vai kūdīšana uz rasu naidu). Trešā aptver **tikai elektroniskajiem tīkliem raksturīgus noziedzīgus nodarījumus**, piemēram, uzbrukumi informācijas sistēmām, pakalpojumu atteikšana un nelikumīga piekļuve (*hacking*). Šāda veida uzbrukumi var būt vērsti arī pret ārkārtīgi būtiskām infrastruktūrām Eiropā un iespaidot pastāvošās ātrās reaģēšanas sistēmas daudzās jomās, kas var izraisīt postošas sekas visai sabiedrībai. Visu šo kategoriju noziedzīgo nodarījumu kopīga pazīme ir tā, ka tos iespējams veikt masveidā un atrodoties lielā attālumā no seku iestāšanās vietas. Tādējādi izmantotās izmeklēšanas metodes no tehniskā viedokļa ļoti bieži ir vienādas. Šīs kopīgās pazīmes ir šī paziņojuma galvenā tēma.

1.2. Jaunākās attīstības tendences kibernoziedzības jomā

1.2.1. Vispārīgs raksturojums

Ņemot vērā nepārtraukto noziedzīgo darbību attīstību un uzticamas informācijas trūkumu, ir grūti iegūt pilnīgu ainu par pašreizējo situāciju. Tomēr ir novērojamas atsevišķas vispārīgas tendences:

- kibernoziegumu skaits pieaug un noziedzīgās darbības kļūst arvien izsmalcinātākas un starptautiski izvērstākas[1],

[1] Lielākā daļa no šajā paziņojumā izmantotajiem apgalvojumiem par aktuālajām tendencēm ir iegūti no Ietekmes novērtējuma pētījuma paziņojumam par kibernoziegumiem, ko Komisija pasūtīja 2006. gadā (Līguma Nr.JLS/2006/A1/003).

- ir nepārprotamas norādes, ka kibernoziegumos arvien vairāk iesaistās organizētās noziedzības grupas,

- taču kriminālvajāšanas gadījumi Eiropā, kuru pamatā būtu pārrobežu sadarbība tiesību aizsardzības jomā, nepalielinās.

1.2.2. Tradicionālie noziedzīgie nodarījumi elektroniskajos tīklos

Lielu daļu noziedzīgu nodarījumu ir iespējams veikt, izmantojot elektroniskos tīklus, taču elektroniskajiem tīkliem īpaši raksturīgi noziedzīgi nodarījumi, kuru skaits aizvien pieaug, ir dažāda veida krāpšanas un krāpšanas mēģinājumi. Tādus paņēmienus kā identitātes zagšana, pikšķerēšana (*phishing*)[2], surogātpasts un ļaunprātīgi kodi var izmantot liela apmēra krāpšanām. Nelikumīga valsts vai starptautiska mēroga tirdzniecība ar interneta starpniecību arī ir kļuvusi par aktuālu, augošu problēmu. Tā ietver tirdzniecību ar narkotikām, apdraudētām sugām un ieročiem.

1.2.3. Nelegāla satura informācija

Eiropā ir pieejamas arvien vairāk tīmekļa vietnes ar nelegālu saturu, kurās atspoguļota seksuāla vardarbība pret bērnu, kūdīšana uz terora aktiem, nelikumīga vardarbības slavināšana, terorisms, rasisms un ksenofobija. Tiesību aizsardzības pasākumi pret šādām tīmekļa vietnēm ir ļoti sarežģīti, jo to īpašnieki un administratori bieži atrodas citās valstīs nekā tās, kurām šī informācija ir domāta, un bieži arī ārpus Eiropas Savienības. Šīs tīmekļa vietnes var ļoti ātri pārvietot, arī ārpus ES teritorijas, un jēdziena „pretlikumīgs" definīcijas dažādās valstīs ievērojami atšķiras.

