Na osnovu člana 45. stav 1. Zakona o Vladi („Službeni glasnik PC”, br. 55/05, 71/05 – ispravka, 101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US, 44/14 i 30/18 – dr. zakon),

Vlada donosi

STRATEGIJU ZA BORBU PROTIV VISOKOTEHNOLOŠKOG KRIMINALA
za period 2019-2023. godine

1. UVODNI DEO

Republika Srbija je u obavezi da donese i sprovodi strategiju i akcioni plan za efektivno rešavanje visokotehnološkog kriminala u skladu sa strateškim i operativnim pristupom Evropskoj uniji (EU) u pogledu visokotehnološkog kriminala. Navedena obaveza prevashodno proizilazi iz Pregovaračkih merila za Poglavlje 24 – Pravda, sloboda, bezbednost. Evropska Unija je konstatovala da je Republika Srbija ratifikovala Konvenciju o visokotehnološkom kriminalu (sačinjena u Budimpešti, engl. *Budapest Convention*) 2009. godine i pozvala Republiku Srbiju da dodatno uskladi svoje zakonodavstvo sa Direktivom *2013/40/EU* o napadima na informacione sisteme.

Ministarstvo unutrašnjih poslova je, u skladu sa Zakonom o ministarstvima („Službeni glasnik RS”, br. 44/14, 14/15, 96/15 – dr. zakon i 62/17) nosilac izrade navedenog strateškog dokumenta u saradnji sa ostalim državnim institucijama, tj. zainteresovanim stranama.

U planu za podršku transformacije Zapadnog Balkana u okviru Strategije za verodostojnu perspektivu proširenja i pojačanu saradnju sa državama sa područja Zapadnog Balkana istaknuta je potreba za povećanom podrškom u izgradnji kapaciteta u oblasti visokotehnološkog kriminala, uključujući saradnju sa Evropskom grupom za trening i edukaciju o visokotehnološkom kriminalu i buduće učešće u okviru Agencije za evropsku mrežu i informacionu bezbednost.

U okviru Akcionog plana za Poglavlje 24 – Pravda, sloboda i bezbednost, gde je nosilac aktivnosti **Ministarstvo unutrašnjih poslova**, nalaze se tri preporuke sa osam definisanih aktivnosti, koje Republika Srbija treba da ispuni u okviru pristupnog procesa u EU, sa fokusom na unapređenje organizacionih, kadrovskih i tehničkih kapaciteta, analiziranja trenutnog normativnog i organizacionog okvira i preduzimanja radnji u cilju usaglašavanja sa pravnim tekovinama EU u oblasti visokotehnološkog kriminala i ojačavanje saradnje između državnih organa i institucija. Imajući u vidu da je jedna od glavnih karakteristika dela visokotehnološkog kriminala njihova transnacionalna priroda, od procesa evropskih integracija se očekuje povećanje ekspeditivnosti rada u predmetima visokotehnološkog kriminala, u smislu bržeg protoka informacija potrebnih za otkrivanje i gonjenje učinilaca krivičnih dela, te bržeg odgovaranja po međusobnim zahtevima za pružanje međunarodne pravne pomoći, a sve kroz jačanje kapaciteta državnih organa Republike Srbije, a naročito Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala.

Pored navedenih preporuka, Republika Srbija je nakon otvaranja Poglavlja 24 – Pravda, sloboda i bezbednost dobila prelazno merilo koje ima za cilj izradu Strategije za borbu protiv visokotehnološkog kriminala i koje glasi: „Srbija priprema, donosi i sprovodi strategiju i akcioni plan za efektivnu borbu protiv visokotehnološkog kriminala u skladu sa strateškim i operativnim pristupom EU u pogledu visokotehnološkog kriminala. Srbija ojačava svoje operativne kapacitete (u pogledu osoblja i opreme u Jedinici za visokotehnološki kriminal) kako bi rešila problem visokotehnološkog kriminala i usklađuje

svoje zakonodavstvo sa relevantnim pravnim tekovinama EU, uključujući u pogledu seksualnog zlostavljanja dece na internetu, obezbeđuje specijalizovane obuke i podiže nivo svesti javnosti i među državnim službenicima po pitanju visokotehnološkog kriminala".

Na osnovu navedenih međunarodnih i nacionalnih dokumenata iz ove oblasti Republika Srbija je donela prvu Strategiju za borbu protiv visokotehnološkog kriminala sa pratećim Akcionim planom za njeno sprovođenje.

Strategija predstavlja nastavak i proširenje aktivnosti kojima je cilj jačanje efikasnosti svih subjekata u oblasti suzbijanja visokotehnološkog kriminala u Republici Srbiji. Posebno je usmerena na nastavak usklađivanja zakonodavstva s međunarodnim standardima, dalje unapređenje kapaciteta nosilaca borbe protiv visokotehnološkog kriminala, unapređenje preventivnog i proaktivnog pristupa društva u suzbijanju svih oblika kriminala u toj oblasti, unapređenje interresorne saradnje u društvu, kao i saradnje Republike Srbije na regionalnom i međunarodnom nivou u oblasti visokotehnološkog kriminala.

