CyberCrime@IPA

Zajednički projekat EU/VE */Vijeća Europe/* o Regionalnoj saradnji u borbi protiv kibernetičkog kriminala

Strateški prioriteti saradnje u borbi protiv kibernetičkog kriminala

Usvojeni od strane

Sastanak ministara i visokih dužnosnika ministarstava unutrašnjih poslova i sigurnosti, ministarstava pravde i tužilaštava zemalja i područja koji učestvuju u projektu CyberCrime@IPA projektu[1]

Dubrovnik, Hrvatska, 15. februar 2013. godine

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, Hrvatska, Crna Gora, Srbija, "Bivša Jugoslavenska Republika Makedonija", Turska i Kosovo*.
* Ovaj naziv ne dovodi u pitanje stajališta o statusu, i u skladu je sa UNSC 1244 */Rezolucija Vijeća sigurnosti UN-a/* i mišljenjem ICJ-a */Međunarodni sud pravde/* o Kosovskoj deklaraciji nezavisnosti

Sadržaj

Napomena: Ovaj dokument je pripremljen uz podršku CyberCrime@IPA zajedničkog projekta Europske unije i Vijeća Europe o regionalnoj saradnji u suzbijanju kriminaliteta: Jačanje kapaciteta u borbi protiv kibernetičkog kriminala.

Kontakt

Za više informacija molimo da se obratite:

Sektor za zaštitu podataka i kibernetički kriminal
Opća uprava za ljudska prava i vladavinu zakona
Vijeće Europe
Strazbur, 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 borbi protiv kibernetičkog kriminala

Mi, ministri i visoki dužnosnici koji predstavljamo ministarstva unutrašnjih poslova i sigurnosti, ministarstva pravde i državna tužilaštva
zemalja i područja obuhvaćenih CyberCrime@IPA projektom

Učestvujući na ovoj regionalnoj Konferencijie o strateškim prioritetima u vezi s kibernetičkim kriminalom, održanoj u Dubrovniku, Hrvatska, od 13. do 15. februara 2013. godine, u saradnji s Vijećem Europe i Europskom unijom

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

- Zabrinuti zbog opasnosti od kibernetičkog kriminala koji negativno utiče na povjerenje i vjeru u informacijske tehnologije, prava i sigurnosti pojedinaca, posebno uključujući djecu;

- Imajući na umu pozitivnu obavezu vlada da štite pojedince od kibernetičkog kriminala;

- Vodeći računa o potrebi poštivanja temeljnih prava i sloboda, uključujući i zaštitu pojedinaca s obzirom na obradu ličnih podataka, prilikom zaštite društva od kriminala;

- Uzevši u obzir potrebu za saradnjom između javnog i privatnog sektora za prevenciju i kontrolu kibernetičkog kriminala i zaštitu računarskih sistema;

- Vjerujući da učinkovite mjere borbe protiv kibernetičkog kriminala zahtijevaju učinkovitu regionalnu i međunarodnu saradnju;

- Naglašavajući vrijednost Budimpeštanske konvencije o kibernetičkom kriminalu kao smjernice za domaće zakonodavstvo i okvira za međunarodnu saradnju;

- Sa zahvalnošću ističemo važnost Evropske Unije, odnosno njihove finansijske podrške u zaštiti od kibernetičkog kriminala i borbe protiv istog;

- Osobito uzimajući u obzir, jačanje (stvaranje) partnerstva između Evropskog Kibernetičkog centra (EC3), Europola i naših pravosudnih tijela;

- Zahvalni na podršci koju pružaju Europska unija i Vijeće Europe kroz CyberCrime@IPA regionalni projekat;

- Nadovezujući se na postignuti napredak i na akciju u vezi s kibernetičkim kriminalom već poduzetu u zemljama i područjima u regiji, u isto vrijeme svjesni da su potrebni daljnji napori;

podržavamo

strateške prioritete u vezi s kibernetičkim kriminalom

prezentirane na ovoj konferenciji

i

odlučni smo da

- Slijedimo strategije za borbu protiv kibernetičkog kriminala kako bi se osigurao učinkovit kaznenopravni odgovor na krivična djela protiv i pomoću računara, kao i za bilo koje krivično djelo koje uključuje elektronske dokaze;