1.2.4. Tikai elektroniskajiem tīkliem raksturīgie noziedzīgie nodarījumi

Ļoti izplatīti ir kļuvuši liela apmēra uzbrukumi informācijas sistēmām vai organizācijām un indivīdiem (bieži ar tā saucamo robottīklu (*botnets*)[3] palīdzību). Nesen ir novēroti arī sistemātiski, labi koordinēti un plaša mēroga tieši uzbrukumi īpaši nozīmīgām valsts informācijas infrastruktūrām. Situāciju vēl vairāk pasliktina tehnoloģiju apvienošana un ar vien progresējošā informācijas sistēmu savstarpējā sasaiste, kas padara šīs sistēmas vēl neaizsargātākas. Uzbrukumi bieži ir labi organizēti un tos izmanto izspiešanai. Ziņojumu skaits par šādiem uzbrukumiem ir samazinājies daļēji iespējams arī tāpēc, ka uzņēmumam var rasties zaudējumi, ja sabiedrībai kļūst zināms, ka tam ir problēmas ar drošību.

1.3. Mērķi

Ņemot vērā šo attīstību, steidzami ir nepieciešama rīcība gan valstu, gan visas Eiropas mērogā, kas būtu vērsta pret visa veida kibernoziedzību, kas rada nozīmīgus un aizvien pieaugošus draudus īpaši nozīmīgām infrastruktūrām, sabiedrībai, uzņēmējdarbībai un pilsoņiem. Indivīdu aizsardzību pret kibernoziedzību nereti sarežģī jautājumi par tiesas piekritību, piemērojamām tiesībām, pārrobežu piespiedu izpildi vai elektronisko pierādījumu atzīšanu un izmantošanu. Kibernoziedzības pārrobežu raksturs pastiprina šīs grūtības. Lai stātos pretī aprakstītajiem draudiem, Komisija ierosina izstrādāt vispārīgu politiku, lai uzlabotu Eiropas un starptautiskā līmeņa sadarbību cīņai ar kibernoziedzību.

---

[2] Pikšķerēšana nozīmē mēģinājumu elektroniskās komunikācijas ceļā krāpnieciski iegūt slepenu informāciju, kā paroles un kredītkaršu informāciju, maskējoties par uzticamu personu.

[3] Robottīkls nozīmē tādu datoru tīklu, kas inficēti ar vienoti no attāluma vadāmu programmatūru.

Mērķis ir pastiprināt cīņu ar kibernoziedzību valstu, Eiropas un starptautiskajā līmenī. Dalībvalstis un Komisija jau sen ir atzinušas nepieciešamību turpmāk izstrādāt īpašu ES politiku. Kibernoziedzības apkarošanas tiesību aizsardzības un krimināltiesību aspekti ir šī ierosinājuma galvenie jautājumi, un ierosinātā politika papildinās pārējos ES pasākumus kibertelpas drošības uzlabošanai. Politika paredzēs: uzlabotu operatīvo sadarbību tiesību aizsardzības jomā, labāku politiskā līmeņa sadarbību un koordināciju starp dalībvalstīm, politisko un tiesisko sadarbību ar trešām valstīm, informētības veicināšanu, apmācību, izpēti, pastiprinātu dialogu ar ekonomikas nozaru pārstāvjiem un iespējamus likumdošanas pasākumus.

Politika kibernoziedzības apkarošanai un krimināvajāšanai tiks izstrādāta un ieviesta, pilnībā ievērojot cilvēka pamattiesības, jo īpaši tiesības uz vārda brīvību, tiesības uz privātās un ģimenes dzīves neaizskaramību un personas datu aizsardzības tiesības. Uzsākot likumdošanas procesu šīs politikas īstenošanai, vispirms tiks veikta rūpīga pārbaude attiecībā uz atbilstību minētajām pamattiesībām, jo īpaši ES Pamattiesību hartai. Jānorāda, ka visos gadījumos, uz kuriem attiecas tā saucamā Elektroniskās tirdzniecības direktīva[4], politiskās iniciatīvas realizēs, ievērojot šī tiesību akta 12. un 15. pantu.

Šī paziņojuma mērķi var iedalīt šādos trīs galvenos operatīvos pasākumos:

- uzlabot un veicināt koordināciju un sadarbību starp kibernoziedzības apkarošanas un citām kompetentajām iestādēm un ekspertiem Eiropas Savienībā,

- sadarbībā ar dalībvalstīm, attiecīgām ES un starptautiskām organizācijām un citiem interesentiem izstrādāt saskaņotu ES politisko regulējumu cīņai ar kibernoziedzību,

- paaugstināt kibernoziedzības radīto briesmu un zaudējumu apzināšanās līmeni.

