Vijeće
Europske unije

Bruxelles, 11. travnja 2017.
(OR. en)

5250/1/17
REV 1 DCL 1

GENVAL 3
CYBER 9

DEKLASIFIKACIJA

dokumenta:	5250/1/17 REV 1
od:	17. ožujka 2017.
novi status:	Javno
Predmet:	Izvješće o ocjenjivanju sedmog kruga uzajamnih ocjenjivanja pod nazivom „Praktična provedba i djelovanje europskih politika o sprečavanju kiberkriminaliteta i borbi protiv njega” – izvješće o Hrvatskoj

Za delegacije se u prilogu nalazi verzija gore navedenog dokumenta sa sniženim stupnjem tajnosti.

Tekst dokumenta jednak je tekstu prethodne verzije.

Vijeće
Europske unije

Bruxelles, 17. ožujka 2017.
(OR. en)

5250/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 3
CYBER 9

IZVJEŠĆE

Predmet:	Izvješće o ocjenjivanju sedmog kruga uzajamnih ocjenjivanja pod nazivom „Praktična provedba i djelovanje europskih politika o sprečavanju kiberkriminaliteta i borbi protiv njega” – izvješće o Hrvatskoj

PRILOG

Sadržaj

1 SAŽETAK

- Posjet na licu mjesta Hrvatskoj održan je od 29. rujna do 1. listopada 2015. Ritam posjeta bio je intenzivan, a vrijeme na raspolaganju učinkovito iskorišteno. Ocjenjivanju Hrvatske trebalo je posvetiti više vremena kako bi se dobio jasniji i detaljniji uvid u situaciju. Međutim, stručnjaci su imali priliku razgovarati s vrlo sposobnim i predanim kolegama iz glavnih relevantnih vladinih dionika, konkretno Ureda Vijeća za nacionalnu sigurnost Hrvatske, CERT-a, Ministarstva unutarnjih poslova i Ministarstva pravosuđa. U razgovorima su sudjelovali i predstavnici Državnog odvjetništva i pravosuđa, a potonji su održali impresivnu prezentaciju o sudskoj praksi.

- Europska komisija, Europol / Europski centar za kiberkriminalitet (EC3), Eurojust i ENISA nisu sudjelovali u posjetu na licu mjesta niti su na drugi način doprinijeli ocjenjivanju Hrvatske. Stoga ocjenjivački tim smatra da je sudjelovanje glavnih aktera EU-a nadležnih za kibersigurnost i borbu protiv kiberkriminaliteta u sedmom krugu uzajamnih ocjenjivanja upitno.

- Ured Vijeća za nacionalnu sigurnost Hrvatske čvrsto preporučuje hrvatskim vlastima da u potpunosti provedu Nacionalnu strategiju kibernetičke sigurnosti i njezin akcijski plan. Ocjenjivački tim podupire tu molbu.

- Ocjenjivački tim općenito smatra da Hrvatska raspolaže odgovarajućim strukturama i dostupnim resursima za poduzimanje mjera protiv kiberkriminaliteta. No, može se reći da se suočava s manjkom sveukupne koordinacije, nadzora i financijske potpore; tijekom posjeta tim je primijetio nedostatke na institucijskoj razini od kojih su neki posljedica nedovoljne upućenosti visokorangiranih donositelja odluka te manjka financijskih sredstava.

- Konkretno, iako se čini da se sposobni stručnjaci većinom međusobno poznaju i nastoje koordinirati najbolje što mogu, institucijska koordinacija trebala bi postati obvezan prioritet na svim razinama.

  Kaznena djela u kiberprostoru čine oko 0,5 % svih službeno evidentiranih kaznenih djela počinjenih tijekom 2015. u Hrvatskoj. To dakle može dovesti u pitanje učinkovitost otkrivanja, progona i kažnjavanja kiberkriminaliteta u zemlji te točnost službenih statističkih podataka. Ocjenjivački tim nije primio dovoljno informacija da bi mogao utvrditi stvarne uzroke te situacije.

- Samo policija raspolaže strukturama i službenicima specijaliziranim za kiberkriminalitet. Iako ne postoje posebne pravosudne strukture usmjerene na to područje, neki visokokvalificirani stručnjaci ponekad su pozvani da pruže savjet svojim kolegama.

- Iako se hrvatskim policijskim službenicima pruža opće i specijalizirano osposobljavanje u području kiberkriminaliteta, utvrđeno je da bi trebalo poduzeti dodatne financijske i organizacijske napore kako bi se ponuđeno osposobljavanje poboljšalo te kako bi se stručnjacima osiguralo dovoljno vremena da pohađaju tečajeve.

- Prije pristupanja Europskoj uniji Hrvatska je uspješno sudjelovala u raznim programima Instrumenta pretpristupne pomoći (IPA), osobito u projektu pod nazivom „Regionalna suradnja u području kaznenog pravosuđa: jačanje kapaciteta u borbi protiv kiberkriminaliteta u jugoistočnoj Europi" koji je doveo do osnivanja Regionalnog pilot centar za osposobljavanje pravosudnih dužnosnika za borbu protiv kiberkriminaliteta; taj Centar koji se nalazi u Zagrebu, u Hrvatskoj, trebalo bi održavati i razvijati kao glavni resurs za osposobljavanje pravosudnih stručnjaka.

- Valjalo bi napomenuti da hrvatske vlasti, u skladu sa svojim resursima i raspoloživosti, također sudjeluju u nizu drugih aktivnosti i projekata na međunarodnoj i europskoj razini.

- Nadležne hrvatske vlasti poduzimaju značajne napore kako bi spriječile kiberkriminalitet provodeći aktivnosti s ciljem informiranja i obrazovanja javnosti. Konkretno, hrvatski nacionalni CERT vrlo je aktivan.

- Jednako tako, postojanje platforme za suradnju između policijskih tijela i bankovnog sustava treba smatrati konstruktivnim korakom prema učinkovitoj i produbljenoj suradnji s privatnim partnerima.

2 UVOD

Slijedom donošenja Zajedničke akcije 97/827/PUP od 5. prosinca 1997.[1] uspostavljen je mehanizam za ocjenjivanje primjene i provedbe međunarodnih obveza u borbi protiv organiziranog kriminala na nacionalnoj razini. U skladu s člankom 2. Zajedničke akcije Radna skupina za opće poslove uključujući evaluaciju (GENVAL) odlučila je na sastanku 3. listopada 2013. da bi sedmi krug uzajamnih ocjenjivanja trebao biti posvećen praktičnoj provedbi i djelovanju europskih politika za sprečavanje kiberkriminaliteta i borbu protiv njega.

Države članice pozdravile su odabir kiberkriminaliteta kao teme sedmog kruga uzajamnih ocjenjivanja. Međutim, zbog širokog raspona kaznenih djela obuhvaćenih terminom kiberkriminalitet, dogovoreno je da će se ocjenjivanje usmjeriti na ona kaznena djela za koja države članice smatraju da zaslužuju posebnu pozornost. Stoga su ocjenjivanjem obuhvaćena tri posebna područja: kibernapadi, seksualno zlostavljanje djece / dječja pornografija na internetu i internetske kartične prijevare uz sveobuhvatno ispitivanje pravnih i operativnih aspekata borbe protiv kiberkriminaliteta, prekogranične suradnje i suradnje s relevantnim agencijama EU-a. Direktiva 2011/93/EU o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije[2] (datum prenošenja u nacionalno zakonodavstvo 18. prosinca 2013.) i Direktiva 2013/40/EU[3] o napadima na informacijske sustave (datum prenošenja u nacionalno zakonodavstvo 4. rujna 2015.) posebno su značajne u tom kontekstu.

1 Zajednička akcija od 5. prosinca 1997. (97/827/PUP), SL L 344, 15.12.1997., str. 7 – 9.
2 SL L 335, 17.12.2011., str. 1.
3 SL L 218, 14.8.2013., str. 8.

Štoviše, u Zaključcima Vijeća o strategiji EU-a za kibernetičku sigurnost iz lipnja 2013.[4] ponovno se kao cilj ističe ratifikacija Konvencije Vijeća Europe o kibernetičkom kriminalu (Konvencija iz Budimpešte)[5] od 23. studenoga 2001. čim prije to bude moguće te se u preambuli naglašava da „EU ne poziva na stvaranje novih međunarodnih pravnih instrumenata za kiberpitanja". Tu Konvenciju nadopunjuje Protokol o ksenofobiji i rasizmu putem računalnih sustava[6].

Iskustva iz prošlih ocjenjivanja pokazuju da među državama članicama postoje razlike u pogledu faza provedbe relevantnih pravnih instrumenata te bi informacije iz aktualnog postupka ocjenjivanja mogle biti korisne i onim državama članicama koje možda nisu provele sve aspekte različitih instrumenata. Ipak, cilj je provesti sveobuhvatno i interdisciplinarno ocjenjivanje koje nije usmjereno samo na provedbu različitih instrumenata povezanih s borbom protiv kiberkriminaliteta nego na operativne aspekte u državama članicama.

Stoga će njime, osim suradnje s državnim odvjetništvom, biti obuhvaćena i suradnja policijskih tijela s Eurojustom, Europskom agencijom za mrežnu i informacijsku sigurnost (ENISA) i Europolom / centrom EC3 te način na koji se povratne informacije od navedenih aktera usmjeravaju prema odgovarajućim policijskim i socijalnim službama. Ocjenjivanje je usmjereno na provedbu nacionalnih politika za suzbijanje kibernapada i prijevara te dječje pornografije. Ocjenjivanjem su također obuhvaćene operativne prakse u državama članicama u pogledu međunarodne suradnje i potpore žrtvama kiberkriminaliteta.

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS br. 185; otvoren za potpisivanje 23. studenoga 2001., stupio na snagu 1. srpnja 2004.

6 CETS br. 189; otvoren za potpisivanje 28. siječnja 2003., stupio na snagu 1. ožujka 2006.

GENVAL je 1. travnja 2014. usvojio redoslijed posjeta državama članicama. Hrvatska je bila 14. država članica u kojoj je trebalo izvršiti ocjenjivanje u ovom krugu ocjenjivanja. U skladu s člankom 3. Zajedničke akcije, predsjedništvo je sastavilo popis stručnjaka za provođenje ocjenjivanja. Države članice imenovale su stručnjake sa značajnim praktičnim znanjem iz predmetnog područja u skladu s pisanim zahtjevom koji je delegacijama 28. siječnja 2014. uputio predsjednik GENVAL-a.

Ocjenjivački timovi sastoje se od tri nacionalna stručnjaka kojima pomažu dva člana osoblja Glavnog tajništva Vijeća i promatrači. Za sedmi krug uzajamnih ocjena GENVAL se složio s prijedlogom predsjedništva da bi Europsku komisiju, Eurojust, ENISA-u i Europol / centar EC3 trebalo pozvati kao promatrače.

Nacionalni stručnjaci zaduženi za ocjenjivanje Hrvatske bili su g. Branislav Bohacik (Slovačka), gđa Andrea Raffaelli (Italija) i g. Tamas Pal (Mađarska), a njima se u posjetu zemlji pridružila gđa Claire Rocheteau iz Glavnog tajništva Vijeća. Posjetu nisu prisustvovali promatrači iz Europola / centra EC3, Eurojusta, ENISA-a i Europske komisije.

Ovo su izvješće izradili nacionalni stručnjaci uz pomoć Glavnog tajništva Vijeća na temelju rezultata proizašlih iz ocjenjivačkog posjeta Hrvatskoj od 29. rujna do 1. listopada 2015. te na temelju detaljnih odgovora Hrvatske na ocjenjivački upitnik i detaljnih odgovora na naknadna pitanja.

3 OPĆA PITANJA I STRUKTURE

3.1 Nacionalna strategija kibernetičke sigurnosti

U vrijeme posjeta na licu mjesta dionici su preispitivali Nacrt nacionalne strategije kibernetičke sigurnosti te su pripreme za njezino donošenje bile u tijeku. Nacionalna strategija kibernetičke sigurnosti donesena je 7. listopada 2015. (Narodne novine 108/2015). Vlada Republike Hrvatske osnovala je Nacionalno Vijeće za kibernetičku sigurnost i Operativno-tehničku koordinaciju za kibernetičku sigurnost u lipnju 2016. (Narodne novine 61/2016).

Hrvatske vlasti potvrdile su da borba protiv kiberkriminaliteta u Republici Hrvatskoj predstavlja jedno od prioritetnih područja kibersigurnosti.

Jedan od strateških ciljeva Strategije jest razvoj i podizanje svijesti o kiberprostoru. U tom pogledu akcijski plan sadrži osam provedbenih mjera, od kojih je jedna posebno usmjerena na informiranje javnosti u slučaju pojave računalnih incidenata koji se mogu lako proširiti i utjecati na velik broj korisnika. Prijevod Nacionalne strategije kibernetičke sigurnosti na engleski može se pronaći na: www.uvns.hr/en.

3.2 Nacionalni prioriteti u području kiberkriminaliteta

Kako bi se ostvarilo **pravo djeteta na nenasilno okruženje** u zajednici u kojoj živi te uspostavile dugoročne, sustavne, planirane i organizirane djelatnosti s ciljem suzbijanja nasilja nad djecom u zajednici i medijima te borbe protiv elektroničkog nasilja, Nacionalnom strategijom, kako je opisana ocjenjivačkom timu, predviđaju se sljedeće mjere:

- korištenje medijima za promicanje nulte stope tolerancije na nasilje nad djecom u zajednici i medijima te na elektroničko nasilje, naglašavanjem odgovornosti svih članova društva kada je riječ o nasilju nad djecom izvan škole i obitelji;
- dosljedna primjena zakonodavstva;
- razvoj učinkovitih sankcija za neusklađenost sa zakonodavstvom u pogledu nasilja u medijima i na internetu;
- redovito izvješćivanje nadležnih institucija o navedenome.

U području osposobljavanja projekt Instrumenta pretpristupne pomoći iz 2010. pod nazivom „Regionalna suradnja u području kaznenog pravosuđa: jačanje kapaciteta u borbi protiv kiberkriminaliteta u jugoistočnoj Europi" doveo je do uspostave pokusnog Regionalnog centra (u daljnjem tekstu: Centar) u Zagrebu za osposobljavanje pravosudnih dužnosnika za borbu protiv kiberkriminaliteta. Projekt je proveden u razdoblju od studenoga 2010. do travnja 2013. Osnivanje Centra jedan je od ključnih rezultata projekta u kojem su sudjelovale sljedeće zemlje koje se sada koriste uslugama Centra: Albanija, Bosna i Hercegovina, Crna Gora, Hrvatska, Kosovo, Makedonija, Srbija i Turska. Republika Hrvatska (koja je prva od država uključenih u projekt postala članica EU-a) odabrana je za državu u kojoj će se osnovati pokusni centar.

Na konferenciji održanoj u veljači 2013. u Dubrovniku visoki dužnosnici iz ministarstava pravosuđa i ministarstava unutarnjih poslova svih država koje su sudjelovale u projektu potpisali su Izjavu o strateškim prioritetima suradnje u borbi protiv kiberkriminaliteta u kojoj je osnivanje pokusnog centra u Hrvatskoj također prepoznato kao jedan od strateških prioriteta.

S obzirom na to da Nacionalna strategija kibernetičke sigurnosti još nije donesena, Pravosudna akademija predložit će da se nacionalno i regionalno osposobljavanje pravosudnih dužnosnika za borbu protiv kiberkriminaliteta uključi u Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti u onom dijelu koji se tiče osposobljavanja sudaca i državnih odvjetnika.

Hrvatska aktivno sudjeluje u radu podprioriteta za kibernapade Europske multidisciplinarne platforme za borbu protiv kaznenih djela (EMPACT), a hrvatski stručnjaci bili su članovi skupine za razvoj operativnih akcijskih planova za 2014. i 2015. Hrvatska je voditeljica aktivnosti 5.1.: „Nacrti smjernica i/ili operativnih postupaka za poboljšanje operativnih nacionalnih kontaktnih točaka (NCP) za razmjenu informacija u skladu s člankom 13. Direktive 2013/40/EU o napadima na informacijske sustave".

Hrvatska sudjeluje i u sljedećim aktivnostima: razvoju zajedničkih instrumenata za ciljano onesposobljavanje najvećih distributera, sustava i usluga zlonamjernog softvera koji utječu na dvije države članice ili više njih; utvrđivanju visokovrijednih ciljeva prikladnih za odgovor koji uključuje suradnju dvaju ili više država članica; uspostavi Europske stručne skupine za kiberkriminalitet koja će se baviti svim aspektima borbe protiv kiberkriminaliteta na razini stručnjaka; prikupljanju informacija o zlonamjernom softveru koji je povezan s aktualnim napadima, a koje bankarski sektor šalje centru EC3 te njihovu prosljeđivanju Sustavu za analizu zlonamjernog softvera (EMAS) EUROPOL-a; pružanju potpore državama članicama i operativnim partnerima u integraciji metoda pranja novca i povrata imovine kao sastavnog dijela operativnih aktivnosti u tom operativnom akcijskom planu, uz što je veće moguće iskorištavanje prilika za financijsku istragu usmjerenu na ciljeve utvrđene u operativnim aktivnostima tog plana operativnih aktivnosti; razmjeni najboljih praksi i iskustava u području suradnje s trećim zemljama; mjerama za omogućavanje razvoja i održavanja materijala za osposobljavanje u skladu s potrebama u pogledu osposobljavanja; okviru kompetencija za ocjenjivanje/osposobljavanje koji je uspostavljen u operativnom akcijskom planu za 2014.; razvoju i primjeni rješenja za pseudonimizirano unakrsno podudaranje i prepoznavanje sličnosti podataka.

U Nacionalnoj strategiji kibernetičke sigurnosti navode se sljedeći opći prioriteti:

- sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira;
- provođenje aktivnosti i mjera u svrhu jačanja sigurnosti i pouzdanosti kiberprostora;
- uspostava učinkovitijeg mehanizma za razmjenu i prijenos podataka te pristup podacima;
- jačanje svijesti o sigurnosti u kiberprostoru;
- razvoj usklađenih obrazovnih programa;
- poticanje razvoja e-usluga;
- poticanje istraživanja i razvoja;
- sustavni pristup međunarodnoj suradnji.

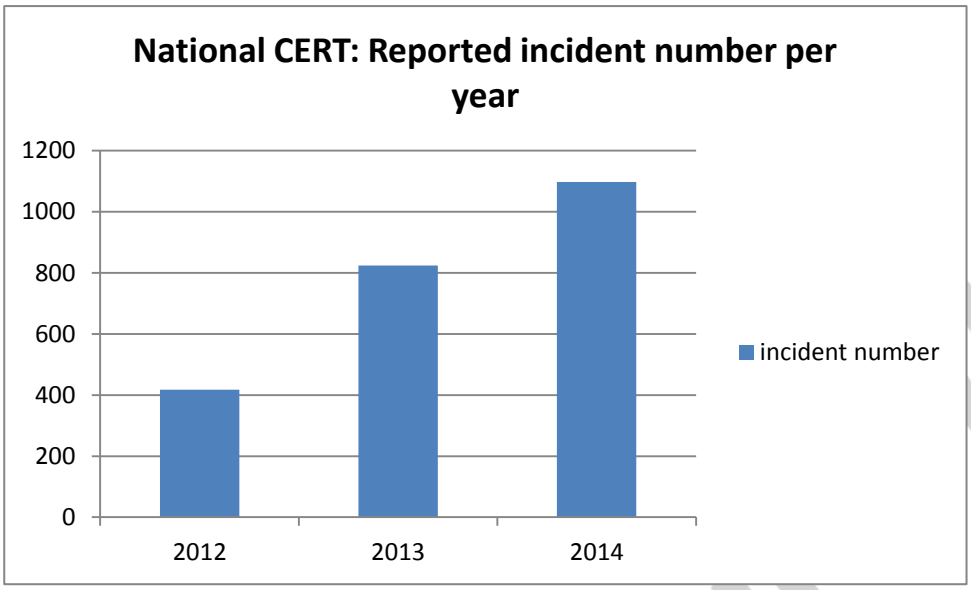
Hrvatski nacionalni prioritetni zadaci povezani su sa strateškim ciljevima i operativnim akcijskim planovima EU-a, s obzirom na to da hrvatska policija aktivno sudjeluje u projektima EMPACT-a u području kibernapada. Stoga i to predstavlja jedan od ciljeva u pogledu sprečavanja, istraživanja i borbe protiv kiberkriminaliteta.

3.3 Statistika o kiberkriminalitetu

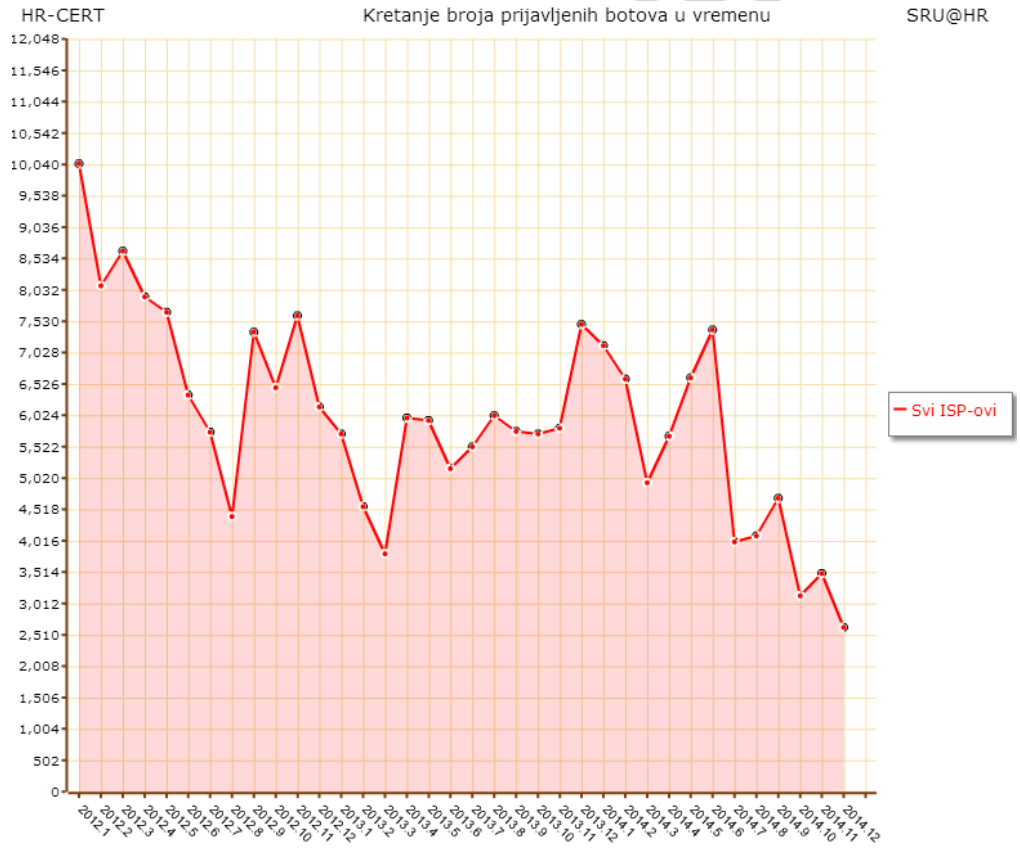
3.3.1. Glavni trendovi koji dovode do kiberkriminaliteta

Tijekom 2014. broj prijavljenih slučajeva kaznenih djela kiberkriminaliteta u kojima su sudjelovali poznati počinitelji nastavio se povećavati u skladu s očekivanjima te je prijavljena 131 osoba, što predstavlja povećanje od 11 % u odnosu na prethodnu godinu. Broj prijavljenih slučajeva nizak je zato što kaznena djela kiberkriminaliteta čine samo 0,5 % svih kaznenih djela za koja su odgovorni odrasli počinitelji.

Broj kiberincidenata koje je obradio Nacionalni CERT povećao se u posljednje tri godine, kao što je vidljivo na slici. Većina incidenata povezana je s kompromitiranim poslužiteljima koji poslužuju krivotvorene internetske stranice korištene za prijevaru (*phishing*) ili zlonamjerni softver.



Broj identificiranih botova u zemlji neznatno je opao u posljednje tri godine, a najveći zabilježeni broj bio je uzrokovan zarazom zlonamjernim softverom Zeus u 2014.



3.3.2. Broj registriranih slučajeva kiberkriminaliteta

Državno odvjetništvo Republike Hrvatske, djelujući u okviru svoje nadležnosti, vodi evidenciju statističkih podataka o kaznenim djelima počinjenim u području kiberkriminaliteta.

Ministarstvo pravosuđa trenutačno priprema posebno izvješće u okviru projekta za nadogradnju sustava e-File, kojim će se omogućiti statističko praćenje kaznenih predmeta prema kriteriju svih kaznenih djela navedenih u Kaznenom zakonu, uključujući kaznena djela kiberkriminaliteta.

Statistički podaci Nacionalnog CERT-a prikupljaju se na temelju prijavljenih incidenata te se rješavaju i pohranjuju odvojeno.
Statistički podaci Državnog odvjetništva Republike Hrvatske za 2013. pokazuju sljedeće:
– za kazneno djelo mamljenja djece za zadovoljenje spolnih potreba (članak 161. Kaznenog zakona (Narodne novine br. 125/11, 144/12, 56/15, 61/1), u daljnjem tekstu: Kazneni zakon) podneseno je pet kaznenih prijava, podignute su četiri optužnice i donesene tri presude;
– za kazneno djelo iskorištavanja djece za pornografiju (članak 163. Kaznenog zakona) podneseno je 26 kaznenih prijava, pokrenute su tri istrage, podignute 23 optužnice i doneseno 16 presuda;
– za kazneno djelo upoznavanja djece s pornografijom (članak 165. Kaznenog zakona) podneseno je sedam kaznenih prijava i podignuta jedna optužnica;
– za teška kaznena djela spolnog zlostavljanja i iskorištavanja djeteta (članak 166. Kaznenog zakona) podneseno je 12 kaznenih prijava, pokrenute su četiri istrage, podignuto 11 optužnica i doneseno osam presuda;

– za kazneno djelo neovlaštenog pristupa (članak 266. Kaznenog zakona) podneseno je sedam kaznenih prijava, podignuto pet optužnica i doneseno pet presuda;
– za kazneno djelo ometanja rada računalnog sustava (članak 267. Kaznenog zakona) podnesena je jedna kaznena prijava;
– za kazneno djelo računalnog krivotvorenja (članak 270. Kaznenog zakona) podnesena je jedna kaznena prijava, podignuta jedna optužnica i donesene dvije presude;
– za kazneno djelo računalne prijevare (članak 271. Kaznenog zakona) podneseno je 105 kaznenih prijava, pokrenuta jedna istraga, podignute 103 optužnice i doneseno 64 presuda.

U 2014. većina kaznenih prijava (113) i dalje se odnosila na kazneno djelo računalne prijevare, kako je navedeno u članku 271. Kaznenog zakona. U tom razdoblju ukupno su 102 osobe optužene za tu vrstu kaznenog djela. U 2014., nakon podizanja optužnica, sudovi su donijeli 92 presude, od kojih 88 osuđujućih, a deset počinitelja kaznenog djela računalne prijevare kažnjeno je zatvorskim kaznama uz zapljenu materijalne koristi.

