KOMISIJA EVROPSKIH SKUPNOSTI

Bruselj, 22.5.2007
COM(2007) 267 konč.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU IN EVROPSKEMU ODBORU REGIJ

Na poti k splošni politiki o boju proti kibernetskemu kriminalu

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

SPOROČILO KOMISIJE
EVROPSKEMU PARLAMENTU, SVETU
IN EVROPSKEMU ODBORU REGIJ

Na poti k splošni politiki o boju proti kibernetskemu kriminalu

1. UVOD

1.1. Kaj je kibernetski kriminal?

Varnost vedno bolj pomembnih informacijskih sistemov v naših družbah zajema več vidikov, katerih ključni element je boj proti kibernetskemu kriminalu. Ker ni dogovorjene opredelitve kibernetskega kriminala, se pojmi „kibernetski kriminal“, „računalniški kriminal“, „kriminal, povezan z računalniki“ ali „kriminal visoko razvite tehnologije“ pogosto uporabljajo kot sopomenke. Za namen tega sporočila „kibernetski kriminal“ pomeni „kazniva dejanja, storjena z uporabo elektronskih komunikacijskih omrežij in informacijskih sistemov ali proti takšnim omrežjem in sistemom“.

V praksi se pojem kibernetski kriminal uporablja za tri kategorije kriminalnih dejavnosti. Prva zajema **klasične oblike kaznivih dejanj** kot je goljufija ali ponarejanje, čeprav se v okviru kibernetskega kriminala nanašajo posebej na kazniva dejanja, storjena preko elektronskih komunikacijskih omrežij in informacijskih sistemov (v nadaljnjem besedilu: elektronska omrežja). Druga kategorija se nanaša na objavo **nezakonitih vsebin** preko elektronskih medijev (tj. vsebine, povezane s spolnim zlorabljanjem otrok ali spodbujanjem k rasnemu sovraštvu). Tretja vključuje **kazniva dejanja, značilna posebej za elektronska omrežja**, tj. napadi na informacijske sisteme, napadi za zavrnitev storitve in vdori v sisteme (hacking). Napadi te vrste so lahko usmerjeni tudi v ključne kritične infrastrukture v Evropi in vplivajo na obstoječe sisteme hitrega opozarjanja na več področjih z morebitnimi katastrofalnimi posledicami za celotno družbo. Za vsako od teh kategorij kaznivih dejanj je značilno, da so lahko storjena masovno in z dolgo geografsko razdaljo med kaznivim dejanjem in njegovimi posledicami. Zato so tehnični vidiki uporabljenih preiskovalnih metod pogosto enaki. Te skupne točke bodo tvorile osrednji dela tega sporočila.

1.2. Novosti na področju kibernetskega kriminala

1.2.1. Na splošno

Zaradi kriminalnih dejavnosti, ki se nenehno razvijajo, in pomanjkanja zanesljivih informacij je težko dobiti natančno sliko trenutnega stanja. Vendar je kljub temu mogoče opaziti nekatere splošne trende:

- število kibernetskih kaznivih dejanj narašča in kriminalne dejavnosti postajajo vedno bolj prefinjene in internacionalizirane[1]

[1] Večina trditev v tem Sporočilu o trenutnih trendih je bila povzeta iz Študije za oceno učinka komunikacije na kibernetski kriminal, ki jo je naročila Komisija leta 2006 (Pogodba št. JLS/2006/A1/003).

- jasni kazalniki kažejo vse večjo vpletenost organiziranih hudodelskih združb v kibernetski kriminal;

- kljub temu pa se število evropskih kazenskih pregonov na podlagi čezmejnega sodelovanja na področju kazenskega pregona ni povečalo.