2. ESOŠIE TIESISKIE LĪDZEKĻI CĪŅAI AR KIBERNOZIEDZĪBU

2.1. Līdzekļi un pasākumi ES līmenī

Šis paziņojums par politiku cīņai ar kibernoziedzību apkopo un papildina 2001. gada paziņojumu par „Drošākas informācijas sabiedrības izveidi, uzlabojot informācijas infrastruktūru drošību un apkarojot datornoziegumus”[5] (turpmāk – 2001. gada paziņojums). Ar 2001. gada paziņojumu tika ierosināts izstrādāt atbilstošas materiālo un procesuālo tiesību normas gan pašmāju, gan pārrobežu noziedzīgo darbību apkarošanai. No šī ierosinājuma izrietēja vairāki nozīmīgi priekšlikumi. Jo īpaši tas attiecas uz priekšlikumu Pamatlēmumam 2005/222/TI par uzbrukumiem informācijas sistēmām[6]. Šajā sakarībā jānorāda, ka tika pieņemti arī citi vispārīgāki tiesību akti, kas aptvēra cīņas ar kibernoziedzību atsevišķus aspektus, kā piemēram, Pamatlēmums 2001/413/TI par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem[7].

---

4 Eiropas Parlamenta un Padomes 2000. gada 8. jūnija Direktīva 2000/31/EK par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (OV C 178., 17.7.2000, 1.lpp.)

5 COM(2000) 890, 26.1.2001.

6 OV L 69, 16.3.2005, 67. lpp.

7 OV L 149, 2.6.2001, 1. lpp.

Pamatlēmums 2004/68/TI par bērnu seksuālās izmantošanas apkarošanu[8] ir labs piemērs tam, cik nopietnu uzmanību Komisija pievērš **bērnu aizsardzībai,** jo īpaši attiecībā uz jebkāda veida materiālu par seksuālo vardarbību pret bērnu nelikumīgu publicēšanu, izmantojot informācijas sistēmas, šī horizontālā prioritāte saglabāsies arī nākotnē.

Informācijas sabiedrības drošības problēmu risināšanai Eiropas Kopiena ir izstrādājusi trīsdaļīgu pieeju, lai nodrošinātu tīklu un informācijas drošību, kas ietver: īpašus tīklu un informācijas drošības pasākumus, elektronisko sakaru regulējumu un cīņu ar kibernoziedzību. Lai gan minētos trīs aspektus zināmā mērā var attīstīt atsevišķi, tie ir savstarpēji cieši saistīti, un tāpēc ir nepieciešama to cieša savstarpēja koordinēšana. Paralēli 2001. gada paziņojumam Komisija 2001. gadā ar kibernoziedzību cieši saistītajā tīklu un informācijas drošības jomā pieņēma Paziņojumu par tīklu un informācijas drošību: priekšlikums Eiropas politikas pieejai[9]. „e-Privātuma" Direktīva 2002/58/EK paredz publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem pienākumu nodrošināt viņu sniegto pakalpojumu drošumu. Turpat ir paredzēti noteikumi pret surogātpastu un spiegprogrammatūru. Tīklu un informācijas drošības politika kopš tā laika attīstās un tās ietvaros ir īstenoti vairāki pasākumi, jaunākie no tiem ir Paziņojums par drošas informācijas sabiedrības stratēģiju, kas paredz atjaunot stratēģiju[10] un piedāvā shēmu, kā turpināt un uzlabot saskaņoto pieeju tīklu un informācijas drošībai, Paziņojums par surogātpasta, spiegprogrammatūru un ļaunprātīgu programmatūru apkarošanu[11] un Paziņojums par ENISA izveidošanu 2004. gadā[12]. ENISA galvenais mērķis ir uzkrāt īpašās zināšanas, lai uzlabotu sadarbību starp valsts un privāto sektoru un sniegtu atbalstu Komisijai un dalībvalstīm. Nozīmīgu vietu cīņā ar kibernoziedzību ieņem arī **pētījumu rezultāti** informācijas sistēmu drošības nodrošināšanas tehnoloģiju jomā. Tādējādi informācijas un sakaru tehnoloģijas un drošība ir iekļautas ES Septītās pētniecības pamatprogrammas (*FP7*) mērķu sarakstā, kas paredzēta laika periodam no 2007. līdz 2013. gadam[13]. Elektronisko sakaru tiesiskā regulējuma pārskats varētu būt par pamatu grozījumiem ar drošību saistītajos „e-Privātuma" Direktīvas 2002/58/EK un Universālā pakalpojuma Direktīvas 2002/22/EK[14] noteikumos.