Ispunjenjem strateških ciljeva i daljim razvojem međunarodne i regionalne saradnje u ovoj oblasti, Republika Srbija će doprineti ne samo sigurnosti u zemlji nego i u regionu. Strategija za borbu protiv visokotehnološkog kriminala predstavlja dokument kojim Vlada utvrđuje institucionalni odgovor na pojavne oblike visokotehnološkog kriminala, definiše uloge i nadležnosti državnih organa, identifikuje ciljeve i utvrđuje osnovne pravce delovanja na suzbijanju svih vidova visokotehnološkog kriminala.

U ovoj strategiji određene imenice navedene su u muškom rodu, a koriste se kao neutralne za muški i ženski rod.

Strategija se donosi na period od 2019. do 2023. godine.

Akcioni plan 2019-2020. za sprovođenje Strategije za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine čini njen sastavni deo.

2. OSNOVNI POJMOVI

Zakonodavni okvir Republike Srbije definiše visokotehnološki („sajber") kriminal u članu 2. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS", br. 61/05 i 104/09), navodeći da visokotehnološki kriminal u smislu tog zakona predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Pod proizvodima u elektronskom obliku posebno se podrazumevaju računarski programi i autorska dela koja se mogu upotrebiti u elektronskom obliku.

Međunarodni slobodno dostupni izvori navode da visokotehnološki, tj. „sajber" kriminal predstavlja oblik kriminalnog ponašanja kod koga se korišćenje računarske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, gde se računar ili računarska mreža upotrebljavaju kao sredstvo ili cilj izvršenja.

Računari i računarska tehnologija se mogu zloupotrebljavati na razne načine, a sam kriminalitet koji se realizuje pomoću računara može imati oblik bilo kog od tradicionalnih vidova kriminaliteta, kao što su krađe, utaje, pronevere, dok se podaci koji se neovlašćeno pribavljaju zloupotrebom informacionih sistema mogu na razne načine koristiti za sticanje protivpravne koristi.

Može se konstatovati da je visokotehnološki kriminal takav oblik kriminalnog ponašanja kod koga je visokotehnološko okruženje u kome se računarske mreže pojavljuju kao sredstvo, cilj, dokaz ili okruženje izvršenja krivčnog dela. Pri tome se pod „sajber prostorom" podrazumeva ili vrsta „zajednice" sačinjene od mreže računara u

kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova ili „prostor koji kreiraju kompjuterske mreže".

Zakonom o potvrđivanju Konvencije o visokotehnološkom kriminalu („Službeni glasnik RS – Međunarodni ugovori", broj 19/09), u članu 1. propisane su sledeće definicije od značaja za visokotehnološki kriminal:

- „računarski sistem" označava svaki uređaj ili grupu međusobno povezanih ili zavisnih uređaja, od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka;
- „računarski podatak" označava svako predstavljanje činjenica, informacija ili koncepata u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju;
- „davalac usluge" označava svaki javni ili privatni subjekt koji korisnicima svoje usluge pruža mogućnost komuniciranja preko računarskog sistema i svaki drugi subjekt koji obrađuje ili čuva računarske podatke u ime takve komunikacione usluge ili korisnika takve usluge;
- „podatak o saobraćaju" označava svaki računarski podatak koji se odnosi na komunikaciju preko računarskog sistema, proizvedenu od računarskog sistema koji je deo lanca komunikacije, a u kojoj su sadržani podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju ili vrsti predmetne usluge.

Krivičnim zakonikom („Službeni glasnik RS", br. 85/05, 88/05 – ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14 i 94/16), u članu 112. propisane su sledeće definicije od značaja za visokotehnološki kriminal:

- „pokretnom stvari" se smatra i svaka proizvedena ili sakupljena energija za davanje svetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program;
- „računarski podatak" je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju;
- „računarskom mrežom" smatra se skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke;
- „računarskim programom" smatra se uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara;
- „računarski virus" je zlonamerni računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka;
- „ispravom" se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice koja ima značaj za pravne odnose, kao i računarski podatak;
- spis, pismo, pošiljka i dokument mogu biti i u elektronskom obliku;
- „računar" je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke;
- „računarski sistem" je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka.

Zakonikom o krivičnom postupku („Službeni glasnik RS”, br. 72/11, 101/11, 121/12, 32/13, 45/13 i 55/14), u članu 2. su propisane sledeće definicije od značaja za visokotehnološki kriminal:

- „elektronski zapis” je zvučni, video ili grafički podatak dobijen u elektronskom (digitalnom) obliku;
- „elektronska adresa” je niz znakova, slova, cifara i signala koji je namenjen za određivanje odredišta veze;
- „elektronski dokument” je skup podataka koji je određen kao elektronski dokument u skladu sa zakonom koji uređuje elektronski dokument;
- „elektronski potpis” je skup podataka koji je određen kao elektronski potpis, u skladu sa zakonom koji uređuje elektronski potpis.

