CyberCrime@IPA

Zajednički projekt EU/VE o regionalnoj suradnji u borbi protiv računalnog kriminaliteta

Strateški prioriteti u suradnji protiv računalnog kriminaliteta

koji su usvojeni na

Sastanku ministara i visokih dužnosnika ministarstava unutarnjih poslova i sigurnosti, ministarstava pravosuđa i državnih odvjetništava u državama i područjima koje sudjeluju u CyberCrime@IPA projektu[1]

Dubrovnik, Hrvatska, 15. veljače 2013

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

[1]Albanija, Bosna i Hercegovina, Crna Gora, Hrvatska, Srbija, „Bivša Jugoslavenska Republika Makedonija", Turska i Kosovo*.
* Imenovanje je bez predrasuda na poziciju ili status te u skladu s UNSC 1244 i mišljenjem Međunarodnog suda pravde o Deklaraciji o nezavisnosti Kosova

Sadržaj

Deklaracija ministara i visokih dužnosnika o strateškim prioritetima u suzbijanju računalnog kriminaliteta 3

Dodatak: Strateški prioriteti u suzbijanju računalnog kriminaliteta 5

1. Strateški prioritet: Politike i strategije suzbijanja računalnog kriminaliteta 5
2. Strateški prioritet: Potpuna i učinkovita pravna osnova za postupanje kaznenog pravosuđa 6
3. Strateški prioritet: Specijalizirane jedinice za računalni kriminalitet 7
4. Strateški prioritet: Obuka policijskih službenika 8
5. Strateški prioritet: Obuka pravosudnih dužnosnika 9
6. Strateški prioritet: Financijske istrage i sprječavanje i kontrola prijevara i pranja novca na Internetu 10
7. Strateški prioritet: Suradnja između policijskih službenika i davatelja Internetskih usluga 11
8. Strateški prioritet: Efikasnija regionalna i međunarodna suradnja 12

Napomena: Ovaj je dokument pripremljen uz potporu CyberCrime@IPA zajedničkog projekta Europske unije i Vijeća Europe o regionalnoj suradnji u kaznenom pravosuđu: Jačanje kapaciteta u borbi protiv računalnog kriminaliteta.

Kontakt

Za daljnje informacije molimo kontaktirajte:

Odjel za zaštitu podataka i borbu protiv kibernetičkog kriminala
Opća uprava za ljudska prava i pravne poslove
Vijeće Europe
Strasbourg, Francuska
Tel : +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Deklaracija ministara i visokih dužnosnika o strateškim prioritetima u suzbijanju računalnog kriminaliteta

Mi, ministri i visoki dužnosnici ministarstava unutarnjih poslova i sigurnosti, ministarstava pravosuđa i državnih odvjetništava država i područja koje sudjeluju u CyberCrime@IPA projektu

- sastajući se na ovoj regionalnoj Konferenciji o strateškim prioritetima u suzbijanju računalnog kriminaliteta održanoj u Dubrovniku, Hrvatska, od 13.-15. veljače 2013. godine, u suradnji s Vijećem Europe i Europskom unijom;

- svjesni prednosti informacijskih i komunikacijskih tehnologija koje mijenjaju naša društva;

- svjesni rizika od računalnog kriminaliteta koji negativno utječe na povjerenje u informacijske tehnologije kao i na prava i sigurnost pojedinaca, uključujući osobito djecu;

- prepoznajući pozitivnu obvezu vlada da zaštite pojedince od računalnog kriminaliteta;

- obzirni prema potrebi poštivanja temeljnih prava i sloboda, uključujući zaštitu pojedinaca u odnosu na obradu osobnih podataka pri zaštiti društva od kriminaliteta;

- uzimajući u obzir potrebu za suradnjom između javnog i privatnog sektora u sprječavanju i kontroli računalnog kriminaliteta i zaštite računalnih sustava;

- vjerujući da učinkovite mjere protiv računalnog kriminaliteta zahtijevaju učinkovitu regionalnu i međunarodnu suradnju;

- naglašavajući vrijednost Konvencije o kibernetičkom kriminalu iz Budimpešte kao smjernice za nacionalno zakonodavstvo i okvira za međunarodnu suradnju;