1.2.2. Klasična kazniva dejanja, povezana z elektronskimi omrežji

Večino kaznivih dejanj je mogoče storiti z uporabo elektronskih omrežij, zlasti pogoste in razširjene oblike kaznivih dejanj, povezanih z elektronskimi omrežji, pa so zlasti različne vrste goljufij in poskusov goljufij. Instrumenti kot je kraja identitete, lažno predstavljanje[2], nezaželena elektronska pošta in zlonamerne kode se lahko uporabijo za storitev goljufije v velikem obsegu. Tudi nezakonito nacionalno ali mednarodno trgovanje na spletu postaja vse večji problem. To vključuje trgovino z drogami, ogroženimi vrstami in orožjem.

1.2.3. Nezakonita vsebina

V Evropi je dostopnih vedno več spletnih strani z nezakonito vsebino, ki zajemajo spolno zlorabljanje otrok, spodbujanje k terorističnim dejanjem, nezakonito spodbujanje k nasilju, terorizmu, rasizmu in ksenofobiji. Kazensko preganjanje takšnih strani je izjemno težavno, saj se lastniki in upravljavci spletnih strani pogosto ne nahajajo v ciljni državi, ampak v drugih državah, in pogosto zunaj EU. Spletne strani je mogoče zelo hitro prestaviti, tudi zunaj območja EU in opredelitev nezakonitosti se med državami precej razlikuje.

1.2.4. Kazniva dejanja, značilna posebej za elektronska omrežja

Zdi se, da postajajo napadi v velikem obsegu na informacijske sisteme ali organizacije in posameznike (pogosto preko tako imenovanih botnetov[3]) vse pogostejši. Nedavno je bilo mogoče opaziti tudi neposredne, sistematične in dobro usklajene napade v velikem obsegu proti ključni informacijski infrastrukturi države. To se je zaostrilo z tehnologijami, ki se združujejo, in pospešenim medsebojnim povezovanjem informacijskih sistemov, kar je povečalo ranljivost teh sistemov. Napadi so pogosto dobro organizirani in uporabljeni za namene izsiljevanja. Sklepati je mogoče, da je obseg prijavljanja kršitev zmanjšan delno zaradi poslovne škode, ki lahko nastane, če težave z varnostjo postanejo javne.

1.3. Cilji

V skladu s spreminjajočim se okoljem se je pojavila nujna potreba po ukrepanju – na nacionalni in evropski ravni – proti vsem oblikam kibernetskega kriminala, ki so vse večje grožnje za ključno infrastrukturo, družbo, gospodarstvo in državljane. Varstvo posameznikov pred kibernetskemu kriminalu je pogosto oslabljeno zaradi vprašanj določanja ustrezne sodne pristojnosti, prava, ki se uporablja, čezmejnega kazenskega pregona ali priznanja in uporabe elektronskih dokazov. Pretežno čezmejna razsežnost kibernetskega kriminala poudarja takšne težave. Komisija za obravnavanje teh groženj uvaja splošno politično pobudo za izboljšanje usklajevanja v boju proti kibernetskemu kriminalu na evropski in mednarodni ravni.

---

[2] Lažno predstavljanje pomeni poskus goljufive pridobitve občutljivih podatkov, kot so gesla in podatki o kreditni kartici, z izdajanjem za zaupanja vredno osebo v elektronskem sporočilu.

[3] Botnet se nanaša na omrežje kompromitiranih računalnikov, na katerih so nameščeni programski roboti in se upravljajo na daljavo.

Cilj te pobude je okrepiti boj proti kibernetskemu kriminalu na nacionalni, evropski in mednarodni ravni. Države članice in Komisija za prednostno nalogo že dalj časa štejejo zlasti nadaljnji razvoj posebne politike EU. Pobuda bo usmerjena v razsežnosti kazenskega pregona in kazenskega prava tega boja in politika bo dopolnjevala druge ukrepe EU za splošno izboljšanje varnosti v kibernetskem prostoru. Politika bo sčasoma vključevala: izboljšano operativno sodelovanje na področju kazenskega pregona; boljše politično sodelovanje in usklajevanje med državami članicami; politično in pravno sodelovanje s tretjimi državami; povečanje ozaveščenosti; usposabljanje; raziskave; okrepljen dialog z industrijo in možne zakonodajne ukrepe.