3. ANALIZA STANjA SA PREPORUKAMA

3.1. Međunarodno-pravni i međunarodni strateški okvir

Ustavom Republike Srbije je propisano da su opšteprihvaćena pravila međunarodnog prava i potvrđeni međunarodni ugovori sastavni deo pravnog poretka Republike Srbije i neposredno se primenjuju, s tim da potvrđeni međunarodni ugovori moraju biti u skladu s Ustavom.

1. Konvencija o visokotehnološkom kriminalu (Budimpešta 2001)

Konvencija trenutno predstavlja jedini međunarodno-pravno priznat i kontinentalno raširen pravni instrument u oblasti visokotehnološkog kriminala, koji u svom tekstu objedinjuje precizno određene, i što je još bitnije, upotrebljive i savremene metode postupanja nadležnih državnih organa, ali ne samo njih, već i drugih institucija i organizacija u ovoj oblasti, sve u cilju uspostavljanja delotvornog međunarodnog mehanizma, koji je sastavljen od više organskih celina na nivou pojedinih zemalja koje su potpisale ili ratifikovale ovu Konvenciju.[1] Konvencija za svoj cilj ima, na prvom mestu, harmonizaciju domaćih materijalno krivično pravnih odredbi u oblasti visokotehnološkog kriminala, omogućavanje domaćem krivičnom procesno-pravnom okviru da nadležnim državnim organima pruži ovlašćenja koja su neophodna za otkrivanje i gonjenje izvršilaca ovih krivičnih dela, kao i uspostavljanje brzog i efektivnog okvira međunarodne saradnje u ovoj oblasti.[2]

Konvencija o visokotehnološkom kriminalu je osmišljena u cilju sprečavanja dela koja su usmerena protiv integriteta, poverljivosti i dostupnosti kompjuterskih sistema, mreža i podataka, a samim tim i sprečavanja zloupotrebe tih sistema, mreža i podataka tako što će se pokrenuti kaznene mere za takvo delovanje kao što je opisano u Konvenciji i pri čemu će se primeniti kazne za efikasnu borbu protiv krivičnih dela, i na taj način će se na unutrašnjem i međunarodnom nivou olakšati otkrivanje, istraga i gonjenje za izvršena krivična dela i omogućiti da se obezbede uslovi za brzu i pouzdanu međunarodnu saradnju.

U skladu sa Konvencijom, Republika Srbija odredila je dve kontakt tačke mreže 24/7 koje omogućavaju hitno reagovanje i razmenu podataka u predmetima visokotehnološkog kriminala među svim državama potpisnicama. Jedna kontakt tačka je

[1] VTK vodič, str. 21.
[2] VTK vodič, str. 23.

Posebni tužilac za visokotehnološki kriminal, dok je druga kontakt tačka Odeljenje za suzbijanje visokotehnološkog kriminala, pri Ministarstvu unutrašnjih poslova.

2. Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema (2003).

Osnovni cilj ovog protokola jeste da dopuni odredbe Konvencije o visokotehnološkom kriminalu u pogledu dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema.[3] On definiše pojam rasističkog i ksenofobičnog materijala i propisuje mere koje države članice treba da preduzmu na nacionalnom nivou.

3. Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (tzv. Lanzarot konvencija - Savet Evrope 2007. godine, stupila na snagu 2010. godine i ratifikovana iste godine od strane Republike Srbije)

Ovom konvencijom su, između ostalog, posebno definisana krivična dela u vezi sa dečijom pornografijom, kao posebnim oblikom seksualne eksploatacije i zloupotrebe dece. Pored toga, ova konvencija preporučuje da svaka strana potpisnica usvaja mere koje mogu biti neophodne da bi se osiguralo da lica, jedinice ili službe zadužene za istragu budu specijalizovane u oblasti borbe protiv seksualnog iskorišćavanja i seksualnog zlostavljanja dece ili da ta lica budu obučena u te svrhe (tzv. princip specijalnosti). Ona, takođe, propisuje da će svaka zemlja potpisnica preduzeti sve neophodne zakonodavne ili druge mere kako bi omogućila jedinicama istražnih službi da identifikuju žrtve krivičnih dela, posebno pomoću analize pornografskog materijala kao što su fotografije i audio-vizuelni zapisi emitovani ili stavljeni na raspolaganje pomoću informacione i komunikacione tehnologije.

4. Odluka Saveta Evropske unije o suzbijanju dečije pornografije na internetu 2000/375/JHA

Ovom odlukom je preporučeno da, ako je potrebno, a uzimajući u obzir upravnu strukturu svake države članice, mere za promovisanje efikasne istrage i krivičnog progona za krivična dela na tom području, mogu biti i ustanovljavanje posebnih jedinica pri organima nadležnim za izvršavanje zakona koja imaju potrebna stručna znanja i sredstva kako bi efikasno postupali na temelju informacija o mogućoj proizvodnji, obradi, distribuciji i posedovanju dečije pornografije. Ovom odlukom je preporučeno da države članice ustanove vlastiti sistem nadzora suzbijanja proizvodnje obrade, posedovanja i distribucije materijala s dečijom pornografijom.