- primjećujući rastuću važnost koju Europska unija posvećuje računalnoj sigurnosti i borbi protiv računalnog kriminaliteta;

- posebice uzimajući u obzir da je potrebno graditi partnerstvo između Europskog centra za računalni kriminalitet (EC3) pri Europolu i naših tijela za provedbu zakona;

- zahvalni na potpori pruženoj od Europske unije i Vijeća Europe kroz CyberCrime@IPA regionalni projekt;

- gradeći na postignutom napretku i radnjama poduzetim protiv računalnog kriminaliteta u državama i područjima u regiji, istovremeno utvrđujući da su potrebni daljnji napori;

Potvrđujemo

strateške prioritete u suzbijanju računalnog kriminaliteta predstavljene na ovoj konferenciji

i

obvezujemo se

- provoditi strategije suzbijanja računalnog kriminaliteta kako bi se osigurao učinkovit odgovor kaznenog pravosuđa na kaznena djela počinjena protiv računala ili pomoću računala kao i svih kaznenih djela koja uključuju elektroničke dokaze;

- usvojiti potpuno i učinkovito zakonodavstvo o računalnom kriminalitetu koje poštuje zahtjeve u svezi ljudskih prava i vladavine prava;

- jačati specijalizirane policijske jedinice i specijalizaciju službi državnog odvjetništva u odnosu na računalni kriminalitet i elektroničke dokaze;

- provoditi održive strategije obuke policijskih službenika;

- pružiti potporu obuci sudaca i državnih odvjetnika o računalnom kriminalitetu i elektroničkim dokazima;

- provoditi sveobuhvatne strategije za zaštitu djece od seksualnog iskorištavanja i zlostavljanja na Internetu u skladu s Konvencijom iz Lanzarotea;

- promicati financijske istrage i sprječavanje i kontrolu prijevara i pranja novca na Internetu;

- jačati suradnju s privatnim sektorom, pogotovo između policijskih službenika i davatelja Internetskih usluga;

- uključiti u učinkovitu regionalnu i međunarodnu suradnju;

- podijeliti naša iskustva s drugim svjetskim regijama u cilju potpore jačanju kapaciteta u borbi protiv računalnog kriminaliteta;

- promicati poštivanje Konvencije o kibernetičkom kriminalu iz Budimpešte na globalnoj razini.

Deklaracija jednoglasno usvojena u

Dubrovniku, Hrvatska, 15. veljače 2013.

Dodatak: Strateški prioriteti u suzbijanju računalnog kriminaliteta

1. Strateški prioritet: Politike i strategije suzbijanja računalnog kriminaliteta

Kako se društva mijenjaju pod utjecajem informacijskih i komunikacijskih tehnologija, njihova je sigurnost postala politički prioritet mnogih vlada. To se odražava u donošenju strategija o računalnoj sigurnosti s primarnim fokusom na zaštitu ključne informacijske infrastrukture. Međutim, vlade također imaju pozitivnu obvezu zaštite ljudi i njihovih prava od računalnog kriminaliteta i dovođenja počinitelja pred lice pravde.

Sukladno tome, vlade trebaju razmotriti pripremu specifičnih strategija suzbijanja računalnog kriminaliteta ili unaprijediti komponente o računalnom kriminalitetu u okviru strategija ili politika o računalnoj sigurnosti.

Nadležna tijela trebaju razmotriti sljedeće aktivnosti:

- **Donošenje politika ili strategija suzbijanja računalnog kriminaliteta** s ciljem osiguravanja djelotvornog odgovora kaznenog pravosuđa na kaznena djela počinjena protiv računala ili pomoću računala, kao i na sva kaznena djela koja uključuju elektroničke dokaze. Kao elemente takvih politika ili strategija potrebno je razmotriti preventivne mjere, zakonodavstvo, specijalizirane policijske jedinice i službe državnog odvjetništva, međuagencijsku suradnju, obuku policijskih i pravosudnih službenika, javno/privatnu suradnju, učinkovitu međunarodnu suradnju, financijske istrage i sprječavanje prijevara i pranja novca te zaštitu djece od seksualnog nasilja.