- Usvojimo cjelovite i učinkovite zakone o kibernetičkom kriminalu koji zadovoljavaju zahtjeve ljudskih prava i vladavine zakona;

- Jačamo specijalizirane jedinice za provedbu zakona i specijalizaciju tužilaštava s obzirom na kibernetički kriminal i elektronske dokaze;

- Provedemo održive strategije za obuku policije;

- Podržimo osposobljavanje sudaca i tužitelja u vezi s kibernetičkim kriminalom i elektronskim dokazima;

- Slijedimo sveobuhvatne strategije kako bi zaštitili djecu od online seksualnog iskorištavanja i seksualnog zlostavljanja u skladu s Lanzarote Konvencijom;

- Promoviramo finansijske istrage i prevenciju i kontrolu prevara i pranja novca na Internetu;

- Jačamo saradnju s privatnim sektorom, posebno između tijela za provedbu zakona i pružaoca internetskih usluga;

- Učestvujemo u učinkovitoj regionalnoj i međunarodnoj saradnji;

- Podijelimo naša iskustvo s drugim regijama svijeta kako bi podržali izgradnju kapaciteta protiv kibernetičkog kriminala;

- Promoviramo privrženost Budimpeštanskoj Konvenciji o kibernetičkom kriminalu na globalnoj razini.

Deklaracija usvojena uz odobravanje u
Dubrovniku, Hrvatska, 15. februara 2013.godine

Prilog: Strateški prioriteti u vezi s kibernetičkim kriminalom

1.1. Strateški prioritet: Politike i strategije za borbu protiv kibernetičkog kriminala

Budući da su informacijske i komunikacijske tehnologije izmijenile društva, sigurnost IKT-a postala je prioritet za mnoge vlade. To se ogleda u donošenju strategija za kibernetičku sigurnost s primarnim fokusom na zaštitu kritične informacijske infrastrukture. Međutim, vlade također imaju pozitivnu obavezu da zaštite ljude i njihova prava od kibernetičkog kriminala i da prijestupnike privedu pravdi.

Vlade bi stoga trebale razmotriti pripreme specifičnih strategija za borbu protiv kibernetičkog kriminala ili kako da poboljšaju komponente kibernetičkog kriminala unutar strategija ili politika za kibernetičku sigurnost.

Relevantni organi trebaju razmotriti sljedeće akcije:

- **Usvojiti politike ili strategije za borbu protiv kibrnetičkog kriminala** s ciljem osiguravanja učinkovitog kaznenopravnog odgovora na krivična djela protiv i pomoću računara, kao i za bilo koje krivično djelo koje uključuje elektronski dokaz. Kao elemente takvih politika ili strategija, razmotriti preventivne mjere, zakonodavstvo, specijalizirane jedinice za provođenje zakona i tužilaštva, međuagencijsku saradnju, osposobljavanje policije i pravosuđa, saradnju između javnog i privatnog, učinkovitu međunarodnu saradnju, finansijske istrage i sprječavanje prevara i pranja novca, te zaštitu djece od seksualnog nasilja.

- **Osigurati da su zahtjevi ljudskih prava i vladavine zakona ispunjeni** prilikom poduzimanje mjera protiv kibernetičkog kriminala.

- **Uspostaviti online platforme za javno prijavljivanje kibernetičkog kriminala.** To bi trebalo osigurati bolje razumijevanje prijetnji i trendova kibernetičkog kriminala i olakšati kaznenopravnu akciju. Takve platforme također se mogu koristiti za informiranje javnosti i upozorenja o prijetnjama.

- **Kreirati svijest i promovirati preventivne mjere** na svim razinama.