5. Direktiva Evropskog parlamenta o borbi protiv seksualne zloupotrebe, seksualne eksploatacije i dečije pornografije 2011/92EU

Ovom direktivom se preporučuje državama članicama da preduzmu neophodne mere da omoguće istražnim jedinicama ili službama da identifikuju žrtve krivičnih dela (seksualna zloupotreba, seksualna eksploatacija, dečija pornografija i tzv. „grooming"),

[3] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, Art.1.

posebno analizom materijala dečije pornografije, kao što su fotografije i audio-video zapisi emitovani ili stavljeni na raspolaganje pomoću informacione i komunikacione tehnologije.

6. Direktiva 2013/40/EU Evropskog parlamenta i Saveta EU o napadima na informacione sisteme i zameni Okvirne odluke Saveta 2005/222/JHA

Ova direktiva se odnosi na napade usmerene protiv informacionih sistema. Njen cilj je da približi krivičnim zakonodavstvima zemalja članica EU oblast napada na informacione sisteme, uspostavljanjem minimalnih pravila koji se odnose na definiciju krivičnih dela i odgovarajućih krivičnopravnih sankcija, kao i unapređenje saradnje između nadležnih organa koji uključuju pripadnike policije i drugih specijalizovanih agencija za sprovođenje zakona članica EU, kao i nadležnih specijalizovanih agencija i tela same Evropske Unije, kao što su EUROJUST, EUROPOL ili njegov Evropski centar za borbu protiv sajber kriminala (EC 3), kao i uključivanje u rad Evropska agencija za bezbednost mreža i podataka (ENISA).[4]

7. Bezbednosna agenda Evropske unije za period od 2015. do 2020. godine

Bezbednosna agenda prepoznaje terorizam, organizovani kriminal i borbu protiv visokotehnološkog kriminala kao tri najozbiljnije pretnje po bezbednost EU i ključne prioritete kojima se treba baviti. Ona ima za cilj da iskoristi postojeće instrumente za saradnju nacionalnih policija i EU agencija, da te instrumente unapredi i obezbedi njihovo puno sprovođenje kroz sistematsku koordinaciju svih relevantnih aktera u borbi protiv terorizma. EU je ustanovila Inicijativu za borbu protiv terorizma na Zapadnom Balkanu (eng. Western Balkan Counter-Terrorism initiative), koja ima za cilj da pomogne zemljama Zapadnog Balkana u borbi protiv pretnji džihadista i ekstremizma, da onemogući onlajn komunikaciju terorista i njihovo finansiranje, kao i da poboljša bezbednost na državnim granicama.[5]

8. Strategija sajber bezbednosti Evropske unije iz 2013. godine – „Otvoren, bezbedan i zaštićen sajber prostor”

Predstavlja prvi sveobuhvatni dokument koji je EU izradila u ovoj oblasti. Ona predstavlja sveobuhvatnu viziju EU kako na najbolji način sprečiti i odgovoriti na sajber smetnje i napade, a sa druge strane omogućiti razvoj informacionih tehnologija. Ona promoviše poštovanje osnovnih EU vrednosti, definiše nedozvoljeno ponašanje, zagovara primenu postojećih međunarodnih propisa u oblasti visokotehnološkog kriminala, pomaže drugim državama izvan EU u izgradnji kapaciteta za borbu protiv visokotehnološkog kriminala i promoviše saradnju u ovoj oblasti.

9. IOCTA (Internet organised crime threat assessment 2017) – Procena pretnje od Internet organizovanog kriminala

Predstavlja četvrti po redu, godišnji izveštaj, Evropolovog centra za visokotehnološki kriminal koji pruža podatke o trenutnom stanju, trendovima i nastanku novih pretnji u oblasti visokotehnološkog kriminala. U izveštaju su prepoznate sledeće pretnje u oblasti visokotehnološkog kriminala i date preporuke:

[4] VTK vodič, str. 39.
[5] Nova bezbednosna agenda, str. 2

Kriminal koji zavisi od naprednih tehnologija – Organi za sprovođenje zakona moraju da nastave da se fokusiraju na aktere koji razvijaju i pružaju sredstva i usluge sajber kriminala, a u odnosu na ključne pretnje identifikovane u ovom izveštaju: programere ransomware-a, bankarske „trojanace" i druge „malvere" i dobavljače sredstava za DDoS[6] napad, usluge usmerene protiv antivirusna i „botnete". Organi za sprovođenje zakona i privatni sektor moraju nastaviti da rade zajedno na analizi pretnji i inicijativama prevencije, kao što je to slučaj sa projektom No More Ransom, kako bi se podigla svest, dao savet i besplatna sredstva za dešifrovanje žrtvama ransomware. Zaposleni u sektorima kritične infrastrukture moraju biti bolje obrazovani, pripremljeni i opremljeni za sprečavanje sajber napada, koristeći EU i nacionalne napore i resurse, naročito NIS direktivu i Opštu uredbu o zaštiti podataka (GDPR).