Broj kaznenih djela povezanih sa seksualnim iskorištavanjem i zlostavljanjem djeteta koja su obuhvaćena definicijom „kiberkriminaliteta” povećava se, kao što je vidljivo na sljedećoj tablici u kojoj se uspoređuju podaci za 2013. i 2014.

SEKSUALNO ZLOSTAVLJANJE I ISKORIŠTAVANJE DJETETA[7]

2013. – 2014.

KAZNENO DJELO	2013.	2014.
Čl. 161. Mamljenje	14	11
Čl. 163. Iskorištavanje djece za pornografiju	61	141
Čl. 164. Iskorištavanje djece za pornografske predstave	3	0
Čl. 165. Upoznavanje djece s pornografijom	24	19
UKUPNO	102	171

Rasprostranjenost kaznenih djela porasla je za 67,6 % na 131,1 % većinom zbog velikog porasta broja kaznenih djela obuhvaćenih „iskorištavanjem djece za pornografiju" (Čl. 163 Kaznenog zakona).

Nov i raširen oblik zlostavljanja odvija se putem društvenih mreža; počinitelji pokreću internetske forume, stranice/prostor na društvenim mrežama i drugim internetskim komunikacijskim alatima kako bi prikupljali i objavljivali fotografije djevojčica/dječaka snimljene bez njihova znanja pri obavljanju njihovih svakodnevnih aktivnosti, pri čemu počinitelji objavljuju fotografije na društvenim mrežama u svrhu otkrivanja, prozivanja, vrijeđanja i ismijavanja žrtava. Tko ugrozi dobrobit djeteta objavom osobnih podataka ili njegove fotografije i izazove uznemirenost kod djeteta ili porugu vršnjaka ili drugih osoba, osobito putem računalnog sustava ili mreže, izlaže se kaznenom progonu zbog počinjenja kaznenog djela na temelju članka 178. Povreda privatnosti djeteta.

Kazneno djelo	2013.	2014.
Čl. 178. Povreda privatnosti djeteta	9	35

Nakon posjeta na licu mjestu ocjenjivačkom timu proslijeđene su sljedeće su statistike o kaznenim djelima počinjenima protiv računalnih sustava, programa i podataka za razdoblje od 2013. do 2015.:

[7] Kazneni zakon (Narodne novine 125/11, 144/12)

KAZNENI ZAKON

KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA[8]

kazneno djelo / godina (razdoblje)	2013.	2014.	siječanj – kolovoz 2015.
Članak 266. **Neovlašteni pristup**	**16**	**16**	**15**
Članak 267. **Ometanje rada računalnog sustava**	**4**	**1**	**1**
Članak 268. **Oštećenje računalnih podataka**	**2**	**4**	**2**
Članak 269. **Neovlašteno presretanje računalnih podataka**	**4**	**3**	**5**
Članak 270. **Računalno krivotvorenje**	**86**	**169**	**72**
Članak 271. **Računalna prijevara**	**583**	**960**	**835**
Članak 272. **Zlouporaba naprava**	**12**	**19**	**10**

[8] Ove statistike predstavljaju broj kaznenih djela koje je policija prijavila državnim odvjetnicima u Hrvatskoj za navedeno razdoblje. Brojevi ne predstavljaju broj počinitelja. Valjalo bi napomenuti da uglavnom ima manje počinitelja od prijavljenih kaznenih djela jer jedan počinitelj može počiniti više od jednog kaznenog djela te ne završe sva prijavljena kaznena djela na sudovima.

3.4. Nacionalni proračun namijenjen sprečavanju i borbi protiv kiberkriminaliteta i potpora iz fondova EU-a

Hrvatska će uskoro dovršiti projekt bratimljenja (twinning) pod nazivom „Jačanje kapaciteta Ministarstva unutarnjih poslova u suzbijanju kibernetičkog kriminala", koji zajednički provode španjolsko Ministarstvo unutarnjih poslova, austrijsko Savezno ministarstvo unutarnjih poslova i hrvatsko Ministarstvo unutarnjih poslova. Projekt je dio inicijative bratimljenja koju je pokrenula Europska komisija s ciljem pružanja pomoći zemljama korisnicama u jačanju njihovih administrativnih kapaciteta za provedbu pravne stečevine EU-a. Cilj tog projekta vrijednog 700 000 EUR koji financira Europska unija bilo je jačanje kapaciteta Ministarstva unutarnjih poslova za učinkovitu borbu protiv kiberkriminaliteta na nacionalnoj i međunarodnoj razini, u skladu s relevantnim politikama i strategijama EU-a.

Ministarstvo unutarnjih poslova u okviru programa pretpristupne pomoći Instrumenta pretpristupne pomoći Europske komisije za 2009. provelo je projekt pod nazivom „Izgradnja kapaciteta u području suzbijanja seksualnog iskorištavanja i seksualnog zlostavljanja djece te pružanja pomoći policije ranjivim žrtvama kriminaliteta". Cilj tog projekta bilo je daljnje jačanje institucijskih kapaciteta tijela kaznenog progona te pravosudnog sustava i sustava socijalne skrbi. Njime se također nastojalo povećati svijest javnosti o sprečavanju i suzbijanju seksualnog iskorištavanja i seksualnog zlostavljanja djece te o pružanju pomoći policije i pravosudnih tijela ranjivim žrtvama kaznenih djela. To se jačanje ostvaruje uspostavom održivog sustava potpore za daljnji prijenos razvijenih vještina, znanja i najbolje prakse te promicanjem cjelovitog pristupa putem suradnje relevantnih državnih tijela, NVO-a i poslovnog sektora. Projekt se sastojao od dviju komponenata (bliska suradnja i nabava) koje su uključivale sljedeće aktivnosti: prikupljanje podataka i analizu sustava Ministarstva unutarnjih poslova i pravosudnog sustava za borbu protiv seksualnog iskorištavanja i seksualnog zlostavljanja djece, donošenje

Protokola o postupanju u slučaju zlostavljanja i zanemarivanja djece, sastavljanje priručnika sa standardnim operativnim postupcima za provedbu istraga u slučajevima seksualnog iskorištavanja i seksualnog zlostavljanja djece, uspostavu specijaliziranog internetskog servisa za pružanje potrebnih informacija ranjivim žrtvama kaznenih djela i prijavljivanje kaznenih djela putem interneta, kampanju podizanja svijesti s ciljem poticanja prijavljivanja kaznenih djela počinjenih na štetu djece, smjernice za policijske službenike o pomoći ranjivim žrtvama kaznenih djela, osposobljavanje policijskih službenika, tužitelja i sudaca za provedbu kriminalističkih istraga u slučajevima seksualnog iskorištavanja i seksualnog zlostavljanja djece, pružanje pomoći ranjivim žrtvama kaznenih djela, osposobljavanje za uporabu tehničke opreme i osposobljavanje policijskih službenika, instruktora, tužitelja i sudaca s ciljem daljnjeg prenošenja znanja i vještina.

Nabava je komponenta koja uključuje opremanje prostorija za obavljanje informativnih razgovora s djecom te informatičku opremu i forenzičke programe koji bi trebali olakšati kriminalističke istrage i poboljšati njihovu kvalitetu, a namijenjeni su za pretraživanje računala i mobilnih telefona te pohranu medija i obradu podataka. Provedbom projekta znatno je poboljšano iskustvo djece žrtava u sudskom postupku i u postupcima koje provodi policija. Za vrijeme projekta, od rujna 2011. do travnja 2013. u suradnji s policijskim stručnjacima iz Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske održano je pet radionica kojima je prisustvovalo 100 policijskih službenika iz svih 20 policijskih uprava i čiji je cilj bio pružiti osnovno znanje o različitim kaznenim djelima počinjenim na štetu djece na internetu, uspješnoj provedbi istraga te korištenju otvorenim izvorima na internetu u policijskim istragama. Održane su i radionice s praktičnim vježbama s ciljem poboljšanja kvalitete kriminalističkih istraga i prikupljanja dokaza. Uz to, 20 policijskih službenika na naprednim je radionicama prošlo osposobljavanje za korištenje dvama forenzičkim računalnim programima koji se upotrebljavaju u mnogim policijskim upravama u Europskoj uniji (Net Clean Analyse DI i C4All) i čija je primarna svrha kategorizacija sadržaja dječje pornografije pronađenog tijekom pretraživanja računala koji pripada osumnjičeniku. Na tim radionicama policijski službenici osposobljeni su i za izradu baze podataka s dječjom pornografijom i upravljanje njome te naposljetku za identifikaciju žrtve kao jedini pravi i učinkoviti način za sprečavanje daljnjeg zlostavljanja djeteta.

Osim toga, u suradnji s Instrumentom EU-a za tehničku pomoć i razmjenu informacija (TAIEX) organiziran je niz radionica namijenjenih jačanju kapaciteta policije za borbu protiv distribucije dječje pornografije putem interneta. Teme radionica bile su, među ostalim, „Prikupljanje informacija putem interneta – otvoreni izvori", „Pretraživanje mjesta događaja" itd. Organizirani su i studijski posjeti državama članicama EU-a s većim iskustvom u borbi protiv te vrste kriminaliteta. Hrvatska je izjavila da je primila i upotrebljavala pristup „Softveru za zaštitu djece" kao učinkovitom načinu borbe protiv dječje pornografije.

Nacionalni CERT posljednje 2,5 godine sudjeluje u projektu EU-a pod nazivom ACDC (Centar za naprednu računalnu zaštitu), koji je sufinancirala Europska komisija. Hrvatska je ostvarila korist od projekta nakon što je pokrenut portal s besplatnim i komercijalnim alatima za zaštitu od zlonamjernog softvera za sve korisnike interneta u Hrvatskoj kako bi im se omogućilo da zaštite svoje radne stanice od zaraze. Hrvatska je uspostavila mrežu osjetila za otkrivanje napada neželjenom elektroničkom poštom (spam) i drugim zlonamjernim softverom koji pogađaju Hrvatsku, s ciljem borbe protiv mreža zaraženih računala (botnet). Ocjenjivački tim obaviješten je o čvršćoj suradnji između hrvatskog CERT-a i partnera u drugim državama članicama, kao što su Slovenija i Poljska.

Zavod za sigurnost informacijskih sustava (ZSIS) financira se iz godišnjeg hrvatskog državnog proračuna. ZSIS ne raspolaže namjenskim proračunskim sredstvima za sprečavanje i borbu protiv kiberkriminaliteta niti prima financijska sredstva EU-a.

3.5. Zaključci

- U vrijeme posjeta na licu mjesta prva je Nacionalna strategija kibernetičke sigurnosti, zajedno s akcijskim planom za njezinu provedbu, podnesena s ciljem donošenja. Ocjenjivački tim obaviješten je nakon posjeta na licu mjesta da je Nacionalna strategija kibernetičke sigurnosti donesena 7. listopada 2015. (Narodne novine 108/2015).

- Statistika o kiberkriminalitetu rascjepkana je jer svako nadležno tijelo vodi vlastitu evidenciju na temelju različitih kriterija. Općenito, statistički podaci predstavljeni ocjenjivačkom timu ne omogućavaju stjecanje jasnog uvida u stanje u pogledu kiberkriminaliteta u Hrvatskoj.

- Tijekom posjeta na licu mjesta Nacionalni CERT predstavio je neke primjere dobre suradnje, osobito s kolegama u Poljskoj i Sloveniji.

- Hrvatska sudjeluje u radu Europske radne skupine za kiberkriminalitet (EUCTF) te podprioritetâ EMPACT-a za prevare s kreditnim karticama (CCF) i računalne napade (CA), a u posljednjem je posebno aktivna. Hrvatska u trenutku posjeta na licu mjesta nije sudjelovala u podprioritetu EMPACT-a za seksualno iskorištavanje djece (CSE) zbog manjka kvalificiranih resursa.

- Hrvatska sudjeluje i u projektu bratimljenja „Jačanje kapaciteta Ministarstva unutarnjih poslova u suzbijanju kibernetičkog kriminala" zajedno sa Španjolskom i Austrijom.

4 NACIONALNE STRUKTURE

4.1 Pravosuđe (tužiteljstvo i sudovi)

4.1.1. Unutarnja struktura

Poslove povezane s progonom počiniteljâ kaznenih djela i drugih kažnjivih djela, uključujući kiberkriminalitet, obavljaju Državno odvjetništvo Republike Hrvatske, 15 županijskih državnih odvjetništava, 22 općinska državna odvjetništva te Ured za suzbijanje korupcije i organiziranog kriminala, kao posebno državno odvjetništvo.

Državno odvjetništvo neovisno je i samostalno pravosudno tijelo koje vodi Glavni državni odvjetnik Republike Hrvatske. Unutarnja struktura državnih odvjetništava većinom obuhvaća kaznene i građansko-upravne odjele, dok Državno odvjetništvo Republike Hrvatske ima četiri odjela (Kazneni odjel, Građansko-upravni odjel, Odjel za unutarnji nadzor i Odjel za međunarodnu pravnu pomoć i suradnju).

Hrvatske vlasti izjavile su da s obzirom na relativno malen broj kaznenih djela počinjenih protiv računalnih sustava, programa i podataka u Hrvatskoj ne postoji državno odvjetništvo specijalizirano za računalni kriminalitet.

Gradski i općinski sudovi kao sudovi opće nadležnosti nadležni su za postupanje sa slučajevima kiberkriminaliteta. Ako su ta djela istodobno u nadležnosti Ureda za suzbijanje korupcije i organiziranog kriminala, kazneni postupak vodi se pred Općinskim kaznenim sudom u Zagrebu (postoje posebno organizirani odjeli za postupanje s kaznenim djelima u nadležnosti Ureda), općinskim sudovima u Osijeku, Rijeci i Splitu te četirima najvećim županijskim sudovima u Zagrebu, Splitu, Rijeci i Osijeku.

4.1.2. Kapacitet za uspješni kazneni progon i prepreke njegovoj provedbi

Nakon ratifikacije Konvencije o kibernetičkom kriminalu i usklađivanja kaznenog zakonodavstva s Konvencijom, Državno odvjetništvo u Hrvatskoj već je započelo pripreme u pogledu osoblja i organizacije u svrhu učinkovitog progona, istrage i obrade svih oblika kiberkriminaliteta. Državnom odvjetništvu povjerene su nove zadaće i odgovornosti u skladu s najnovijim izmjenama Kaznenog zakona i novim statusom državnog odvjetnika kojem je Zakonom o kaznenom postupku dodijeljena vodeća uloga u vođenju i provedi izvida i istraga u vezi s tim vrstama kaznenih djela.

Zakon o područjima i sjedištima državnih odvjetništava (Narodne novine 128/14) doveo je do racionalizacije mreže državnih odvjetništava, tj. objedinjavanja i pripajanja manjih državnih odvjetništava velikima. Racionalizacijom i organizacijom državnih odvjetništava nadležnih za postupanje s kažnjivim djelima povezanim s kiberkriminalitetom, osigurava se učinkovitost traženja i istrage u području kiberkriminaliteta, uz stalni kontakt sa specijaliziranim Odjelom za visokotehnološki kriminalitet u okviru policije.

U većim državnim odvjetništvima (Zagreb, Novi Zagreb, Velika Gorica, Split, Rijeka, Osijek) državni odvjetnici i zamjenici koji rade na predmetima kiberkriminaliteta navode se u godišnjem rasporedu poslova.

Državno odvjetništvo raspolaže institucijskim i ljudskim resursima potrebnim za uspješan kazneni progon kaznenih djela kiberkriminaliteta. Određeni broj državnih odvjetnika prošao je posebno osposobljavanje u okviru programa Pravosudne akademije za provedbu nekoliko projekata koje financira Europska unija (programi CARD i IPA povezani s izgradnjom kapaciteta i borbom protiv kiberkriminaliteta). Za rad u području kiberkriminaliteta nije potrebno samo osnovno već i posebno osposobljavanje te kontinuirana nadogradnja u svrhu uspješnog ciljanja, otkrivanja, istrage, progona i izricanja kazni.

Tijekom regionalnog projekta IPA-a u 2010. državni odvjetnici i zamjenici državnih odvjetnika aktivno su sudjelovali u programima obrazovanja i osposobljavanja za instruktore. Kao dio Regionalnog centra Pravosudne akademije za osposobljavanje sudaca i tužitelja, jedan od instruktora dolazi iz redova tužitelja.

Putem takvog dodatnog stručnog osposobljavanja u Državnom odvjetništvu stvorena je skupina državnih odvjetnika koji se mogu učinkovito baviti predmetima iz područja kiberkriminaliteta te pružati pomoć drugim državnim odvjetnicima u Republici Hrvatskoj.

Hrvatska je naglasila da se uvođenjem sustava CTS (Case Tracking system – sustav za praćenje kaznenih predmeta) Državnom odvjetništvu Republike Hrvatske omogućava da prati statistiku rada državnih odvjetnika u svim fazama kaznenog postupka. Takvo praćenje omogućava da se pravodobno otkriju manjkavosti i nedostatci te da se ukaže na to da je potrebno kvalitetnije obraditi te predmete i eventualno provesti dodatno osposobljavanje. To će sigurno dovesti do boljeg funkcioniranja i veće učinkovitosti istrage i progona što će omogućiti izricanje primjerenih kazni za počinitelje kaznenih djela kiberkriminaliteta.

U praksi je utvrđeno da postoje problemi u vezi s kaznenim progonom počinitelja računalnih kaznenih djela, osobito kažnjivog djela računalne prijevare utvrđenog u članku 271. Kaznenog zakona, u predmetima s međunarodnom dimenzijom. Hrvatska je uočila povećani broj napada zlonamjernim računalnim programima na štetu korisnika internetskih sustava hrvatskih poslovnih banaka. Ti programi omogućuju provedbu neovlaštenih bankovnih transakcija s računa žrtava na račune privatnih ili pravnih osoba u Hrvatskoj ili inozemstvu (npr. posrednika za prijenos novca) koje potom prikupljaju novac putem Western Uniona ili sličnih pružatelja financijskih usluga i predaju ga inozemnim posrednicima ili počiniteljima. Ti posrednici ili tzv. posrednici za prijenos novca zadržavaju dio novca, koji se prenosi na njihove tekuće račune.

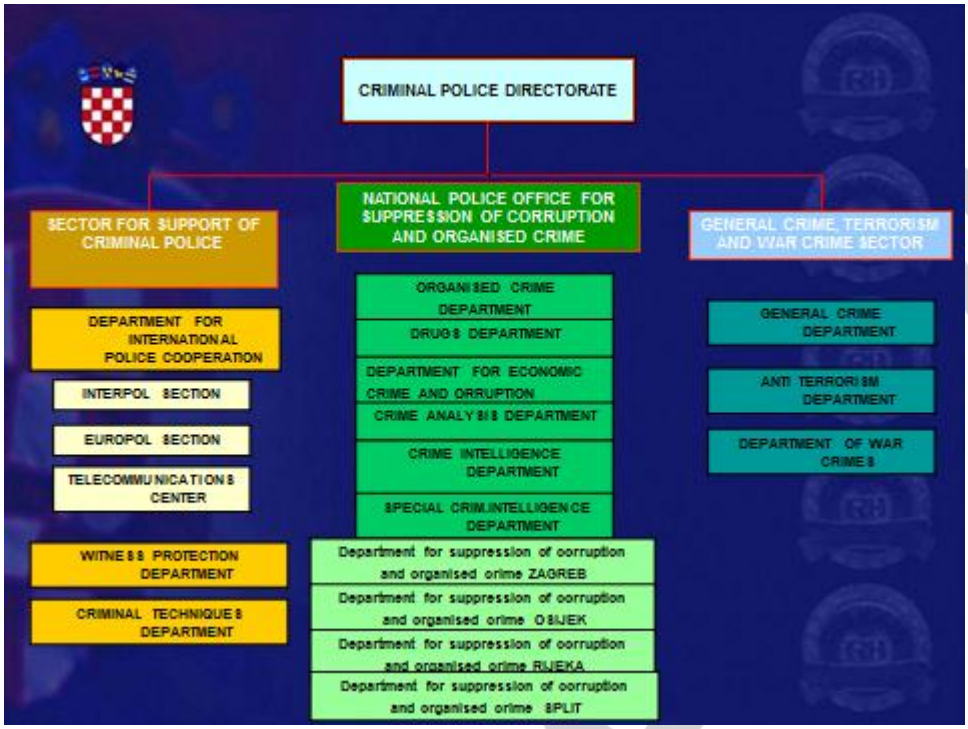
Utvrđivanje identiteta počiniteljâ teže je kada je riječ o stranim državljanima, a kazneno djelo je počinjeno u inozemstvu, iako se njegove posljedice osjećaju u Hrvatskoj. Hrvatske vlasti izjavile su da, iako se takvi slučajevi rješavaju žurno uz upotrebu „instrumenata" pravosudne suradnje kao što su odluke o zamrzavanju imovine i osiguranju dokaza (Okvirna Odluka Vijeća 2003/577/PUP od 22. srpnja 2003. o izvršenju odluka o zamrzavanju imovine i osiguranju dokaza u Europskoj uniji), u praksi se počinitelji rijetko pronalaze, a privremene mjere za zapljenu materijalne koristi od kaznenog djela rijetko se određuju.

Tijekom 2014. Državno odvjetništvo Republike Hrvatske donijelo je 16 odluka o zamrzavanju imovine i osiguranju dokaza u postupcima povezanim s računalnom prijevarom kako je utvrđena u članku 271. Kaznenog zakona. Privremene mjere za zapljenu materijalne koristi od kaznenog djela nisu određene ni u jednom slučaju jer su u vrijeme donošenja odluka o zamrzavanju imovine i osiguranju dokaza sporna sredstva već bila podignuta i nisu se više nalazila na bankovnim računima ili nisu bila dovoljna za provedbu privremenih mjera zapljene takve materijalne koristi.

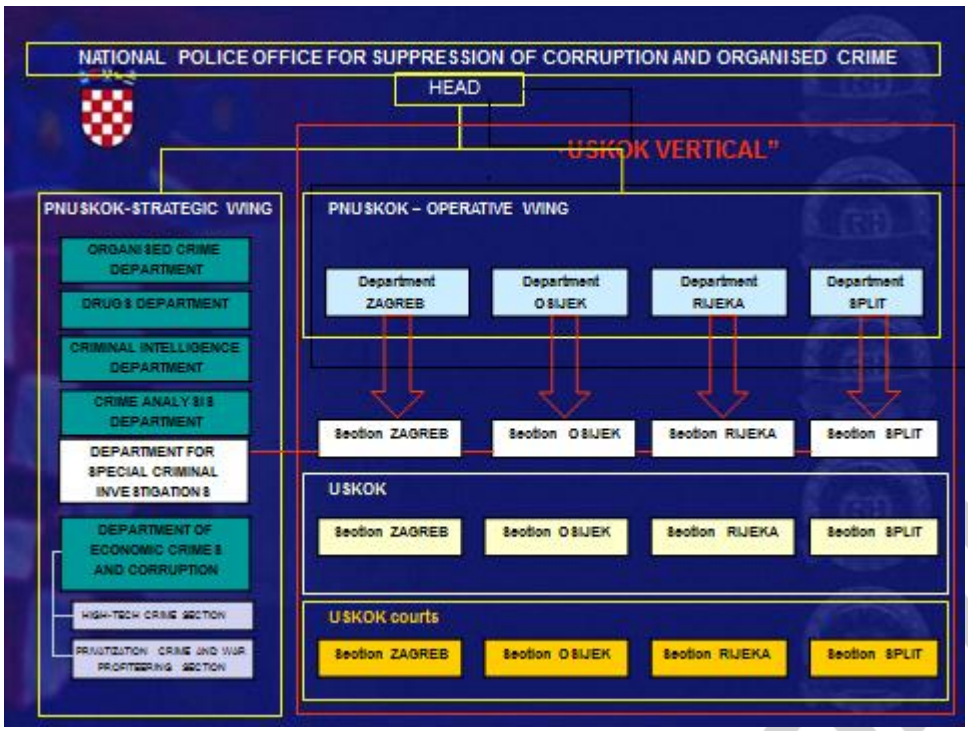
4.2. Tijela kaznenog progona

Nacionalna razina

Uprava kriminalističke policije policijski je odjel na nacionalnoj razini odgovoran za istrage svih vrsta kaznenih djela, uključujući kiberkriminalitet.

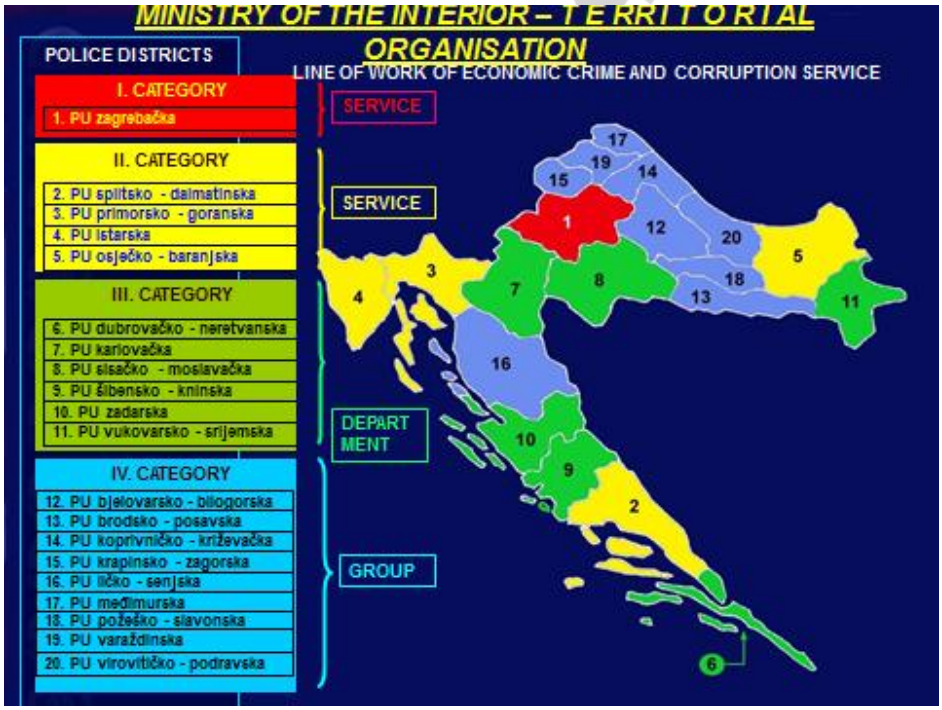


U 2008. u okviru te Uprave osnovan je novi odjel pod nazivom **Policijski nacionalni ured za suzbijanje korupcije i organiziranog kriminala (PNUSKOK).** PNUSKOK se sastoji od središnjeg, strateškog krila (unutar Uprave kriminalističke policije) i četiri regionalna odjela u četirima velikim hrvatskim gradovima. Ta je struktura organizacijski kompatibilna sa strukturom Ureda za suzbijanje korupcije i organiziranog kriminala (USKOK). Temeljna načela rada nacionalnih odjela jesu prilagodljivost i fleksibilnost. Odjel za visokotehnološki kriminalitet sastavni je dio PNUSKOK-a i odgovoran je za borbu protiv kiberkriminaliteta na nacionalnoj razini. Dijagram u nastavku prikazuje strukturu Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminala:



Regionalna razina

U Hrvatskoj postoji 20 regionalnih policijskih centara pod nazivom **policijske uprave**. Oni obavljaju policijske poslove Ministarstva unutarnjih poslova unutar teritorija svoje županije. Policijske uprave podijeljene su u četiri kategorije. Slika u nastavku prikazuje teritorijalni ustroj regionalnih policijskih odjela:



Odjel za visokotehnološki kriminalitet zasad djeluje samo na nacionalnoj razini. U 20 regionalnih policijskih centara specijalizirani policijski službenici unutar Odjela za gospodarski kriminalitet zaduženi su za istrage u području kiberkriminaliteta koje obavljaju uz svoje druge policijske dužnosti npr. provedbu istraga u području gospodarskog kriminaliteta i analizu kriminaliteta (vidi dijagram u nastavku):

Odjel za visokotehnološki kriminalitet nadležan je za istrage kaznenih djela kiberkriminaliteta navedenih u Konvenciji Vijeća Europe o kibernetičkom kriminalu: neovlašten pristup, ometanje računalnih sustava, oštećivanje računalnih podataka, neovlašteno presretanje računalnih podataka, računalno krivotvorenje, računalna prijevara, zloporaba naprava i teška kaznena djela protiv računalnih sustava, programa i podataka. Odjel za visokotehnološki kriminalitet nadležan je za istrage kaznenih djela povrede intelektualnog vlasništva i kaznenog djela krivotvorenja lijekova ili medicinskih proizvoda.