- **Osigurati da se poštuju zahtjevi u svezi ljudskih prava i vladavine prava** pri poduzimanju mjera protiv računalnog kriminaliteta.

- **Ustanoviti Internetske platforme za izvješćivanje javnosti o računalnom kriminalitetu.** One trebaju osigurati bolje razumijevanje prijetnji i trendova u računalnom kriminalitetu te olakšati djelovanje kaznenog pravosuđa. Takve platforme mogu se također koristiti za informiranje javnosti i za upozorenja na prijetnje.

- **Podizanje svijesti i promicanje preventivnih mjera** na svim razinama.

- **Sudjelovati u javno/privatnoj suradnji,** uključujući posebice suradnju između policijskih službenika i davatelja Internetskih usluga.

- **Sudjelovati u međunarodnoj suradnji u najvećoj mogućoj mjeri.** To uključuje potpuno korištenje postojećih bi- i multilateralnih sporazuma, a osobito Konvencije o kibernetičkom kriminalu iz Budimpešte. Potrebno je provesti mjere i obuku u svrhu ubrzavanja uzajamne pravne pomoći. Vlade (potpisnice i promatrači Konvencije) trebaju aktivno sudjelovati u radu Odbora Konvencije o kibernetičkom kriminalu (T-CY) i sudjelovati u suradnji Europskog centra za računalni kriminalitet (EC3) i drugih inicijativa Europske unije.

- **Redovito ocjenjivati učinkovitost odgovora kaznenog pravosuđa na računalni kriminalitet te voditi statistike**. Takve analize trebaju pomoći i unaprijediti rad kaznenog pravosuđa te učinkovito alocirati sredstva.

2. Strateški prioritet: Potpuna i učinkovita pravna osnova za postupanje kaznenog pravosuđa

Odgovarajuće zakonodavstvo predstavlja osnovu za mjere kaznenopravnog sustava protiv računalnog kriminaliteta i korištenje elektroničkih dokaza u kaznenim postupcima. Države i područja koja sudjeluju u CyberCrime@IPA projektu ostvarile su veliki napredak u usklađivanju vlastitih zakona s Konvencijom iz Budimpešte kao i s povezanim standardima Vijeća Europe i Europske unije o zaštiti podataka, o zaštiti djece od seksualnog nasilja ili o prihodima stečenim kaznenim djelom i pranju novca.[1] Međutim, potrebno je daljnje jačanje kapaciteta u tom području, a zakonodavstvo često tek treba biti provjereno u praksi.

Donošenje potpunog i djelotvornog zakonodavstva koje poštuje zahtjeve u svezi ljudskih prava i vladavine prava treba biti strateški prioritet.

Nadležna tijela trebaju razmotriti sljedeće aktivnosti:

- **Daljnje unaprjeđenje odredaba postupovnog prava o pristupu policijskih službenika elektroničkim dokazima.** To treba uključivati zakone i provedbene propise o korištenju odredaba o hitnoj zaštiti pohranjenih podataka (prateća ocjena Odbora Konvencije o kibernetičkom kriminalu), ali također i druga pravila i smjernice o pristupu podacima u posjedu tijela privatnog sektora.

- **Ocijeniti učinkovitost zakonodavstva.** Primjena zakona i propisa u praksi treba biti redovito ocjenjivana. Potrebno je voditi statističke podatke o istragama, kaznenom progonu i presudama u relevantnim predmetima, a primijenjeni postupci trebaju biti dokumentirani.

- **Osigurati da ovlasti policijskih službenika podliježu uvjetima i zaštitnim mehanizmima u skladu s člankom 15. Konvencije iz Budimpešte.** To treba uključivati sudski nadzor prekomjernih ovlasti, ali također i poštovanje načela proporcionalnosti i nužnosti.