- **Uključiti se u javno/privatnu saradnju,** uključujući, posebno, saradnju između tijela za provedbu zakona i pružaoca internetskih usluga**.**

- **Uključiti se u međunarodnu saradnju u najvećoj mogućoj mjeri.** To uključuje i potpuno korištenje postojećih bilateralnih i multilateralnih i regionalnih sporazuma, posebno Budimpeštanske konvencije o kibernetičkom kriminalu. Mjere i obuke za ubrzavanje međunarodne pravne pomoći trebaju se provesti. Vlade (ugovornice i posmatrači Konvencije) trebaju aktivno učestvovati u radu Odbora Konvencije o kibernetičkom kriminalu (T-CY) i trebaju se uključiti u saradnju s Europskom centrom za borbu protiv kibernetičkog kriminala (EC3) i druge inicijative Europske unije.

- **Ocijeniti, na redovnoj osnovi, učinkovitost kaznenopravnog odgovora na kibernetički kriminal i održavati statistiku.** Takve analize pomoći će odrediti i poboljšati performanse kaznenopravnog djelovanja i alociranja resursa na učinkovit način.

1.2. Strateški prioritet: Potpuna i učinkovita pravna osnova za kaznenopravnu akciju

Odgovarajuće zakonodavstvo je osnova za kaznenopravne mjere u odnosu na kibernetički kriminal i korištenje elektronskih dokaza u krivičnom postupku. Zemlje i područja koja učestvuju u CyberCrime@IPA projektu napravili su veliki napredak u usklađivanju svog zakonodavstva s Budimpeštanskom konvencijom, kao i srodnim standardima Vijeća Europe i Europske unije o zaštiti podataka, o zaštiti djece od seksualnog nasilja ili o prihodima od kriminala i pranja novca. [1] Međutim, potrebno je daljnje jačanje, a često zakonodavstvo mora još da prođe i test praktične primjene.

Usvajanje cjelovitog i učinkovitog zakonodavstva koje zadovoljava zahtjeve ljudskih prava i vladavine zakona treba biti strateški prioritet.

Relevantni organi trebaju razmotriti sljedeće akcije:

- **Dalje unaprijediti odredbe procesnog prava o pristupu policije i pravosuđa elektronskim dokazima.** To bi trebalo uključivati zakone i provedbene propise o korištenju odredaba brzog čuvanja podataka Budimpeštanske konvencije (nastavak na procjenu Odbora Konvencije o kibernetičkom kriminalu), ali i drugih pravila ili smjernica o pristupu podacima u posjedu privatnih osoba.

- **Procijeniti učinkovitost zakonodavstva.** Primjenu zakona i propisa u praksi treba redovno ocjenjivati. Statističke podatke o istraženim, procesuiranim i presuđenim slučajevima treba održavati, a primijenjene procedure treba dokumentirati.

- **Osigurati da su policijske ovlasti podložne uslovima i garancijama u skladu s članom 15. Budimpeštanske konvencije.** To bi trebalo uključivati sudski nadzor prekoračenja ovlasti, ali i poštivanje načela proporcionalnosti i nužnosti.

- **Jačanje zakonodavstva o zaštiti podataka u skladu s međunarodnim i europskim standardima.** Vlade su ohrabrene da osiguraju da je njihovo nacionalno zakonodavstvo zaštite podataka u skladu s načelima ETS 108 konvencije Vijeća Europe o zaštiti podataka, te da učestvuju u trenutnom procesu modernizacije Konvencije. Isto vrijedi i za buduće standarde zaštite podataka Europske unije. To će olakšati transgraničnu razmjenu podataka također i za potrebe provođenja zakona.

- **Upotpuniti zakone i poduzeti preventivne i zaštitne mjere na zaštiti djece od online seksualnog nasilja.** Mada su mnoge odredbe Lanzarote Konvencije provedene, u nekim zemljama ili područjima pitanja kao što su "posjedovanje dječje pornografije", "svjesno dobivanje pristupa" i "dotjerivanje" još uvijek treba riješiti.