Politika o boju in pregonu kibernetskega kriminala bo določena in se bo izvajala s popolnim spoštovanjem temeljnih pravic, zlasti svobode izražanja, spoštovanja zasebnega in družinskega življenja ter varstva osebnih podatkov. Za vsak zakonodajni ukrep, sprejet v okviru te politike, bo najprej izvedeno preverjanje skladnosti s temi pravicami, zlasti z Listino EU o temeljnih pravicah. Treba je tudi poudariti, da bodo vse takšne politične pobude izvedene s popolnim spoštovanjem členov 12 do 15 tako imenovane Direktive o e-poslovanju[4], v primerih, ko se ta pravni instrument uporablja.

Cilj tega sporočila je mogoče razdeliti na tri glavna operativna področja, in sicer:

- izboljšati in olajšati usklajevanje in sodelovanje med enotami za boj proti kibernetskemu kriminalu, drugimi zadevnimi organi in drugimi strokovnjaki v Evropski uniji;

- razviti z usklajevanjem z državami članicami, zadevnimi organizacijami EU in mednarodnimi organizacijami ter drugimi interesnimi skupinami skladen politični okvir EU o boju proti kibernetskemu kriminalu;

- povečati ozaveščenosti o stroških in nevarnostih kibernetskega kriminala.

2. OBSTOJEČI PRAVNI INSTRUMENTI ZA BOJ PROTI KIBERNETSKEMU KRIMINALU

2.1. Obstoječi instrumenti in ukrepi na ravni EU

To sporočilo o politiki kibernetskega kriminala utrjuje in razvija Sporočilo iz leta 2001 o oblikovanju varnejše informacijske družbe z izboljšanjem varnosti informacijskih infrastruktur in bojem proti računalniškemu kriminalu[5] (v nadaljnjem besedilu: Sporočilo iz leta 2001). V Sporočilu iz leta 2001 so bili predlagani ustrezni materialni in procesni pravni predpisi, ki obravnavajo domače in transnacionalne kriminalne dejavnosti. Temu je sledilo več pomembnih predlogov. Ti vključujejo zlasti predlog, na podlagi katerega je bil sprejet Okvirni sklep 2005/222/PNZ o napadih na informacijske sisteme[6]. V zvezi s tem je treba tudi omeniti, da so bili sprejeti drugi, splošnejši predpisi, ki tudi zajemajo vidike boja proti kibernetskemu kriminalu, kot je Okvirni sklep 2001/413/PNZ o boju proti goljufiji in ponarejanju v zvezi z negotovinskimi plačilnimi sredstvi[7].

---

4 Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (UL L 178, 17.7.2000, str. 1).

5 COM(2000) 890, 26.1.2001.

6 UL L 69, 16.3.2005, str. 67.

7 UL L 149, 2.6.2001, str. 1.

Okvirni Sklep 2004/68/PNZ o spolnemu izkoriščanju otrok[8] je dober primer, kako Komisija namenja posebno pozornost **varstvu otrok,** zlasti v povezavi z bojem proti vsem oblikam vsebin, povezanih s spolnim zlorabljanjem otrok, ki so nezakonito objavljene z uporabo informacijskih sistemov; ta horizontalna prednostna naloga se bo ohranila tudi v prihodnosti.