- **Jačati zakonodavstvo u području zaštite podataka u skladu s međunarodnim i europskim standardima.** Vlade su potaknute osigurati da njihovo nacionalno zakonodavstvo o zaštiti podataka bude u skladu s načelima Konvencije Vijeća Europe o zaštiti podataka (ETS 108) te sudjelovati u trenutnom procesu modernizacije Konvencije. Isto se odnosi i na buduće standarde Europske unije u zaštiti podataka. To će olakšati prekograničnu razmjenu podataka u svrhu kaznenog progona.

- **Upotpuniti zakonodavstvo i poduzeti preventivne i zaštitne mjere u zaštiti djece od seksualnog nasilja na Internetu**. Dok je većina odredbi Konvencije iz Lanzarotea provedena, u nekim je državama ili područjima još uvijek potrebno razmotriti pitanja poput „posjedovanja dječje pornografije", „svjesnog pristupanja" i „vrbovanja" (*grooming*).

- **Prilagoditi zakonodavstvo o financijskim istragama, oduzimanju prihoda stečenih kaznenim djelom i o financiranju terorizma na Internetsko okruženje.** Propisi i pravila trebaju prije svega osigurati brzu nacionalnu i međunarodnu razmjenu podataka.

[1] Vidjeti npr. Konvenciju Vijeća Europe za zaštitu pojedinaca pri automatskoj obradi osobnih podataka (ETS 108), „Konvenciju iz Lanzarotea" o zaštiti djece od seksualnog iskorištavanja i zlostavljanja (CETS 201), Konvenciju o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenoga kaznenim djelom i o financiranju terorizma (CETS 198).

3. Strateški prioritet: Specijalizirane jedinice za računalni kriminalitet

Računalni kriminalitet i elektronički dokazi zahtijevaju specijalizirani odgovor tijela kaznenog pravosuđa. Službe policije i državnog odvjetništva trebaju biti sposobne voditi istrage i sudske postupke za kaznena djela protiv računalnih podataka i sustava, kaznena djela počinjena uporabom računala kao i elektroničke dokaze povezane s bilo kojim kaznenim djelom. U tijeku je stvaranje ili jačanje policijskih jedinica za računalni kriminalitet u svim državama i područjima koja sudjeluju u CyberCrime@IPA projektu, dok se u nekima razmatra i specijalizacija državnih odvjetnika. Ovaj je proces treba nastaviti. Ključno je shvatiti da se tehnologija mijenja iz dana u dan dok radno opterećenje jedinica za računalni kriminalitet i forenziku kontinuirano raste. Financiranje (osoblje, oprema, softver) i održavanje specijaliziranih vještina kao i prilagodba takvih jedinica na nove uvjete predstavljaju stalni izazov.

Kontinuirano jačanje specijaliziranih jedinica za računalni kriminalitet treba biti strateški prioritet.

Nadležna tijela trebaju razmotriti sljedeće aktivnosti:

- **Ustanoviti – gdje to još nije napravljeno – specijalizirane jedinice za računalni kriminalitet unutar kriminalističke policije.** Konačni ustroj i funkcije takvih jedinica trebaju biti rezultat pažljive analize potreba i trebaju biti utemeljene na zakonu.

- **Unaprijediti specijalizaciju državnih odvjetnika.** Razmotriti osnivanje specijaliziranih jedinica državnih odvjetnika ili, alternativno, grupe specijaliziranih državnih odvjetnika koji bi savjetovali ili pomagali drugim državnim odvjetnicima u predmetima koji uključuju računalni kriminalitet i elektroničke dokaze.

- **Redovita analiza funkcija i financiranja specijaliziranih jedinica.** Ova aktivnost treba omogućiti prilagodbe, a time i nošenje s novim izazovima i rastućim zahtjevima.

- **Olakšati suradnju i razmjenu dobrih praksi između specijaliziranih jedinica** na regionalnoj i međunarodnoj razini.

- **Poboljšati postupke za istrage računalnog kriminaliteta i rukovanje elektroničkim dokazima.** U tom je smislu potrebno ispitati i razmotriti provedbu nacionalnih i međunarodnih standarda i dobrih praksi. Također se može razmotriti korištenje Vodiča za elektroničke dokaze koji je pripremljen u okviru CyberCrime@IPA projekta.