U vrijeme posjeta Odjel za visokotehnološki kriminalitet nije bio nadležan za istrage u vezi s dječjom pornografijom na računalnom sustavu ili mreži (to je u nadležnosti Odjela za maloljetničku delinkvenciju i kriminalitet na štetu mladeži i obitelji) niti za prijevare s bankovnim karticama (to je u nadležnosti Odjela za organizirani kriminalitet u okviru PNUSKOK-a). Odjel za visokotehnološki kriminalitet postao je za to nadležan od listopada 2015. zajedno s Odjelom za maloljetničku delinkvenciju i kriminalitet na štetu mladeži i obitelji.

Odjel za maloljetničku delinkvenciju i kriminalitet na štetu mladeži i obitelji središnje je policijsko tijelo na nacionalnoj razini koje prati i analizira kaznena djela počinjena na štetu djece, osobito ona koja uključuju seksualno iskorištavanje djece i mladih putem interneta. Odjel je nadležan za: praćenje novih oblika kaznenih djela; utvrđivanje najprikladnijeg načina sprečavanja takvih kaznenih djela i pružanje stručne pomoći policijskim upravama; nadzor, organizaciju i poduzimanje kriminalističkih istraga složenijih kaznenih djela na nacionalnoj razini. Nadalje, Odjel je nadležan za suradnju s drugim tijelima državne uprave te organizacijama civilnog društva, međunarodnim organizacijama i drugim tijelima, a sudjeluje i u izradi normativnih akata. Policijski službenici u Odjelu nadležni su i za identifikaciju žrtava te rad na Interpolovoj Međunarodnoj bazi podataka o seksualnom iskorištavanju djece (ICSE), a prijave Nacionalnom centru za nestalu i iskorištavanu djecu (NCMEC) dostavljaju se putem mrežne aplikacije za sigurnu razmjenu informacija (SIENA). Protokolom o postupanju u slučaju zlostavljanja i zanemarivanja djece standardizirani su postupci u navedenom okviru aktivnosti, koji uključuju međusektorsku suradnju s ciljem pružanja potpore djeci žrtvama. Spomenuta suradnja znači da bi policija trebala odmah obavijestiti nadležno tijelo socijalne skrbi o seksualnom iskorištavanju djeteta kako bi se osiguralo da dijete primi pomoć i potporu.

Žrtve imaju temeljno pravo biti primjereno obaviještene te ih stoga policija tijekom prvog kontakta informira o svim njihovim općim i posebnim pravilima. Djetetu i njegovu skrbniku ta se prava predstavljaju u standardiziranom pisanom obliku. Policijski službenici specijalizirani za mladež provode informativne razgovore s djecom žrtvama seksualnog iskorištavanja.

Na nacionalnoj razini Odjel za maloljetničku delinkvenciju i kriminalitet na štetu mladeži i obitelji nadležan je za kriminalističke istrage u vezi sa seksualnim zlostavljanjem djece (uključujući zlostavljanje na internetu). Taj Odjel, čija su obilježja i nadležnost već opisani, zapošljava šest policijskih službenika, od kojih je dvoje prvenstveno odgovorno za: provedbu, praćenje i koordinaciju istraga složenih kaznenih djela zlostavljanja i iskorištavanja djece putem interneta. Ti službenici također pružaju tehničku pomoć policijskim upravama te prate i odgovaraju na prijave putem sustava prijavljivanja na internetu „Red Button" i prijave NCMEC-u. Osim toga, to dvoje službenika Odjela odgovorni su za identifikaciju žrtava i rad na Interpolovoj međunarodnoj bazi podataka dječje pornografije (ICSE).

Na regionalnoj razini policijskih uprava uspostavljeni su odjeli ili skupine (ovisno o veličini policijske uprave) koji se bave maloljetničkom delinkvencijom i kaznenim djelima na štetu djece i obitelji. Nadalje, na lokalnoj razini u svim policijskim postajama nalazi se policijski službenik odgovoran za mladež. Svi takvi službenici u Republici Hrvatskoj prošli su specijalistički tečaj za provedbu istraga kaznenih djela na štetu djece i za rad s djecom žrtvama. Osim općeg tečaja namijenjenog policijskim službenicima koji rade s mladima mnogi od tih službenika prošli su različite oblike dodatnog osposobljavanja, primjerice tečajeve koje organizira Policijska akademija, projekte IPA-a, radionice TAIEX-a te međunarodne seminare i tečajeve.
U Hrvatskoj postoji 260 specijaliziranih policijskih službenika za mladež.

Centar za forenzična ispitivanja, istraživanja i vještačenja „Ivan Vučetić" sa sjedištem u Zagrebu ustrojstvena je jedinica policije nadležna za proces pretvorbe materijalnog traga izuzetog s mjesta počinjenja kaznenog djela u pravovaljani materijalni dokaz. Centar je javna ustanova specijalizirana za forenziku koja obavlja kriminalističko-tehničke poslove i vještačenja te izravno sudjeluje u otkrivanju gotovo svih kaznenih djela i njihovih počinitelja na hrvatskom državnom području.

Tijekom nepunih šest desetljeća postojanja, Centar je izrastao u suvremenu instituciju koja danas stoji rame uz rame s europskim i svjetskim forenzičnim institutima. Od 1998. Centar je punopravan član Europske mreže instituta forenzične znanosti (ENFSI), krovne organizacije nacionalnih forenzičnih instituta Europe koja okuplja ukupno 56 članica iz gotovo svih zemalja Europe. Centar zapošljava dvoje digitalnih forenzičara. Ocjenjivački tim obaviješten je o velikom radnom opterećenju tih stručnjaka.

Policijske ovlasti mogu se izvršavati tijekom istraga svih kaznenih djela i ne postoje posebne policijske ovlasti za istrage u području kiberkriminaliteta.

Uprava kriminalističke policije provela je projekt Instrumenta pretpristupne pomoći za 2009. pod nazivom „Izgradnja kapaciteta u području suzbijanja seksualnog iskorištavanja i seksualnog zlostavljanja djece te pružanja pomoći policije ranjivim žrtvama kriminaliteta”.

Osim tog projekta, uspostavljena je suradnja s Instrumentom EU-a za tehničku pomoć i razmjenu informacija (TAIEX) na nizu radionica namijenjenih jačanju kapaciteta policije za borbu protiv distribucije dječje pornografije putem interneta. Policijski službenici pohađaju različite seminare i tečajeve koje organizira CEPOL.

Policijska akademija također organizira razne obrazovne programe i stručne tečajeve za policijske službenike koji provode kriminalističke istrage u tom području.

Policijska akademija, CEPOL i druga tijela u budućnosti će nastaviti surađivati na pružanju sadržaja u pogledu obrazovanja i osposobljavanja za policijske službenike koji se bave takvom vrstom kriminalističkih istraga.

4.3. Druga tijela / institucije / javno-privatno partnerstvo

Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) sa sjedištem u Zagrebu pravna je osoba s javnim ovlastima u okviru djelokruga i nadležnosti propisanih Zakonom o elektroničkim komunikacijama koji je stupio na snagu 1. srpnja 2008. i posebnim zakonom kojim se uređuje područje poštanskih usluga. HAKOM je neovisna, samostalna i neprofitna pravna osoba s javnim ovlastima. Rad HAKOMA javan je. HAKOM-om upravlja Vijeće koje čini pet članova, uključujući predsjednika i zamjenika predsjednika. Predsjednika, zamjenika predsjednika i članove Vijeća imenuje na razdoblje od pet godina i razrješava Hrvatski sabor na prijedlog Vlade Republike Hrvatske. Vijeće HAKOM-a donosi odluke većinom glasova. HAKOM ima stručnu službu koja obavlja stručne, administrativne i tehničke poslove Agencije, a ustrojena je su skladu sa Statutom HAKOM-a i njegovim drugim općim aktima. Nadležnost HAKOM-a propisana je člankom 12. Zakona o elektroničkim komunikacijama (NN 73/08) i člankom 38. Zakona o poštanskim uslugama (NN 88/09).

Strateški ciljevi HAKOM-a su:

promicanje regulacije tržišta elektroničkih komunikacija;
promicanje regulacije tržišta poštanskih usluga;
podupiranje rasta ulaganja i inovacija na tržištu elektroničkih komunikacija;
podupiranje rasta ulaganja i inovacija na tržištu poštanskih usluga;
osiguravanje učinkovitog iskorištavanja ograničenih resursa;
ubrzanje rasta proizvoda i usluga širokopojasnih mreža;
pružanje povoljnih ponuda komunikacijskih i poštanskih usluga;
poboljšanje zaštite korisnika i pružanja informacija korisnicima;
izgradnja učinkovitog i sveobuhvatnog informacijskog sustava;
definiranje i provedba učinkovitih procesa;
stjecanje multidisciplinarnih kompetencija u području regulacije tržišta.

Nacionalni CERT. Prema Zakonu o informacijskoj sigurnosti hrvatski nacionalni CERT nacionalno je tijelo za sprečavanje i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu: CARNet). CERT usklađuje sigurnosne postupke u slučaju incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj ili u drugim zemljama i organizacijama, kada su povezani s Republikom Hrvatskom. On usklađuje rad tijela koja rade na sprečavanju i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.

Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo za sigurnost informacijskih i mrežnih sustava vladinih tijela, jedinica lokalne i regionalne samouprave te pravnih osoba s javnim ovlastima. Kao takav ima prvenstvenu zadaću pružati pomoć tijelima državne vlasti Republike Hrvatske u provedbi preventivnih mjera za smanjenje rizika od računalnih sigurnosnih incidenata, a u slučaju incidenta odgovoran je za uklanjanje incidenta ili posreduje u postupku njegova uklanjanja. Kibersigurnost za vladina tijela uključuje sprečavanje računalnih sigurnosnih incidenata i pružanje odgovora na računalne sigurnosne incidente. ZSIS, na zahtjev, stručnim znanjem pomaže tijelima kaznenog progona u kriminalističkim istragama koje ta tijela vode.

ZSIS djeluje na sljedećim tehničkim područjima sigurnosti informacijskih sustava:

1. standardi sigurnosti informacijskih sustava;
2. sigurnosna akreditacija informacijskih sustava;
3. upravljanje kriptomaterijalima koji se upotrebljavaju u razmjeni klasificiranih podataka;
4. koordinacija sprečavanja i odgovora na računalne ugroze sigurnosti informacijskih sustava.

Nacionalni CERT i ZSIS surađuju na sprečavanju i zaštiti od računalnih ugroza sigurnosti informacijskih sustava te sudjeluju u izradi preporuka i normi u Republici Hrvatskoj iz područja sigurnosti informacijskih sustava.

ZSIS kao vladin CERT zadužen je za koordinaciju sprečavanja bilo kakvog računalnog sigurnosnog incidenta, od kojih se neki često mogu klasificirati kao kiberkriminalitet u njegovoj nadležnosti. ZSIS je odgovoran za vladina tijela, jedinice lokalne i regionalne samouprave te pravne osobe s javnim ovlastima.

Prema Zakonu o informacijskoj sigurnosti Nacionalni CERT odgovoran je za usklađivanje postupanja u slučaju incidenata na javnim informacijskim sustavima u zemlji. ZSIS zapošljava devet osoba, a bavi se odgovorom na incidente, forenzičkom istragom incidenata i zlonamjernog softvera te obavještajnim radom u vezi s kiberprijetnjama koji se temelji na prikupljanju i analizi informacija o kiberincidentima.

Unutar svojeg djelokruga rada ZSIS je odgovoran za koordinaciju sprečavanja i uklanjanja računalnih sigurnosnih incidenata, od kojih se neki mogu klasificirati kao kiberkriminalitet.

4.4. Suradnja i koordinacija na nacionalnoj razini

4.4.1. Pravne obveze ili obveze u vezi s politikama

U skladu s Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (u daljnjem tekstu: Pravilnik) operatori su dužni jednom godišnje Hrvatskoj regulatornoj agenciji za mrežne djelatnosti (HAKOM) dostaviti dokumentiranu sigurnosnu politiku za prethodnu godinu koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme. Operatori su obvezni obavijestiti HAKOM:

– u slučaju pojave sigurnosnih incidenata povezanih s internetom sukladno kriterijima za izvješćivanje iz Dodatka 2. Pravilniku;

– u slučaju neovlaštenog povezivanja s javnom komunikacijskom mrežom ili dijelom mreže te u slučaju kršenja sigurnosti ili integriteta javnih komunikacijskih usluga, koji su značajnije utjecali na obavljanje djelatnosti javnih komunikacijskih mreža i/ili usluga sukladno kriterijima za izvješćivanje iz Dodatka 2. Pravilniku;
Člankom 204. Zakona o kaznenom postupku propisano je da je svatko dužan prijaviti kazneno djelo za koje se postupak pokreće po službenoj dužnosti, koje mu je dojavljeno ili za koje je saznao. Hrvatska tako u praksi ima primjere pružatelja internetskih usluga ili pružatelja usluga smještaja (hosting) koji prijavljuju da se neki korisnici služe njihovim uslugama za distribuciju dječje pornografije.

U Hrvatskoj je suradnja s privatni sektorom u području kiberkriminaliteta i kibersigurnosti većinom uređena Zakonom o elektroničkim komunikacijama i Zakonom o elektroničkoj trgovini. Zakonom o elektroničkim komunikacijama pružateljima internetskih usluga nameću se određene obveze s ciljem povećanja učinkovitosti istraga. Konkretno, u članku 109. navodi se da su operatori javnih komunikacijskih mreža i operatori javno dostupnih elektroničkih komunikacijskih usluga obvezni zadržati elektroničke podatke u svrhu omogućivanja provedbe istrage, otkrivanja i kaznenog progona kaznenih djela.

U Nacionalnoj strategiji kibernetičke sigurnosti također se navode neke smjernice za suradnju između privatnog i javnog sektora.

Za suradnju između kartične industrije, banaka, policije i državnih tužitelja odgovoran je Odbor za prijevaru s platnim karticama. Taj Odbor djeluje u okviru Hrvatske udruge banaka, a čine ga predstavnici banaka, Državnog odvjetništva i policije. Aktivnosti Odbora provode se na radnim sastancima koji se održavaju kvartalno (4 puta godišnje). Na tim sastancima članovi Odbora razmjenjuju informacije o novim oblicima zlouporabe i novim tehnologijama zaštite.

Članovi Odbora za prijevaru s platnim karticama informacije šalju elektroničkom poštom na adrese s popisa zaštićenog ključevima programa PGP. Odbor obučava zaposlenike banaka, državne tužitelje i policijske službenike, a jednom godišnje organizira radionice na kojima sudionike informira o novim zbivanjima i tehnologijama. Svi hrvatski izdavatelji kreditnih kartica prešli su na tehnologiju čip kartica (standard EMV – Europay, MasterCard, Visa). Jačanje autorizacijskog koda za transakcije putem interneta obavlja se putem tehnologije „3D Secure" te upotrebom najnovije tehnologije koja omogućuje praćenje proaktivnog djelovanja i kojom se prepoznaju malverzacije.

Policijski službenici uključeni su u multidisciplinarni rad koji za cilj ima osiguranje učinkovitog nacionalnog odgovora na prijetnju kiberkriminaliteta. Kontinuirano surađuju s Nacionalnim CERT-om (Nacionalni tim za hitne računalne intervencije). Ministarstvo unutarnjih poslova, Ministarstvo znanosti, obrazovanja i sporta te Hrvatska akademska i istraživačka mreža (CARNet), kao Nacionalni CERT, potpisali su 15. veljače 2015. Ugovor o suradnji na sprečavanju i rješavanju računalnih incidenata i drugih oblika računalnog kriminaliteta.

Tim je ugovorom obuhvaćeno:
– rješavanje računalnih sigurnosnih incidenata u kojima je barem jedna strana iz Hrvatske;
– sprečavanje računalnih sigurnosnih incidenata;
– povećanje sigurnosti za korisnike računalne i informacijske tehnologije;
– suradnja s drugim relevantnim institucijama i tijelima na izradi odgovarajućih zakonodavnih rješenja za praćenje razvoja društva, što zahtijeva specijalizirano osposobljavanje policijskih službenika, upotrebu posebne opreme i primjenu posebnih metoda potrebnih za učinkovitu borbu protiv računalnog kriminaliteta;

Policija i *Zavod za sigurnost informacijskih sustava (ZSIS)* također kontinuirano surađuju, osobito u pogledu koordinacije sprečavanja i odgovora na računalne ugroze informacijske sigurnosti.

4.4.2. Sredstva dodijeljena za poboljšanje suradnje

Ne postoje sredstva posebno dodijeljena za suradnju s privatnim sektorom.
Policijskim službenicima koji istražuju internetske kartične prijevare u njihovim istragama pomažu policijski službenici Odjela za visokotehnološki kriminalitet na nacionalnoj i/ili regionalnoj razini ako je potrebno forenzičko ispitivanje. Forenzički softver i hardver koji se upotrebljavaju tijekom istraga kibernapada upotrebljavaju se i u slučajevima internetskih kartičnih prijevara. Kako će broj istraga u području kiberkriminaliteta u kojima je potrebno koristiti se računalima i/ili internetskom forenzikom u budućnosti rasti, to bi se trebalo odražavati u broju policijskih službenika osposobljenih za računalnu i internetsku forenziku.

U praksi se suradnja s privatnim sektorom u sprečavanju kiberkriminaliteta i borbi protiv njega do sad smatra općenito uspješnom.

Kad se radi o suradnji u kojoj je privatni sektor žrtva ili strana koja je pretrpjela gubitak, hrvatske vlasti tvrde da je suradnja obično veoma dobra. U većini slučajeva privatni sektor pomaže policiji u pojašnjavanju okolnosti povezanih s kaznenim djelima i u pružanju potrebnih podataka, osiguranju dokaza itd. Suradnja je najbolja s financijskim sektorom (banke), posebno u pogledu bankovnih zlonamjernih softvera i računalnih prevara povezanih s internetskim bankarstvom. Većina banaka u Hrvatskoj članice su Hrvatske udruge banaka, a rad Udruge organiziran je u odborima. Predstavnik Odjela za visokotehnološki kriminalitet član je Odbora za informacijsku sigurnost koji se sastaje jednom mjesečno kako bi se raspravljalo o svim pitanjima kiberkriminaliteta i kibersigurnosti.

Hrvatske vlasti izjavile su da su u pogledu internetskih kartičnih prijevara oprema, resursi, kapaciteti i znanje nadležnog tijela (tijelâ kaznenog progona) zadovoljavajući. Također su zaključile da je, uzimajući u obzir dinamiku kaznenih djela, potrebno promicati suradnju između tijela nadležnih za kazneni progon i svih sudionika u kartičnom poslovanju (sektora kreditnih kartica, banaka, izvršitelja obrade, dobavljača).

4.5. Zaključci

- Hrvatska uglavnom ima uspostavljene standardne strukture za rješavanje slučajeva kiberkriminaliteta; iako među nekim od tih struktura postoje različiti oblici suradnje, bolja koordinacija među svim dionicima bila bi od koristi za zemlju;

- središnji Odjel zadužen za visokotehnološki kriminalitet sastoji se od samo petero policijskih službenika koji koordiniraju istrage diljem cijele zemlje, a njihove odgovornosti obuhvaćaju i međunarodnu policijsku suradnju te aktivnosti osposobljavanja na terenu; kartične prijevare odgovornost su Službe organiziranog kriminaliteta; međutim, obje službe surađuju u skladu s potrebama i raspoloživošću;

- slučajevima zlostavljanja djece putem računalnih sustava ili mreža bavi se Odjel maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji;

- potvrđuje se da bi policija na lokalnoj razini trebala biti bolje pripremljena za razumijevanje pitanja kiberkriminaliteta.

- Ne postoje državni odvjetnici ili suci specijalizirani za slučajeve u kojima je uključeno računalo ili slučajeve kiberkriminaliteta; iako su hrvatske vlasti navele da su neki državni odvjetnici osposobljeni za učinkovito rješavanje slučajeva kiberkriminaliteta i pružanje pomoći kolegama, i dalje postoji potreba za dodatnim strukturama posvećenima poboljšanju učinkovitosti borbe protiv kiberkriminaliteta na razini kaznenog progona, kao i na razini suda (npr. uspostavom kontaktnih točaka);

- hrvatske vlasti nadležne za kiberkriminalitet redovito surađuju i održavaju sastanke s bankovnim sektorom; međutim, utvrđena je potreba za razvijanjem strukturiranih javnih/privatnih partnerstava, posebno u pogledu suradnje između tijela kaznenog progona i pružatelja usluga.

5 PRAVNI ASPEKTI

5.1 Kazneno materijalno pravo koje se odnosi na kiberkriminalitet

5.1.1. Konvencija Vijeća Europe o kibernetičkom kriminalu

Republika Hrvatska stranka je Konvencije Vijeća Europe o kibernetičkom kriminalu. Hrvatski sabor donio je 3. srpnja 2002. Zakon o potvrđivanju Konvencije Vijeća Europe o kibernetičkom kriminalu. Konvencija je stupila na snagu u odnosu na Republiku Hrvatsku 1. srpnja 2004.
U skladu s preuzetim obvezama iz Konvencije, izmjene Kaznenog zakona donesene su 2004. Republika Hrvatska 26. ožujka 2003. potpisala je Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava. Iako je Dodatni protokol stupio na snagu 21. lipnja 2008., izmjenama Kaznenog zakona iz 2004. predviđeno je kazneno djelo rasne ili drugih oblika diskriminacija, i utvrđeno da su poricanje, znatno umanjenje, odobravanje ili opravdavanje kaznenog djela genocida ili zločina protiv čovječnosti počinjeni putem računalnih sustava kaznena djela.

5.1.2. Opis nacionalnog zakonodavstva

Kaznenim zakonom kažnjava se namjera počinjenja kaznenog djela, ali i utvrđuje kazna za nehaj.

Člankom 28. Kaznenog zakona stoga se propisuje da se kazneno djelo može počiniti s izravnom ili neizravnom namjerom. Počinitelj postupa s izravnom namjerom kad je svjestan obilježja kaznenog djela i hoće ili je siguran u njihovo ostvarenje, a s neizravnom namjerom postupa kad je svjestan da može ostvariti obilježja kaznenog djela pa na to pristaje.

Člankom 29. Kaznenog zakona propisuje se kazna za nehaj i utvrđuje da se kazneno djelo može počiniti sa svjesnim ili nesvjesnim nehajem. Počinitelj postupa sa svjesnim nehajem kad je svjestan da može ostvariti obilježja kaznenog djela, ali lakomisleno smatra da se to neće dogoditi ili će to moći spriječiti. Počinitelj postupa s nesvjesnim nehajem kad nije svjestan da može ostvariti obilježja kaznenog djela, iako je prema okolnostima bio dužan i prema svojim osobnim svojstvima mogao biti svjestan te mogućnosti.

U vezi s olakotnim i otegotnim čimbenicima, člankom 47. Kaznenog zakona propisuje se što će sud uzeti u obzir prilikom ocjene kazne. Pri izboru vrste i mjere kazne sud će, polazeći od stupnja krivnje i svrhe kažnjavanja, ocijeniti sve okolnosti koje utječu da kazna po vrsti i mjeri bude lakša ili teža (olakotne i otegotne okolnosti), a osobito jačinu ugrožavanja ili povrede zaštićenog dobra, pobude iz kojih je kazneno djelo počinjeno, stupanj povrede počiniteljevih dužnosti, način počinjenja i skrivljene učinke kaznenog djela, prijašnji počiniteljev život, njegove osobne i imovinske prilike te njegovo ponašanje nakon počinjenja kaznenog djela, odnos prema žrtvi i trud da naknadi štetu.

Nadalje, u slučaju više kaznenih djela ili ponavljanja djela sud će, u skladu s člankom 418. stavkom 5. Zakona o kaznenom postupku (Narodne novine br. 152/08, 76/09, 80/11, 121/11 – pročišćeni tekst, 91/12 – Odluka Ustavnog suda Republike Hrvatske, 143/12, 56/13, 145/13 i 152/14, u daljnjem tekstu: Zakon o kaznenom postupku), tijekom dokaznog postupka kao zadnje dokaze na završetku dokaznog postupka i prije ispitivanja optuženika pročitati podatke iz kaznene evidencije kao i druge podatke o osuđivanosti za kažnjive radnje. Isto tako, prilikom određivanja kazne za počinitelja sud će, u skladu s člankom 47. Kaznenog zakona, među ostalim ocijeniti prijašnji počiniteljev život.

Odredbe članaka 36., 37., 38. i 39. Kaznenog zakona odnose se na počiniteljstvo, poticanje, pomaganje te kažnjavanje supočinitelja i sudionika.

U članku 36. Kaznenog zakona počinitelj se definira kao osoba koja sama ili posredstvom druge osobe počini kazneno djelo. Počini li više osoba na temelju zajedničke odluke kazneno djelo tako da svaka od njih sudjeluje u počinjenju radnje ili na drugi način bitno pridonese počinjenju kaznenog djela, svaka od njih kažnjava se kao počinitelj (supočinitelj), a nehajna odgovornost supočinitelja temelji se na zajedničkoj povredi dužne pažnje.

Odredbe o poticanju utvrđene su u članku 37. Kaznenog zakona. U tom dijelu Zakonom se propisuje da tko drugoga s namjerom potakne na počinjenje kaznenog djela, kaznit će ga se kao da ga je sam počinio. Isto tako, tko drugoga s namjerom potakne na počinjenje kaznenog djela za koje je pokušaj kažnjiv, a djelo ne bude niti pokušano, kaznit će ga se kao za pokušaj toga kaznenoga djela. U slučaju neprikladnog pokušaja poticanja, poticatelj može dobiti smanjenu kaznu.

U skladu s člankom 38. Kaznenog zakona, tko drugome s namjerom pomogne u počinjenju kaznenog djela mora se kazniti kao da ga je sam počinio.