2.2. Starptautiskie līdzekļi

Informācijas tīklu globālā rakstura dēļ kibernoziedzības apkarošanas politika nevar būt efektīva, ja to realizē tikai Eiropas Savienības robežās. Noziedznieki var uzbrukt informācijas sistēmām vai izdarīt noziedzīgus nodarījumus ne tikai no vienas dalībvalsts otrā, bet arī atrodoties ārpus Eiropas Savienības jurisdikcijas. Tāpēc Komisija ir aktīvi piedalījusies starptautiskās diskusijās un sadarbības pasākumos, piemēram, G8 Lionas – Romas Progresīvo tehnoloģiju noziedzības apkarošanas grupā un Interpola vadītajos projektos. Īpaši uzmanīgi Komisija seko Starptautiskā progresīvo tehnoloģiju noziedzības apkarošanas diennakts informācijas apmaiņas tīkla (27/4 tīkls)[15] darbībai, kurā apvienojušās ievērojams skaits valstu visā pasaulē, ieskaitot lielāko daļu ES dalībvalstu. G8 tīkls ar diennakts informācijas

---

8 OV L13, 20.1.2004, 44. lpp.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.
12 Eiropas Parlamenta un Padomes Regula (EK) Nr. 460/2004 (2004. gada 10. marts), ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru, (OV L 77, 13.3.2004, 1. lpp.).
13 Vairākus nozīmīgus un veiksmīgus izpētes projektus Eiropas Savienība atbalstīja jau Sestās pētniecības un tehnoloģiju attīstības pamatprogrammas ietvaros.
14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.
15 Skat. Eiropas Padomes konvencijas par kibernoziegumiem 35. pantu.

apmaiņas punktu palīdzību nodrošina iespēju paātrināti nodibināt sakarus starp dalībvalstīm lietās, kas saistītas ar elektroniskajiem pierādījumiem un kurās steidzami nepieciešama ārvalstu tiesību aizsardzības iestāžu palīdzība.

Viens no nozīmīgākajiem Eiropas un starptautiskajiem līdzekļiem šajā jomā ir Eiropas Padomes 2001. gada Konvencija par kibernoziegumiem[16]. Konvencija, kas tika pieņemta un stājās spēkā 2004. gadā, ietver vienotas dažādu kibernoziegumu definīcijas un ir pamats funkcionējošai dalībvalstu tiesiskajai sadarbībai. To ir parakstījušas daudzas valstis, ieskaitot Amerikas Savienotas Valstis un citas valstis ārpus Eiropas, kā arī visas ES dalībvalstis. Vairākas ES dalībvalstis tomēr vēl nav ratificējušas konvenciju vai tās papildprotokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. Ņemot vērā Konvencijas lielo nozīmi, Komisija rosinās dalībvalstis un attiecīgās trešās valstis ratificēt Konvenciju un apsver iespēju, ka Eiropas Kopiena varētu kļūt par Konvencijas dalībnieci.

3. KIBERNOZIEDZĪBAS APKAROŠANAS ĪPAŠO LĪDZEKĻU TURPMĀKĀ ATTĪSTĪBA

3.1. Operatīvās sadarbības tiesību aizsardzības jomā pastiprināšana un ES līmeņa apmācības pasākumi

Galvenā vājā vieta tieslietu, brīvības un drošības jomā ir steidzamas **pārrobežu operatīvās sadarbības** iespēju trūkums vai to nepietiekama izmantošana. Tradicionālā savstarpējās palīdzības sistēma ir izrādījusies lēna un neefektīva, kad jārisina steidzamas kibernoziedzības lietas, tomēr jauni sadarbības līdzekļi vēl nav pietiekami attīstīti. Kaut arī valstu tiesu un tiesību aizsardzības iestādes Eiropā cieši sadarbojas ar Eiropola, Eirojust un citu struktūru starpniecību, pastāv acīmredzama nepieciešamība pastiprināt un noskaidrot pienākumus. Komisijas uzsāktās konsultācijas norāda, ka šie ārkārtīgi svarīgie sadarbības kanāli netiek pilnībā izmantoti. Eiropā gan operatīvajā, gan stratēģiskajā līmenī ir vajadzīga vēl labāk koordinēta pieeja, un tai ir jāietver informācijas apmaiņa un labākā pieredze.