Za rešitev težav v zvezi z varnostjo v informacijski družbi je Evropska skupnost razvila tridelni pristop za varnost omrežij in informacij: posebne ukrepe za varnost omrežij in informacij, regulativni okvir za elektronske komunikacije in boj proti kibernetskemu kriminalu. Čeprav je te tri vidike do določene mere mogoče razvijati ločeno, je zaradi številnih soodvisnosti potrebno tesno usklajevanje. Na povezanem področju varnosti omrežij in informacij je bilo vzporedno s sporočilom iz leta 2001 o kibernetskemu kriminalu sprejeto Sporočilo Komisije iz leta 2001 o varnosti omrežij in informacij: Predlog za pristop politike EU[9]. Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/ES določa obveznost za ponudnike javno dostopnih elektronskih komunikacijskih storitev, naj zagotovijo varnost svojih storitev. Vsebuje tudi določbe proti nezaželeni elektronski pošti in vohunski programski opremi. Politika o varnosti omrežij in informacij se je od takrat razvijala preko številnih ukrepov, nazadnje s Sporočilom o strategiji za varno informacijsko družbo[10], ki določa prenovljeno strategijo in zagotavlja okvir za nadaljnji razvoj in izboljšanje skladnega pristopa k varnosti omrežij in informacij, s Sporočilom o boju proti nezaželeni elektronski pošti ter vohunski in zlonamerni programski opremi[11], ter z ustanovitvijo ENISA leta 2004[12]. Glavni cilj ENISA je razviti strokovno znanje, da se spodbudi sodelovanje med javnim in zasebnim sektorjem ter zagotovi pomoč Komisiji in državam članicam. **Rezultati raziskave** na področju tehnologij za zavarovanje informacijskih sistemov bodo tudi imeli pomembno vlogo pri boju proti kibernetskemu kriminalu. Zato so informacijske in komunikacijske tehnologije in tudi varnost navedene kot cilji v Sedmem okvirnem raziskovalnem programu EU (OP 7), ki velja za obdobje 2007–2013[13]. Pregled regulativnega okvira za elektronske komunikacije bi lahko imel za posledico spremembe, da se poveča učinkovitost z varnostjo povezanih določb, Direktive o zasebnosti in elektronskih komunikacijah ter Direktive o univerzalnih storitvah 2002/22/ES[14].

2.2. Obstoječi mednarodni instrumenti

Zaradi globalne narave informacijskih omrežij nobena politika o kibernetskem kriminalu ne more biti učinkovita, če so prizadevanja omejena znotraj EU. Storilci kaznivih dejanj lahko napadajo informacijske sisteme ali storijo kazniva dejanja iz ene države članice v drugo in z lahkoto tudi zunaj območja pristojnosti EU. Zato je Komisija dejavno sodelovala v mednarodnih razpravah in strukturah za sodelovanje, tj. v Skupini G8 Lyon-Rim za kriminal visoko razvite tehnologije in projektih, ki jih vodi Interpol. Komisija posebej podrobno spremlja delo omrežja za 24-urne stike za mednarodni kriminal visoko razvite tehnologije (omrežje 24/7)[15], v katerem sodeluje veliko število držav po svetu, vključno z večino držav

---

8 UL L 13, 20.1.2004, str. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.
12 Uredba št. 460/2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij, (UL L 77, 13.3.2004, str. 1.).
13 Evropska unija je že v okviru Šestega okvirnega programa za raziskave in tehnološki razvoj podprla številne ustrezne in uspešne raziskovalne projekte.
14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.
15 Glej člen 35 Konvencije Sveta Evrope o kibernetski kriminaliteti.

članic EU. Omrežje G8 je mehanizem za hitre stike med sodelujočimi državami s kontaktnimi točkami, ki delujejo 24 ur na dan, za primere, ki vključujejo elektronske dokaze, in tiste, ki zahtevajo nujno pomoč tujih organov kazenskega pregona.

Verjetno je glavni evropski in mednarodni instrument na tem področju Konvencija Sveta Evrope iz leta 2001 o kibernetski kriminaliteti[16]. Konvencija, ki je bila sprejeta in je začela veljati leta 2004, vsebuje skupne opredelitve različnih vrst kibernetskega kriminala in določa podlago za uspešno pravosodno sodelovanje med državami pogodbenicami. Podpisale so jo mnoge države, vključno z Združenimi državami Amerike in drugimi neevropskimi državami, ter vse države članice. Vendar številne držav članice še niso ratificirale te Konvencije ali dodatnih protokolov h Konvenciji, ki obravnavajo dejanja, povezana z rasizmom ali ksenofobijo, storjena preko računalniških sistemov. Ob upoštevanju dogovorjene pomembnosti Konvencije bo Komisija spodbudila države članice in zadevne tretje države, naj ratificirajo Konvencijo in razmislijo o možnosti, da Evropska skupnost postane pogodbenica Konvencije.