U pogledu kažnjavanja sudionika, u skladu s člankom 39. Kaznenog zakona svaki supočinitelj i sudionik (poticatelj i pomagač) kažnjava se u skladu sa svojom krivnjom, a posebne osobne okolnosti zbog kojih zakon propisuje oslobođenje od kazne, ublažavanje kazne, blaži ili teži oblik kaznenog djela uzet će se u obzir samo onom supočinitelju ili sudioniku kod kojega postoje.

A/ Okvirna odluka Vijeća 2005/222/PUP o napadima na informacijske sustave i Direktiva 2013/40/EU o napadima na informacijske sustave

Donošenjem Zakona o izmjenama i dopunama Kaznenog zakona u 2015. Republika Hrvatska prenijela je u nacionalno zakonodavstvo Direktivu 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave. Uzimajući u obzir kratko vremensko razdoblje koje je proteklo od prenošenja Direktive u nacionalno zakonodavstvo, Republika Hrvatska do sad nije imala problema u njezinoj provedbi.

Glavom XXV. Kaznenog zakona reguliraju se kaznena djela protiv računalnih sustava, programa i podataka kako slijedi:

Neovlašteni pristup

Članak 266.

(1) Tko neovlašteno pristupi računalnom sustavu ili računalnim podacima, kažnjava se kaznom zatvora do dvije godine.

(2) Tko kazneno djelo iz stavka 1. ovoga članka počini u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, Ustavnog suda Republike Hrvatske i međunarodne organizacije koje je Republika Hrvatska član, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa, kažnjava se kaznom zatvora do tri godine.

(3) Za pokušaj kaznenog djela iz stavka 1.i 2. ovoga članka počinitelj se kažnjava.

(4) Kazneno djelo iz stavka 1. ovoga članka progoni se po prijedlogu.

Ometanje rada računalnog sustava

Članak 267.

(1) Tko onemogući ili oteža rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju, kažnjava se kaznom zatvora do tri godine.

(2) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj se kažnjava.

Oštećenje računalnih podataka

Članak 268.

(1) Tko neovlašteno u cijelosti ili djelomično ošteti, izmijeni, izbriše, uništi, učini neuporabljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe, kažnjava se kaznom zatvora do tri godine.

(2) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj se kažnjava.

Neovlašteno presretanje računalnih podataka

Članak 269.

(1) Tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke, kažnjava se kaznom zatvora do tri godine.

(2) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj se kažnjava.

(3) Podaci koji su nastali počinjenjem kaznenog djela iz stavka 1. ovoga članka se uništavaju.

Računalno krivotvorenje

Članak 270.

(1) Tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim ili nedostupnim računalne podatke koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao vjerodostojni, ili tko takve podatke uporabi ili nabavi radi uporabe, kažnjava se kaznom zatvora do tri godine.

(2) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj se kažnjava.

(3) Podaci koji su nastali počinjenjem kaznenog djela iz stavka 1. ovoga članka se uništavaju.

Računalna prijevara

Članak 271.

(1) Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome, kažnjava se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je kaznenim djelom iz stavka 1. ovoga članka pribavljena znatna imovinska korist ili prouzročena znatna šteta, počinitelj se kažnjava kaznom zatvora od jedne do osam godina.

(3) Podaci koji su nastali počinjenjem kaznenog djela iz stavka 1. i 2. ovoga članka uništavaju se.

Zlouporaba naprava

Članak 272.

(1) Tko izradi, napravi, uveze, proda, posjeduje ili čini drugome dostupne uređaje ili računalne programe ili računalne podatke stvorene ili prilagođene za počinjenje kaznenih djela iz članka 266., članka 267., članka 268., članka 269., članka 270. i članka 271. ovoga Zakona s ciljem da ih uporabi za počinjenje nekog od tih djela, kažnjava se kaznom zatvora do tri godine.

(2) Tko izradi, nabavi, uveze, proda, posjeduje ili čini drugome dostupne računalne lozinke, pristupne šifre ili druge podatke kojima se može pristupiti računalnom sustavu s ciljem da ih se uporabi za počinjenje kaznenih djela iz članka 266., članka 267., članka 268., članka 269., članka 270. i članka 271. ovoga Zakona, kažnjava se s kaznom zatvora do dvije godine.

(3) Počinitelj kaznenog djela iz stavka 1. ovoga članka ne kažnjava se kaznom strožom od one koja je propisana za kazneno djelo koje je imao za cilj.

(4) Posebne naprave i programi iz stavka 1. ovoga članka oduzimaju se, a podaci iz stavka 1. i 2. ovoga članka uništavaju se.

Teška kaznena djela protiv računalnih sustava, programa i datoteka

Članak 273.

(1) Tko kazneno djelo iz članka 267. do članka 270. ovoga Zakona počini u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, Ustavnog suda Republike Hrvatske i međunarodne organizacije koje je Republika Hrvatska član, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa, kažnjava se kaznom zatvora od šest mjeseci do pet godina.

(2) Istom kaznom iz stavka 1. kažnjava se tko kazneno djelo iz članka 266. do članka 269. ovoga Zakona počini prikrivajući stvarni identitet i uzrokujući zabludu o ovlaštenom nositelju identiteta.
(3) Tko kazneno djelo iz članka 267. do članka 269. ovoga Zakona počini sredstvom namijenjenim za izvršenje napada na veći broj računalnih sustava ili kojim je prouzročena znatna šteta, kažnjava se kaznom zatvora od jedne do osam godina.

B/ Direktiva 2011/93/EU o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije

Donošenjem Zakona o izmjenama i dopunama Kaznenog zakona i Zakona o izmjenama i dopunama Zakona o kaznenom postupku (Narodne novine 145/13), Direktiva 2011/93/EU Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije, te o zamjeni Okvirne odluke Vijeća 2004/68/PUP prenesena je u hrvatsko zakonodavstvo. Ista Direktiva prenesena je i putem Zakona o izmjenama i dopunama Zakona o sudovima za mladež (Narodne novine 84/11, 143/12, 148/13 i 56/15).

Republika Hrvatska nije imala nikakvih teškoća u pogledu provedbe ove Direktive. U Glavi XVII. Kaznenog zakona posebno se reguliraju kaznena djela spolnog zlostavljanja i spolnog iskorištavanja djeteta, kako slijedi.

Mamljenje djece za zadovoljenje spolnih potreba

Članak 161.

(1) Punoljetna osoba koja osobi mlađoj od petnaest godina, u namjeri da ona ili druga osoba nad njom počini kazneno djelo iz članka 158. ovoga Zakona, putem informacijsko komunikacijskih tehnologija ili na drugi način predloži susret s njom ili drugom osobom i koja poduzme mjere da do tog susreta dođe, kažnjava se kaznom zatvora do tri godine.

(2) Tko prikuplja, daje ili prenosi podatke o osobi mlađoj od petnaest godina radi počinjenja kaznenog djela iz stavka 1. ovoga članka, kažnjava se kaznom zatvora do jedne godine.

(3) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj kažnjava.

Iskorištavanje djece za pornografiju

Članak 163.

(1) Tko dijete namamljuje, vrbuje ili potiče na sudjelovanje u snimanju dječje pornografije ili tko organizira ili omogući njezino snimanje, kažnjava se kaznom zatvora od jedne do osam godina.

(2) Kaznom iz stavka 1. ovoga članka kažnjava se tko neovlašteno snima, proizvodi, nudi, čini dostupnim, distribuira, širi, uvozi, izvozi, pribavlja za sebe ili drugoga, prodaje, daje, prikazuje ili posjeduje dječju pornografiju ili joj svjesno pristupa putem informacijsko komunikacijskih tehnologija.

(3) Tko dijete silom ili prijetnjom, obmanom, prijevarom, zlouporabom ovlasti ili teškog položaja ili odnosa zavisnosti, prisili ili navede na snimanje dječje pornografije, kažnjava se kaznom zatvora od tri do dvadeset godina.

(4) Posebne naprave, sredstva, računalni programi ili podaci namijenjeni, prilagođeni ili uporabljeni za počinjanje ili olakšavanje počinjenja kaznenog djela iz stavka 1., 2. i 3. ovoga članka se oduzimaju, a pornografski materijal koji je nastao počinjenjem kaznenog djela iz stavka 1., 2. i 3. ovoga članka se uništava.

(5) Dijete se ne kažnjava za proizvodnju i posjedovanje pornografskog materijala koji prikazuje njega samog ili njega i drugo dijete ako su oni sami taj materijal proizveli i posjeduju ga uz pristanak svakog od njih i isključivo za njihovu osobnu upotrebu.

(6) Dječja pornografija je materijal koji vizualno ili na drugi način prikazuje pravo dijete ili realno prikazano nepostojeće dijete ili osobu koja izgleda kao dijete, u pravom ili simuliranom spolno eksplicitnom ponašanju ili koji prikazuje spolne organe djece u spolne svrhe. Materijali koji imaju umjetnički, medicinski ili znanstveni značaj ne smatraju se pornografijom u smislu ovoga članka.

C/ Internetske kartične prijevare

Građani obično ne prijavljuju internetske prijevare s platnom karticom. Građani/klijenti obično nisu ni svjesni da je došlo do prijevare s platnom karticom. Najčešće banka / izdavatelj kartice otkrije prijevaru tijekom praćenja transakcija. Banke prijavljuju internetske prijevare s platnim karticama policiji.

5.2 Postupovna pitanja

5.2.1. Istražne tehnike

U skladu s člankom 332. stavkom 1. Zakona o kaznenom postupku dopušteno je provoditi posebne dokazne radnje kad su kaznena dijela počinjena protiv računalnih sustava, programa i podataka, te je dopušteno presretanje, prikupljanje i snimanje računalnih podataka.

Nadalje, člankom 257. Zakona o kaznenom postupku utvrđuju se pravila za pretragu i oduzimanje informacijskih sustava / računalnih podataka. Predviđa se da pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage. Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim utvrđenim uređajima, te davatelj komunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprečava uništenje ili mijenjanje podataka. Tijelo koje poduzima pretragu može provedbu tih mjera naložiti stručnom pomoćniku.

Članak 261. Zakona o kaznenom postupku (na temelju članka 263. Zakona o kaznenom postupku) primjenjuje se na podatke pohranjene u računalima i s njima povezanim uređajima, te uređajima koji služe prikupljanju i prijenosu podataka, nositelje podataka i na pretplatničke informacije kojima raspolaže davatelj usluga. Navedenim člankom predviđa se da će se predmeti koji se imaju oduzeti prema Zakonu o kaznenom postupku, ili koji mogu poslužiti pri utvrđivanju činjenica u postupku, privremeno oduzeti i osigurati će se njihovo čuvanje, a tko drži takve predmete dužan ih je predati na zahtjev državnog odvjetnika, istražitelja ili policije. Državni odvjetnik, istražitelj ili policija držatelja predmeta upozorit će na posljedice koje proizlaze iz odbijanja postupanja po zahtjevu. Cjelovita snimka, zapis i dokumentacija čuvaju se zapečaćeni u državnom odvjetništvu (članak 338., stavak 2. Zakona o kaznenom postupku).

U skladu s člankom 263. Zakona o kaznenom postupku takvi podaci na pisani zahtjev moraju se predati državnom odvjetniku u cjelovitom, izvornom, čitljivom i razumljivom obliku. Državni odvjetnik u zahtjevu određuje rok u kojemu se imaju predati podaci. Relevantne podatke snimit će u realnom vremenu tijelo koje provodi radnju. Pri pribavljanju, snimanju, zaštiti i čuvanju podataka posebno će se voditi računa o propisima koji se odnose na čuvanje tajnosti određenih podataka (članci od 186. do 188. Zakona o kaznenom postupku). Podaci koji se ne odnose na kazneno djelo a potrebni su osobi prema kojoj se provodi mjera mogu se snimiti na odgovarajuće sredstvo i vratiti toj osobi i prije okončanja postupka.

Na prijedlog državnog odvjetnika sudac istrage može rješenjem odrediti zaštitu i čuvanje svih računalnih podataka pohranjenih u računalima, dok je potrebno, a najdulje šest mjeseci. Nakon toga računalni podaci će se vratiti osim ako su, među ostalim, uključeni u počinjenje kaznenih djela protiv računalnih sustava, programa i podataka u skladu s Kaznenim zakonom.

U slučaju sumnji o počinjenju kaznenog djela protiv računalnih sustava, programa i podataka, osim u slučaju pretraga (članak 257. Zakona o kaznenom postupku), mogu se provesti posebne dokazne radnje (članak 332. Zakona o kaznenom postupku).

U slučaju pretrage zakonom se predviđa da su na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage. Također, po nalogu tijela koje poduzima pretragu, osoba koja se koristiti računalom ili ima pristup računalu i drugim uređajima iz stavka 1. ovog članka, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprečava uništenje ili mijenjanje podataka.

Posebne dokazne radnje u skladu s člankom 332. Zakona o kaznenom postupku moraju se provesti ako se izvidi kaznenih djela ne bi mogli provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće. Na pisani obrazloženi zahtjev državnog odvjetnika, sudac istrage može pisanim obrazloženim nalogom odrediti poduzimanje mjera. One će biti usmjerene protiv osobe za koju postoje osnove sumnje da je sama počinila ili zajedno s drugim osobama sudjelovala u počinjenju kaznenog djela protiv računalnih sustava, programa i podataka. Te mjere obuhvaćaju sljedeće posebne dokazne radnje kojima se privremeno ograničavaju određena ustavna prava građana, među ostalim: nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu, kao i presretanje, prikupljanje i snimanje računalnih podataka.

Istražne tehnike koje se upotrebljavaju za istrage u području kiberkriminaliteta uvijek ovise o vrsti istrage, načinu počinjenja, kao i o tome što se može pretpostaviti o počinitelju. Također, provođenje istrage povezane s kiberkriminalitetom zahtijeva velik raspon različitih stručnih znanja. Stoga su, zajedno s policijskim službenicima iz Odjela za visokotehnološki kriminalitet koji su posebno osposobljeni za slučajeve kiberkriminaliteta, često uključeni i stručnjaci iz Službe za posebne istražne tehnike. Istražne tehnike u svim vrstama istrage regulirane su i provode se u skladu sa Zakonom o kaznenom postupku.

Dobar nedavni primjer istražnih tehnika pružila je istraga računalne prijevare povezane sa zlonamjernim softverom provedena u cijeloj zemlji, koja je zahtijevala računalnu forenzičku istragu i analizu zlonamjernog softvera, kao i dodatnu međunarodnu suradnju na temelju Konvencije iz Budimpešte i uporabu mreže za kiberkriminalitet koja je dostupna 24/7 u svrhu očuvanja podataka i međusobnu pravnu pomoć u suradnji s Ministarstvom pravosuđa kako bi se prikupili osigurani dokazi.

5.2.2. Forenzika i šifriranje

U skladu s člankom 332. stavkom 1. Zakona o kaznenom postupku, ako se izvidi kaznenih djela ne bi mogli provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće, na pisani obrazloženi zahtjev državnog odvjetnika, sudac istrage može odrediti posebne dokazne radnje kojima se privremeno ograničavaju određena ustavna prava, npr. nadzor i snimanje telefonskih razgovora i drugih komunikacija na daljinu.

U Republici Hrvatskoj ne provode se elektronička forenzička ispitivanja ili forenzička ispitivanja na daljinu.

ZSIS se bavi pitanjem zlonamjernog softvera Cryptolocker s glavnim ciljem pružanja pomoći pogođenim stranama u vraćanju šifriranih podataka. U tom kontekstu ZSIS je imao problema u dešifriranju i vraćanju kompromitiranih korisničkih podataka. ZSIS upravlja kriptomaterijalom koji se upotrebljava za razmjenu klasificiranih informacija između Republike Hrvatske i stranih zemalja te samo provodi mjere i norme za zaštitu informacijskih sustava. ZSIS nema pravnu nadležnost za presretanje, dešifriranje ili analizu podataka o prometu ili korisničkih podataka koji potječu od stranaka uključenih u kaznene istrage u području kiberkriminaliteta ili su na bilo koji način povezani s njima.

Hrvatsko Ministarstvo unutarnjih poslova svjesno je problema koji proizlaze iz šifriranja podataka, ali zasad u Republici Hrvatskoj ne postoji ustanova koja se može baviti tim problemom.

5.2.3 E-dokazi

U članku 87. stavcima 18., 19. i 20 Kaznenog zakona navedene su definicije računalnog sustava, računalnih podataka i računalnog programa:

• računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja,

• računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu,

• računalni program je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju.

Elektronički (digitalni) dokazi jesu podaci koji su pribavljeni kao dokazi u elektroničkom (digitalnom) obliku, a prikupljaju se primjenom sljedećih odredaba Zakona o kaznenom postupku – članka 257. (Pretraga pokretne stvari i bankovnog sefa), članka 262. (Privremeno oduzimanje predmeta) i članka 263. (Privremeno oduzimanje predmeta).

Prema članku 257., pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage. Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim uređajima, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprečava uništenje ili mijenjanje podataka.

Predmeti koji su oduzeti prema Kaznenom zakonu oduzimaju se privremeno i osigurava se njihovo čuvanje. To se odnosi i na podatke pohranjene u računalima i s njima povezanim uređajima, te uređajima koji služe prikupljanju i prijenosu podataka, nositelje podataka i na pretplatničke informacije kojima raspolaže davatelj usluga. Takvi podaci na zahtjev državnog odvjetnika moraju se predati u cjelovitom, izvornom, čitljivom i razumljivom obliku. Na prijedlog državnog odvjetnika sudac istrage može rješenjem odrediti zaštitu i čuvanje računala najdulje šest mjeseci. Nakon toga računalni podaci će se vratiti osim ako su uključeni u počinjenje kaznenih djela protiv računalnih sustava, programa i podataka u skladu s Kaznenim zakonom.

Kako ti podaci predstavljaju dokaze u postupku, državni odvjetnik podići će optužnicu nakon što je završena istraga. Prema članku 342. Zakona o kaznenom postupku optužnica sadrži, među ostalim, dokaze na kojima se optužnica temelji, nakon čega će se upotrebljavati na sudu.

U Republici Hrvatskoj ne postoje posebna pravila za dopuštenost e-dokaza, već se primjenjuju općenita pravila o nedopuštenosti dokaza.

U članku 10. Zakona o kaznenom postupku navodi se da se sudske odluke ne mogu temeljiti na dokazima pribavljenim na nezakonit način (nezakoniti dokazi).

Nezakoniti su dokazi koji su pribavljeni kršenjem Ustavom, zakonom ili međunarodnim pravom propisane zabrane mučenja, nečovječnog ili ponižavajućeg postupanja; koji su pribavljeni povredom Ustavom, zakonom ili međunarodnim pravom zajamčenih prava obrane, prava na ugled i čast, te prava na nepovredivost osobnog i obiteljskog života te koji su pribavljeni povredom odredaba kaznenog postupka i koji su izričito predviđeni Zakonom o kaznenom postupku, za koje se saznalo iz nezakonitih radnji. Sudska odluka ne može se temeljiti na dokazima pribavljenim na nezakonit način.

Člankom 419. Zakona o kaznenom postupku predviđa se da sve strane imaju pravo predlagati svjedoke i vještake te izvoditi dokaze. Međutim, vijeće može odlučiti da se izvedu dokazi koji nisu predloženi ili od kojih je predlagatelj odustao.

Zakonom o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije (Narodne novine 91/10, 81/13, 124/13 i 26/15) uređuje se pravosudna suradnja u kaznenim stvarima između domaćih nadležnih pravosudnih tijela i nadležnih pravosudnih tijela drugih država članica Europske unije i odnosi se među ostalim na europski nalog za pribavljanje dokaza. U skladu s tim Zakonom, tijelo nadležno prema domaćem pravu izdaje nalog za osiguranje imovine ili dokaza koji se nalaze u drugoj državi članici u svrhu osiguranja dokaza ili omogućavanja naknadnog oduzimanja imovine za potrebe kaznenih postupaka koji se vode u Republici Hrvatskoj.

Zakonom o međunarodnoj pravnoj pomoći u kaznenim stvarima (Narodne novine 178/04) uređuje se međunarodna pravna pomoć u kaznenim postupcima koji su u tijeku u Republici Hrvatskoj ili u stranoj državi, kao što je pribavljanje i prosljeđivanje predmeta koji će biti predočeni kao dokaz. Zamolbe za međunarodnu pravnu pomoć upućuju se stranim nadležnim tijelima putem Ministarstva pravosuđa. Domaća pravosudna tijela mogu, uz uvjet uzajamnosti ili kada je to predviđeno međunarodnim ugovorom, postupovne akte i sudske odluke osobama koje se nalaze u inozemstvu uputiti izravno poštom.

5.3. Zaštita ljudskih prava / temeljnih sloboda

Ustavom Republike Hrvatske jamči se sloboda mišljenja i izražavanja misli, što posebno obuhvaća slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa i slobodno osnivanje svih ustanova javnog priopćavanja. Zabranjuje se cenzura. Novinari imaju pravo na slobodu izvještavanja i pristupa informaciji. Prava zajamčena Ustavom uređuju se Zakonom o medijima, Zakonom o elektroničkim medijima i Zakonom o Hrvatskoj radioteleviziji.

Pravo na pristup informacijama zajamčeno je Ustavom. Zakonom o pravu na pristup informacijama uređuje se pravo na pristup informacijama i ponovnu uporabu informacija koje posjeduju tijela javne vlasti, propisuju se načela, ograničenja, postupak ostvarivanja pristupa i ponovne uporabe informacija te zaštite tog prava.

Jedno od temeljnih ljudskih prava, pravo na zaštitu osobnih podataka, u Republici Hrvatskoj uređuje se Zakonom o zaštiti osobnih podataka (Narodne novine 103/03, 118/06, 41/08 i 130/11; 106/12 – pročišćeni tekst). U skladu s člankom 1. stavkom 3. tog Zakona, zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama. U tom pogledu Zakon o zaštiti osobnih podataka primjenjiv je u slučaju kiberkriminaliteta, ovisno o posebnim okolnostima svakog slučaja, posebno provedbom aktivnosti nadzora u pogledu zaštite osobnih podataka, bez obzira radi li se o zahtjevu ispitanika za zaštitom prava, prijedlogu treće strane ili službenoj dužnosti.

U Nacionalnom programu zaštite i promicanja ljudskih prava za razdoblje od 2013. do 2016. godine, koji je Vlada Republike Hrvatske donijela u travnju 2013., kao prioritetna područja utvrđena su područja slobode medija, prava na pristup informacijama i prava na zaštitu osobnih podataka. Za svako od tih područja predstavljen je niz mjera čiji je cilj jačanje zaštite i promicanja tih prava.

U skladu s člankom 332. Zakona o kaznenom postupku posebne dokazne radnje kojima se privremeno ograničavaju određena ustavna prava mogu se odrediti i za kaznena djela protiv računalnih sustava, programa ili podataka, kao i za kaznena djela protiv intelektualnog vlasništva ako su počinjena uporabom računalnih sustava ili mreža.

Ako se izvidi kaznenih djela ne bi mogli provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće, na pisani obrazloženi zahtjev državnog odvjetnika, sudac istrage može protiv osobe za koju postoje osnove sumnje da je sam počinila ili zajedno s drugim osobama sudjelovala u spomenutim kaznenim djelima, pisanim, obrazloženim nalogom odrediti posebne dokazne radnje:

1) nadzor i snimanje telefonskih razgovora i drugih načina komunikacije na daljinu;

2) presretanje, prikupljanje i snimanje računalnih podataka;

3) ulazak u prostorije radi provođenja nadzora i snimanje prostorija;

4) tajno praćenje i snimanje osoba i predmeta;

5) uporabu prikrivenih istražitelja i pouzdanika;

6) simuliranu prodaju i otkup predmeta, simulirano davanje potkupnine i simulirano primanje potkupnine,;

7) pružanje simuliranih poslovnih usluga ili sklapanje simuliranih pravnih poslova;

8) nadzirani prijevoz i isporuka predmeta kaznenog djela.

Iznimno, ako postoji opasnost od odgode i ako državni odvjetnik ima razloga vjerovati da na vrijeme neće moći pribaviti nalog suca istrage, nalog može na vrijeme od dvadeset četiri sata izdati državni odvjetnik. Nalog s oznakom vremena izdavanja i dopis u kojem će obrazložiti razloge za njegovo izdavanje državni odvjetnik mora u roku od osam sati od izdavanja dostaviti sucu istrage. Ujedno će ako smatra da treba nastaviti s provođenjem posebne dokazne radnje podnijeti sucu istrage pisani obrazloženi zahtjev za njezino daljnje provođenje. Sudac istrage odmah po primitku naloga i dopisa ispituje jesu li postojali uvjeti za izdavanje naloga te je li postojala opasnost od odgode.

Sudac istrage rješenjem odmah odlučuje o zakonitosti naloga državnog odvjetnika. Ako sudac istrage odobri nalog državnog odvjetnika, a državni odvjetnik je podnio zahtjev za daljnje provođenje dokazne radnje, određuju se posebne radnje. Ako se sudac istrage ne složi s nalogom državnog odvjetnika, on traži da o tome odluku donese vijeće. Vijeće o zahtjevu suca istrage odlučuje u roku od dvanaest sati od primitka zahtjeva. Ako je vijeće potvrdilo nalog državnog odvjetnika, a državni odvjetnik je zahtijevao daljnje provođenje dokazne radnje, vijeće izdaje nalog za dokaznu radnju. Ako vijeće ne odobri nalog, u rješenju nalaže da se odmah obustave radnje, a podaci prikupljeni na temelju naloga državnog odvjetnika predaju se sucu istrage koji ih uništava. O uništenju podataka sudac istrage sastavlja zapisnik.

Posebne dokazne radnje nadzora i snimanja telefonskih razgovora i drugih komunikacija na daljinu mogu se odrediti i prema osobama za koje postoje osnove sumnje da počinitelju ili od počinitelja kaznenih djela protiv računalnih sustava, programa ili podataka prenose priopćenja i poruke u svezi s djelom, odnosno da se počinitelj služi njihovim priključcima na telefon ili drugim telekomunikacijskim uređajem, koje kriju počinitelja kaznenog djela ili mu prikrivanjem sredstava kojima je kazneno djelo počinjeno, tragova kaznenog djela ili predmeta nastalih ili pribavljenih kaznenim djelom ili na drugi način pomažu da ne bude otkriven.

Operativno-tehnički centar za nadzor telekomunikacija koji obavlja tehničku koordinaciju s davateljem telekomunikacijskih usluga u Republici Hrvatskoj dužan je policiji osigurati potrebnu tehničku pomoć. Posebne dokazne radnje izvršava policija.

Prema članku 339.a Zakona o kaznenom postupku, ako postoji sumnja da je registrirani vlasnik ili korisnik telekomunikacijskog sredstva počinio kazneno djelo protiv računalnih sustava, programa ili podataka, policija može, na temelju naloga suca istrage, a radi prikupljanja dokaza, putem Operativno-tehničkog centra za nadzor telekomunikacija od operatera javnih komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama, utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju, te identifikacijske oznake uređaja.

5.4. Nadležnost

5.4.1. Načela koja se primjenjuju na istrage kiberkriminaliteta

Prema članku 11. Kaznenog zakona, kazneno zakonodavstvo Republike Hrvatske primjenjuje se i na svakoga tko počini kazneno djelo na domaćem brodu ili zrakoplovu, bez obzira na to gdje se brod ili zrakoplov nalazi u vrijeme počinjenja kaznenog djela.