- **Prilagoditi propise o finansijskoj istrazi, oduzimanju prihoda stečenih počinjenjem krivičnog djela i o pranju novca i finansiranju terorizma u online okruženju.** Pravila i propisi trebaju posebno omogućiti brzu domaću i međunarodnu razmjenu informacija.

[1] Za primjer vidi Konvenciju Vijeća Europe za zaštitu pojedinaca u pogledu automatske obrade ličnih podataka (ETS 108), "Lanzarote Konvenciju" o seksualnom iskorištavanju i seksualnom zlostavljanju djece (CETS 201), Konvencija o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenog kaznenim djelom i o finansiranju terorizma (CETS 198).

1.3. Strateški prioritet: Specijalizirane jedinice za kibernetički kriminal

Kibernetički kriminal i elektronski dokazi zahtijevaju specijaliziran odgovor pravosudnih i policijskih organa. Tijela za provedbu zakona i tužiteljstva moraju biti u mogućnosti istražiti i procesuirati krivična djela protiv računarskih podataka i sistema, krivična djela počinjena pomoću računara, kao i elektronske dokaze u odnosu na bilo koji zločin. U svim zemljama i područjima koji učestvuju u CyberCrime@IPA projektu, stvaranje ili jačanje jedinica za borbu protiv kibernetičkog kriminala, policijskog tipa, je u toku, a specijalizacija tužilaca se u nekim od njih razmatra. Ovaj proces treba slijediti. Bitno je shvatiti da se tehnologija mijenja svakodnevno i da se opterećenje jedinica za borbu protiv kibernetičkog kriminala i forenzičkih jedinica stalno povećava. Osiguravanje resursa (osoblje, oprema, softver) i održavanje specijalnih vještina i prilagodba takvih jedinica novonastalim zahtjevima, stalni je izazov.

Stalno jačanje specijaliziranih jedinica za borbu protiv kibernetičkog kriminala trebalo bi biti strateški prioritet.

Relevantni organi trebaju razmotriti sljedeće akcije:

- **Uspostaviti – tamo gdje to još uvijek nije učinjeno – specijalizirane jedinice za kibernetički kriminal u okviru kriminalističke policije.** Tačno ustrojstvo i funkcije trebaju biti rezultat pomne analize potreba i zasnovani na zakonu.

- **Pojačati specijalizaciju tužilaca.** Razmotriti uspostavljanje specijaliziranih tužilačkih jedinica ili, alternativno, grupe specijaliziranih tužilaca za vođenje ili pomaganje drugim tužiocima u predmetima koji uključuju kibernetički kriminal i elektronske dokaze.

- **Preispitati funkcije i osiguravanje resursa specijaliziranih jedinica, na redovnoj osnovi.** To bi trebalo omogućiti prilagodbe i time odgovoriti na nove izazove i veće zahtjeve.

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

- **Unaprijediti procedure za istrage kibernetičkog kriminala i postupanje s elektronskim dokazima.** Ispitati i razmotriti provedbu državnih i međunarodnih standarda i dobrih praksi u ovom smislu. Razmotriti korištenje Vodiča o elektronskim dokazima koji je razvijen u okviru CyberCrime@IPA projekta.

1.4. Strateški prioritet: Obuka policije

Tijela za provedbu zakona trebaju biti u mogućnosti ne samo da istraže krivična djela protiv i pomoću računarskih sistema, već također da obrade elektronske dokaze u odnosu na bilo koju vrstu kriminala. Uz eksponencijalni rast u korištenju informacijskih tehnologija od strane društva, izazovi provođenja zakona su isto tako porasli. Svi policijski službenici - od onih koji prvi dolaze na mjesto zločina do visoko specijaliziranih računarskih forenzičkih istražitelja - trebaju biti osposobljeni za postupanje s kibernetičkim kriminalom i elektronskim dokazima na njihovim ličnim razinama. Elementi strategija za obuku policije su identificirani, ali još uvijek nisu u potpunosti provedeni.[2]

Provedba održivih strategija obuke s ciljem obučavanja policijskih službenika na odgovarajućoj razini trebala bi biti strateški prioritet.