3. NADALJNJI RAZVOJ POSEBNIH INSTRUMENTOV ZA BOJ PROTI KIBERNETSKEMU KRIMINALU

3.1. Krepitev operativnega sodelovanja na področju kazenskega pregona in prizadevanja za usposabljanje na ravni EU

Pomanjkanje ali nezadostna uporaba neposrednih struktur za **čezmejno operativno sodelovanje** ostaja glavna pomanjkljivost na območju svobode, varnosti in pravice. Tradicionalna medsebojna pomoč v nujnih primerih kibernetskega kriminala se je izkazala za počasno in neučinkovito, nove strukture sodelovanja pa še niso razvite v zadostni meri. Medtem ko nacionalni pravosodni organi in organi kazenskega pregona v Evropi tesno sodelujejo preko Europola, Eurojusta in drugih struktur, ostaja očitna potreba po krepitvi in razjasnitvi obveznosti. Posvetovanja, ki jih je izvedla Komisija, kažejo, da ti ključni načini sodelovanja niso optimalno uporabljeni. Bolj usklajen evropski pristop mora biti operativen in strateški, zajemati pa mora tudi izmenjavo informacij in najboljših praks.

Komisija bo v bližnji prihodnosti namenila posebno pozornost potrebam po **usposabljanju**. Dejstvo je, da nastaja zaradi tehnološkega razvoja potreba po nenehnem usposabljanju o vprašanjih kibernetskega kriminala za organe kazenskega pregona in pravosodne organe. Zato je predvidena okrepljena in bolj usklajena finančna podpora s strani EU za večnacionalne programe usposabljanja. Komisija si bo v tesnem sodelovanju z državami članicami in drugimi pristojnimi organi, kot so Europol, Eurojust, Evropska policijska akademija (CEPOL) in Evropska mreža za pravno usposabljanje (EJTN), prizadevala tudi za usklajevanje in medsebojno povezovanje vseh zadevnih programov usposabljanja na ravni EU.

Komisija bo leta 2007 organizirala **srečanje** strokovnjakov kazenskega pregona iz držav članic in tudi iz Europola, CEPOL-a ter EJTN, na katerem se bo razpravljalo o načinih izboljšanja strateškega in operativnega sodelovanja ter tudi usposabljanja o kibernetskemu kriminalu v Evropi. Med drugim bo obravnavana vzpostavitev stalne kontaktne točke EU za izmenjavo informacij in platforme EU za usposabljanje o kibernetskemu kriminalu. Srečanje v letu 2007 bo prvo v vrsti načrtovanih srečanj za bližnjo prihodnost.

---

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

3.2. Okrepitev dialoga z industrijo

Zasebni in tudi javni sektor imata interes za skupno razvijanje načinov ugotavljanja in preprečevanja škode, nastale s kaznivimi dejanji. Skupna udeležba zasebnega in javnega sektorja, ki temelji na medsebojnem zaupanju in skupnemu cilju zmanjšanja škode, naj bi bila učinkovit način za krepitev varnosti tudi v boju proti kibernetskemu kriminalu. Javno-zasebni vidiki politike Komisije o kibernetskem kriminalu bodo sčasoma postali del načrtovane globalne politike EU o dialogu med javnim in zasebnim sektorjem, ki bo zajemala celotno področje evropske varnosti. To politiko bo zlasti razvijal Evropski forum za raziskave in inovacije na področju varnosti, ki ga Komisija namerava ustanoviti v bližnji prihodnosti in ki bo prerazporedil zadevne interesne skupine iz javnega in zasebnega sektorja.

Razvoj sodobnih informacijskih tehnologij in elektronskih komunikacijskih sistemov v glavnem nadzirajo zasebni operaterji. Zasebne družbe izvajajo ocene groženj, uvajajo programe za boj proti kriminalu in razvijajo tehnične rešitve za preprečevanje kriminala. Industrija je pokazala zelo pozitiven odnos do pomoči javnim organom v boju proti kibernetskemu kriminalu, zlasti s prizadevanji za boj proti otroški pornografiji[17] in drugim vrstam nezakonite vsebine na internetu.