„Onlajn" seksualna eksploatacija dece - Zemlje članice EU treba da obezbede da je bilo koje istraživačko sredstvo ili mera koja se koristi za borbu protiv ozbiljnog i/ili organizovanog kriminala dostupno i koristi se u potpunosti u istraživanju „onlajn" seksualne eksploatacija dece (CSE). Sistemi za evidentiranje i analizu kriminala u zemljama članicama EU treba da se nadograde, kako bi bolje odražavali i beležili različite vrste „onlajn" seksualnih krivičnih dela, koja su prijavljena od strane dece ili su povezana sa decom, kao žrtvama. Od suštinskog je značaja održavati zajedničke, visokokvalitetne i višejezične aktivnosti prevencije i podizanja svesti na nivou cele EU, kako bi jake i efikasne poruke stigle do onih kojima su potrebne. Integracija u edukaciju, kao i edukacija roditelja takođe su neophodni.

Prevare vezane za plaćanje - Organi za sprovođenje zakona i privatni sektor treba da nastave da razvijaju inicijative zasnovane na međusobnoj saradnji i razmeni informacija u borbi protiv prevara vezanih za plaćanje, uključujući prevare u kojima kartice nisu prisutne, gradeći uspešne modele kao što su Global Airline Action Days i e-Commerce Action weeks.

„Onlajn" kriminalna tržišta - Organi za sprovođenje zakona treba da razviju globalno koordinisan strateški pregled pretnje „Darkneta", prate i razumeju nove pretnje i relevantna dešavanja. Takva analiza bi omogućila buduću koordinaciju globalne akcije za destabilizaciju i zatvaranje kriminalnih tržišta.

Preplitanje sajber kriminala i terorizma - Snažan odgovor na džihadističke sajber i „onlajn" pretnje zahteva koordiniranu akciju među mnoštvom zainteresovanih strana, organima za sprovođenje zakona, obaveštajnim agencijama, kao i privatnom sektoru i akademskoj zajednici, određujući džihadistička dela u kontekstu sajber kriminala.

Unakrsni faktori kriminala - Inovacije, u smislu proaktivnih i adaptivnih pristupa, strategije za borbu protiv kriminala, kao i saradnja u smislu učešća svih relevantnih partnera, treba da budu jezgro bilo kog odgovora na sajber kriminal. Postoji potreba da se nastavi razvijati koordinisana akcija na nivou EU i šire, kako bi se odgovorilo na sajber kriminal, učeći iz uspešnih operacija.

„Onlajn" trgovina falsifikovanom robom – Povreda prava intelektualne svojine je široko rasprostranjena i predstavlja fenomen koji je u stalnom porastu. Evropol i Zavod za intelektualnu svojinu Evropske unije (*EUIPO*) su, u julu 2016. godine, zajednički osnovali Koaliciju za koordinaciju kriminala u oblasti intelektualne svojine (IPC3) u cilju jačanja borbe protiv falsifikovanja i piraterije.

3.2. Usklađivanje politike Republike Srbije u oblasti visokotehnološkog kriminala sa politikom EU

[6] **DoS** (eng. Denial of Service) napad je napad na računarski servis kojim se korisnicima onemogući njegovo korištenje.

Republika Srbija je 2009. godine ratifikovala Konvenciju za visokotehnološki kriminal iz Budimpešte iz 2001. godine i Dodatni protokol, koja predstavljaju osnov EU Acquis u oblasti borbe protiv visokotehnološkog kriminala.

Strategijom za verodostojnu perspektivu proširenja i pojačanu saradnju sa državama sa područja Zapadnog Balkana iskazana je podrška regionu u izgradnji i razvoju institucionalnih i stručnih kapaciteta u oblasti visokotehnološkog kriminala.

Akcionim planom za Poglavlje 24 – Pravda, sloboda i bezbednost, čiji je nosilac **Ministarstvo unutrašnjih poslova**, predviđeno je usklađivanje sa zakonodavstvom EU u oblasti visokotehnološkog kriminala, a akcenat je na unapređenju organizacionih, kadrovskih i tehničkih kapaciteta, analizi trenutnog normativnog i organizacionog okvira i jačanju saradnje između državnih organa i institucija.

Posebni tužilac za visokotehnološki kriminal, kao predstavnik Republike Srbije, učestvuje u radu T-CY Komiteta Konvencije o visokotehnološkom kriminalu koji čine ovlašćeni predstavnici zemalja koje su ratifikovale navedenu konvenciju Saveta Evrope. Pored toga, Posebni tužilac je učestvovao u radu radne grupe ovog komiteta na izradi noveliranih uputstava za primenu Konvencije koja su postala sastavni deo izvornog teksta, čime je dat značajan doprinos razvoju međunarodnog prava u ovoj oblasti. Takođe, značajno je učestvovanje Posebnog tužioca u radu Grupe za prekogranični kriminal ove konvencije i u aktivnostima koje se tiču izrade daljih Preporuka i Smernica za primenu konvencije, a posebno izrade Drugog dodatnog protokola uz ovu konvenciju na temu međunarodne saradnje zemalja potpisnica.