4. Strateški prioritet: Obuka policijskih službenika

Policijske službe trebaju biti sposobne ne samo istraživati kaznena djela protiv ili počinjena pomoću računalnih sustava, već se baviti i elektroničkim dokazima u odnosu na sve vrste kriminaliteta. S eksponencijalnim rastom uporabe informacijskih tehnologija u društvu rasli su i izazovi za policijske službe. Svi policijski službenici – od onih koji su prvi stigli na mjesto događaja do visoko specijaliziranih forenzičkih istražitelja – moraju, svaki na svojoj razini, biti osposobljeni za bavljenje računalnim kriminalitetom i elektroničkim dokazima. Elementi strategija za obuku policijskih službenika su utvrđeni, ali još nisu u potpunosti primijenjeni.[2]

Provedba održivih strategija obuke policijskih službenika na odgovarajućoj razini treba biti strateški prioritet.

Nadležna tijela trebaju razmotriti sljedeće aktivnosti:

- **Provedba nacionalne strategije obuke policijskih službenika.** Cilj je osigurati da policijske službe imaju vještine i sposobnosti koje su potrebne za istraživanje računalnog kriminaliteta, osiguravanje elektroničkih dokaza, provođenje forenzičke analize računala za kaznene postupke, pomaganje drugim agencijama te davanje doprinosa mrežnoj sigurnosti. Ulaganje u takvu obuku je opravdano ako se uzme u obzir oslanjanje društva na informacijske tehnologije te rizike povezane s time.

- **Uključiti pravila i protokole o rukovanju elektroničkim dokazima u sve razine nacionalne obuke.** Važno je prepoznati da elektronički dokazi imaju utjecaja na sve kriminalne aktivnosti te je obuka u prepoznavanju i radu s elektroničkim dokazima potrebna svim policijskim službenicima a ne samo onima u specijaliziranim jedinicama. Takva obuka se može temeljiti na Vodiču za elektroničke dokaze koji je pripremljen u okviru CyberCrime@IPA projekta.

- **Razmotriti uvođenje individualnih planova obuke za specijalizirane istražitelje.** Promjene u tehnologiji i načinu na koji kriminalci zlorabe tu tehnologiju znače da postoji potreba za prikladnim brojem visoko obučenog osoblja koje je kompetentno i sposobno provoditi istrage i/ili ispitivanja digitalnih dokaza na najvišoj razini. To će također unaprijediti njihov položaj unutar kaznenopravnog sustava.

- **Razmotriti primjenu postupaka u svrhu dobivanja najbolje vrijednosti iz ulaganja u obuku o računalnom kriminalitetu.** Obuka o računalnom kriminalitetu i računalnoj forenzici je vrlo skupa. Kako bi osigurale adekvatan povrat svojih ulaganja, države trebaju osigurati da takvo osoblje bude imenovano i ostane na položajima koji odražavaju njihovu razinu znanja i vještina. S tim ciljem strategije obuke i ljudskih resursa trebaju biti komplementarne.

[2] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

5. Strateški prioritet: Obuka pravosudnih dužnosnika

Kako – uz kaznena djela počinjena protiv računala ili pomoću računala – rastući broj drugih vrsta kaznenih djela uključuje dokaze pohranjene u računalnim sustavima ili drugim uređajima za pohranu podataka, u konačnici će svi suci i državni odvjetnici morati biti spremni na bavljenje elektroničkim dokazima. U državama i područjima koja sudjeluju u CyberCrime@IPA projektu ostvaren je napredak u tome da su moduli obuke pripremljeni, predavači osposobljeni, te su održani pilot osnovni i napredni tečajevi. Uz to, u tijeku je osnivanje Regionalnog pilot centra za obuku pravosudnih dužnosnika o suzbijanju računalnog kriminaliteta i elektroničkim dokazima. Potrebno je institucionalizirati ta postignuća.

Omogućavanje svim sucima i državnim odvjetnicima da vode postupke i donose presude o računalnom kriminalitetu te da u kaznenim postupcima koriste elektroničke dokaze treba ostati strateški prioritet.