Tuvākā nākotnē Komisija īpašu uzmanību pievērsīs **apmācības** vajadzībām. Ir neapstrīdams fakts, ka tehnoloģiju attīstība rada nepieciešamību pēc nepārtrauktas tiesu un tiesību aizsardzības iestāžu apmācības attiecībā uz jautājumiem, kas skar kibernoziedzību. Tāpēc ir paredzēts pastiprināt un labāk koordinēt Eiropas Savienības finansiālo atbalstu daudznacionālajām apmācības programmām. Komisija strādās ciešā sadarbībā ar dalībvalstīm un citām kompetentām organizācijām, kā piemēram Eiropolu, Eirojust, Eiropas Policijas akadēmiju (CEPOL) un Eiropas Juridiskās tālākizglītības tīklu (EJTT), lai nodrošinātu visu attiecīgo apmācības programmu ciešu saistību un ES līmeņa koordināciju.

Komisija 2007. gadā rīkos dalībvalstu tiesību aizsardzības iestāžu, Eiropola, CEPOL un EJTT ekspertu **sanāksmi**, lai apspriestu, kā Eiropā uzlabot stratēģisko un operatīvo sadarbību, kā arī apmācību kibernoziedzības jomā. Kopā ar citiem jautājumiem tiks apsvērta iespēja izveidot gan pastāvīgu ES informācijas apmaiņas punktu, gan ES kibernoziedzības apmācības platformu. Tuvākajā laikā ir plānotas vairākas šādas sanāksmes, un 2007. gada sanāksme būs pirmā.

---

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

3.2. Dialoga ar ekonomikas nozaru pārstāvjiem uzlabošana

Gan privātais, gan valsts sektors ir ieinteresēti kopīgi izstrādāt metodes, lai noteiktu un novērstu noziedzīgo darbību radīto kaitējumu. Šāda privātā un valsts sektora sadarbība, kuras pamatā ir savstarpēja uzticēšanās un kopīgs mērķis – samazināt kaitējumu, varētu būt efektīvs līdzeklis drošības paaugstināšanai, kā arī cīņai ar kibernoziedzību. Komisijas kibernoziedzības politikas aspekti, kas skar valsts un privātā sektora sadarbību, ar laiku tiks iekļauti Komisijas plānotajā ES vispārīgajā politikā par privātā un valsts sektora dialogu, kas aptvers visas ar Eiropas drošību saistītās jomas. Politikas izstrādē īpaši iesaistīsies Eiropas Drošības izpētes un jauninājumu forums, ko Komisija plāno izveidot tuvākajā laikā un kurā būs sagrupēti nozīmīgi valsts un privātā sektora interesenti.

Moderno informācijas tehnoloģiju un elektronisko sakaru sistēmu attīstību lielākoties kontrolē privātie uzņēmumi. Privātās sabiedrības nodarbojas ar draudu novērtējumu, izstrādā programmatūru cīņai pret noziegumiem un attīsta tehniskos risinājumus to novēršanai. Ekonomikas nozaru pārstāvji demonstrē ļoti pozitīvu attieksmi, palīdzot valsts iestādēm cīņā ar kibernoziedzību, jo īpaši pūloties apkarot bērnu pornogrāfiju[17] un citus nelegāla satura informācijas izpausmes veidus internetā.

Vēl viens nopietns jautājums ir acīmredzamais informācijas, īpašo zināšanu un labāko prasmju apmaiņas trūkums starp valsts un privāto sektoru. Privātie uzņēmēji bieži vien, lai aizsargātu komercdarbības modeļus un noslēpumus, nepakļaujas prasībai informēt un sniegt ziņas tiesību aizsardzības iestādēm par noziedzīga rakstura parādībām, vai arī šāda prasība tiesiski nemaz nepastāv. Šāda informācija tomēr ir vajadzīga, lai valsts iestādes varētu izstrādāt efektīvu un atbilstošu kibernoziedzības apkarošanas politiku. Iespējas uzlabot starpnozaru informācijas apmaiņu apsvērs, ņemot vērā personas datu aizsardzības regulējumu.