Uprava za sprečavanje pranja novca aktivno učestvuje u sledećim pregovaračkim poglavljima o pristupanju EU:

- Poglavlje 4 – Slobodno kretanje kapitala – koje se, pre svega, odnosi na usklađivanje propisa iz oblasti kretanja kapitala i tekućih plaćanja, kao i na borbu protiv pranja novca i finansiranja terorizma. U oblasti sprečavanja pranja novca i finansiranja terorizma, zahteva se od banaka i drugih ekonomskih operatera da identifikuju klijente i prijave određene transakcije, za koje postoji sumnja da se radi o pranju novca ili finansiranju terorizma. Novac koji je predmet opisanih transakcija može proisteći i od krivičnih dela koja se dovode u vezu sa visokotehnološkim kriminalom.
- Poglavlje 23 – Pravosuđe i osnova prava – Jedan od osnovnih delova navedenog poglavlja je i borba protiv korupcije u kojoj Uprava aktivno učestvuje kroz praćenje i analizu transakcija lica, koje mogu biti povezane sa viskootehnološkim kriminalom.
- Poglavlje 24 – Pravda, sloboda i bezbednost – Jedan od delova ovog poglavlja je i borba protiv organizovanog kriminala u kojoj Uprava za sprečavanje pranja novca aktivno učestvuje. Visokotehnološki kriminal i pravni propisi koji se odnose na ovu problematiku su, takođe, predmet razgovora u okviru ovog poglavlja.

Privredna komora Srbije u ovom trenutku ima vodeću ulogu u formiranju federacije identiteta u okviru novih servisa e Uprave, što je jedan od osnova za uspostavljanje standardizovane razmene podataka u okviru evropskih integracija.

Ministarstvo trgovine, turizma i telekomunikacija vodi Pregovaračku grupu 10 – Informaciono društvo i mediji. U okviru usklađivanja sa pravnim okvirom EU u ovoj oblasti, Ministarstvo je zaduženo za transponovanje odredbi iz oblasti elektronskih komunikacija i informacionog društva. U godišnjem Izveštaju Evropske komisije o napretku Republike Srbije za 2016. godinu se ističe da je postignut izvestan napredak naročito sa usvajanjem Zakona o informacionoj bezbednosti kojim se uspostavljaju nadležni organi za informacionu bezbednost i nacionalni CERT (eng. CERT - Computer Emergency

Response Team, Tim za hitno reagovanje na napade na IKT sistem). Potrebno je da Republika Srbija izvrši potpuno usklađivanje Zakona o informacionoj bezbednosti sa Direktivom broj 2016/1148 o merama za visok zajednički nivo bezbednosti mrežnih i informacionih sistema u Evropskoj uniji i prema do sada utvrđenim rokovima navedeno bi trebalo da se završi do trećeg kvartala 2018. godine.

3. 3. Zakonski i strateški okvir visokotehnološkog kriminala u Republici Srbiji

3.3.1. Zakoni, međunarodni ugovori i podzakonski akti

Krivični zakonik („Službeni glasnik RS", br. 85/05, 88/05 - ispravka, 107/05 - ispravka, 72/09, 111/09, 121/12, 104/13, 108/14 i 94/16) propisuje sledeća krivična dela protiv bezbednosti računarskih podataka: oštećenje računarskih podataka i programa (član 298), računarska sabotaža (član 299), pravljenje i unošenje računarskih virusa (član 300), računarska prevara (član 301), neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302), sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303), neovlašćeno korišćenje računara ili računarske mreže (član 304), pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a). Za navedena krivična dela krivično gonjenje je u isključivoj nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. Takođe, u Krivičnom zakoniku se definiše značenje pojedinih izraza od važnosti za oblast visokotehnološkog kriminala.

Zakonik o krivičnom postupku („Službeni glasnik RS", br. 72/11, 101/11, 121/12, 32/13, 45/13 i 55/14) propisuje niz posebnih dokaznih radnji koje se mogu primeniti u krivičnim postupcima protiv učinilaca krivičnih dela iz stvarne nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. I u ovom zakoniku se definiše značenje izraza od važnosti za oblast visokotehnološkog kriminala.

Konvencijom o visokotehnološkom kriminalu („Službeni glasnik RS – Međunarodni ugovori", broj 19/09) predviđeno je uvođenje adekvatnih instrumenata kada je reč o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela, ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje. Takođe, predviđeno je osnivanje kontakt tačke ili tački „24/7 mreže" koja bi služila kao podrška policijskim i drugim organima zemalja koje su ratifikovale Konvenciju, kao kontakt za sva obaveštenja i početna tačka za sve zahteve koji se tiču procesuiranja i istraživanja krivičnih dela visokotehnološkog kriminala.

Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema („Službeni glasnik RS – Međunarodni ugovori", broj 19/09) predviđa inkriminisanje akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema. Njegova osnovna svrha je da se inkriminišu ponašanja koja nisu obuhvaćena Konvencijom, a koja se tiču širenja mržnje, netolerancije i netrpeljivosti prema rasnim, nacionanim, verskim i drugim grupama i zajednicama, korišćenjem računara kao sredstava komunikacije i širenja propagande.

Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja („Službeni glasnik RS – Međunarodni ugovori", broj 1/10)

reguliše sprečavanje i borbu protiv seksualnog iskorišćavanja i seksualnog zlostavljanja dece, kao i zaštitu prava dece – žrtava seksualnog iskorišćavanja i seksualnog zlostavljanja, te unapređenje nacionalne i međunarodne saradnje u borbi protiv seksualnog iskorišćavanja i seksualnog zlostavljanja dece.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS”, br. 61/05 i 104/09) definiše okvir za otkrivanje, krivično gonjenje i suđenje za krivična dela protiv bezbednosti računarskih podataka, intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara; krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu podvesti pod visokotehnološki kriminal.

Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije („Službeni glasnik RS”, broj 94/16) uređuje obrazovanje, organizaciju, nadležnost i ovlašćenja državnih organa i posebnih organizacionih jedinica državnih organa, radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela određena ovim zakonom. Krivična dela visokotehnološkog kriminala mogu imati elemenat organizovanosti.

Ispunjavajući preuzete obaveze iz Konvencije o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja, Republika Srbija je donela **Zakon o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnim licima** („Službeni glasnik RS”, broj 32/13), a kojim su prvi put uvedene posebne mere prema učiniocima krivičnih dela protiv polne slobode prema maloletnim licima, između ostalog, kao što su obavezno javljanje nadležnom organu policije i Uprave za izvršenje krivičnih sankcija, odnosno zabrana posećivanja mesta na kojima se okupljaju maloletna lica (vrtići, škole i sl.), kao i da je propisano posebno vođenje evidencija osuđenih lica.

Zakon o elektronskim komunikacijama („Službeni glasnik RS”, br. 44/10, 60/13 - US i 62/14) uređuje uslove i način za obavljanje delatnosti u oblasti elektronskih komunikacija, nadležnosti državnih organa u oblasti elektronskih komunikacija, zaštitu prava korisnika i pretplatnika, bezbednost i integritet elektronskih komunikacionih mreža i usluga, tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka, nadzor nad primenom ovog zakona, mere za postupanje suprotno odredbama ovog zakona, kao i druga pitanja od značaja za funkcionisanje i razvoj elektronskih komunikacija u Republici Srbiji.

Zakonom o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16 i 94/17) se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornost pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite. Zakonom je određeno da je **Ministarstvo trgovine, turizma i telekomunikacija** nadležno za poslove informacione bezbednosti. U cilju ostvarivanja saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti Vlada osniva **Telo za koordinaciju poslova informacione bezbednosti**, koje u svom radu formira **stručne**

radne grupe Tela za koordinaciju. Poslove prevencije i zaštite od bezbednosnih rizika u IKT (informaciono-komunikacionim tehnološkim) sistemima u Republici Srbiji vrši **Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima** (Nacionalni CERT), za čiji rad je nadležna **Regulatorna agencija za elektronske komunikacije i poštanske usluge**. [7] **Poseban centar za prevenciju bezbednosnih rizika u IKT sistemima** (Poseban CERT) obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično. **Centar za bezbednost IKT sistema u republičkim organima** (CERT republičkih organa) obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima republičkih organa, izuzev IKT sistema samostalnih operatora. Zakonom o informacionoj bezbednosti definisani su **IKT sistemi od posebnog značaja**, kao i **samostalni operatori IKT sistema** (Ministarstvo unutrašnjih poslova, Ministarstvo odbrane, Ministarstvo spoljnih poslova, službe bezbednosti) koji su u obavezi da u skladu sa zakonom donesu akt o bezbednosti IKT sistema. Ministarstvo unutrašnjih poslova i Ministarstvo odbrane, kao samostalni operatori IKT sistema izradili su Predloge akta o bezbednosti, koji još uvek nisu doneti. Aktom o bezbednosti određuju se mere zaštite, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja.

Zakon o odgovornosti pravnih lica za krivična dela („Službeni glasnik RS”, broj 97/08) uređuje uslove odgovornosti pravnih lica za krivična dela, krivične sankcije koje se mogu izreći pravnim licima i pravila postupka u kojem se odlučuje o odgovornosti pravnih lica, izricanju krivičnih sankcija, donošenju odluke o rehabilitaciji, prestanku mere bezbednosti ili pravne posledice osude i izvršenju sudskih odluka.

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima („Službeni glasnik RS”, broj 20/09) uređuje postupak pružanja međunarodne pravne pomoći u krivičnim stvarima u slučajevima kada ne postoji potvrđen međunarodni ugovor ili kada određena pitanja njime nisu uređena.

Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine („Službeni glasnik RS”, br. 46/06 i 104/09 – dr. zakoni) uređuje posebna ovlašćenja organa državne uprave i organizacija koje vrše javna ovlašćenja radi efikasne zaštite prava intelektualne svojine u skladu sa propisima kojima se uređuje pravo intelektualne svojine.

Zakon o sprečavanju pranja novca i finansiranja terorizma („Službeni glasnik RS”, broj 113/17) propisuje mere i radnje koje Uprava za sprečavanje pranja novca preduzima ukoliko postoji sumnja da će novac koji je proistekao iz nekog krivičnog dela iz kojeg proističe imovinska korist (između ostalih i krivična dela koja se dovode u vezu sa visokotehnološkim kriminalom) biti integrisan u legalne novčane tokove.