Drugo vprašanje zadeva očitno pomanjkanje izmenjave informacij, strokovnega znanja in najboljših praks med javnim in zasebnim sektorjem. Da bi zaščitili poslovne modele in skrivnosti so operaterji zasebnega sektorja pogosto nenaklonjeni sporočanju ali posredovanju informacij o kaznivih dejanjih organom kazenskega pregona, ali jih za to ne zavezuje jasna pravna obveznost. Vendar bi bile takšne informacije morda potrebne, da bi javni organi lahko oblikovali učinkovito in ustrezno politiko boja proti kriminalu. Možnosti za izboljšanje medsektorske izmenjave informacij bodo obravnavane tudi ob upoštevanju obstoječih pravil o varstvu osebnih podatkov.

Komisija že igra pomembno vlogo v različnih javno-zasebnih strukturah, ki se ukvarjajo s kibernetskim kriminalom, kot je Skupina za preprečevanje goljufij[18]. Komisija je prepričana, da mora učinkovita splošna politika za boj proti kibernetskemu kriminalu vključevati tudi strategijo za sodelovanje med javnim sektorjem in operaterji v zasebnem sektorju, vključno z organizacijami civilne družbe.

Da se doseže javno-zasebno sodelovanje na tem področju, bo Komisija leta 2007 organizirala konferenco za strokovnjake kazenskega pregona in predstavnike zasebnega sektorja, zlasti ponudnike internetnih storitev, na kateri se bo razpravljalo o načinih izboljšanja javno-zasebnega operativnega sodelovanja v Evropi[19]. Konferenca bo obravnavala vsa vprašanja, za katera se šteje, da dodajajo vrednost v obeh sektorjih, zlasti pa:

- izboljšanje operativnega sodelovanja na področju boja proti nezakonitim dejavnostim in vsebinam na internetu, zlasti na področju terorizma, vsebin, povezanih s spolnim zlorabljanjem otrok, in drugih nezakonitih dejavnosti, ki so še posebej občutljive z vidika varstva otrok;

---

[17] Nedavni primer sodelovanja na tem področju je sodelovanje med organi kazenskega pregona in družbami, ki izdajajo kreditne kartice, preko katerega so slednje pomagale policiji izslediti kupce otroške pornografije na spletu.

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

[19] Konferenca se lahko šteje za nadaljevanje foruma EU, navedenega v razdelku 6.4 sporočila o računalniškem kriminalu.

- uvedba javno-zasebnih dogovorov, katerih namen je blokiranje spletnih strani v EU, ki vsebujejo nezakonito vsebino, zlasti vsebine, povezane z spolnim zlorabljanjem otrok;

- oblikovanje evropskega modela za izmenjavo potrebnih in ustreznih informacij v zasebnem in javnem sektorju, ki bo med drugim krepil vzajemno zaupanje in upošteval interese vseh sodelujočih;

- vzpostavitev omrežja kontaktnih točk kazenskega pregona v zasebnem in javnem sektorju.

3.3. Zakonodaja

Splošna uskladitev opredelitev kaznivih dejanj in nacionalnih kazenskih zakonov na področju kibernetskega kriminala še vedno ni ustrezna zaradi različnih vrst kaznivih dejanj, zajetih s tem pojmom. Ker je učinkovito sodelovanje med organi kazenskega pregona pogosto odvisno od obstoja vsaj delno usklajenih opredelitev kaznivih dejanj, je usklajevanje zakonodaj držav članic še vedno dolgoročen cilj[20]. Glede na nekatere ključne opredelitve kaznivih dejanj je bil pomemben korak že storjen z Okvirnim sklepom o napadih na informacijske sisteme. Kakor je navedeno zgoraj, so se pozneje pojavile nove grožnje in Komisija pozorno spremlja ta razvoj zaradi pomembnosti stalnega ocenjevanja potrebe po dodatni zakonodaji. Spremljanje nastajajočih groženj je podrobno usklajeno z Evropskim programom za varovanje ključne infrastrukture.