Nadležna tijela trebaju razmotriti sljedeće aktivnosti:

- **Široka primjena obuke pravosudnih dužnosnika o računalnom kriminalitetu i elektroničkim dokazima.** Nacionalne institucije za obuku sudaca i državnih odvjetnika trebaju integrirati osnovne i napredne module obuke o računalnom kriminalitetu i elektroničkim dokazima u svoje redovne programe obuke za početnu obuku i obuku u službi.

- **Konsolidirati Regionalni pilot centar za obuku pravosudnih dužnosnika u Zagrebu, Hrvatska.** Nacionalne institucije za obuku pravosudnih dužnosnika iz regije trebaju surađivati s Regionalnim pilot centrom za obuku pravosudnih dužnosnika u svezi ažuriranja materijala za obuku, dokumentiranja i širenja dobrih praksi te pružanja regionalne obuke.

- **Uvesti mjere koje osiguravaju da je obuka pravosudnih dužnosnika o računalnom kriminalitetu i elektroničkim dokazima obvezna.** Tijekom projekta postalo je očito da je obuka sudaca i državnih odvjetnika bila dobrovoljna u većini područja uključenih u projekt. To je dovelo do više slučajeva gdje su sudionici bili prisutni na obuci tijekom vrlo kratkih razdoblja i nisu u potpunosti iskoristili prednosti obuke koja je pružena.

- **Uvesti evidenciju obuke za suce i državne odvjetnike.** Kako bi osigurali da je pružena obuka iskorištena na najbolji način, preporuča se vođenje evidencije svih obuka koje su primili pojedinci tako da ih se može obavijestiti o potrebi daljnje specijalizirane obuke te kako bi se osiguralo da prave osobe prođu obuku i da su njihove vještine primjereno iskorištene.

6. Strateški prioritet: Financijske istrage i sprječavanje i kontrola prijevara i pranja novca na Internetu

Većina zločina koji uključuju Internet i druge informacijske tehnologije usmjerena je na stvaranje ekonomske dobiti kroz različite vrste prijevare ili druge oblike ekonomskih i ozbiljnih kaznenih djela. Na taj način nastaju veliki iznosi prihoda koji su stečeni kaznenim djelom i koji cirkuliraju Internetom.

Sukladno tome, financijske istrage usmjerene na traganje, privremeno oduzimanje i oduzimanje prihoda stečenih kaznenim djelom i mjere za sprječavanje prijevare te sprječavanje i kontrolu pranja novca na Internetu trebaju postati strateški prioritet.

Vlade trebaju razmotriti sljedeće aktivnosti:

- **Ustanoviti Internetsku platformu za izvješćivanje javnosti o prijevarama na Internetu i općenito o računalnom kriminalitetu.** Korištenje standardiziranih obrazaca za izvješćivanje omogućit će bolju analizu prijetnji i trendova, kriminalnih operacija i organizacija, te uzoraka tokova novca i pranja novca. To će olakšati poduzimanje mjera tijela kaznenog pravosuđa i financijskih obavještajnih jedinica u cilju kaznenog progona počinitelja te zapljene i oduzimanja prihoda stečenih kaznenim djelom. Platforma uz to treba imati i preventivnu funkciju (podizanje svijesti javnosti, upozorenja na prijetnje, alati i savjeti). Što su više nacionalne platforme usklađene s onima iz drugih država i područja, to će biti lakše provoditi regionalne i međunarodne analize i mjere.

- **Promicati pro-aktivne paralelne financijske istrage** u istragama računalnog kriminaliteta ili kaznenih djela koja uključuju informacijske tehnologije/Internet. To će zahtijevati povećanu međuagencijsku suradnju između tijela nadležnih za računalni kriminalitet i za financijske istrage i financijskih obavještajnih jedinica. Zajednička obuka mogla bi olakšati takvu suradnju među agencijama.

- **Stvoriti pouzdane forume** (nacionalne i regionalne) za razmjenu podataka između javnog i privatnog sektora o računalnim prijetnjama vezanim uz financijski sektor. Nacionalni forumi trebaju biti dostupni ključnim dionicima (poput predstavnika financijskog sektora, davatelja Internetskih usluga, jedinica za računalni kriminalitet, financijskih obavještajnih jedinica, timova za odgovor na ugrožavanje računalne sigurnosti). Njihova je svrha identificirati prijetnje, trendove, alate i rješenja za zaštitu financijskog sektora od računalnog kriminaliteta. Regionalni forum treba se sastojati od foruma koji su ustanovljeni na nacionalnim razinama.