Relevantni organi trebaju razmotriti sljedeće akcije:

- **Provedba domaće strategije obuke policije.** Cilj bi trebao biti da se osigura da agencije za provedbu zakona imaju vještine i nadležnosti potrebne za istragu kibernetičkog kriminala, zaštitu elektronskih dokaza, obavljanje računarskih forenzičkih analiza za krivični postupak, pomaganje drugim agencijama i doprinos sigurnosti mreže. Ulaganje u takve obuke je opravdano s obzirom na oslanjanje društva na informacijske tehnologe i povezane rizike.

- **Uključiti pravila i protokole o postupanju s elektronskim dokazima u sve razine nacionalnih obuka.** Važno je prepoznati da elektronski dokaz utiče na sve krivične aktivnosti, te je obuka u prepoznavanju i ophođenju s elektronskim dokazima potrebna svim operativcima provedbe zakona, a ne samo onima u specijaliziranim jedinicama. Ovaj trening bi se mogao temeljiti na Vodiču o elektronskim dokazima razvijenom u okviru CyberCrime@IPA projekta.

- **Razmisliti o uvođenju pojedinačnih planova obuke za stručnjake istražitelje.** Promjene u tehnologiji i način na koji kriminal zloupotrebljava tehnologiju znači da postoji potreba za odgovarajućim brojem visoko osposobljenih kadrova koji su kompetentni i sposobni za provođenje istraga i / ili ispitivanje digitalnih dokaza na najvišoj razini. To će također poboljšati njihov status u okviru kaznenopravnog sistema.

- **Razmisliti o provedbi procedura s ciljem osiguranja najbolje vrijednost iz ulaganja u obuku o kibernetičkom kriminalu.** Obuka iz kibernetičkog kriminala i računarske forenzike vrlo je skupa. Kako bi se osiguralo da se ostvari adekvatan povrat iz uloženog, zemlje trebaju osigurati da je osoblje postavljeno na i da je ostalo na pozicijama koje odražavaju razinu znanja i vještina koje isti imaju. U tu svrhu, obuke i strategije ljudskih resursa trebaju biti pozdravljene*.

* *Prim.prev.:* Doslovan prevod, a ukoliko se radi o štamparskoj greški, 'complementary' umjesto 'complimentary' značilo bi 'komplementarne'.

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

1.5. Strateški prioritet: Osposobljavanje u oblasti pravosuđa

Obzirom da – pored krivičnih djela protiv i pomoću računara - sve veći broj drugih vrsta krivičnih djela uključuje dokaze o računarskim sistemima ili drugim uređajima za pohranu podataka, samim tim i svi suci i tužioci trebaju biti spremni da postupaju s elektronskim dokazima. Napredak je ostvaren u zemljama i područjima koja učestvuju u CyberCrime@IPA projektu u tome da su moduli obuka pripremljeni, treneri obučeni i osnovni i napredni tečajevi organizovani na pilot osnovi. Osim toga, trenutno je u procesu osnivanja Regionalni pilot centar za osposobljavanje u oblasti pravosuđa na temu kibernetičkog kriminala i sudskih dokaza. Ovi uspjesi trebaju biti institucionalizirani.

Osposobljavanje svih sudaca i tužilaca da procesuiraju i donose presude za kibernetički kriminal i koriste elektronske dokaze u krivičnom postupku trebalo bi ostati strateški prioritet.

Relevantni organi trebaju razmotriti sljedeće akcije:

- **Integrirati osposobljavanje u oblasti pravosuđa na temu kibernetičkog kriminala i elektronskih dokaza.** Domaće institucije za osposobljavanje sudaca i tužilaca trebaju integrirati osnovne i napredne module obuke o kibernetičkom kriminalu i elektronskim dokazima u svoj redovni program obuka za početno i stručno osposobljavanje.