Osim toga, kazneno zakonodavstvo Republike Hrvatske primjenjuje se prema hrvatskom državljaninu i osobi koja ima prebivalište u Republici Hrvatskoj, koja izvan područja Republike Hrvatske počini bilo koje kazneno djelo, ako je to kazneno djelo kažnjivo i prema zakonu države u kojoj je počinjeno. Ta odredba primjenjivat će se i kad počinitelj stekne hrvatsko državljanstvo nakon počinjenja kaznenog djela.

Nadalje, kazneno zakonodavstvo Republike Hrvatske primjenjuje se prema strancu koji izvan područja Republike Hrvatske počini kazneno djelo za koje se po hrvatskom zakonodavstvu može izreći kazna zatvora od pet godina ili teža kazna, ako je to kazneno djelo kažnjivo i prema zakonu države u kojoj je počinjeno i ako je izručenje počinitelja zakonom ili međunarodnim ugovorom dopušteno. Takva se situacija dosad nije dogodila.

5.4.2. Pravila u slučaju sukoba nadležnosti i upućivanje Eurojustu

Kazneno zakonodavstvo Republike Hrvatske primjenjuje se prema hrvatskom državljaninu i osobi koja ima prebivalište u Republici Hrvatskoj, koja izvan područja Republike Hrvatske počini kazneno djelo, ako je to kazneno djelo kažnjivo i prema zakonu države u kojoj je počinjeno.

U slučajevima kaznenih djela mamljenja djece za zadovoljenje spolnih potreba, iskorištavanja djece za pornografiju i teških kaznenih djela spolnog zlostavljanja i iskorištavanja djeteta, kazneno zakonodavstvo Republike Hrvatske primijenit će se i kad kazneno djelo nije kažnjivo prema zakonu države u kojoj je počinjeno.

Kazneno zakonodavstvo Republike Hrvatske primjenjuje se prema strancu koji izvan područja Republike Hrvatske prema državljaninu Republike Hrvatske, osobi koja ima prebivalište u Republici Hrvatskoj ili pravnoj osobi registriranoj u Republici Hrvatskoj počini bilo koje kazneno djelo, ako je to kazneno djelo kažnjivo i prema zakonu države u kojoj je počinjeno. Sud ne može izreći težu kaznu od one koja je propisana zakonom zemlje u kojoj je kazneno djelo počinjeno.

U takvim slučajevima kazneni postupak pokreće se samo ako se počinitelj nalazi na području Republike Hrvatske.

Republika Hrvatska još uvijek u praksi nije primijenila komunikaciju predviđenu Okvirnom odlukom Vijeća 2009/948/PUP.

5.4.3. Nadležnost za djela kiberkriminaliteta počinjena u „oblaku”

Činjenica je da su prijestupnici koji seksualno zlostavljaju djecu putem interneta sve više „skriveni” jer sve više upotrebljavaju internetsko pohranjivanje u „oblaku” da bi pohranili nezakonit sadržaj. Zbog toga je otežano otkrivanje prijestupnika i pružanje dokaza o kaznenoj odgovornosti u kaznenim postupcima. U slučajevima kada je osumnjičenik spreman surađivati ili postoje drugi izvori informacija u pogledu korisničkih imena i lozinaka, pribavlja se sudski nalog za pretragu računa osumnjičenika u vezi s takvim uslugama, s ciljem prikupljanja i registracije sadržaja. Nadalje, u nekim slučajevima Hrvatska šalje zahtjev za čuvanje vlasniku usluge u kojem traži da zadrži nezakonit sadržaj na računu osumnjičenika dok Hrvatska ne dostavi zahtjev za međunarodnu pravnu pomoć.

5.4.4. Percepcija Hrvatske u pogledu pravnog okvira za borbu protiv kiberkriminaliteta

Hrvatske vlasti izrazile su stajalište da je nacionalno pravo potpuno usklađeno s europskim zakonodavstvom u tom području i izjavile su da je Konvencija Vijeća Europe o kibernetičkom kriminalu prenesena, te stoga Republika Hrvatska smatra da je postojeći pravni okvir primjeren i za istrage i za kazneni progon slučajeva kiberkriminaliteta počinjenih izvan državnog područja Republike Hrvatske.

Međutim, također su izrazile mišljenje da je zakonodavstvo zastarjelo i da se u njemu ne očituje tehnološki razvoj te da je potrebno izmijeniti ga, ne samo na nacionalnoj razini već i međunarodno, s ciljem rješavanja niza sumnji u tom području. Najveći je problem opći nedostatak zakona o univerzalnom minimalnom standardu kojim bi se pružatelje usluga obvezalo da tijelima kaznenog progona pruže informacije koje bi pomogle u utvrđivanju identiteta prijestupnika.

5.5. Zaključci

- Ocjenjivački tim nije imao priliku dubinski analizirati relevantno hrvatsko zakonodavstvo s obzirom na to da ne postoji engleski prijevod pročišćenog zakonodavstva;

- dok su hrvatske vlasti u više navrata navodile da je nacionalno zakonodavstvo usklađeno sa svim obvezama EU-a i međunarodnim obvezama, ukazano je na neke slabosti u učinkovitosti zakonodavstva za borbu protiv kiberkriminaliteta; kao primjer je navedeno nepostojanje posebnog pravnog okvira u vezi sa ZIT-ovima o kiberkriminalitetu i kiberpatrolama.

6 OPERATIVNI ASPEKTI

6.1 Kibernapadi

6.1.1. Priroda kibernapada

U 2015. Nacionalnom CERT-u prijavljene su sljedeće vrste incidenata.

Vrsta incidenta u razdoblju 1.1.2015. – 17.7.2015.	Broj incidenata
Kompromitirani serveri koji poslužuju zlonamjerni softver	148
Kompromitirani serveri koji poslužuju phishing stranice	135
Phishing napadi	45
Neovlaštena promjena internetskih stranica	27

Kompromitirani serveri većinom su posluživali zlonamjerni server ili phishing sadržaj stranim korisnicima interneta i upotrebljavani su kao infrastruktura. Hrvatska je 2014. i 2015. doživjela dvije masovne zaraze povezane s trima vrstama zlonamjernog softvera Zeus, a u nedavnoj kampanji širenja zlonamjernog softvera kiberkriminalci upotrijebili su kompromitirane portale ili servere trećih strana preko kojih su posluživali oglase s ciljem širenja zlonamjernog softvera.

Osim toga, nedavno su uklonjena dva poslužitelja za upravljanje i kontrolu putem kojih se širi botnet (botnet command and control servers), njihov je sadržaj analiziran i obaviješteni su relevantni CERT-ovi ili tijela kaznenog progona. Iz toga je naučeno da bi podatke trebalo dijeliti samo onima koji ih nužno trebaju kako bi se učinkovito bavilo takvim slučajevima.

6.1.2. Mehanizam za odgovor na kibernapade

Hrvatska posjeduje multidisciplinarni mehanizam za odgovor na ozbiljan kibernapad predviđen u Nacionalnoj strategiji kibernetičke sigurnosti. Ozbiljan kibernapad rješavao bi se koordinacijom između Nacionalnog CERT-a, tijela kaznenog progona i pružatelja internetskih usluga.

Središnja tijela državne uprave, u suradnji s nadležnim regulatornim agencijama, odgovorna su u okviru svojih ovlasti za utvrđivanje (uspostavu) određenih sustava ili njihovih dijelova kao ključnih nacionalnih infrastruktura, te za osiguravanje upravljanja ključnim infrastrukturama i njihovom zaštitom.

Voditelj središnjeg tijela državne uprave donosi odluku o utvrđivanju ključne nacionalne infrastrukture na temelju odluke Vlade Republike Hrvatske o potvrđivanju utvrđene ključne infrastrukture, te prosljeđuje tu odluku s ciljem njezine provedbe vlasniku/operateru tih infrastruktura i središnjem tijelu državne uprave odgovornom za područje zaštite i spašavanja.

Vlasnici/operateri utvrđenih (uspostavljenih) ključnih infrastruktura izravno su odgovorni za rad i zaštitu ključnih infrastruktura u svim okolnostima.
Nacionalnom strategijom kibernetičke sigurnosti i akcijskim planom za provedbu Strategije predviđene su aktivnosti čiji je cilj poboljšanje organizacije tog područja putem preciznijeg utvrđivanja kriterija za prepoznavanje ključne komunikacijske i informacijske infrastrukture, uspostave minimalnih standarda sigurnosti za informacijske sustave koji su od presudne važnosti za dobro funkcioniranje ključnih infrastruktura te osiguranja provedbe tih standarda (provedba od strane vlasnika/operatera, nadzor).”

Hrvatske vlasti, i u svojim odgovorima na upitnik i tijekom posjeta na licu mjesta, naglasile su da „odgovor na kibernapade gotovo nikad nije pitanje samo jedne nadležnosti, tj. on obično znači da se dvije ili više različitih institucija uključuju u istragu / prikupljanje dokaza / analizu / pravni postupak". Ministarstvo unutarnjih poslova također mora surađivati s uredom tužitelja, te često surađuje s nacionalnim ili vladinim CERT-om, pružateljima internetskih usluga, privatnim sektorom, akademskom zajednicom itd., kao i s drugim tijelima kaznenog progona na međunarodnoj razini. Hrvatskoj je stoga potrebna brza i učinkovita komunikacija kako bi se skratili postupci u kojima se bavi slučajevima kiberprijetnji.

Postojanjem mreže različitih vrsta stručnih znanja policiji bi se omogućilo da dobije odgovarajuću potporu u slučajevima u kojima se zahtijeva viša razina tehničkih znanja i određenih vještina (na primjer suradnja s vladinim CERT-om u određenim slučajevima povezanima sa zlonamjernim softverom). Bez obzira na to, uzimajući u obzir brz tehnološki razvoj i potrebu za svakodnevnim prilagođavanjem novim trendovima i naprednijim načinima rada, osposobljavanje na svim razinama (policija, tužitelji i suci), i pravnim i tehničkim, od presudne je važnosti kako bi se učinkovito bavilo slučajevima povezanima s kiberkriminalitetom.

Osim općih programa osposobljavanja potrebnih za sva relevantna tijela uključena u istragu, i dalje nedostaje stručnjaka koji imaju dovoljno znanja i tehničkih vještina za provedbu neovisne istrage počevši od prikupljanja dokaza i njihove obrade/analize za upotrebu u naknadnim pravnim postupcima. Zbog toga često dolazi do grešaka i nesporazuma u odnosu na nadležnog tužitelja.

Za međunarodnu suradnju i traženje podataka iz druge zemlje često su potrebna dulja vremenska razdoblja, što u slučajevima povezanima s kiberkriminalitetom može biti od presudne važnosti (zbog nepostojanosti podataka).Zbog različitih pravnih obveza u pogledu zadržavanja podataka, pribavljanje relevantnih informacija iz različitih zemalja ponekad je nemoguće ili veoma sporo.

Analiziranje velikih (i rastućih) količina podataka zahtijeva sve više vremena i učinkovitiju tehnologiju, kao i veću stručnost.

6.2. Mjere protiv dječje pornografije i seksualnog zlostavljanja na internetu

6.2.1. Programske baze podataka za identifikaciju žrtava i mjere za sprečavanje ponovne viktimizacije

Ne postoje određene nacionalne ili lokalne baze podataka. Hrvatska tijela kaznenog progona koriste se samo Interpolovom Međunarodnom bazom podataka o seksualnom iskorištavanju djece (ISCE) za identifikaciju žrtava.

U svim slučajevima objave, razmjene, posjedovanja ili pohranjivanja materijala koji prikazuje zlostavljanje djece na serverima ili računalima u Hrvatskoj sadržaj će se oduzeti, blokirati, izbrisati (ukloniti), a svaka osoba koja pristupi takvim materijalima kazneno će se progoniti jer su posjedovanje, objava, razmjena i pohranjivanje materijala koji prikazuju seksualno iskorištavanje djece te pristup takvim materijalima kazneno djelo. Sav navedeni materijal bit će oduzet i uništen u skladu s kaznenim pravom.

6.2.2. Mjere za borbu protiv seksualnog iskorištavanja / zlostavljanja na internetu, slanja poruka i fotografija seksualnog sadržaja (sexting), virtualnog nasilja

Člankom 161. Kaznenog zakona definira sa kazneno djelo mamljenja djece za zadovoljenje spolnih potreba. Punoljetna osoba koja osobi mlađoj od petnaest godina, u namjeri da ona ili druga osoba nad njom počini kazneno djelo spolne zlouporabe djeteta starijeg od petnaest godina, putem informacijsko komunikacijskih tehnologija ili na drugi način predloži susret s njom ili drugom osobom i koja poduzme mjere da do tog susreta dođe, kažnjava se kaznom zatvora do tri godine. Tko prikuplja, daje ili prenosi podatke o osobi mlađoj od petnaest godina radi počinjenja tog kaznenog djela kažnjava se kaznom zatvora do jedne godine. Za pokušaj kaznenog djela mamljenja djece za zadovoljenje spolnih potreba počinitelj se kažnjava.

Nadalje, u Kaznenom zakonu predviđa se mogućnost izricanja sigurnosnih mjera protiv počinitelja kaznenih djela spolnog zlostavljanja i iskorištavanja djece. Sigurnosnu mjeru zabrane pristupa internetu sud izriče počinitelju koji je kazneno djelo počinio putem interneta ako postoji opasnost da će zlouporabom interneta ponovno počiniti kazneno djelo (članak 75. Kaznenog zakona). Sigurnosna mjera zabrane pristupa internetu izriče se u trajanju od šest mjeseci do dvije godine. Počinitelju koji je osuđen na kaznu zatvora, a nije mu izrečena uvjetna osuda niti je kazna zatvora zamijenjena radom za opće dobro, mjera će se izreći u trajanju koje je od šest mjeseci do dvije godine dulje od izrečene kazne zatvora. Sud će o pravomoćno izrečenoj mjeri obavijestiti regulatorno tijelo nadležno za elektroničke komunikacije koje će osigurati njezino provođenje.

U skladu s člankom 76. Kaznenog zakona, u slučajevima kada je kazna u potpunosti izdržana i ako je počinitelju izrečena kazna zatvora za kazneno djela spolnog zlostavljanja i iskorištavanja djece određuje se zaštitni nadzor. Ako je kazna u potpunosti izdržana jer osuđeniku nije odobren uvjetni otpust, nad njime će se odmah po izlasku iz zatvora započeti provoditi zaštitni nadzor. Nadzor se temelji na pojedinačnom programu postupanja koji izrađuje, pomaže provesti i čije provođenje nadgleda nadležno tijelo za probaciju. Probacija traje tri godine. Sud može, na prijedlog nadležnog tijela za probaciju, produljiti razdoblje probacije prije njegova isteka za dodatnu godinu ako postoji rizik ponovnog počinjenja bilo kojeg kaznenog djela spolnog zlostavljanja i iskorištavanja djece.

Kako bi se uhvatilo ukoštac s posljedicama navedenih kriminalnih aktivnosti ili ih se ublažilo, Hrvatska je ubrzala osposobljavanje koje pruža policijskim službenicima zaduženima za mlade kako bi lakše mogli prepoznati različite oblike ove vrste kriminala te pružiti učinkovitiji odgovor. Osposobljavanje se provodi u suradnji s Policijskom akademijom, te je dio ranije spomenute suradnje s različitim međunarodnim institucijama i institucijama EU-a (CEPOL, TAIEX).

Policijski službenici zaduženi za mlade na lokalnoj razini, u suradnji s policijskim službenicima zaduženima za prevenciju i nekim lokalnim obrazovnim ustanovama organizirali su govore za učenike i studente kako bi im dali informacije o različitim zločinima ili neprikladnom ponašanju na internetu, o ponašanju kojim štite sami sebe i o različitim rizicima, kao i neke informacije i savjete o tome gdje i kako mogu tražiti pomoć.

6.2.3. Preventivne mjere protiv seksualnog turizma, pornografskih predstava u kojima sudjeluju djeca i drugih kaznenih djela

U skladu s člankom 14. Kaznenog zakona, kazneno zakonodavstvo Republike Hrvatske primjenjuje se prema hrvatskom državljaninu i osobi koja ima prebivalište u Republici Hrvatskoj koja počini kazneno djelo ako je to kazneno djelo kažnjivo i prema zakonu države u kojoj je počinjeno. Ta odredba primjenjuje se i kad počinitelj stekne hrvatsko državljanstvo nakon počinjenja kaznenog djela.

Imajući na umu navedeno, kazneno zakonodavstvo Republike Hrvatske primjenjivat će se u slučajevima u kojima je počinitelj počinio kazneno djelo spolne zlouporabe djeteta mlađeg od petnaest godina u skladu s člankom 158. Kaznenog zakona, kazneno djelo spolne zlouporabe djeteta starijeg od petnaest godina u skladu s člankom 159. Kaznenog zakona, kazneno djelo mamljenja djece za zadovoljenje spolnih potreba u skladu s člankom 161. Kaznenog zakona, kazneno djelo podvođenja djeteta u skladu s člankom 162. Kaznenog zakona, kazneno djelo iskorištavanja djece za pornografiju u skladu s člankom 163. Kaznenog zakona, kazneno djelo iskorištavanja djece za pornografske predstave u skladu s člankom 164. Kaznenog zakona ili teška kaznena djela spolnog zlostavljanja i iskorištavanja djeteta prema članku 166. Kaznenog zakona, kad kazneno djelo nije kažnjivo prema zakonu države u kojoj je počinjeno.

Osim toga, kada hrvatski državljani sudjeluju u mirovnim operacijama ili drugim međunarodnim aktivnostima izvan područja Republike Hrvatske i u takvim operacijama ili aktivnostima počine kazneno djelo, primjena zakonodavstva Republike Hrvatske ravna se prema odredbama Kaznenog zakona, ako međunarodnim ugovorom kojeg je Republika Hrvatska stranka nije predviđeno drugačije.

Kaznenim zakonodavstvom zabranjeno je oglašavanje pornografskih predstava u kojima sudjeluje dijete i kažnjivo je prema članku 162. Kaznenog zakona. Hrvatska nije razvila specifične mjere za suzbijanje pornografskih predstava u kojima sudjeluju djeca na internetu u realnom vremenu.

Internetska stranica „Red Button" (https://redbutton.mup.hr) 29. rujna 2013., koja omogućuje prijavu putem interneta svih oblika zlostavljanja djece. Od pokretanja aplikacije sredinom 2015. Hrvatska je primila više od 2300 prijava, ali većina ih je bila povezana s legalnim pornografskim sadržajem.

Internetska stranica Ministarstva unutarnjih poslova (http://www.mup.hr/main.aspx?id=13047) i internetske stranice Centra za sigurniji internet (http://www.sigurnijiinternet.hr) sadrže savjete za djecu i njihove roditelje o sigurnosti na internetu, na njima se ističu rizici i daju savjeti o tome što učiniti ako dijete postane žrtva.

Na internetskoj stranici Ministarstva unutarnjih poslova (http://www.mup.hr/main.aspx?id=13047) dostupne su informacije o nezakonitom, štetnom ili kažnjivom ponašanju.

6.2.4. Akteri i mjere za borbu protiv internetskih stranica koje sadrže dječju pornografiju ili kojima se ona širi

Istraga tih zločina odgovornost je Odjela za maloljetničku delinkvenciju i kriminalitet na štetu mladeži koji surađuje s policijskim službenicima iz drugih odjela osposobljenima za prikupljanje forenzičkih dokaza.

Odredbama Zakona o elektroničkim komunikacijama (Narodne novine 73/08, 91/11, 133/12, 71/14) uređuje se provedba mjera u pogledu slanja neželjenih elektroničkih poruka, kao i obveze operatora usluga elektroničke pošte. Zakonom se također uređuje provedba mjera za zaštitu podataka i sigurnost elektroničkih komunikacija, kao i ovlasti Hrvatske regulatorne agencije za mrežne djelatnosti.

Pravilnikom koji je donijelo Vijeće Hrvatske regulatorne agencije propisuju se način i uvjeti djelotvornog sprečavanja i suzbijanja zlouporaba i prijevara u pružanju usluga elektroničke pošte. Nadalje, navedenim Zakonom izriče se plaćanje novčane kazne ako pravna osoba u svojstvu operatora usluga elektroničke pošte ne omogući filtriranje dolazne elektroničke pošte, ne objavi adresu elektroničke pošte za prijavu zlouporaba, ne postupa s prigovorima u vezi sa zlouporabom elektroničke pošte ili ne poduzima odgovarajuće mjere u slučaju utvrđivanja zlouporaba pretplatnikova korisničkog računa elektroničke pošte ili ne poduzima mjere radi sprečavanja ili suzbijanja zlouporaba ili prijevara u pružanju usluga elektroničke pošte.

Hrvatska ne primjenjuje filtriranje ili blokiranje pristupa. Ali, kako je već spomenuto, sav sadržaj koji prikazuje seksualno zlostavljanje i iskorištavanje djece mora biti uklonjen snagom zakona. Stoga su svi pružatelji internetskih ili elektroničkih usluga u Republici Hrvatskoj obvezni ukloniti takve sadržaje objavljene ili pohranjene na njihovim serverima i obavijestiti policiju ili Državno odvjetništvo.

Hrvatska akademska i istraživačka mreža, koja je pružatelj usluga za sve škole i visoka učilišta u Hrvatskoj, filtrira sadržaj blokiranjem pristupa više skupina internetskih stranica posvećenih kockanju, seksu, oružju itd.

Ako hrvatske vlasti saznaju da je nezakonit sadržaj smješten na serverima izvan nadležnosti Republike Hrvatske, o tome obavješćuju tijelo kaznenog progona nadležne države putem redovnih policijskih kanala (Europol ili Interpol). Prije nego što to učine, pokušavaju osigurati dokaze koje mogu prikupiti na internetu.

6.3. Internetske kartične prijevare

Hrvatski građani obično ne prijavljuju internetske kartične prijevare. Prema hrvatskim vlastima, građani/klijenti obično nisu ni svjesni da je došlo do prijevare s platnom karticom.
U većini slučajeva banka / izdavatelj kartice otkrije prijevaru tijekom praćenja transakcija. Banke prijavljuju internetske kartične prijevare policiji.

6.4. Drugi fenomeni kiberkriminaliteta

Kako bi se organiziranom kriminalu ograničila mogućnost pristupa podacima o karticama i transakcijama, svi hrvatski izdavatelji/stjecatelji platnih kartica strogo primjenjuju mjere industrije platnih kartica PCIDSS (Standard sigurnosti podataka industrije platnih kartica – Payment Card Industry Data Secure System). Primjenjuju se sljedeće mjere protiv skidanja magnetskog zapisa s kartice (*skimming*): ugradnja opreme za sprečavanje skidanja magnetskog zapisa s kartice (TMB tehnologija), video nadzor na bankomatima, medijska kampanja koju je pokrenula Hrvatska udruga banaka i uvođenje beskontaktnih kartica.

Hrvatska nema poseban pravni okvir za Bitcoins i druge virtualne valute, iako su u zemlji dostupni Bitcoin bankomati a virtualne valute upotrebljavaju se kao metoda plaćanja na internetskim stranicama; zasad nije prijavljen nijedan slučaj koji uključuje virtualne valute.

Hrvatski tužitelji izvijestili su ocjenjivački tim da bi virtualne valute mogle biti obuhvaćene pravnom definicijom imovine te bi njihovo oduzimanje stoga moglo biti moguće.

6.5. Zaključci

- Jednako kao što postoji općenita potreba za strukturiranijom i sistematičnijom koordinacijom / razmjenom informacija među različitim subjektima uključenima u kibersigurnost i borbu protiv kiberkriminaliteta, Hrvatska bi imala koristi od bliskije suradnje na operativnoj razini između Nacionalnog CERT-a i policijskih tijela;

- ocjenjivački tim bio je impresioniran znanjem i sposobnošću hrvatskih tijela kaznenog progona koja se posebno bave seksualnim iskorištavanjem djece;

- posjetom na licu mjesta postalo je očito da, hrvatski forenzički stručnjaci, iako dobro poznaju informacijske tehnologije i uređaje, imaju poteškoća u brzom prilagođavanju svojih vještina novim trendovima u kriminalitetu (koji se mijenjaju jako brzo) zbog velikog radnog opterećenja. Forenzičkim stručnjacima trebalo bi dati dovoljno sredstava, vremena i alata kako bi se redovito osposobljavali i kako bi im se omogućilo da razvijaju svoje vještine.

7 MEĐUNARODNA SURADNJA

7.1 Suradnja s agencijama EU-a

7.1.1 Formalni zahtjevi suradnje s Europolom / centrom EC3, Eurojustom, ENISA-om

Suradnja s Europolom:

Sporazum o operativnoj i strateškoj suradnji između Hrvatske i Europola potpisan je 2006. i bio je na snazi do pristupanja Hrvatske EU-u 1. srpnja 2013. Projekt proširenja Europola (Europol Enlargement Project) pokrenut je 2012. s ciljem usklađivanja prije pristupanja punopravnom članstvu Europola i uspješno je dovršen do 1. srpnja 2013. Nakon tog datuma, Odluka Vijeća od 6. travnja 2009. o osnivanju Europskog policijskog ureda (Europol) (2009/371/PUP) postala je pravni temelj za suradnju između Hrvatske i Europola. Ne postoje posebni nacionalni zakoni o suradnji između Hrvatske i Europola.

Prema članku 40. Pravilnika o postupanju policijskih službenika, policijski službenik može prikupljati podatke, među ostalim, iz podataka zaprimljenih od Interpola, Europola ili drugih međunarodnih organizacija ili policija drugih država.

Prema Zakonu o tajnosti podataka, ZSIS je dužan ne dijeliti informacije koje su klasificirane. Potrebno je potpisati sporazum o sigurnosti između zemalja za dijeljenje klasificiranih informacija. ZSIS-u je dopušteno dijeliti neklasificirane informacije o incidentima povezanima s kibersigurnošću ako te informacije mogu pomoći u rješavanju incidenta. Obično bi ZSIS-u trebalo proslijediti formalni zahtjev elektroničkom poštom ili u pisanom obliku.

7.1.2 Ocjena suradnje s Europolom / centrom EC3, Eurojustom, ENISA-om

Hrvatska sudjeluje u EUCTF-u (Radna skupina EU-a za kiberkriminalitet) i tamo je predstavlja voditelj Odjela za visokotehnološki kriminalitet. Hrvatska trenutačno ne sudjeluje u kiberpatrolama.

U slučajevima kiberkriminaliteta s međunarodnim elementom, Republika Hrvatska općenito primjenjuje Konvenciju Vijeća Europe o kibernetičkom kriminalu iz 2001., kao i mrežu koja je dostupna 24/7. U hitnim postupcima koji uključuju kiberkriminalitet Hrvatskoj u slučajevima transnacionalnog organiziranog kriminala koji je počinjen na državnom području više država članica EU-a pomažu Europska pravosudna mreža u kaznenim stvarima i Eurojust.

Republika Hrvatska sudjelovala je u koordinacijskom sastanku koji je organizirao Eurojust u vezi sa slučajem kiberkriminaliteta. Hrvatske vlasti doprinose Eurojusta smatraju veoma korisnima.