Komisija jau šobrīd aktīvi līdzdarbojas dažādās publiski – privātās struktūrās, kas nodarbojas ar kibernoziedzību, piemēram, Krāpšanas novēršanas ekspertu grupa[18]. Komisija ir pārliecināta, ka efektīvai vispārīgai politikai cīņai ar kibernoziedzību ir jāietver arī stratēģija valsts un privātā sektora pārstāvju sadarbībai, sabiedriskās organizācijas ieskaitot.

Lai veicinātu plašāku valsts un privātā sektora sadarbību šajā jomā, Komisija 2007. gadā rīkos tiesību aizsardzības darba ekspertu un privātā sektora pārstāvju, jo īpaši interneta pakalpojumu piegādātāju, konferenci, lai apspriestu, kā Eiropā uzlabot abu sektoru operatīvo sadarbību[19]. Konferencē paredzēts apskatīt visus tematus, kas svarīgi abiem sektoriem, bet jo īpaši:

- operatīvās sadarbības uzlabošanai cīņai ar nelegālām darbībām un nelegāla satura informāciju internetā, jo īpaši pievēršot uzmanību tādām jomām kā terorisms, seksuālā vardarbība pret bērniem un citas prettiesiskas darbības, kas ir īpaši nozīmīgas no bērnu aizsardzības viedokļa,

---

17 Viens no jaunākajiem piemēriem sadarbībai šajā jomā ir sadarbība starp tiesību aizsardzības iestādēm un kredītkaršu sabiedrībām, kuras palīdzēja policijai izsekot bērnu pornogrāfijas pircējus tiešsaistē.

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

19 Šo konferenci varētu uzskatīt par turpinājumu ES forumam, kas minēts paziņojuma par datornoziedzību 6.4. sadaļā.

- ierosinājumam noslēgt savstarpējas vienošanās, kuru mērķis būtu Eiropas Savienībā bloķēt tīmekļa vietnes ar nelegālu saturu, jo īpaši materiālus par seksuālo vardarbību pret bērniem,

- Eiropas informācijas apmaiņas modeļa izstrādei, lai privātā un valsts sektora starpā notiktu būtiskās un nepieciešamās informācijas apmaiņa, ņemot vērā visu iesaistīto pušu intereses un uzturot savstarpējās uzticēšanās gaisotni,

- tiesību aizsardzības kontaktu punktu tīkla izveide gan valsts, gan privātajā sektorā.

3.3. Likumdošana

Nodarījumu veidu lielās dažādības dēļ, kurus aptver kibernoziedzības definīcija, vispārēja horizontāla noziegumu definīciju un valstu krimināllikumu harmonizācija kibernoziedzības jomā šobrīd vēl nav lietderīga. Tā kā tiesību aizsardzības iestāžu efektīva sadarbība bieži ir atkarīga no tā, vai pastāv vismaz daļēji saskaņotas nozieguma definīcijas, dalībvalstu tiesību aktu tuvināšana joprojām ir ilgtermiņa mērķis[20]. Attiecībā uz atsevišķām svarīgākajām noziegumu definīcijām ir sperts nopietns solis uz priekšu, pieņemot Pamatlēmumu par uzbrukumiem informācijas sistēmām. Kā jau iepriekš aprakstīts, kopš tā laika ir parādījušies jauni draudi, un Komisija, ņemot vērā to, cik svarīgi ir nepārtraukti novērtēt, vai nav radusies nepieciešamība papildināt tiesisko regulējumu, cieši seko līdzi šai attīstībai. Pieaugošo draudu uzraudzība notiek cieši saskaņā ar Eiropas Programmu svarīgāko infrastruktūras objektu aizsardzībai.