- **Učvrstiti Regionalni pilot centar za osposobljavanje u oblasti pravosuđa u Zagrebu, Hrvatska.** Domaće institucije za osposobljavanje u oblasti pravosuđa iz regije trebaju sarađivati s Regionalnim pilot centrom za osposobljavanje u oblasti pravosuđa u pogledu ažuriranja tečajnih materijala, dokumentiranja i širenja dobre prakse i pružanja regionalne obuke.

- **Uvesti mjere kako bi se osiguralo da je obuka sudija i tužioca obavezana u oblasti kibernetičkog kriminala i elektronskih dokaza .** Bilo je očito tokom projekta da je obuka za suce i tužitelje dobrovoljna u većini projektnih područja. To je dovelo do brojnih slučajeva u kojima su učesnici samo pohađali obuku u vrlo kratkim periodima tečaja i nisu u potpunosti imali korist od obuke koja je pružena.

- **Uvesti evidenciju o edukaciji za pojedinačne suce i tužioce.** Kako bi se osiguralo da je obuka pružena sucima i tužiteljima iskorištena na najbolji način, poželjno je da se vodi evidencija o svim edukacijama koje su prošli pojedinci, kako bi se došlo do podataka o zahtjevima za dalje specijalističko usavršavanje i osiguralo da su pravi ljudi educirani i njihove vještine iskorištene na odgovarajući način.

1.6. Strateški prioritet: Finansijske istrage i prevencija i kontrola prevara i pranja novca na Internetu

Većina krivičnih djela koja uključuju Internet i druge informacijske tehnologije usmjerena je na ostvarivanje ekonomske dobiti putem različitih vrsta prevara i drugih oblika ekonomskih i teških krivičnih djela. Time se ostvaruju veliki iznosi dobiti stečeni počinjenjem krivičnog djela i kruže Internetom.

Zbog toga bi finansijske istrage koje za cilj imaju traganje za, privremeno oduzimanje i oduzimanje prihoda stečenih počinjenjem krivičnog djela i mjere za sprječavanje prevara i za sprječavanje i kontrolu pranja novca na Internetu trebale postati strateški prioritet.

Vlade trebaju razmotriti sljedeće akcije:

- **Uspostaviti online platformu za javno prijavljivanje prevara na Internetu i o kibernetičkom kriminalu u cjelini.** Korištenje standardiziranih predložaka za prijavljivanje omogućit će bolju analizu prijetnji i trendova kriminalnih radnji i organizacija, kao i strukture tokova novca i pranja novca. To će olakšati akcije pravosudnih i policijskih tijela i finansijskih obavještajnih jedinica za gonjenje počinitelja i za privremeno oduzimanje i oduzimanje prihoda stečenih počinjenjem krivičnog djela. Platforma također treba imati preventivne funkcije (javna svijest i edukacija, upozorenja o prijetnjama, instrumenti i savjeti). Što su domaće platforme više usklađene s onima u drugim zemljama i područjima, više će se olakšati regionalne i međunarodne analize i akcije.

- **Promovirati proaktivne paralelne finansijske istrage** prilikom istrage kibernetičkog kriminala ili krivičnih djela koja uključuju informacijske tehnologije/Internet. To zahtijeva povećanu međuagencijsku saradnju između tijela nadležnih za kibernetički kriminal i za finansijske istrage, kao i finansijske obavještajne jedinice. Zajednički trening može olakšati takvu međuagencijsku saradnju.

- **Kreirati pouzdane forume** (domaće i regionalne) za javnu/privatnu razmjenu informacija o kibernetičkim prijetnjama vezano za finansijski sektor. Domaći forumi trebali bi biti dostupni ključnim akterima (kao što su predstavnici finansijskog sektora, pružaoci internetskih usluga, jedinice za borbu protiv kibernetičkog kriminala, finansijske obavještajne jedinice, interventni timovi za incidente vezane za kompjutersku sigurnost). Njihova je svrha identificirati prijetnje, trendove, instrumente i rješenja kako bi zaštitili finansijski sektor od kibernetičkog kriminala. Regionalni forumi trebali bi se sastojati od foruma uspostavljenih na domaćoj razini.