U pogledu suradnje s Europolom / centrom EC3, Odjel za visokotehnološki kriminalitet uključen je u istragu koja je u tijeku, a započela je u ožujku 2014., kojom su obuhvaćeni mnogobrojni napadi zlonamjernim softverom i znatna financijska šteta u Hrvatskoj. Istraga se provodi i na nacionalnoj i na međunarodnoj razini i tiče se računalnih prijevara koje se provode uporabom bankovnog zlonamjernog softvera, kao i slučajeva pranja novca koji uključuju razgranatu mrežu nacionalnih/međunarodnih posrednika za prijenos novca.

Odjel za maloljetničku delinkvenciju i kriminalitet na štetu mladeži i obitelji stalno surađuje s Europolom / centrom EC3 / skupinom FP Twins. Suradnja se u većini slučajeva tiče pripreme i razmjene informacija o određenim operativnim aktivnostima koje se u okviru skupine FP Twins pripremaju neovisno i u suradnji s drugim tijelima kaznenog progona. Također, FP Twins obavješćuje nacionalna tijela o izvješćima američkog Nacionalnog centra za nestalu i iskorištavanu djecu.

Što se tiče kontakata Hrvatske s ENISA-om, oni su više savjetničke nego operativne prirode.

Hrvatska je radila na nekoliko slučajeva na kojima je surađivala s Europolom, ENISA-om i CERT-ovima u drugim državama članicama. Najveći slučaj bila je kampanja ZeuS koja je kulminirala u proljeće 2014. kada je zaražen velik broj uređaja u Hrvatskoj. Hrvatska je Europolu dostavila sve pojedinosti iz svojih istraga i podijelila informacije s CERT-ovima u svim drugim državama članicama.

Hrvatska ima ograničene ljudske i tehničke resurse u području kiberkriminaliteta te u tom pogledu Hrvatska snažno pozdravlja uspostavu centra EC3 koji ima analitički odjel (npr. AWF Cyborg). Hrvatska pogotovo uvažava ulogu centra EC3 u prikupljanju i analizi podataka, analizi zlonamjernog softvera i alat „Malware sandbox" za izravno prenošenje i analizu zlonamjernog softvera.

Odjel maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji ocijenio je doprinos Europola / centra EC3 vrlo pozitivnim i uvažava njihovu pomoć i suradnju.
Hrvatski nacionalni CERT pozdravio bi informacije o botovima nakon što EUROPOL/EC3 uklone botnete kako bi obavijestio krajnje korisnike o zarazama njihovih radnih stanica.

Hrvatska je zadovoljna suradnjom sa svim navedenim organizacijama. Hrvatska je uvjerena da je uvijek moguće poboljšati navedene aspekte, osobito u području dijeljenja informacija.

EC3 (FP Cyborg), EUCTF, EMPACT Cyber Attacks i ECTEG četiri su stupa koja pružaju solidnu potporu suradnji i koordinaciji među tijelima kaznenog progona država članica u području kiberkriminaliteta. Postoji prostor za napredak, pogotovo u području osposobljavanja. Osposobljavanje policijskih službenika ključno je za odgovor na kibernapade i borbu protiv seksualnog zlostavljanja djece na internetu. Prilagođeni programi za osposobljavanje policijskih službenika od presudne su važnosti. Kao odličan primjer osposobljavanja Europola, Hrvatska bi naglasila tečaj Europola o borbi protiv seksualnog iskorištavanja djece na internetu. Hrvatska cijeni rad koje se dosad poduzeli članovi ECTEG-a, pogotovo projekte koji su provedeni u suradnji sa Sveučilištem u Dublinu (University College Dublin (UCD)). Kako bi se pružila slična obuka u području istraga kibernapada, Hrvatska smatra da bi bilo korisnije kada bi se ECTEG u potpunosti uklopio u EC3.

7.1.3 Operativni rezultati ZIT-ova i kiberpatrola

Republika Hrvatska nije sudjelovala u ZIT-ovima povezanim s kiberkriminalitetom. To bi moglo imati veze s činjenicom da Hrvatska još nije pristupila Konvenciji o uzajamnoj pravnoj pomoći u kaznenim stvarima iz 2000.
U Republici Hrvatskoj ne postoji pravni okvir za kiberpatrole.
Međutim, hrvatske vlasti izjavile su da bi u najvećoj mogućoj mjeri podržale takve oblike operativne suradnje.

7.2 Suradnja hrvatskih vlasti i Interpola

Od lipnja 2013. tijela kaznenog progona u Republici Hrvatskoj povezana su s međunarodnom bazom podataka o seksualnom iskorištavanju djece, a policijski službenici Odjela maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji aktivno rade s njom.

Suradnju s Interpolom ocjenjuju uglavnom dobrom. Interpolovi kanali uglavnom se rabe za komunikaciju s trećim stranama, inače se preferira Europol. Svaka država s Interpolom surađuje sukladno vlastitom nacionalnom zakonodavstvu, stoga iskustva mogu biti različita. Što se tiče kiberkriminaliteta, Hrvatska u većini slučajeva traži podatke koji su relevantni za kriminalističke istrage podnošenjem obavijesti ili zahtjeva.

Prikupljanje informaciji ovisi o zemlji od koje Hrvatska te informacije traži kao i njezinu nacionalnom zakonodavstvu. Npr. većina zemalja uzajamnu pravnu pomoć (međunarodnu pravnu pomoć) traži za podatke o vlasništvu nad IP adresama, podatke o prometu, računima koji se rabe za transakcije itd. Zahtjevi za uzajamnu pravnu pomoć šalju se putem Ministarstva pravosuđa; taj postupak obično komplicira istragu i traje.

Iako još nisu rabili pomoć iz tog izvora, smatraju da bi Interpolov globalni centar za inovacije u Singapuru mogao pružati korisnu potporu u borbi protiv kiberkriminaliteta na globalnoj razini.

Suradnjom u području uspostave i stvaranja baze podataka o seksualnom iskorištavanju djece i „Baseline projekta" s Interpolovim odjelom za kriminalitet na štetu mladeži proširene su mogućnosti za identifikaciju žrtava te se pomoglo kriminalističkim istragama kao i razmjeni informacija s drugim tijelima kaznenog progona putem centra EC3.

7.3 Suradnja s trećim zemljama

U kiberkriminalističkim istragama hrvatska policija otvorena je za svaku suradnju koja bi mogla pomoći u prikupljanju potrebnih podataka i informacija. Ako neka istraga uključuje treće države, one obično komuniciraju putem svoje službe za međunarodnu suradnju, a svi podaci dijele se komunikacijskim kanalima Interpola ili Europola. Hrvatska se također koristi alatima koji su uspostavljeni Budimpeštanskom konvencijom kao što su kontaktne točke koje djeluju 24/7. Što se tiče suradnje s trećim zemljama u regiji, Hrvatska je sudjelovala u zajedničkoj obuci o sprečavanju i borbi protiv kiberkriminaliteta.

Na ministarskoj konferenciji 5. prosinca 2012. Republika Hrvatska sudjelovala je u osnivanju Globalnog saveza protiv seksualnog zlostavljanja djece na internetu. Hrvatska je tako odredila svoju politiku o seksualnom iskorištavanju djece u području kiberkriminaliteta.

Budući da je suradnja s trećim zemljama obično različita od suradnje sa zemljama EU-a, pogotovo zbog institucijskog okvira, te obično iziskuje više vremena i uključuje više faza, Europol može pomoći u objedinjavanju postupaka čime bi se znatno doprinijelo učinkovitosti suradnje s trećim zemljama. Analitičke mogućnosti centra EC3 pogotovo su korisne za istrage koje se provode u nekoliko zemalja (Hrvatska ima praktična iskustva s istragom OA MIR u vezi s kiberprijevarama i zlonamjernim softverom u području bankarstva te je uz pomoć Europola organiziran operativni sastanak).

Ocjenjivački tim informiran je o praktičnim slučajevima suradnje s trećim zemljama, kako uspješnim tako i onim neuspješnim. Primjerice, u jednom ozbiljnom slučaju zlonamjernog softvera velika susjedna treća zemlja nije surađivala, a čak niti uzajamna pravna pomoć nije funkcionirala.

7.4 Suradnja s privatnim sektorom

U članku 339.a Zakona o kaznenom postupku navodi se da se, ako postoji sumnja da je registrirani vlasnik ili korisnik telekomunikacijskog uređaja počinio kazneno djelo protiv računalnog sustava, programa ili podataka ili drugo djelo za koje je propisana kazna zatvora veća od 5 godina policija može, na temelju naloga suca istrage i u svrhu prikupljanja dokaza, zatražiti provjeru identiteta, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama, utvrđivanje položaja komunikacijskog uređaja, utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju i utvrđivanje identifikacijske oznake uređaja od pružatelja usluge javne komunikacije putem Operativno-tehničkog centra za nadzor telekomunikacija. Slično tome, za registriranog vlasnika ili korisnika telekomunikacijskog uređaja povezanog s osobom za koju se sumnja da je počinila kazneno djelo protiv računalnog sustava, programa ili podataka ili drugo djelo za koje je propisana kazna zatvora veća od 5 godina policija može, na temelju naloga suca istrage, zatražiti navedenu provjeru od pružatelja usluge javne komunikacije putem Operativno-tehničkog centra za nadzor telekomunikacija.

Prema Zakonu o elektroničkim komunikacijama pružatelji internetskih usluga imaju određene obveze i odgovornosti kako slijedi:
pružatelji internetskih usluga moraju poduzeti odgovarajuće tehničke i organizacijske mjere za zaštitu sigurnosti svojih usluga, a operatori javnih komunikacijskih mreža moraju poduzeti potrebne mjere za zaštitu sigurnosti elektroničkih komunikacijskih mreža i usluga. Tim se mjerama mora pružiti razina sigurnosti istovjetna postojećoj razini rizika za sigurnost mreže, uzimajući u obzir dostupna tehnička i tehnološka rješenja i povezane troškove. Poduzete mjere provode se kako bi se spriječio i na najmanju mjeru sveo učinak sigurnosnih incidenata na korisnike i međupovezane pružatelje mreža za elektroničku komunikaciju. (Članak 99.)

Od pružatelja internetskih usluga i javno dostupnih usluga elektroničke komunikacije te pravnih i fizičkih osoba koje, pod određenim odredbama, pružaju elektroničke komunikacijske mreže ili elektroničke komunikacijske usluge na hrvatskom državnom području traži se da o vlastitom trošku osiguraju i održavaju funkciju tajnog nadzora elektroničkih komunikacijskih mreža i usluga kao i vodove elektroničke komunikacije do operativnog i tehničkog tijela odgovornog za aktivaciju mjera tajnog nadzora elektroničkih komunikacija i upravljanje njima, u skladu sa zakonom kojim se uređuje područje nacionalne sigurnosti (članak 108.);

I pružatelji internetskih usluga i javno dostupne elektroničke komunikacijske usluge moraju zadržati podatke o elektroničkim komunikacijama u skladu s člankom 110. Zakona kako bi se omogućili istraga, otkrivanje i kazneni progon kaznenih djela u skladu sa zakonom o kaznenom postupku te u svrhu zaštite nacionalne sigurnosti u skladu sa zakonodavstvom u području obrane i nacionalne sigurnosti (članak 109.) itd.

Što se tiče uklanjanja internetskih stranica, u Republici Hrvatskoj jedino sud može naložiti pružatelju usluga da ukloni nezakonit sadržaj ili onemogući pristup do njega. Pristup pojedinim internetskim stranicama ili njihovo brisanje također se može blokirati na temelju sudskog naloga.

Hrvatska akademska i istraživačka mreža (CARNET), kao upravitelj nacionalne vršne domene, može u skladu s Pravilnikom o organizaciji i upravljanju nacionalnom internetskom domenom privremeno deaktivirati određenu hrvatsku (.hr) domenu ako su prekršene određene odredbe tog pravilnika ili ako postoji ozbiljna sumnja da korisnik djeluje suprotno načelima dobre vjere te se upotrebom domene krše prava trećih strana i stoga uzrokuje ozbiljna i nepopravljiva šteta ili ako korisnik namjerava neovlašteno prenijeti registriranu domenu drugoj osobi.

Međugranična suradnja u području internetskih kartičnih prijevara rutinski se odvija s izdavateljima kreditnih kartica (Visa, MasterCard i American Express) razmjenom informacija putem Europola i Interpola te bilateralnom suradnjom.

Hrvatska tijela kaznenog progona uspostavila su određenu suradnju i kontakte s lokalnim podružnicama ili najbližim podružnicama u regiji. Primjer je suradnja s poduzećem Google Hrvatska kojoj su se obratili u slučajevima kada je Hrvatska trebala neke podatke koje je ona mogla pružiti.

7.5 Alati međunarodne suradnje

7.5.1 Uzajamna pravna pomoć

Hrvatska nije stranka Konvencije o uzajamnoj pravnoj pomoći iz 2000. Tijekom posjeta na licu mjesta ocjenjivačkom je timu kazano da proces pristupanja Konvenciji još traje.

Ministarstvo pravosuđa Republike Hrvatske nadležno je tijelo za zaprimanje i slanje zahtjeva za uzajamnu pravnu pomoć. Iznimno, nadležna domaća pravosudna tijela mogu izravno poslati zahtjev za uzajamnu pravnu pomoć stranim pravosudnim tijelima ako je to izričito navedeno u odredbama Zakona o međunarodnoj pravnoj pomoći u kaznenim stvarima ili u međunarodnim sporazumima (izravna komunikacija), na temelju reciprociteta. U takvim slučajevima domaća pravosudna tijela šalju primjerak zahtjeva za uzajamnu pravnu pomoć Ministarstvu pravosuđa. U hitnim slučajevima i u slučaju reciprociteta Ministarstvo pravosuđa može slati i zaprimati zahtjeve za uzajamnu pravnu pomoć putem Interpola. U slučaju izravne komunikacije to isto može učiniti i nadležno domaće pravosudno tijelo.

Republika Hrvatska nema sveobuhvatni statistički sustav koji bi pokrivao cijelo područje uzajamne pravne pomoći. Ministarstvo pravosuđa izjavilo je da su u tijeku određeni projekti kojima bi se poboljšao taj sustav koji spada u njegovu nadležnost. Nema specifičnih postupaka ili uvjeta koji se trebaju ispuniti u Republici Hrvatskoj u vezi sa zahtjevima za uzajamnu pravnu pomoć povezanima s kiberkriminalitetom. Takvi zahtjevi rješavaju se na isti način kao i oni koji se odnose na druge vrste kaznenih djela.

Prilikom pružanja međunarodne pravne pomoći nacionalne vlasti primjenjuju nacionalne zakone. Zakonom o kaznenom postupku utvrđuju se uvjeti za potvrdu da je putem telekomunikacija uspostavljen kontakt kako bi se pribavili dokazi. Budući da ta radnja zadire u osnovna ljudska prava, regulirana je posebnim člankom Zakona kojim se jamči veći stupanj zaštite osnovnih ljudskih prava, a osobito prava na privatnost registriranih vlasnika ili korisnika telekomunikacijskih uređaja. Sama radnja može uključivati:

– provjeru identiteta, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama
– utvrđivanje položaja komunikacijskog uređaja
– utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju
– utvrđivanje identifikacijske oznake uređaja.

Hitni zahtjevi odmah se rješavaju. Prosječno je vrijeme odgovora oko 2 mjeseca ako se rabe uobičajeni načini komunikacije sa središnjim tijelima i tijelima određenima Konvencijom.

Mogu se zatražiti sve radnje dozvoljene Zakonom o kaznenom postupku. Elektronički dokazi mogu se prikupljati pretragom računala i srodnih uređaja, drugih uređaja koji se koriste za prikupljanje, pohranu i prijenos podataka, telefona, računalnih i drugih komunikacijskih i podatkovnih medija. Na zahtjev tijela koje obavlja pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili podatkovnom mediju i davatelj telekomunikacijskih usluga dužni su osigurati pristup računalu, uređaju ili podatkovnom mediju i pružiti informacije potrebne za nesmetanu uporabu i ostvarenje ciljeva pretrage. Na zahtjev tijela koje provodi pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili podatkovnom mediju i davatelj telekomunikacijskih usluga dužni su odmah poduzeti mjere kojima se sprečava uništenje ili mijenjanje podataka.

Podaci pohranjeni na računalu i srodnim uređajima i drugim uređajima koji se koriste za pohranu i prijenos podataka mogu se privremeno oduzeti i pohraniti ako su radi o predmetima koji su određeni za oduzimanje u skladu s Kaznenim zakonom ili ako mogu pomoći u utvrđivanju činjenica u postupku.

Ako se izvidi kaznenih djela ne mogu provesti na drugi način ili ako bi to uzrokovalo nesrazmjerne poteškoće, sudac istrage može, na pisani obrazloženi zahtjev državnog odvjetnika, protiv osobe za koju postoji sumnja da je počinila ili zajedno s drugim osobama sudjelovala u kaznenom djelu izdati nalog za određivanje posebnih mjera za prikupljanje dokaza kojima se privremeno ograničavaju ustavna prava građana, i to:

1) nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu,
2) presretanje, prikupljanje i snimanje računalnih podataka,
3) ulazak u prostorije radi provođenja nadzora i tehničko snimanje prostorija,
4) tajno praćenje i tehničko snimanje osoba i predmeta,
5) uporaba prikrivenih istražitelja i pouzdanika,
6) simulirana prodaja i otkup predmeta, simulirano davanje potkupnine i simulirano primanje potkupnine,
7) pružanje simuliranih poslovnih usluga ili sklapanje simuliranih pravnih poslova,
8) nadzirani prijevoz i isporuka predmeta kaznenog djela.

Jedan od najčešćih razloga zahtjeva za uzajamnu pravnu pomoć jest provjera IP adrese, tj. presretanje sadržaja u računalnom sustavu.

Europska pravosudna mreža u kaznenim stvarima i Eurojust pomažu Republici Hrvatskoj u slučajevima transnacionalnog organiziranog kriminala koji je počinjen na državnom području više država članica EU-a kako bi se hitno djelovalo u slučajevima kiberkriminaliteta. Republika Hrvatska zasada nije pokrenula nikakve koordinacijske sastanke u gore navedenim slučajevima, ali je pozivana na takve sastanke.

Policija održava mrežu za kiberkriminalitet koja djeluje 24/7.

Razmjena dokaza i prikupljanje dokaza iz inozemstva provodi se uglavnom u skladu s odredbama Konvencije o kibernetičkom kriminalu iz 2001. i njezina Dodatnog protokola iz 2003. (osobito što se tiče zadržavanja podataka u skladu s člancima 29. i 30. Konvencije u svrhu njihove privremene zapljene kao dio uzajamne pravne pomoći koja je regulirana člankom 31. Konvencije), Europske konvencije o uzajamnoj pomoći u kaznenim stvarima iz 1959. i bilateralnih ugovora.

Najdulje razdoblje za zadržavanje podataka u Hrvatskoj jest jedna godina. U slučaju zahtjeva za čuvanje, podaci se mogu sačuvati na razdoblje od 30 dana; zahtjev za uzajamnu pravnu pomoć trebalo bi poslati unutar tog razdoblja.

Kazneni progon ustupit će se u slučajevima kada se primjenjuju odredbe iz članka 65. Zakona o uzajamnoj pravnoj pomoći u kaznenim stvarima (kazneno djelo ne smije podlijegati kazni većoj od deset godina zatvora, djelo je počinjeno na državnom području Republike Hrvatske, a počinitelj je stranac s prebivalištem u inozemstvu).

Kao što je ranije izneseno, u slučajevima kada se uzajamna pravna pomoć pruža za Sjedinjene Američke Države pravnu osnovu predstavlja načelo reciprociteta sukladno članku 17. Zakona o međunarodnoj pravnoj pomoći u kaznenim stvarima u kojem se navodi da domaća pravosudna tijela udovoljavaju zahtjevima za uzajamnu pravnu pomoć koje su poslala pravosudna tijela države s kojom Republika Hrvatska nije sklopila sporazum o uzajamnoj pravnoj pomoći samo ako se očekuje da će se odgovoriti recipročno na temelju uvjerenja države koja podnosi zahtjev. Republika Hrvatska nije imala nikakvih problema oko provedbe zahtjeva za uzajamnu pravnu pomoć u tim slučajevima.

Ako u kibernapadima sudjeluju kriminalci izvan EU-a, Hrvatska se koristi i instrumentima uzajamne pravne pomoći kao što su Konvencija Ujedinjenih naroda protiv transnacionalnoga organiziranog kriminaliteta, Konvencija Ujedinjenih naroda protiv korupcije i Konvencija Ujedinjenih naroda protiv nezakonitog prometa opojnih droga i psihotropnih supstancija. Npr. u slučajevima koji uključuju uzajamnu pravnu pomoć u vezi sa Sjedinjenim Američkim Državama, pravna osnova za svaku radnju je načelo reciprociteta iz članka 17. Zakona o uzajamnoj pravnoj pomoći u kaznenim stvarima u kojem se navodi da će zahtjevima za uzajamnu pravnu pomoć pravosudnih tijela zemlje s kojom Republika Hrvatska nije potpisala sporazum o uzajamnoj pravnoj pomoći domaća pravosudna tijela udovoljiti samo ako se očekuje da će dotična država podnijeti sličan zahtjev domaćim pravosudnim tijelima na temelju uvjerenja države koja podnosi zahtjev.

Osnovni postupci koji se odnose na međunarodnu suradnju pretpostavljaju korištenje instrumentima uzajamne pravne pomoći kako bi Hrvatska mogla prikupiti dokaze iz inozemstva.

U nekim se slučajevima policijski službenici koriste uslugama koje neki pružatelji elektroničkih usluga daju policijskim tijelima za komunikaciju i osiguravanje bržeg i učinkovitijeg odgovora na, npr., iskorištavanje djece za pornografiju (npr. Tim za intervenciju u kaznenom progonu za Facebook, Skype i Instagram). Međunarodna policijska suradnja s policijskim tijelima u nekim zemljama (npr. Sjedinjene Američke Države, Australija, Novi Zeland itd.) bila je vrlo uspješna u slučajevima koji su se odnosili na seksualno zlostavljanje i iskorištavanje djece.

7.5.2 Instrumenti uzajamnog priznavanja

Uočeni su problemi s kaznenim progonom prijestupnika povezanih s računalnim kriminalom, pogotovo računalnih prijestupnika. Hrvatska je uočila povećani broj napada zlonamjernim računalnim programima na štetu korisnika internetskih sustava hrvatskih poslovnih banaka. Ti programi omogućuju neovlaštene bankovne transakcije s računa oštećenih strana na račune privatnih pojedinaca ili pravnih osoba u Hrvatskoj ili inozemstvu (npr. posrednici za prijenos novca) koji potom šalju novac putem Western Uniona ili sličnih pružatelja financijskih usluga inozemnim posrednicima ili počiniteljima. Ti posrednici ili tzv.„novčane mule“ dobivaju dio novca koji se prenosi na njihove tekuće račune.

Republika Hrvatska pogođena je tim kaznenim djelima koja često čine strani državljani iz inozemstva što otežava identifikaciju prijestupnika. Usprkos hitnim mjerama i alatima za pravosudnu suradnju kao što su nalozi za zamrzavanje imovine ili osiguranje dokaza (Okvirna odluka Vijeća 2003/577/PUP od 22. srpnja 2003. o izvršenju odluka o zamrzavanju imovine i osiguranju dokaza u Europskoj uniji) u praksi se prijestupnik rijetko utvrdi, tj. rijetko se donose privremene mjere zamrzavanja imovine i oduzimanja imovinske koristi stečene kaznenim dijelom.

Državno odvjetništvo Republike Hrvatske proslijedilo je 16 naloga za zamrzavanje imovine i osiguranje dokaza u kaznenim postupcima za računalnu prijevaru u 2014., kako je navedeno u članku 271. Kaznenog zakona, međutim imovinska korist stečena kaznenim dijelom u tim slučajevima nije zamrznuta niti oduzeta jer je u vrijeme provedbe naloga za zamrzavanje imovine novac bio podignut s bankovnog računa te je preostali iznos bio nedovoljan za zamrzavanje i oduzimanje imovinske koristi stečene kaznenim dijelom.

Republika Hrvatska nije razvila nikakvu praksu za ostale instrumente uzajamnog priznavanja EU-a.

Tijekom posjeta na licu mjesta tužitelji su naglasili važnost izravnih kontakata među pravosudnim tijelima.

7.5.3 Predaja/izručenje

a/ Kaznena djela iz područja kiberkiminaliteta kažnjiva kaznom zatvora od najmanje tri godine i kaznena djela s popisa europskog uhidbenog naloga uključena u Kazneni zakon su sljedeća:
– mamljenje djece za zadovoljenje spolnih potreba (članak 161.)
– iskorištavanje djece za pornografiju (članak 163.)
– iskorištavanje djece za pornografske predstave (članak 164.)
– upoznavanje djece s pornografijom (članak 165.)
– teška kaznena djela spolnog zlostavljanja i iskorištavanja djeteta (članak 166.)
– neovlašteni pristup (članak 266.)
– ometanje rada računalnog sustava (članak 267.)
– oštećenje računalnih podataka (članak 268.)
– neovlašteno presretanje računalnih podataka (članak 269.)
– računalno krivotvorenje (članak 270.)
– računalna prijevara (članak 271.)
– zlouporaba naprava (članak 272.)
– teška kaznena djela protiv računalnih sustava, programa i datoteka (članak 273.)

b/ U članku 34. Zakona o međunarodnoj pravnoj pomoći u kaznenim stvarima navodi se da se izručenje u svrhu kaznenog postupka može odobriti samo za kaznena djela koja su prema domaćem pravu kažnjiva kaznom zatvora ili sigurnosnom mjerom s lišavanjem slobode na najduže razdoblje od barem jedne godine ili strožom kaznom. Izručenje radi izvršenja sankcija lišavanjem slobode može se odobriti nakon što je donesena pravomoćna presuda kojom se počinitelj osuđuje na zatvor ili sigurnosnu mjeru s lišavanjem slobode u trajanju od najmanje četiri mjeseca. Iznimno, ako je u zahtjev za izručenje uključeno nekoliko zasebnih kaznenih djela od kojih neka ne ispunjavaju uvjete koji se odnose na duljinu kazne ili u slučaju kaznenih djela koja se kažnjavaju samo novčano, izručenje se može odobriti i za ta kaznena djela.

Županijski uredi državnog odvjetništva ovlašteni su zaprimiti europske uhidbene naloge ovisno o mjestu osoba protiv kojih je podnesen nalog, a županijski uredi državnog odvjetništva i domaći sudovi ovlašteni su slati europske uhidbene naloge tijelima kaznenog progona države izvršenja.

Ministarstvo pravosuđa Republike Hrvatske ovlašteno je slati i primati zahtjeve za izručenje. Komunikacija se odvija na uobičajen način putem ureda Interpola/S.I.Re.N.E-a i Europske pravosudne mreže u kaznenim stvarima.

U svojem odgovoru na upitnik Hrvatska je ustvrdila da nema statistiku o tome području. Međutim, tijekom posjeta na licu mjestu kazano je da Ministarstvo unutarnjih poslova vodi statistiku o izručenim osobama. Ocjenjivački tim nije dobio nikakve podatke.