Šobrīd ir jāapsver arī tas, vai nav radusies nepieciešamība pēc tiesību aktiem, kas būtu vērsti tieši uz kibernoziedzības apkarošanu. Vēl viena īpaša problēma, kuru iespējams nāksies risināt likumdošanas ceļā, ir gadījumi, kad kibernoziegumu veic savienojumā ar **identitātes zādzību**. Vispārīgi ar „identitātes zādzību" izprot personu identificējošas informācijas, piemēram, kredītkartes numura, izmantošanu, lai veiktu citu noziegumu. Lielākajā daļā dalībvalstu noziedznieku tiesātu nevis par identitātes zādzību, bet par krāpšanu vai kādu citu atbilstošu noziedzīgu nodarījumu, ko uzskata par smagāku nodarījumu. Ne visās dalībvalstīs identitātes zādzība pati par sevi ir krimināli sodāma. Bieži vien tomēr identitātes zādzību ir vieglāk pierādīt nekā krāpšanu, tādējādi sadarbība ES tiesību aizsardzības jomā būtu daudz labāka, ja identitātes zādzība būtu krimināli sodāma visās dalībvalstīs. Komisija 2007. gadā uzsāks konsultācijas, lai novērtētu, vai šajā jomā ir nepieciešams uzsākt likumdošanas procesu.

3.4. Statistikas datu apstrāde

Ir panākta vispārēja vienošanās, ka pašreizējais stāvoklis attiecībā uz informāciju par noziedzības izplatīšanos ir absolūti neapmierinošs, un jo īpaši ir nepieciešams uzlabot dalībvalstu datu salīdzināšanu. *Paziņojumā par visaptverošas un saskaņotas ES stratēģijas izstrādi noziedzības un kriminālās tiesvedības novērtēšanai: ES rīcības plāns 2006.–2010. gadam*[21] Komisija nosprauda vērienīgu mērķi – piecu gadu laikā atrisināt šo problēmu. Ekspertu grupa, ko rīcības plānā paredzēts izveidot, uzsāks diskusiju, lai izstrādātu rādītājus kibernoziedzības izplatības novērtēšanai.

---

[20] Šis ilgtermiņa mērķis jau ir minēts 2001. gada paziņojuma 3. lapaspusē.

[21] COM(2006) 437, 7.8.2006.

4. TURPMĀKĀ VIRZĪBA

Komisija turpinās attīstīt vispārīgo politiku cīņai ar kibernoziedzību. Komisijas ierobežoto iespēju dēļ krimināltiesību jomā šī politika var tikai papildināt dalībvalstu un citu struktūru organizētos pasākumus. Rīcību vissvarīgākajos jautājumos, kas nozīmē viena, vairāku vai pat visu no 3. nodaļā aprakstīto līdzekļu izmantošanu, atbalstīs ar „Noziedzības novēršanas un cīņas pret noziedzību" Finanšu programmas līdzekļiem.

4.1. Cīņa ar kibernoziedzību kopumā

- Izveidot pastiprinātu operatīvo sadarbību starp dalībvalstu tiesību aizsardzības un tiesu iestādēm – pirmais pasākums šī mērķa sasniegšanai būs 2007. gada ekspertu sanāksme, kas iespējams ietvers arī centralizēta ES kibernoziedzības informācijas apmaiņas punkta izveidi.

- Palielināt finansiālo atbalstu ierosinājumiem par uzlabotu tiesību aizsardzības un tiesu iestāžu darbinieku apmācību attiecībā uz lietām, kas saistītas ar kibernoziedzību, un visu ar šo jomu saistīto daudznacionālo apmācības programmu koordinācija, izveidojot kopēju ES apmācības platformu.

- Veicināt dalībvalstu un visu valsts iestāžu aktīvāku iesaistīšanos cīņā ar kibernoziedzību, nodrošinot tai pietiekamu finansējumu.

- Atbalstīt izpēti kibernoziedzības jomā.

- Sarīkot vismaz vienu nozīmīgu tiesību aizsardzības iestāžu un privātā sektora pārstāvju konferenci (2007. gadā), jo īpaši, lai rosinātu sadarbību interneta un elektronisko sakaru tīklu prettiesiskas izmantošanas un pret tiem vērstu nelikumīgu darbību apkarošanai un veicinātu efektīvu vispārīgu informācijas apmaiņu, kā arī izstrādāt konkrētu valsts un privātā sektora sadarbības projektu, pamatojoties uz šīs 2007. gada konferences rezultātiem.