- **Uspostaviti pravni okvir za privremeno oduzimanje i oduzimanje prihoda stečenih počinjenjem krivičnog djela i digitalne imovine kao i za sprječavanje pranja novca na Internetu.** Ovo bi trebalo uključivati digitalnu imovinu, kao što su e-novac i virtualne valute. Pravila, propisi i procedure za sprječavanje pranja novca također se trebaju primjenjivati na internetski bazirane platne sisteme.

- **Iskoristiti mogućnosti za učinkovitiju međunarodnu saradnju.** Povezivanje mjera protiv pranja novca i finansijskih istraga sa istragama kibernetičkog kriminala i računarske forenzike pruža dodatne mogućnosti za međunarodnu saradnju. Vlade bi trebale iskoristiti mogućnosti dostupne u skladu s Budimpeštanskom konvencijom o kibernetičkom kriminalu, Konvencijom o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenog kaznenim djelom i o finansiranju terorizma (CETS 198) Vijeća Europe i revidiranih 40 preporuka Radne grupe za finansijsku akciju (FATF). Pored

toga trebalo bi razmotriti nalaze MONEYVAL tipološke studije o kriminalnim tokovima novca na Internetu iz marta 2012. godine.[3]

1.7. Strateški prioritet: Saradnja između policije i pružaoca internetskih usluga

Saradnja između agencija za provedbu zakona i pružaoca internetskih usluga (ISP-ovi) i drugih subjekata privatnog sektora je ključna za zaštitu prava korisnika Interneta i za njihovu zaštitu od kriminala. Učinkovite istrage kibernetičkog kriminala često nisu moguće bez saradnje ISP-ova. Međutim, takva saradnja treba uzeti u obzir različite uloge policije i ISP-ova, kao i prava korisnika na privatnost.

Poboljšana saradnja policije/ISP-a i razmjena informacija između javnog/privatnog sektora u skladu s propisima o zaštiti podataka trebala bi postati strateški prioritet.

Vlade trebaju razmotriti sljedeće akcije:

- **Utvrditi jasna pravila i procedure na domaćoj razini za pristup policije podacima u posjedu ISP-ova i drugih subjekata privatnog sektora u skladu s propisima o zaštiti podataka.** Jasna pravna osnova u skladu s odredbama procesnog prava i garancijama i uslovima Budimpeštanske konvencije o kibernetičkom kriminalu pomoći će zadovoljiti zahtjeve ljudskih prava i vladavine zakona. Smjernice[4] usvojene na Octopus konferenciji Vijeća Europe 2008. godine mogle bi pomoći policiji i ISP-ovima da organizuju i strukturiraju svoju saradnju. Vlade bi trebale olakšati korištenje odredaba brzog čuvanja podataka Budimpeštanske konvencije (članovi 16., 17., 29. i 30.), uzimajući u obzir rezultate procjena Odbora Konvencije o kibernetičkom kriminalu.[5]

- **Jačati kulturu saradnje između policije i ISP-ova.** Memorandumi o razumijevanju između policije i pružaoca internet usluga temeljni su instrument u tom smislu. Regionalna koordinacija takvih memoranduma olakšala bi sposobnost tijela za provedbu zakona da provode istrage preko regionalnih granica, uz znanje da su usporedivi standardi usvojeni u drugim zemljama i područjima. Memorandumi, u kombinaciji s jasnim pravilima i procedurama, također mogu olakšati saradnju s multi-nacionalnim ISP-ovima i drugim subjektima privatnog sektora, uključujući objavljivanje podataka pohranjenih u stranoj državi ili na 'cloud' serverima kojima upravljaju ti ISP-ovi.