Vendar je treba tudi ciljno zakonodajo proti kibernetskemu kriminalu obravnavati zdaj. Posebno vprašanje, ki bi lahko zahtevalo pravno ureditev, se nanaša na primere, ko je kibernetski kriminal storjen v povezavi s **krajo identitete**. „Kraja identitete“ na splošno pomeni uporabo osebnih podatkov, na podlagi katerih je mogoče ugotoviti istovetnost, npr. številko kreditne kartice, kot instrument za storitev drugih kaznivih dejanj. V večini držav članic bo storilec kaznivega dejanja običajno sodno preganjan za goljufijo ali drugo možno kaznivo dejanje, ne pa za krajo identitete; prva se šteje za težjo obliko kaznivega dejanja. Kraja identitete kot taka ni inkriminirana v vseh državah članicah. Pogosto je lažje dokazati kaznivo dejanje kraje identitete kot pa goljufijo, zato bi bilo sodelovanje med organi kazenskega pregona EU učinkovitejše, če bi bila kraja identitete inkriminirana v vseh državah članicah. Komisija bo leta 2007 začela s posvetovanji, da bo ocenila, ali je zakonodaja ustrezna.

3.4. Razvoj statističnih podatkov

Na splošno velja, da je trenutno stanje glede informacij o razširjenosti kaznivih dejanj v glavnem neustrezno, in zlasti da je potrebno znatno izboljšanje, da bi se lahko primerjali podatki med državami članicami. Ambiciozen petletni načrt za reševanje tega problema je bil določen v Sporočilu Komisije o *razvoju skladne in celovite strategije EU za merjenje kriminala in kazenskega pravosodja*: *Akcijski načrt EU 2006–2010* z dne 7. avgusta 2006[21]. Strokovna skupina, ustanovljena na podlagi tega akcijskega načrta, bi pomenila primeren forum za razvoj ustreznih kazalnikov za merjenje obsega kibernetskega kriminala.

---

[20] Ta dolgoročen cilj je bil omenjen že na strani 3 Sporočila iz leta 2001.

[21] COM(2006) 437, 7.8.2006.

4. POT NAPREJ

Komisija bo nadaljevala delo v zvezi s splošno politiko za boj proti kibernetskemu kriminalu. Zaradi omejenih pristojnosti Komisije na področju kazenskega prava bo ta politika lahko zgolj dopolnjevala ukrepe, ki jih sprejmejo države članice in drugi organi. Najpomembnejši ukrepi – vsak od njih bo vseboval uporabo enega, več ali vseh instrumentov, navedenih v poglavju 3 – bodo podprti tudi preko finančnega programa „Preprečevanje in boj proti kriminalu“:

4.1. Boj proti kibernetskemu kriminalu na splošno

- Vzpostaviti okrepljeno operativno sodelovanje med organi kazenskega pregona in pravosodnimi organi držav članic; ukrep, ki se bo začel z organizacijo posebnega srečanja strokovnjakov v letu 2007 in ki bi lahko vključeval vzpostavitev osrednje kontaktne točke EU za kibernetski kriminal;

- povečati finančno podporo za pobude za izboljšano usposabljanje organov kazenskega pregona in pravosodnih organov v zvezi z obravnavanjem primerov kibernetskega kriminala ter sprejeti ukrepe za uskladitev vseh prizadevanj za večnacionalno usposabljanje na tem področju z vzpostavitvijo platforme EU za usposabljanje;

- spodbuditi večjo zavezanost držav članic in vseh javnih organov, da sprejmejo učinkovite ukrepe proti kibernetskemu kriminalu in dodelijo zadostna sredstva za boj proti takšnim kaznivim dejanjem;

- podpirati raziskave, ki so koristne za boj proti kibernetskemu kriminalu;