- **Ustanoviti pravni okvir za privremeno oduzimanje i oduzimanje prihoda stečenih kaznenim djelom i digitalne imovine kao i za sprječavanje pranja novca na Internetu.** Taj okvir treba uključivati digitalnu imovinu, poput e-novca i virtualnih valuta. Pravila, propisi i postupci protiv pranja novca trebaju se također primijeniti na sustave plaćanja bazirane na Internetu.

- **Iskoristiti prilike za učinkovitiju međunarodnu suradnju.** Povezivanje mjera protiv pranja novca i financijskih istraga s istragama računalnog kriminaliteta i računalnom forenzikom otvara dodatne mogućnosti za međunarodnu suradnju. Vlade trebaju iskoristiti mogućnosti koje su dostupne u skladu s Konvencijom o kibernetičkom kriminalu iz Budimpešte, Konvencijom Vijeća Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenoga kaznenim djelom i o financiranju terorizma (CETS 198) i revidiranom verzijom Četrdeset preporuka Radne skupine za financijske djelatnosti (FATF). Također je potrebno razmotriti rezultate tipološke studije MONEYVAL-a o tokovima novca od kaznenih djela na Internetu iz ožujka 2012.[3]

[3] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf

7. Strateški prioritet: Suradnja između policijskih službenika i davatelja Internetskih usluga

Suradnja između policijskih službenika i davatelja Internetskih usluga (DIU) i drugih tijela privatnog sektora ključna je za zaštitu prava korisnika Interneta i njihovu zaštitu od kriminala. Efikasne istrage računalnog kriminaliteta često nisu moguće bez suradnje DIU-a. Međutim, takva suradnja treba uzeti u obzir različite uloge policije i DIU-a kao i prava privatnosti korisnika.

Unaprijeđena suradnja između policije i DIU-a te razmjena podataka između javnog i privatnog sektora u skladu s propisima o zaštiti podataka treba biti strateški prioritet.

Vlade trebaju razmotriti sljedeće aktivnosti:

- **Ustanoviti jasna pravila i postupke na nacionalnoj razini za pristup policijskih službenika podacima u posjedu DIU-a i drugih tijela privatnog sektora u skladu s propisima o zaštiti podataka.** Jasna pravna osnova u skladu s odredbama postupovnog prava i uvjetima i zaštitnim mehanizmima Konvencije o kibernetičkom kriminalu iz Budimpešte pomoći će u zaštiti ljudskih prava i vladavine prava. Smjernice[4] usvojene na globalnoj konferenciji Vijeća Europe 2008. godine mogu pomoći policijskim službenicima i DIU-ima da organiziraju i ustroje svoju suradnju. Vlade trebaju olakšati korištenje odredaba o hitnoj zaštiti pohranjenih podataka (članci 16., 17., 29. i 30.) Konvencije iz Budimpešte uzimajući u obzir rezultate ocjene Odbora Konvencije o kibernetičkom kriminalu.[5]

- **Poticati kulturu suradnje između policijskih službenika i DIU-a.** U tom smislu osnovni alat predstavljaju memorandumi o razumijevanju između policijskih službenika i davatelja Internetskih usluga. Regionalna koordinacija takvih memoranduma o razumijevanju treba olakšati sposobnost tijela kaznenog progona da provode istrage preko regionalnih granica znajući da su usvojeni usporedivi standardi u drugim državama i područjima. Zajedno s jasnim pravilima i procedurama, ti memorandumi također mogu olakšati suradnju multinacionalnih DIU-a i drugih tijela privatnog sektora, uključujući otkrivanje podataka pohranjenih u stranoj nadležnosti ili na virtualnim poslužiteljima (*cloud servers*) kojima upravljaju ti DIU-i.