- Ierosināt un piedalīties publiskos un privātos pasākumos, kas vērsti uz kibernoziedzības radīto zaudējumu un draudu apzināšanās paaugstināšanu, jo īpaši patērētāju vidū, laikus izvairoties no patērētāju un lietotāju uzticības un paļāvības iedragāšanas, pārlieku pievēršot uzmanību tikai negatīvajiem aspektiem.

- Veicināt plašu starptautisko sadarbību kibernoziedzības apkarošanai un aktīvi darboties tajā.

- Rosināt, piedalīties un atbalstīt starptautiskos projektus, kas atbilst Komisijas politikas mērķiem šajā jomā, piemēram, G8 projektus, kas ir saskaņā ar valstu un reģionālajām stratēģijām par sadarbību ar trešām valstīm.

- Ar konkrētu rīcību mudināt dalībvalstis un attiecīgas trešās valstis ratificēt Eiropas Padomes Konvenciju par kibernoziegumiem un tās papildprotokolu un apsvērt iespēju, ka Kopiena varētu kļūt par konvencijas līgumslēdzēju pusi.

- Sadarbībā ar dalībvalstīm izpētīt koordinēto, plaša mēroga uzbrukumu fenomenu dalībvalstu informācijas infrastruktūrai ar nolūku novērst un apkarot šos uzbrukumus, ieskaitot atbilžu koordināciju un informācijas un labāko prakses piemēru apmaiņu.

4.2. Cīņa ar tradicionālajiem noziegumiem elektroniskajos tīklos

- Rosināt un veikt padziļinātu situācijas analīzi ar nolūku sagatavot priekšlikumu īpašam ES tiesiskajam regulējumam attiecībā uz identitātes zādzību.

- Veicināt tehnisko metožu un procedūru izstrādi cīņai ar krāpšanu un nelegālu tirdzniecību internetā, ieskaitot valsts un privātā sektora sadarbības projektus.

- Turpināt mērķtiecīgi strādāt tostarp īpašās jomās, piemēram, Krāpšanas novēršanas ekspertu grupā cīņai ar krāpšanu bezskaidras naudas norēķinos elektroniskajos tīklos.

4.3. Nelegāla satura informācija

- Turpināt izstrādāt pasākumus pret īpaša nelegāla satura informācijas izplatīšanu internetā, jo īpaši attiecībā uz materiāliem, kas atspoguļo seksuālu vardarbību pret bērniem un kūdīšanu uz terorismu, nopietni sekojot līdzi Pamatlēmuma ar bērnu seksuālās izmantošanas apkarošanu īstenošanai.

- Aicināt dalībvalstis piešķirt pietiekamu finansējumu, lai atbalstītu tiesību aizsardzības iestāžu darbu, īpašu uzmanību pievēršot tiešsaistē izplatīto seksuālās vardarbības materiālu upuru identifikācijai.

- Ierosināt un atbalstīt rīcību, kas vērsta pret nelegāla satura informāciju, kas var rosināt nepilngadīgos uz vardarbību vai cita veida prettiesisku uzvedību, piemēram, atsevišķas īpaši vardarbīgas tiešsaistes videospēles.

- Ierosināt un atbalstīt dialogu starp dalībvalstīm un ar trešām valstīm par nelegāla satura informācijas apkarošanas tehniskajām metodēm, kā arī par procedūrām, kā slēgt nelegālas tīmekļa vietnes, nolūkā cita starpā panākt iespējamu oficiālu nolīgumu izstrādi šajā jautājumā ar kaimiņvalstīm un citām valstīm.

- Izstrādāt ES līmeņa brīvprātīgus nolīgumus un vienošanās starp valsts iestādēm un privātā sektora pārstāvjiem, jo īpaši interneta pakalpojumu piegādātājiem, par procedūrām, kā tiek bloķētas un slēgtas nelegālas tīmekļa vietnes.

4.4. Pārskats par paveikto

Šajā paziņojumā vairāki konkrēti pasākumi ir minēti kā nākamie soļi ceļā uz dažādu struktūru sadarbības uzlabošanu Eiropas Savienībā. Komisija īstenos šos pasākumus, novērtēs sasniegto progresu un pasākumu ieviešanas procesu un sniegs ziņojumus Padomei un Parlamentam.