Nema specifičnih postupaka ili uvjeta koji se trebaju ispuniti u Republici Hrvatskoj u vezi sa zahtjevima za izručenje povezanima s kiberkriminalitetom. Takvi zahtjevi rješavaju se na isti način kao i oni koji se odnose na druge vrste kaznenih djela.

Mogu se provoditi privremena uhićenja u svrhu izručenja. Osim oblika i sadržaja koji se traži za svaki zahtjev za izručenje, u zahtjevu za privremeno uhićenje mora se navesti izjava pravosudnih tijela o postojanju pravomoćne presude ili odluke o pritvoru kao i izjava o uhićenju u svrhu izručenja.

Pravni postupak za predaju u Republici Hrvatskoj jest hitan postupak u kojem se primjenjuju rokovi određeni Okvirnom odlukom Vijeća od 13. lipnja 2002. o europskom uhidbenom nalogu i postupku predaje između država članica. Postupak izručenja nešto je sporiji, uzevši u obzir nekoliko faktora kao što su načini komunikacije, isporuka, pravni lijekovi itd. Prosječno vrijeme izručenja iznosi 6 mjeseci.

Republika Hrvatska dosad nije primjenjivala postupak predaje previđen Sporazumom o postupku predaje između država članica EU-a, Islanda i Norveške.
Sjedinjene Američke Države poslale su zahtjev za izručenjem 2014. te je zatražena osoba izručena Sjedinjenim Američkim Državama iz Republike Hrvatske u svrhu kaznenog postupka zbog kršenja povjerljivosti, integriteta i dostupnosti računalnih podataka, programa ili sustava te računalnog krivotvorenja.

7.6 Zaključci

- Hrvatska nije stranka Konvencije o uzajamnoj pravnoj pomoći iz 2000.;

- doprinos Hrvatske međunarodnoj istrazi zlonamjernog softvera ZEUS bio je aktivan i vrlo učinkovit te pokazuje hrvatski operativni kapacitet za suradnju s drugim zemljama;

- hrvatski tužitelji uputili su jasnu poruku da u Hrvatskoj postoji potreba za stvaranjem odgovarajućih aranžmana za razvoj izravnih kontakata između pravosudnih vlasti u inozemstvu;

- tužiteljstvo je napravilo priručnik za stručnjake koji se bave uzajamnom pravnom pomoći, što se može smatrati dobrom praksom;

- potrebno je poboljšati međunarodni pravni okvir (treće zemlje / Rusija);

- hrvatski stručnjaci bili su vrlo aktivni u projektu EMPACT CA te su bili pokretač jedne suradnje na području operativnog akcijskog plana sa Slovenijom. To je vrlo dobar primjer proaktivnog djelovanja.

- Ne postoje sveobuhvatne niti konsolidirane statistike u tom području te bi se to trebalo poboljšati;

- nema iskustava s instrumentima uzajamnog priznavanja osim naloga o zamrzavanju.

8 OSPOSOBLJAVANJE, PODIZANJE SVIJESTI I PREVENCIJA

8.1 Usmjereno osposobljavanje

Kao dio osposobljavanja Pravosudna akademija organizirala je dvije aktivnosti na regionalnoj razini u 2014. u prostorijama Regionalnog centra za edukaciju pravosudnih dužnosnika o suzbijanju kibernetičkog kriminala:

Dvodnevni seminar „Borba protiv kibernetičkog kriminala i dječje pornografije na Internetu“ održan je u siječnju 2014. pred 40 sudionika, u suradnji s instrumentom za tehničku pomoć i razmjenu informacija (TAIEX) i Akademijom za europsko pravo (ERA). Cilj seminara bio je odrediti kako se međunarodno i europsko pravo u području kiberkriminaliteta primjenjuju u različitim državama članicama i državama kandidatima te ocijeniti izglede za uspostavu učinkovite međunarodne suradnje u suzbijanju kiberkriminaliteta. Na seminaru se također raspravljalo o načinu na koji se zemlje koje nisu članice EU-a suočavaju s izazovima kiberkriminaliteta.

Dvodnevni seminar „Kibernetički kriminal“ održan je u listopadu 2014. pred 29 sudionika, u suradnji s Pravosudnom akademijom i poduzećem INsig2 čiji su stručnjaci predavanja održali besplatno. Na seminaru se raspravljalo o sljedećim temama: digitalni dokazi i forenzika, kiberkriminalitet, računala i mreže, internet, mobilni telefoni, elektronički dokumenti i najnoviji trendovi u području kiberkriminaliteta. Na oba seminara sudjelovali su sudionici iz država korisnika Regionalnog centra. Pravosudna akademija namjerava organizirati još jedan regionalni seminar o suzbijanju kiberkriminaliteta do kraja 2015.

Iako su teme povezane s kiberkriminalitetom na štetu djece prethodnih godina uključivane u policijsko obrazovanje u sklopu različitih programa osposobljavanja i specijalizacija, kao i u programe nekih predmeta na Policijskoj akademiji, ciljano specijalističko osposobljavanje policijskih službenika u tom području provodi se tek od 2012. Od 13. veljače 2012. do 24. listopada 2013. održana su 32 seminara (u trajanju od 2 do 14 dana) za više od 800 sudionika (policijskih službenika, socijalnih radnika, tužitelja i sudaca) u sklopu II. komponente projekta IPA 2009 „Jačanje kapaciteta u području borbe protiv seksualnog iskorištavanja i seksualnog zlostavljanja djece te pružanja pomoći policije ranjivim žrtvama kriminaliteta“, u organizaciji Policijske akademije i odjela MUP-a koji se bavi maloljetničkom delinkvencijom i kriminalitetom na štetu mladeži i obitelji. Na tim seminarima sudjelovalo je ukupno 330 policijskih službenika koji se bave maloljetničkom delinkvencijom, gospodarskim kriminalitetom i prevencijom.

U skladu s obvezama koje proizlaze iz projekta IPA 2009 „Jačanje kapaciteta u području borbe protiv seksualnog iskorištavanja i seksualnog zlostavljanja djece te pružanja pomoći policije ranjivim žrtvama kriminaliteta“ i potrebe za stalnim ažuriranjem i poboljšanjem znanja i vještina policijskih službenika, u postojeći program specijalističkog osposobljavanja za policijske službenike i istražitelje za mladež uključeni su sadržaji iz područja kaznenih djela seksualnog iskorištavanja djece na internetu i dječje pornografije. Svake godine održava se specijalizirani tečaj iz maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji za 30 policijskih službenika.

Na drugoj godini studijskog programa Policijske akademije studentima se nudi kolegij Forenzika digitalnih dokaza. Radi se o metodama i tehnikama koja tijela kaznenog progona rabe u prikupljanju, obradi i pohrani podataka i informacija koji se mogu pronaći na elektroničkim medijima kao što su računala, poslužitelji, sustavi u oblaku koji se nalaze na internetu, baze podataka, mobilni i GPS uređaji, memorijske kartice, USB memorijski stikovi i svi drugi elektronički uređaji na kojima je moguće pohranjivati podatke (bijela tehnika, CCTV, itd.). Studenti se osposobljavaju za utvrđivanje i osiguravanje digitalnih dokaza koji su predmet istrage. Također se objašnjava uloga sudskih vještaka u računalnoj forenzici. Studenti se osposobljavaju za napredno korištenje internetom i pretraživanje weba, traženje podataka u datotekama (slike, metapodaci) kao i za sve open source tehnike i softver koji bi mogao biti koristan.

Od studenoga 2012. do danas organizirana su tri takva specijalizirana kolegija koja su pohađala 102 policijska službenika kriminalističke policije. Sadržaj IPA projekta u ukupnom rasporedu kolegija iznosi ukupno 76 nastavnih sati.

Također su razvijeni posebni programi za osposobljavanje mladih policijskih službenika i istražitelja za mladež s ciljem stalnog stručnog usavršavanja putem specijaliziranog seminara „Studij seksualnih zločina na štetu djece putem interneta“ i „Nove tehnologije i elektronski kriminalitet“.

Uz specijalizaciju i stručno usavršavanje policijskih službenika u području kiberkriminaliteta protiv djece, Policijska akademija organizira i seminare i druge tečajeve u području kiberkriminaliteta.
U posljednje tri godine kao dio specijaliziranog tečaja o borbi protiv gospodarskog kriminaliteta i korupcije održana su predavanja na temu visokotehnološkog (računalnog) kriminaliteta. Od 2013. do 2014. ti su tečajevi organizirani za ukupno 60 stručnih polaznika.

Odjel za visokotehnološki kriminalitet odgovoran je za organiziranje i pružanje osposobljavanja u području kiberkriminaliteta za sve policijske službenike zadužene za suzbijanje kiberkriminaliteta kao i za digitalnu forenziku. To osposobljavanje obično organiziraju međunarodne organizacije. S tim u vezi, Hrvatska kad god je to moguće sudjeluje u osposobljavanju koje organiziraju ECTEG i Sveučilište iz Dublina (tečajevi se održavaju u Avili, Španjolskoj jednom godišnje), CEPOL (različiti tečajevi organizirani diljem EU-a), na konferencijama centra EC3 i seminarima koji se održavaju u sjedištu Europola u Haagu, međunarodnim tečajevima OLAF-a za kazneni progon u različitim područjima forenzike (Hercule II i Hercule III) koji se trenutačno održavaju u Zagrebu kao i u osposobljavanju koje španjolska policija provodi za policijske službenike u sklopu projekta IPA 2011 (u 2015. godini).

Hrvatska je članica ECTEG-a od travnja 2014. i redovito sudjeluje na sastancima ECTEG-a u sjedištu Europola. Hrvatski policijski službenici sudjelovali su 2014. i 2015. na tečajevima o forenzici Linuxa koje je organizirao španjolski nacionalni centar za policijsko osposobljavanje u Avili, Španjolskoj.

Za organizaciju osposobljavanja o kiberkriminalitetu nadležan je odjel za stručno osposobljavanje i specijalizaciju Policijske akademije koji svake godine izrađuje planove za policijsko osposobljavanje na temelju prijedloga organizacijskih jedinica Ministarstva unutarnjih poslova, u skladu s njihovim procjenama i potrebama. Međutim, razni oblici osposobljavanja mogu se organizirati lokalno, ali mogu imati međunarodnu dimenziju u obliku konferencija, stručnih i radnih sastanaka u čiju je organizaciju uključena Policijska akademija ako to pojedine organizacijske jedinice zatraže.

Policijski službenici koji to žele mogu pratiti aktivnosti CEPOL-a praćenjem webinara na engleskom jeziku. U 2014. tako su mogli sudjelovati na webinaru „Kiberkriminalitet: otkrivanje, istraga i prevencija“ koji je održan 27. studenoga 2014.

Svi su tečajevi financirani iz uobičajenih proračunskih sredstava. Teško je dati točan podatak o troškovima pojedinog seminara ili osposobljavanja jer to ne ovisi samo o broju sudionika nego i o mjestu na kojem se održava seminar kao i o organizacijskoj jedinici (gradu) iz koje dolaze polaznici. Npr. specijalistički tečaj za policijske službenike i istražitelje za mladež košta oko 350 000 kuna, a specijalistički seminar o „Istraživanju seksualnih zločina na štetu djece putem interneta“ oko 15 000 kuna.

Program osposobljavanja pravosudnih službenika Pravosudne akademije pohađaju suci i zamjenici tužitelja, a neki od njih su kontakt-osobe za međunarodnu suradnju u kaznenim stvarima; međutim, trenutačno ne postoje programi isključivo za one pravosudne službenike koji se bave suzbijanjem kiberkriminaliteta.

Od 2013. u suradnji s veleposlanstvom SAD-a u Republici Hrvatskoj i Policijskom akademijom Ministarstva unutarnjih poslova provodi se projekt „Partnerstvo za obrazovanje“ s ciljem jačanja međunarodne policijske suradnje. U sklopu projekta svake se godine provodi 5 modula o različitim temama. Sudionici su policijski službenici i tužitelji iz regije (Albanija, Bosna i Hercegovina, Crna Gora, Hrvatska, Kosovo, Makedonija, Slovenija i Srbija), a predavači su stručnjaci iz Hrvatske i Sjedinjenih Američkih Država. U projektu svake godine sudjeluje i strani partner tako da je 2013. partner bila Velika Britanija, 2014. Austrija, a 2015. Francuska. Te zemlje sudjeluju sa svojim stručnjacima u raznim područjima. godine održan je petodnevni modul o računalnom kriminalitetu sa predavačima-stručnjacima iz Hrvatske i Sjedinjenih Američkih Država (Sveučilište Purdue). U 2014. održan je petodnevni modul o računalnom kriminalitetu i elektroničkim dokazima: predavači su bili stručnjaci iz Tajne službe SAD-a i privatnog sektora (Global Investigations Citi Security & Investigative Services, Global Security and Investigations, CISSP, FIS Global incidents i EECTF Rome). U 2015. održan je petodnevni modul o upadima u računala i mreže: predavači su bili agenti Tajne službe SAD-a. Na svakom modulu sudjelovalo je četiri predstavnika gore navedenih zemalja (tri policijska službenika i jedan specijalizirani tužitelj). Cilj je projekta ojačati međunarodnu policijsku suradnju i razviti regionalnu mrežu policijskih službenika za borbu protiv svih vrsta kriminaliteta s naglaskom na organizirani, računalni kriminalitet i terorizam.

Pokusni Regionalni centar za osposobljavanje pravosudnih dužnosnika za borbu protiv kiberkriminaliteta (dalje u tekstu: Centar) osnovan je kao dio projekta IPA 2010 „Regionalna suradnja u borbi protiv kiberkriminaliteta u jugoistočnoj Europi“. Cilj projekta bio je ojačati kapacitete pravosudnih tijela i ministarstava unutarnjih poslova država zapadnog Balkana i Turske kako bi se uspostavila učinkovita suradnja u suzbijanju kiberkriminaliteta.

Pokusni centar djeluje u Zagrebu kao organizacijska jedinica Pravosudne akademije, institucije koja je odgovorna za osposobljavanje kandidata za radna mjesta sudaca i zamjenika tužitelja (koji pohađaju Državnu školu za pravosudne dužnosnike), stažista, pravosudnih savjetnika i pravosudnih službenika.

Policijska akademija u svoje kolegije uključuje teme i module koji se odnose na kiberkriminalitet. Npr. na njezinu specijaliziranom stručnom studiju kriminologije (na 2. godini) koji godišnje prati 50 izvanrednih studenata u sklopu kolegija „Kriminalitet djece i maloljetnika“ ima pet sati predavanja koje obuhvaća utvrđivanje žrtava i počinitelja kaznenih djela na štetu djece pomoću open source i darknet alata. Tijekom predavanja studenti su također osposobljeni za korištenje internetskim stranicama www.sigurnijiinternetnet.hr.

Policijska akademija provodi visokoškolski studij „Policijski službenik“ na kojem se policijski službenici obučavaju za osnovno bavljenje svojim poslom.

U sklopu tog studija nastavnik Nikola Protrka predaje jednosemestralni izborni kolegij o digitalnim forenzičkim dokazima. Taj kolegij obuhvaća kriminalističke metode i tehnike u prikupljanju, obradi i pohrani podataka i informacija koji se mogu pronaći na elektroničkim medijima kao što su računala, poslužitelji, sustavi u oblaku koji se nalaze na internetu, baze podataka, mobilni i GPS uređaji, memorijske kartice, USB memorijski stikovi i svi drugi elektronički uređaji na kojima je moguće pohranjivati podatke (bijela tehnika, CCTV, itd.). Studenti se osposobljavaju za utvrđivanje i osiguravanje digitalnih dokaza koji su predmet istrage. Studenti se osposobljavaju za napredno korištenje internetom i pretraživanje weba, traženje podataka u datotekama (slike, metapodaci) kao i za sve *open source* resurse.

U sklopu svog visokoškolskog studijskog programa Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu održava kolegije „Programsko inženjerstvo i informacijski sustavi“, „Telekomunikacije i informatika“. Fakultet organizacije i informatike Sveučilišta u Varaždinu održava kolegij „Sigurnost informacijskih sustava“.

Kako je gore navedeno, hrvatske vlasti sudjelovale su u raznim osposobljavanjima u području kiberkriminaliteta kako na nacionalnoj tako i na međunarodnoj razini. Međutim, kako je kazano nekoliko puta tijekom posjeta na licu mjesta, postoji jasna potreba za sustavnim i zajedničkim obrazovanjem svih tijela koja se bave tim područjem, to jest policije, tužitelja i sudaca.

8.2 Podizanje svijesti

Kao dio nacionalne kampanje „Živim život bez nasilja“ Hrvatska stalno podiže svijest kako bi se javnost potaknula da prijavi kaznena djela na štetu djece. To se osobito odnosi na kampanju provedenu početkom 2010. koja je, kada se pokretala, bila namijenjena samo za žrtve obiteljskog nasilja; međutim, od 2013., Hrvatska je promijenila ciljnu skupinu nacionalne kampanje i proširila njezine ciljeve tako da uključuju i prevenciju svih oblika nasilja usmjerenog protiv djece, uključujući seksualno nasilje, promicanje kulture nenasilja, nediskriminacije i tolerancije te se povezala s Ministarstvom znanosti, obrazovanja i sporta kako bi se kampanja provela u svim školama na državnom području Republike Hrvatske.

Nacionalni CERT stalno distribuira informacije s ciljem podizanja javne svijesti. U tu svrhu informacije se distribuiraju putem internetskih stranica kao upozorenja i vijesti, a nekoliko brošura otisnuto je i distribuirano u dnevnim novinama. Nazivi brošura su sljedeći: „Sigurnije na internetu“, „Kako sigurnije poslovati na internetu“, „Opasnosti Facebooka“ i „Zaštitite svoju privatnost na Facebooku“. Predstavnici Nacionalnog CERT-a često drže javne prezentacije u obliku konferencija ili nacionalnih TV prijenosa.

Javni i civilni sektor poduzeli su brojne aktivnosti i projekte s ciljem prevencije zlostavljanja na internetu, pogotovo u školama. Projekt „Sigurnost djece na internetu“, proveden u pet različitih hrvatskih škola i financiran od Europske unije, rezultirao je izradom kurikuluma o sigurnom korištenju internetom i više od 800 nastavnih sadržaja za učenike, nastavnike i roditelje.

Što se tiče zaštite osobnih podataka, Republika Hrvatska pokrenula je intenzivne mjere za podizanje javne svijesti (putem radionica, konferencija za medije i stručnih predavanja) kako bi se kiberkriminalitet smanjio na najmanju mjeru.

8.3 Prevencija

8.3.1 Nacionalno zakonodavstvo/politika i druge mjere

Kako je gore navedeno, borba protiv kiberkriminaliteta prepoznata je u Hrvatskoj kao jedno od pet prioritetnih područja za koje treba definirati strateške ciljeve i koji su posebno definirani u Nacionalnoj strategiji kibernetičke sigurnosti donesenoj 7. listopada 2015.

Osim toga, sve četiri poveznice u (pet) odabranih područja kibersigurnosti, koje su također definirane u Strategiji, imaju za cilj potporu naporima za borbu protiv kiberkriminaliteta.

Te su poveznice sljedeće: 1. Zaštita osjetljivih informacija, 2. Tehnička koordinacija u obradi sigurnosnih incidenata, 3. Međunarodna suradnja i 4. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.

Jedan od ciljeva „Tehničke koordinacije u obradi sigurnosnih incidenata“ u Nacrtu strategije jest „Redovito provođenje mjera za poboljšanje sigurnosti kroz izdavanje upozorenja i preporuka“.

Osim toga, u dijelu „Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru“ u Nacrtu strategije i akcijskog plana za njezinu provedbu definira se više aktivnosti usmjerenih na sustavno obrazovanje i stjecanje stručnog znanja u području kibersigurnosti, podizanje svijesti o sigurnosti među korisnicima interneta i provedbu određenih mjera od strane operatora s ciljem prevencije sigurnosnih incidenata (npr. objavljivanje preporuka o minimalnim sigurnosnim zahtjevima za korisnike javnih i komercijalnih bežičnih mreža).

Prevencija također predstavlja integralni dio policijskih aktivnosti. U godišnjem radnom planu Ministarstva unutarnjih poslova za 2015. naglašava se prevencija svih oblika kriminaliteta. Služba prevencije specijalizirani je odjel u sklopu Ureda načelnika Policijske uprave i koordinira sve aktivnosti prevencije unutar policije na nacionalnoj i regionalnoj razini.

Zakon o informacijskoj sigurnosti ne utvrđuje posebne mjere povezane sa sviješću o prevenciji i sigurnosti; međutim, kako bi se smanjio broj kiberincidenata, nacionalni CERT pruža sljedeće usluge svojim članovima na temelju najbolje prakse:
– objavljivanje novosti i upozorenja koji se tiču informacijske sigurnosti
– objavljivanje bijelih knjiga i brošura
– povremene TV emisije
– objavljivanje informacija o nedostacima softvera
– skeniranje nedostataka za komercijalne i nekomercijalne institucije na zahtjev
– redovito skeniranje nedostataka za članove CARNeta.

Javni i civilni sektor poduzeli su brojne aktivnosti i projekte s ciljem prevencije zlostavljanja na internetu, pogotovo u školama. Projekt „Sigurnost djece na internetu“, proveden u pet različitih hrvatskih škola i financiran od Europske unije, rezultirao je izradom kurikuluma o sigurnom korištenju internetom i više od 800 nastavnih sadržaja za učenike, nastavnike i roditelje.

Što se tiče zaštite osobnih podataka, Republika Hrvatska pokrenula je intenzivne mjere za podizanje javne svijesti (putem radionica, konferencija za medije i stručnih predavanja) kako bi se kiberkriminalitet smanjio na najmanju mjeru.

APLIKACIJA RED BUTTON ZA PRIJAVU KAZNENIH DJELA NA INTERNETU

https://redbutton.mup.hr/

Ta aplikacija omogućuje svakome da prijavi kaznena djela, incidente na internetu i kriminalne aktivnosti na internetu te je namijenjena svim građanima, ali je posebno pogodna za djecu te omogućuje prijavu internetskog sadržaja koji djeca smatraju nezakonitim, a koji se odnosi na različite oblike iskorištavanja ili zlostavljanja djece. Aplikacija nije zamišljena kao zamjena za prijavu kaznenog djela izravno u policijskoj postaji ili pozivom na hitan broj policije te stoga sadrži posebnu izjavu o odricanju od odgovornosti: *U hitnom slučaju molimo odmah nazovi policiju na broj 192 ili obavijesti odraslu osobu u koju imaš povjerenje i zamoli je da nazove policiju ili dođi u najbližu policijsku upravu ili policijsku postaju i zatraži pomoć policije. Tvoju poruku u mogućnosti smo pročitati isključivo od ponedjeljka do petka, od 8.30 do 15.30 sati. Zbog zakonskih ograničenja u mogućnosti smo zaprimati i odgovarati samo na prijave zaprimljene iz Hrvatske.*

HRVATSKI NACIONALNI TIM ZA HITNE RAČUNALNE INTERVENCIJE

http://www.cert.hr/en/start

Nacionalni CERT izdao je četiri brošure:

1. „Sigurnije poslovanje na internetu“ - http://www.cert.hr/sites/default/files/sigurnije_poslovanje_na_internetu.pdf

2. „Sigurnije na internetu“ - http://www.cert.hr/sites/default/files/sigurnije%20na%20internetu.pdf

3. „Zaštitite svoju privatnost na Facebooku” http://www.cert.hr/sites/default/files/Facebook%20brosura%20v2%20(2012).pdf

4. „Opasnosti Facebooka“ http://www.cert.hr/sites/default/files/Opasnosti%20Facebooka.pdf

CENTAR ZA SIGURNIJI INTERNET

http://www.saferinternet.hr/ or http://www.sigurnijiinternet.hr/

CILJEVI CENTRA ZA SIGURNIJI INTERNET

Primjena novih tehnologija u svakodnevnom životu, učenju, poučavanju i poslu umnogome olakšava posao i učenje, ali traži stalno obrazovanje korisnika tehnologije, pogotovo što se tiče mogućih rizika i opasnosti koje povezivanje s mrežama može predstavljati za odrasle i djecu. Uspostavom Centra za sigurniji internet objedinjuju se aktivnosti različitih organizacija u Hrvatskoj koje se bave tom temom iz različitih perspektiva –psihološke, pedagoške, računalne, informacijske, zakonodavne i sociološke. Time korisnici (djeca, roditelji, nastavnici, odgajatelji i drugi korisnici interneta) dobivaju jedinstveno mjesto za pristup informacijama i obrazovnim materijalima koji obuhvaćaju sve navedene aspekte sigurnosti djece na internetu te im se omogućuje da prijave moguće povrede sigurnosti djece na internetu. Informativni i obrazovni materijali koje je taj centar izradio u suradnji sa svojim partnerima obuhvaćaju sljedeće teme:

– zaštitu osobnih podataka i privatnosti
– online suradnju i komunikaciju
– online učenje i istraživanje
– sigurno pretraživanje internetskih sadržaja
– stvaranje poznanstava, druženje s prijateljima i online zabava.

Cilj Centra također je i zalagati se za institucionalizirano uvođenje računalne i informacijske sigurnosti u obrazovni sustav, npr. kao dio kurikuluma u osnovnim i srednjim školama. Centar je otvoren za partnersku suradnju sa svim zainteresiranim stranama koje se bave sigurnijim online okruženjem za djecu. Centar također već surađuje s nekim međunarodnim organizacijama koje se bave tom tematikom i namjerava produbljivati i proširivati tu suradnju. Važan cilj Centra jest promicanje računalne i informacijske sigurnosti i osvještavanje o važnosti sigurnog online okruženja za djecu kao preduvjeta za zdrav i uspješan razvoj i odrastanje.

Centar za sigurniji internet rukovodi se smjernicama Europske unije za projekt Sigurniji internet. Organiziranjem raznih događaja, okruglih stolova, javnih predavanja, radionica, prezentacija i predavanja osigurat će se ispunjavanje glavnih ciljeva Centra te osvijestiti javnost o važnosti sigurnosti na internetu. Centar djeluje putem strateških partnera, članova Centra i sponzora projekata.

Među strateškim partnerima Centra za sigurniji internet su:

• Agencija za zaštitu osobnih podataka
• Agencija za obrazovanje
• Hrvatska akademska i istraživačka mreža i nacionalni CERT
• HAKOM - hrvatska agencija za poštu i elektroničke komunikacije
• Ministarstvo socijalne politike i mladih
• Ministarstvo unutarnjih poslova
• Ministarstvo uprave
• Ministarstvo znanosti, obrazovanja i sporta
• osnovna škola u Gornjem Bukovcu
• Klinika za zaštitu djece u Zagrebu
• Tehničko veleučilište u Zagrebu
• udruga nastavnika „Suradnici u učenju“
• XV. gimnazija Zagreb.