- **Olakšati prekograničnu razmjenu podataka između privatnog i javnog sektora.** Tijela privatnog sektora u posjedu su velikih količina podataka o ugrožavanju računalne sigurnosti. Prekogranična razmjena takvih podataka treba pomoći u poboljšanju sigurnosti informacijske infrastrukture kao i u istragama protiv počinitelja. Vlade trebaju razmotriti donošenje propisa i sklapanje sporazuma koji dopuštaju razmjenu podataka između privatnog i javnog sektora te poticati razvoj smjernica koje će olakšati razmjenu podataka unutar i izvan nacionalnih granica, uključujući postupovne, tehničke i pravne zaštitne mehanizme kao i mehanizme zaštite podataka.

[4] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp. Smjernice su dostupne na jezicima država i područja koja sudjeluju u CyberCrime@IPA projektu.

[5] Izvješće o ocjeni usvojeno od strane Odbora u prosincu 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

8. Strateški prioritet: Učinkovitija regionalna i međunarodna suradnja

Računalni kriminalitet i elektronički dokazi su po svojoj prirodi transnacionalni što zahtijeva učinkovitu međunarodnu suradnju. Potrebno je neposredno djelovanje u cilju osiguravanja elektroničkih dokaza u stranim nadležnostima i postupka otkrivanja takvih dokaza. Međutim, neučinkovitost međunarodne suradnje, pogotovo uzajamne pravne pomoći, još uvijek se smatra jednom od glavnih prepreka učinkovitom djelovanju protiv računalnog kriminaliteta.

Učiniti međunarodnu suradnju u računalnom kriminalitetu i elektroničkim dokazima učinkovitijom treba biti strateški prioritet.

Vlade trebaju razmotriti sljedeće aktivnosti:

- **Korištenje mogućnosti iz Konvencije o kibernetičkom kriminalu iz Budimpešte i drugih bilateralnih, regionalnih i međunarodnih sporazuma o suradnji u kaznenopravnim stvarima.** To uključuje puno korištenje članaka 23. i 25. Konvencije iz Budimpešte o suradnji između policijskih službi i pravosuđa, uključujući prilagođavanje zakonodavstva i unaprjeđivanje postupaka. Vlade (potpisnice i promatrači Konvencije) trebaju u potpunosti sudjelovati u ocjeni odredaba o međunarodnoj suradnji Konvencije iz Budimpešte koju će u 2013. godini provesti Odbor Konvencije o kibernetičkom kriminalu (T-CY). Ta ocjena treba pratiti ocjenu Odbora iz 2012. te promicati korištenje članaka 29. i 30. Konvencije iz Budimpešte o međunarodnim zahtjevima za zaštitom i otkrivanjem podataka.

- **Osigurati obuku i razmjenu dobrih praksi.** Tijela nadležna za suradnju policije i pravosuđa trebaju se uključiti u nacionalne, regionalne i međunarodne obuke i razmjenu dobrih praksi. To bi trebalo olakšati suradnju na temelju povjerenja.

- **Ocijeniti učinkovitost međunarodne suradnje.** Ministarstva pravosuđa i unutarnjih poslova i državna odvjetništva trebaju prikupljati statističke podatke o zahtjevima za međunarodnu suradnju u računalnom kriminalitetu i elektroničkim dokazima, uključujući vrstu zahtjeva za pomoć, pravodobnost odgovora i korištene postupke. To bi trebalo pomoći u utvrđivanju dobrih praksi te ukloniti prepreke suradnji. Navedena tijela mogu s regionalnim partnerima sudjelovati u analizi pitanja koja negativno utječu na međunarodnu suradnju.

- **Ojačati učinkovitost kontaktnih mjesta dostupnih od 0 do 24 sata, 7 dana u tjednu.** Takva su kontaktna mjesta određena u svim državama i područjima sukladno članku 35. Konvencije iz Budimpešte, ali njihova uloga treba biti unaprijeđena, a one trebaju postati pro-aktivnije i potpuno funkcionalne.

- **Redovito prikupljanje statistika te analiza učinkovitosti neprekidno dostupnih kontaktnih mjesta i drugih oblika međunarodne suradnje**.