- organizirati vsaj eno večjo konferenco (v letu 2007) z organi kazenskega pregona in zasebnimi operaterji, zlasti za začetek sodelovanja v boju proti nezakonitim internetnim dejavnostim v elektronskih omrežjih ter zoper ta omrežja in spodbujati učinkovitejšo izmenjavo neosebnih podatkov ter nadaljevati z delom na podlagi sklepov te konference iz leta 2007 s konkretnimi javno-zasebnimi projekti sodelovanja;

- prevzeti pobudo za javno-zasebne ukrepe, namenjene povečanju ozaveščenosti glede stroškov in nevarnosti kibernetskega kriminala zlasti med potrošniki in v njih sodelovati ter se hkrati izogniti spodkopavanju zaupanja potrošnikov in uporabnikov z osredotočanjem zgolj na negativne vidike varnosti;

- dejavno se vključiti v globalnem mednarodnem sodelovanju v boju proti kibernetskemu kriminalu in ga spodbujati;

- uvesti, prispevati in podpirati mednarodne projekte, ki so skladni s politiko Komisije na tem področju, npr. projekte, ki jih vodi G8 in so skladni z državnimi in regionalnimi strateškimi dokumenti (glede sodelovanja s tretjimi državami);

- sprejeti konkretne ukrepe, da bi vse države članice in zadevne tretje države spodbudili k ratifikaciji Konvencije Sveta Evrope o kibernetski kriminaliteti in njenim dodatnim protokolom ter obravnavali možnost, da Skupnost postane pogodbenica Konvencije.

- proučiti, skupaj z državami članicami, fenomen usklajenih napadov in napadov v velikem obsegu na informacijsko infrastrukturo držav članic z namenom preprečevanja in boja proti tem napadom, vključno z usklajevanjem odgovorov in izmenjavo informacij in najboljših praks.

4.2. Boj proti klasičnim kaznivim dejanjem v elektronskih omrežjih

- Začeti s poglobljeno analizo, da se oblikuje predlog za poseben predpis EU proti kraji identitete;

- spodbuditi razvoj tehničnih metod in postopkov za boj proti goljufiji in nezakonitemu poslovanju na internetu, tudi preko javno-zasebnih projektov sodelovanja;

- nadaljevati in razvijati delo na posebej določenih področjih, kot je strokovna skupina za preprečevanje goljufij na področju boja proti goljufijam z negotovinskimi načini plačevanja v elektronskih omrežjih.

4.3. Nezakonita vsebina

- Nadaljevati razvijanje ukrepov proti določenim nezakonitim vsebinam, zlasti glede vsebin, povezanih s spolnim zlorabljanjem otrok in spodbujanjem k terorizmu, in sicer preko spremljanja izvajanja Okvirnega sklepa o spolnem izkoriščanju otrok;

- pozvati države članice, naj dodelijo zadostna finančna sredstva za okrepitev dela organov kazenskega pregona, s posebnim poudarkom na ugotavljanju žrtev vsebin, povezanih s spolnim zlorabljanjem, ki so razširjane na spletu;

- sprožiti in podpreti ukrepe proti nezakonitim vsebinam, ki bi mladoletnike lahko spodbujale k nasilnim ali drugim hujšim nezakonitim dejanjem, tj. določene vrste izredno nasilnih računalniških igric na spletu;

- začeti in spodbuditi dialog med državami članicami in tretjimi državami o tehničnih metodah za boj proti nezakonitim vsebinam kot tudi o postopkih za ukinitev nezakonitih spletnih strani, tudi z namenom, da se oblikujejo formalni dogovori s sosednjimi državami o tem vprašanju;

- oblikovati prostovoljne sporazume in konvencije na ravni EU med javnimi organi in zasebnimi operaterji, zlasti ponudniki internetnih storitev, glede postopkov za blokiranje in ukinitev nezakonitih internetnih strani.

4.4. Spremljanje izvajanja

V skladu s tem sporočilom so številni ukrepi, namenjeni izboljšanju struktur sodelovanja v EU, določeni kot koraki za nadaljnje ukrepanje. Komisija bo te ukrepe nadgradila, ocenila napredek izvajanja dejavnosti ter poročala Svetu in Parlamentu.