UDRUGA NASTAVNIKA „SURADNICI U UČENJU“
Nacionalna kampanja „Sigurniji internet za djecu i mlade 2013.“

Udruga „Suradnici u učenju“ tijekom prošlih godina organizirala je niz aktivnosti s temom „Sigurniji internet za djecu i mlade“ te predstavljala Hrvatsku kao Odbor za sigurniji internet u organizaciji INSAFE. Prošlogodišnjoj kampanji odazvao se velik broj nastavnika i studenata čiji su radovi predstavljeni na multimedijalnoj izložbi i u priručniku za metodiku „Kako učiti djecu o sigurnijem, prikladnijem i odgovornijem ponašanju na internetu“. U aktivnosti je izravno uključeno 5 000 sudionika te više od 50 000 neizravnih sudionika. Kao rezultat tih aktivnosti hrvatska nacionalna kampanja u konkurenciji 99 zemalja proglašena je 2013. najboljim odborom za sigurniji internet. Tema nacionalne kampanje bila je „Prava i obaveze na internetu“.

Policijski službenici zaduženi za prevenciju provode, u suradnji s policijskim službenicima za mlade na lokalnoj razini, različite programe usmjerene na prevenciju u njihovim lokalnim zajednicama s brojnim partnerima i udrugama civilnog društva kako bi spriječili različite oblike seksualnog zlostavljanja djece putem interneta i društvenih mreža (projekti „Živim život bez nasilja“, „Imam izbor“, „Zajedno možemo učiniti više“ i drugi).

Ministarstvo unutarnjih poslova 2011. pokrenulo je projekt u sklopu kampanje Vijeća Europe za zaustavljanje seksualnog nasilja na štetu djece sa širokim rasponom preventivnih aktivnosti na lokalnoj i regionalnoj razini naziva „Kiko i ruka“. U nekim policijskim odjelima i dalje su u tijeku određene aktivnosti. Glavne su aktivnosti obrazovne i informativne kao što su radionice i predavanja za djecu, roditelje i stručnjake te policijske službenike. Osim osposobljavanja, tematskih konferencija za medije, javnih debata, okruglih stolova, predstava za djecu, javnih promotivnih događaja u sklopu kampanje emitirane su i TV i radijske emisije. Uz promicanje Konvencije i njezinih ciljeva, cilj je takvih aktivnosti podizanje javne svijesti o toj temi i poticanje prijavljivanja takvih događaja kao i informiranje javnosti o tome gdje i kako zatražiti potrebnu pomoć. U kampanji su se koristili standardni promotivni materijali (letci, posteri i videozapisi) s logotipom „Kiko i ruka“.

8.3.2 Javno-privatno partnerstvo (JPP)

Hrvatska se u prevenciji i borbi protiv kiberkriminaliteta ne koristi javno-privatnim partnerstvom na formalni način (ugovori itd.). Međutim, postoje neke zajedničke kampanje, priopćenja za javnost, operativni sastanci i obrazovne aktivnosti.

8.4 Zaključci

- U Hrvatskoj, kao i u većini država članica, postoji općenita potreba da se poboljša obrazovanje novih zaposlenika te poboljša osposobljavanje iskusnih stručnjaka u području kiberkriminaliteta; čini se da je policijsko osposobljavanje uglavnom usmjereno na forenzičke aktivnosti te bi ga trebalo poboljšati čak i na području internetskih istraga;

- tijekom posjeta na licu mjesta tim je obaviješten da je u tijeku projekt za izradu osnovnog paketa za osposobljavanje namijenjenog osobama koje će prvo reagirati, tj. lokalnim policijskim službenicima kako bi mogli odgovarajuće odgovoriti na slučajeve kiberkriminaliteta; takvi projekti trebali bi se snažno poticati;

- pokusni Regionalni centar za osposobljavanje pravosudnih dužnosnika za borbu protiv kiberkriminaliteta, osnovan kao dio projekta IPA 2010 „Regionalna suradnja u borbi protiv kiberkriminaliteta u jugoistočnoj Europi“, i dalje je operativan u Zagrebu kao organizacijska jedinica nacionalne Pravosudne akademije; trebalo bi ga i dalje podupirati te poticati kao dobar primjer regionalne suradnje u području osposobljavanja;

- posjetom na licu mjesta pokazalo se da je sustavna i zajednička obuka policije, tužitelja i sudaca od presudne važnosti za osiguranje da svaki dionik sustava ima jasnu sliku o ulozi i potrebama drugih intervenijenata i tome kako detektirati, pribaviti i upotrijebiti e-dokaze.

9 KONAČNE NAPOMENE I PREPORUKE

9.1. Prijedlozi Hrvatske

Trebalo bi napomenuti da je Republika Hrvatska bila među prvim državama koja je ratificirala Konvenciju o kibernetičkom kriminalu Vijeća Europe i da je Tajništvo Vijeća Europe ocijenilo da Republika Hrvatska ispunjava odredbe Konvencije o kibernetičkom kriminalu u pogledu standardizacije i progona. Hrvatska također aktivno surađuje s drugim stranama te Konvencije unutar Vijeća Europe.

U studenome 2010. pokrenut je zajednički projekt EU-a i Vijeća Europe „CyberCrime@IPA - regionalna suradnja u borbi protiv kibernetičkog kriminaliteta“ koji je završio u lipnju 2013.; osim Republike Hrvatske, korisnici projekta bili su Albanija, Bosna i Hercegovina, Crna Gora, Kosovo, Makedonija, Srbija i Turska. Tijekom početne faze izrađen je detaljni izvještaj o stanju kriminaliteta u svakoj zemlji korisnici projekta te je uspostavljen temelj za poboljšanje zatečenog stanja. Po završetku projekta provedena je nova ocjena stanja kiberkriminaliteta te je utvrđeno da je u svim područjima projekta došlo do znatnih poboljšanja, pogotovo u bilateralnim i multilateralnim odnosima u regiji. Osim toga, utvrđeno je da je projekt rezultirao boljim razumijevanjem kiberkriminaliteta kao društvene prijetnje, da je u tu svrhu potrebno uvesti različite mjere na nacionalnoj, regionalnoj i međunarodnoj razini, uključujući strategije za borbu protiv kiberkriminaliteta te da je potrebno uložiti dodatne resurse u stručno osposobljavanje policijskih službenika. Posljedično, 15. veljače 2013. usvojena je Deklaracija o strateškim prioritetima u borbi protiv kiberkriminaliteta.

Nova Uredba o internoj organizaciji Ministarstva unutarnjih poslova stupila je na snagu 28. lipnja 2012. Njome se poziva na uspostavu Odjela za visokotehnološki kriminalitet u sklopu Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta. Osim toga, u sklopu Forenzičnog centra uvedeni su forenzički stručnjaci za digitalne dokaze. Na regionalnoj razini u svakoj policijskoj upravi djeluju posebno obučeni policijski službenici u službama/odjelima/sektorima za gospodarski kriminalitet koji su odgovorni za područje kiberkriminaliteta i povrede intelektualnog vlasništva. Osim toga, neka kaznena djela u području kiberkriminaliteta (u sklopu Konvencije o kiberkriminalitetu) obuhvaćena su drugim organizacijskim jedinicama: dječja pornografija na računalnom sustavu ili na mreži – Služba općeg kriminaliteta, Odjel maloljetničke delinkvencije; računalne prijevare - Služba organiziranog kriminaliteta; rasna i druga diskriminacija – protuterorizam. Kao članica NATO-a Hrvatska razvija vojnu i civilnu komponentu za obranu protiv prijetnji kiberkriminaliteta – Ministarstvo unutarnjih poslova uključeno je u rad multidisciplinarnih tijela čiji je cilj osigurati učinkovit nacionalni odgovor na prijetnju kiberkriminaliteta.

Osim toga, u suradnji sa svim tijelima odgovornima za kibersigurnost u Hrvatskoj, izrađeni su Nacionalna strategija kibernetičke sigurnosti i akcijski plan.

Hrvatska je provela projekt IPA 2011 „Jačanje kapaciteta Ministarstva unutarnjih poslova u borbi protiv kompjuterskog kriminaliteta“ zajedno sa španjolskim ministarstvom unutarnjih poslova i austrijskim saveznim ministarstvom unutarnjih poslova. Cilj tog projekta bilo je jačanje kapaciteta hrvatskog ministarstva unutarnjih poslova za učinkovitu borbu protiv kiberkriminaliteta na nacionalnoj i međunarodnoj razini, u skladu s povezanim politikama i strategijama EU-a. Projektne aktivnosti organizirane su oko dvije glavne komponente. Prvom komponentom namjeravalo se poboljšati aktivnosti Forenzičnog znanstvenog centra Ministarstva unutarnjih poslova provedbom dugoročne sheme osposobljavanja i programa za osposobljavanje instruktora o temama koje se tiču forenzične istrage kiberkriminaliteta. Druga komponenta bila je usmjerena na nove alate i tehnike koje se rabe u istragama kiberkriminaliteta s ciljem jačanja kapaciteta Uprave hrvatske kriminalističke policije u borbi protiv kiberkriminaliteta na nacionalnoj, regionalnoj, europskoj i međunarodnoj razini.

No, u Ministarstvu unutarnjih poslova i dalje nema dovoljno kapaciteta i resursa, pogotovo što se tiče broja policijskih službenika i razine financijske potpore. Također je potrebna jača integracija tijela kaznenog progona i drugih dionika.

Računalne prijevare najčešći su oblik kaznenih djela kiberkriminaliteta. Uredi državnog odvjetnika podigli su više od 96 optužnica za to kazneno djelo 2014. Osnivanje Regionalnog centra nesumnjivo je odlična ideja i primjer dobre prakse. Sada je na uključenim državama da pojačaju svoje napore u širenju te prakse.

Javni i civilni sektor poduzeli su brojne aktivnosti i projekte s ciljem prevencije zlostavljanja na internetu, pogotovo u školama. Projekt „Sigurnost djece na internetu“, proveden u pet različitih hrvatskih škola i financiran od Europske unije, rezultirao je izradom školskog kurikuluma o sigurnom korištenju internetom i više od 800 nastavnih sadržaja za učenike, nastavnike i roditelje.

Što se tiče zaštite osobnih podataka, Republika Hrvatska pokrenula je intenzivne mjere za podizanje javne svijesti (putem radionica, konferencija za medije i stručnih predavanja) kako bi se kiberkriminalitet smanjio na najmanju mjeru.

U sklopu Operativnog akcijskog plana (OAP) za 2015. prioriteta G EMPACT-a „Kiberkriminalistički napadi“ utvrđen je strateški cilj 5. „doprinijeti uspostavi koordiniranog multidisciplinarnog mehanizma za odgovor u slučaju ozbiljnog kibernapada s prekograničnom dimenzijom, uz dobro definirane uloge, odgovornosti i postupke“. Projektni tim čine HR, SI, DE, PT, IE, EUROPOL, EUROJUST, DG HOME i EUCTF, te on sudjeluje u operativnoj aktivnosti 5.1. „izrada smjernica i/ili operativnih postupaka za poboljšanje operativnih nacionalnih kontaktnih točaka (NCP) za razmjenu informacija u skladu s člankom 13. točkom (b) Direktive 2013/40/EU o napadima na informacijske sustave”.

Ta je aktivnost trenutačno jedina aktivnost osmišljena za provedbu strateškog cilja br. 5. Operativne nacionalne kontaktne točke (NCP) za razmjenu informacija u skladu s člankom 13. Direktive 2013/40/EU o napadima na informacijske sustave osmišljene su za brz odgovor na zahtjeve drugih država članica u pogledu zadržavanja podataka, pronalaženja sumnjivih osoba ili informacija koje su potrebne za provođenje kriminalističkih istraga o kibernapadima. Brza razmjena informacija važna je komponenta koordiniranog multidisciplinarnog mehanizma za odgovor u slučaju ozbiljnog kibernapada s prekograničnom dimenzijom, uz dobro definirane uloge, odgovornosti i postupke.

Prekogranična dimenzija glavno je obilježje kibernapada. Počinitelji su iz jedne zemlje, poslužitelj putem kojeg se čini kazneno djelo nalaze se u drugoj zemlji, a žrtve se obično nalaze u različitim zemljama diljem svijeta. Kako bi se učinkovito borilo protiv kiberkriminaliteta kojim se bave skupine organiziranog kriminala, suradnja među zemljama mora se odvijati u realnom vremenu, tijekom počinjenja kaznenog djela. Boljom suradnjom među državama članicama u očuvanju i prikupljanju dokaza i podataka trebao bi se osigurati uspjeh istraga kiberkriminaliteta s prekograničnom dimenzijom. Rezultat te aktivnosti bit će smjernice i/ili operativni postupci za poboljšanje operativnih nacionalnih kontaktnih točaka (NCP) za razmjenu informacija. Smjernice i/ili operativni postupci trebali bi se ugraditi u svakodnevne aktivnosti NCP-ova država članica. Pokazatelj uspjeha trebao bi biti broj NCP-ova koji je usvojio smjernice i/ili operativne postupke. Hrvatska je voditeljica aktivnosti i surađuje s državama članicama na osiguranju učinkovite razmjene informacija među državama članicama.

Hrvatske su vlasti kao primjere dobre prakse navele „Kiberkoaliciju“ u sklopu NATO-a, uključenost u EMPACT, FP Cyborg, suradnju u operaciji BUG BYTE itd. Sudjelovanje u međunarodnim operacijama za nas je vrlo vrijedno iskustvo te nam pruža dobru priliku za praćenje nacionalnih kapaciteta za odgovor na izazove uslijed velikih operacija i projekata kiberkriminaliteta.

Među primjerima dobre prakse u području prevencije svakako su organiziranje događaja kojima se podiže svijest javnosti i stručnjaka. Kao odgovor, Hrvatska je poduzela nekoliko akcija za ublažavanje botneta i zaustavila širenje zlonamjernog softvera na svojem području.

Hrvatske vlasti rekle su da im za učinkovite mjere u borbi protiv kiberkriminaliteta trebaju dostatni financijski, ljudski i tehnički resursi. Zakonodavstvo mora držati korak s novim i brzorastućim tehnologijama koje često dovode do novih oblika kiberprijetnji. Preventivne aktivnosti trebale bi se intenzivirati kao i suradnja među svim dionicima kibersigurnosti.

Bolja i brža razmjena informacija (npr. analiza zlonamjernog softvera), formaliziranje suradnje i razmjena informacija među vladinim CERT timovima država članica EU-a.

9.2 Preporuke

Što se tiče praktične provedbe Okvirne odluke i direktiva i njihove primjene, stručni tim uključen u ocjenjivanje Hrvatske mogao je odgovarajuće preispitati sustav o toj zemlji.

Hrvatska bi 18 mjeseci nakon ocjenjivanja trebala dalje postupati prema preporukama iz ovog izvješća te izvijestiti Radnu skupinu za opće poslove uključujući evaluacije (GENVAL) o napretku.

Ocjenjivački tim smatrao je da bi bilo prikladno dati nekoliko prijedloga hrvatskim tijelima. Osim toga, na temelju različitih primjera dobre prakse daju se i odgovarajuće preporuke EU-u, njegovim institucijama i agencijama, a posebno Europolu.

9.2.1 Preporuke za Hrvatsku

1. Hrvatsku se potiče da u potpunosti provede Nacionalnu strategiju kibernetičke sigurnosti i njezin akcijski plan;

2. Hrvatska bi trebala razviti mehanizme za dostavljanje detaljne, standardizirane i sveobuhvatne statistike o istragama, gonjenju i osuđujućim presudama u području kiberkriminaliteta na nacionalnoj razini te u odnosu na međunarodnu suradnju; Hrvatska bi osobito trebala dovršiti i provesti rezultate projekta IPA 2010 za razvoj IT sustava za međunarodnu pravnu pomoć (ILA) u prikupljanju statističkih podataka o uzajamnoj pravnoj pomoći i pravosudnoj suradnji koja uključuje kaznena djela kiberkriminaliteta i učiniti ga u potpunosti operativnim;

3. Hrvatska bi trebala znatno ojačati svoje ljudske i tehničke resurse kako bi se borila protiv kiberkriminaliteta, pogotovo u istražnim i forenzičkim policijskim službama;

4. Hrvatska bi se trebala potaknuti na poboljšanje koordinacije među različitim dionicima koji su uključeni u borbu protiv kiberkriminaliteta na nacionalnoj razini;

5. Hrvatska bi trebala poboljšati kako općenito tako i usmjereno napredno osposobljavanje u području kiberkriminaliteta za sve policijske službenike, suce i tužitelje na svim razinama, osobito razmjenom informacija i najbolje prakse između svih uključenih tijela putem zajedničkih obrazovnih aktivnosti;

6. Hrvatska bi trebala nastaviti podupirati, što više može, vrlo korisne aktivnosti regionalnog osposobljavanja pokusnog Regionalnog centra za osposobljavanje pravosudnih dužnosnika za borbu protiv kiberkriminaliteta iz Zagreba;

7. Prema Nacionalnoj strategiji kibernetičke sigurnosti koja za cilj ima „kontinuirano unapređivanje nacionalnog zakonodavnog okvira, uzimajući u obzir međunarodne obveze“, Hrvatska bi trebala dodatno analizirati svoje zakonodavstvo i praksu, osobito u pogledu uvođenja novih istražnih tehnika i kako bi se uzeli u obzir novi trendovi u kiberkriminalitetu (poput virtualnih valuta);

8. Hrvatska bi trebala razmotriti stvaranje mreže kontaktnih točaka za tužitelje koji su posebno osposobljeni u području kiberkriminaliteta na svim razinama tužiteljstva kako bi se poduprlo širenje informacija i najbolja praksa u području kiberkriminaliteta; također je potrebno uspostaviti službene kontaktne točke za sudove;

9. Hrvatska bi trebala promicati izravne kontakte među pravosudnim vlastima u međunarodnoj suradnji u području kiberkriminaliteta;

10. Hrvatska bi trebala razmotriti izradu priručnika o najboljoj praksi, prilagođenog korisnicima, za lokalne policijske službenike kao osobe koje će prve reagirati i za ostale nespecijalizirane policijske službenike;

9.2.2 Preporuke Europskoj uniji, njezinim institucijama i drugim državama članicama

Države članice i institucije Europske unije trebale bi:

11. istražiti mogućnost stvaranja zajedničkih statističkih nazivnika u području kiberkriminaliteta, uključujući usklađenu metodologiju, metode za prikupljanje podataka i procjenu na razini Europske unije;

12. potaknuti organizaciju operativno usmjerenog osposobljavanja na razini EU-a o cijelom životnom ciklusu kiberkriminaliteta gdje bi govornici i polaznici bili policijski službenici, tužitelji i suci te, prema potrebi, stručnjaci iz privatnog sektora;

13. razmotriti načine za poboljšanje vanjske suradnje u području kiberkriminaliteta s trećim zemljama, osobito važnijim susjedima i partnerima;

Europska komisija trebala bi:

14. aktivnije sudjelovati u sedmom krugu uzajamnih procjena kiberkriminaliteta;

15. razmotriti načine za potporu, osobito putem odgovarajućeg sufinanciranja, vrlo korisnih aktivnosti pokusnog Regionalnog centra za obuku pravosudnih dužnosnika o suzbijanju kibernetičkog kriminala u Zagrebu, Hrvatskoj;

16. razmotriti mogućnost davanja tehničkih sredstava potrebnih za suzbijanje kiberkriminaliteta nadležnim tijelima država članica, osobito davanje sredstava za nabavu visokotehnološkog hardvera i softvera za bolje utvrđivanje i pribavljanje e-dokaza; jedna dodana vrijednost toga jest da bi se time omogućilo tijelima država članica da rade i surađuju na usporedivim e-dokazima.

9.2.3 Preporuke Eurojustu/Europolu/ENISA-i i EJTN-u

17. Europska pravosudna mreža u kaznenim stvarima trebala bi uspostaviti redovite zajedničke programe osposobljavanja za policijske službenike, tužitelje i suce u području kiberkriminaliteta; to bi također bilo napravljeno u koordinaciji i suradnji s Eurojustom i Europolom;

18. Europol i Eurojust trebali bi nastaviti i ojačati, koliko god je to moguće, svoj aktivan doprinos sedmom krugu uzajamnih ocjena svih država članica;

19. Europol bi trebao nastaviti poticati blisku suradnju među tijelima kaznenog progona država članica na tehničkom planu putem posebnih radionica ili sastanaka o posebno definiranim zadacima (botneti, Bitcoin, novac koji se pere putem posrednika, prijetnje uslijed zlonamjernog softvera, itd.);

20. Eurojust bi trebao nastaviti pružati potporu državama članicama u području borbe protiv kiberkriminaliteta u sklopu svog mandata, pogotovo putem koordinacijskih sastanaka kao i podupiranjem razmjene najbolje prakse.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

Tuesday 29 September 2015

Ministry of the Interior – General Police Directorate

Visit to High-tech Crime Department

- Welcome
- Organisation and Operations of the High-tech Crime Department
- Case Study – ZeuS Banking Malware
- Overview – National 24/7 Contact Point for Urgent Requests
- Overview – Croatian Participation to EMPACT Cyber Attacks
- Overview – Child Sexual Abuse Online and Child Pornography
- Overview – Online Card Fraud

Visit to Zagreb Regional unit of the National Police Office for the Suppression of Corruption and Organised Crime

- Practical operations – Search and Seizure of Computer Data

Visit to the Centre for Forensic Science, Research and Expertise "Ivan Vučetić"

- Overview – Computer Forensic Examinations

Wednesday 30 September 2015

Visit to State Attorney's Office of the Republic of Croatia

- Presentation of the State Attorney's Office work in cybercrime matters

Visit to National CERT Office

- Introduction to National CERT, its role and operations
  - Legal framework
  - Internal organisation and operations of National CERT
  - Overview of everyday CERT operations

- Introduction to cyber threat intelligence and incident statistics

- International and domestic cooperation:
  - Current cyber defence projects
  -cooperation on EU and NATO cyber defence exercises
  -brief demonstration of National CERT internal and public services
  -overview of National CERT infrastructure

Thursday 1 October 2015

Visit to Ministry of Justice

- Presentation of the national legislation and the transposition/implementation of the EU legislation:
  - Sector for Criminal Law
  - Sector for Mutual Legal Assistance and Judicial Cooperation in Criminal Matters
- Court practice – Municipal court

Visit to the Office of the National Security Council

- Overview of the Organisation, Roles and Activities of the Office
- The New National Cyber Security Strategy
  - Internal Proceedings
  - Approach and Methodology
  - Goals and Implementation
- Discussion

End of the Visit

-/-

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 29 September 2015

Venue: **High-tech Crime Department**

Person interviewed/met	Organisation represented/Function
Ms Darko Žižek	Criminal Police Directorate/ Deputy Head
Ms Kristina Posavec	High-tech Crime Department/Head
Mr Renato Grgurić	High-tech Crime Department /Police officer
Mr Ivan Mijatović	High-tech Crime Department /Police officer
Mr Danko Salopek	Juvenile Delinquency and Crimes against Children Department/Police officer
Mr Željko Brkić	Organised Crime Unit/Police officer

Venue: **Zagreb Regional unit of the National Police Office for the Suppression of Corruption and Organised Crime**

Person interviewed/met	Organisation represented/Function
Mr Zoran Filipović	Zagreb Regional Unit of the National Police Office for the Suppression of Corruption and Organised Crime/Head
Mr Dragan Marić	Zagreb Regional Unit of the National Police Office for the Suppression of Corruption and Organised Crime/Crime Analysis officer
Mr Robert Pešt	Zagreb Regional Unit of the National Police Office for the Suppression of Corruption and Organised Crime/ Crime Analysis officer

Venue: **Centre for Forensic Science, Research and Expertise "Ivan Vučetić"**

Person interviewed/met	Organisation represented/Function
Mr Saša Krnjašić	Centre for Forensic Science, Research and Expertise "Ivan Vučetić" *I* Computer Forensic Expert

Meetings on 30 September 2015

Venue: **State Attorney's Office of the Republic of Croatia**

Person interviewed/met	Organisation represented/Function
Mr Dubravko Palijaš	Chief State Attorney's Office/ Deputy

Venue: **National CERT Office**

Person interviewed/met	Organisation represented/Function
Mr Darko Perhoč	National CERT/Head of National CERT
Mr Tibor Kulcar	National CERT/Computer Security Expert

Meetings on 1 October 2015

Venue: **Ministry of Justice**

Person interviewed/met	Organisation represented/Function
Mrs Sanja Nola	Assistant Minister for Criminal Law and Probation
Mrs Ana Kordej	Head of the Sector for Criminal Law
Mr Dinko Kovačević	Head of the Service for Criminal Law Regulations
Mr Hrvoje Bozić	Senior advisor - specialist in the Service for Criminal Law Regulations

Mr Mislav Matić	Senior administrative advisor in the Department for Regulations of Criminal Procedural Law, Juvenile Law and the Execution of Criminal Sanctions
Mr Bojan Ernjakovic	Senior expert advisor in the Department for Extradition and Mutual Legal Assistance in Criminal Matters
Mrs Cornelija Ivanušić	Judge of the Municipal Court in Velika Gorica
Mrs Dasla Leppee Pažanin	Head of the Service for European Affairs in the Directorate for European Affairs, International and Judicial cooperation

Venue: **The Office of the National Security Council**

Person interviewed/met	**Organisation represented/Function**
Mr Aleksandar Klaić	Assistant Director for Information Assurance
Mr Vinko Kuculo	Senior Advisor in Department for Planning and Oversight of Information Assurance

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN CROATIAN OR OTHER ORIGINAL LANGUAGE	FULL NAME IN CROATIAN OR ORIGINAL LANGUAGE	ENGLISH
CEPOL			European Police College
CERT			Computer Emergency Response Team
CMS			Case Management System
CoE			Council of Europe
CSA			Child Sexual Exploitation
ECJ			Court of Justice of the European Union
EC3			European Cybercrime Centre
EGTEC			European Cybercrime Training and Education Group
EJN			European Judicial Network
EJTN			European Judicial Training Network
EMPACT			European Multidisciplinary Platform Against Criminal Threats
ENISA			European Union Agency for Network and Information Security
EUCTF			European Union Cybercrime Task Force

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN CROATIAN OR OTHER ORIGINAL LANGUAGE	FULL NAME IN CROATIAN OR ORIGINAL LANGUAGE	ENGLISH
EUROJUST			European Unit Judicial Cooperation Unit
EUROPOL			European Police Office
FBI			United States Federal Bureau of Investigations
GENVAL			Working Party on General Matters including Evaluations
ICSE			Interpol's International Child Sexual Exploitation Database
ICT			Information and Communications Technology
INTERPOL			International Criminal Police Organization
IOCTA			Internet Organised Crime Threat Assessment
IOT			Internet of Things
IP			Internet Protocol
IPR			Intellectual Property Rights
IT			Information Technology
J-CAT			Joint Cybercrime Action Task Force
JIT			Joint Investigation Team
JHA			Justice and Home Affairs
LEA			Law Enforcement Authorities
MLA			Mutual Legal Assistance

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN CROATIAN OR OTHER ORIGINAL LANGUAGE	FULL NAME IN CROATIAN OR ORIGINAL LANGUAGE	ENGLISH
MLAT			Mutual Legal Assistance Treaty
MoJ			Ministry of Justice
NAW			Nordic Arrest Warrant
NGO			Non-Governmental Organisation
PPP			Public/Private Partnership
SCADA			Supervisory Control and Data Acquisition
SPACE			EC3's restricted virtual platform
SPOC			Single Point of Contact
TOR			The Onion Router
VPN			Virtual Private Network
VPS			Virtual Private Server