- **Olakšati privatnu/javnu razmjenu informacija preko granica.** Subjekti privatnog sektora drže velike količine podataka o incidentima vezanim za kibernetičku sigurnost. Transgranično dijeljenje takvih podataka pomoglo bi poboljšanju sigurnosti informacijske infrastrukture, kao i za istragu prijestupnika. Vlade bi trebale razmotriti zakone i zaključivanje sporazuma koji omogućuju privatno/javnu razmjenu informacija i potaći razvoj smjernica kako bi se olakšala unutargranična i transgranična razmjena informacija, uključujući proceduralne, tehničke, pravne garancije i garancije zaštite podataka.

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

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

[5] Izvještaj o procjeni usvojen od strane T-CY u decembru 2012. godine (www.coe.int/tcy)

1.8. Strateški prioritet: Učinkovitija regionalna i međunarodna saradnja

Kibernetički kriminal i elektronski dokaz su transnacionalni po prirodi, te tako zahtijevaju učinkovitu međunarodnu saradnju. Hitna akcija je potrebna za osiguranje elektronskih dokaza u stranim državama i za objavljivanje takvih dokaza. Međutim, neučinkovitost međunarodne saradnje, posebno međunarodne pravne pomoći, još uvijek se smatra jednom od glavnih prepreka koje sprječavaju učinkovitu akciju protiv kibernetičkog kriminala.

Činjenje da međunarodna saradnja u vezi s kibernetičkim kriminalom i elektronskim dokazima bude učinkovitija trebalo bi biti strateški prioritet.

Vlade trebaju razmotriti sljedeće akcije:

- **Iskoristiti mogućnosti Budimpeštanske konvencije o kibernetičkom kriminalu i druge bilateralne, regionalne i međunarodne sporazume o saradnji u krivičnim stvarima.** To uključuje potpuno korištenje članova 23.-35. Budimpeštanske konvencije u odnosu na među-policijsku i pravosudnu saradnju, uključujući i zakonodavne prilagodbe i unaprijeđene procedure. Vlade (ugovornice i posmatrači Konvencije) trebaju u potpunosti učestvovati u ocjeni odredaba Konvencije iz Budimpešte o međunarodnoj saradnji u 2013. koju će poduzeti Odbor Konvencije o kibernetičkom kriminalu (T-CY). Oni bi trebali slijediti T-CY ocjenu iz 2012. i promovirati primjenu članova 29. i 30. Budimpeštanske konvencije u vezi međunarodnih zahtjeva za čuvanjem pohranjenih podataka.

- **Osigurati obuku i razmjenu dobrih praksi.** Organi za policijsku i pravosudnu saradnju trebali bi učestvovati u domaćoj, regionalnoj i međunarodnoj obuci i razmjeni dobrih praksi. To bi trebalo olakšati saradnju temeljenu na povjerenju.

- **Procijeniti učinkovitost međunarodne saradnje.** Ministarstva pravde i unutrašnjih poslova i tužiteljstva trebaju prikupiti statističke podatke o zahtjevima za međunarodnu saradnju u pogledu kibernetičkog kriminala i elektronskih dokaza, uključujući i vrstu zahtjeva za pomoć, pravovremenost odgovora i postupaka koji se koriste. To bi trebalo pomoći u identificiranju dobre prakse i ukloniti prepreke za saradnju. Oni mogu učestvovati s regionalnim partnerima u analizi problema koji nepovoljno utiču na međunarodnu saradnju.

- **Ojačati učinkovitosti kontaktnih tačaka dostupnih 24 sata na dan.** Takve kontaktne tačke uspostavljene su u svim zemljama i područjima u skladu s članom 35. Budimpeštanske konvencije, ali njihova uloga treba biti poboljšana i one moraju postati više pro-aktivne i potpuno funkcionalne.

- **Kompilirati statističke podatke o i preispitivati učinkovitost kontaktnih tački dostupnih 24 sata na dan i drugih oblika međunarodne saradnje, na redovnoj osnovi.**