Zakon o ograničavanju raspolaganja imovinom u cilju sprečavanja terorizma i širenja oružja za masovno uništenje („Službeni glasnik RS”, br. 29/15, 113/17 i 41/18), u članu 9. propisuje da Uprava za sprečavanje pranja novca može da zahteva podatke o označenom licu i njihovoj imovini od državnih organa, organizacija i lica kojima su poverena javna ovlašćenja, koji su dužni da podatke dostave. Uprava bez odlaganja o navedenom licu sačinjava izveštaj koji dostavlja ministru nadležnom za poslove finansija,

[7] Zakon o informacionoj bezbednosti, član 14.

koji ako utvrdi da se radi o označenom licu i imovini koja podleže ograničavanju raspolaganja, rešenjem nalaže ograničavanje raspolaganja imovinom tog lica. Ovo se odnosi i na slučajeve kada se izvršenje krivičnog dela označenih lica dovodi u vezu sa visokotehnološkim kriminalom.

Zakon o policiji („Službeni glasnik RS”, br. 6/16 i 24/18) u članu 34a propisuje platformu za bezbednu elektronsku komunikaciju, razmenu podataka i informacija u cilju sprečavanja organizovanog kriminala i drugih oblika teškog kriminala. Vrši se evidentiranje pristupa, kao i razmena podataka o krivičnim delima u skladu sa zakonom kojim se uređuje suzbijanje organizovanog kriminala, korupcije i drugih posebno teških krivičnih dela, uz primenu mera informacione bezbednosti.

Zakon o Bezbednosno-informativnoj agenciji („Službeni glasnik RS”, br. 42/02, 111/09, 65/14 – US, 66/14 i 36/18) propisuje poslove koji se odnose na: zaštitu bezbednosti Republike Srbije i otkrivanje i sprečavanje delatnosti usmerenih na podrivanje ili rušenje Ustavom utvrđenog poretka Republike Srbije; istraživanje, prikupljanje, obradu i procenu bezbednosno-obaveštajnih podataka i saznanja od značaja za bezbednost Republike Srbije i informisanje nadležnih državnih organa o tim podacima, kao i druge poslove određene zakonom. Pored toga, kad posebni razlozi bezbednosti Republike Srbije to zahtevaju, Agencija može da preuzme i neposredno obavi poslove koji su u nadležnosti ministarstva nadležnog za unutrašnje poslove, o čemu odluku sporazumno donose direktor Agencije i ministar nadležan za unutrašnje poslove. U slučaju sukoba nadležnosti odlučuje Vlada, u skladu sa zakonom i drugim propisima. Preuzete poslove pripadnici Agencije obavljaju pod uslovima i na način, kao i primenom ovlašćenja, utvrđenih zakonom i drugim propisima koje primenjuju ovlašćena službena lica i radnici na određenim dužnostima ministarstva nadležnog za unutrašnje poslove, u skladu sa propisima o unutrašnjim poslovima.

Zakon o Vojsci Srbije („Službeni glasnik RS”, br. 116/07, 88/09 i 101/10 – dr. zakon, 10/15, 88715 – US i 36/18) u članu 53. uređuje nadležnost Vojne policije za obavljanje poslova suzbijanja kriminaliteta u Ministarstvu odbrane i Vojsci Srbije, odnosno da ovlašćena službena lica Vojne policije sprovode operativnu i kriminalističku obradu prema zaposlenom u Ministarstvu odbrane i pripadnicima Vojske Srbije za koga postoje osnovi sumnje da je u službi ili u vezi sa službom izvršio krivično delo za koje se goni po službenoj dužnosti, pri čemu u postupanju imaju obaveze i ovlašćenja u skladu sa zakonom kojim se uređuje krivični postupak, Zakonom o policiji i propisima donetim na osnovu tog zakona. Vojna policija može primeniti službena ovlašćenja i prema civilima u slučaju kada postoje osnovi sumnje da su učinili krivično delo na štetu Ministarstva odbrane ili Vojske Srbije za koje se goni po službenoj dužnosti. Polazeći od citiranih odredbi, borbu protiv, pre svega, sve većeg broja napada sajber kriminalaca na informaciono-komunikacione sisteme u Ministarstvu odbrane i Vojsci Srbije, odnosno procesuiranje krivičnih dela visokotehnološkog kriminala, u skladu sa Zakonikom o krivičnom postupku, Krivičnim zakonikom i Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, preduzimaju ovlašćena službena lica Vojne policije.

Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji („Službeni glasnik RS”, broj 88/09, 55/12 – US i 17/13) u članu 5. uređuje nadležnost Vojnobezbednosne agencije za obavljanje bezbednosne i kontraobaveštajne zaštite Ministarstva odbrane i Vojske Srbije u okviru koje obavlja bezbednosne,

kontraobaveštajne i ostale poslove i zadatke od značaja za odbranu Republike Srbije, u skladu sa zakonom i propisima donetim na osnovu zakona. U odredbi člana 6. stav 2. tačka 4. utvrđeno je da je Vojnobezbednosna agencija ovlašćena da otkriva, istražuje i prikuplja dokaze za krivična dela protiv bezbednosti računarskih podataka, propisana Krivičnim zakonikom, kao i drugim zakonima kada su navedena krivična dela usmerena protiv Ministarstva odbrane i Vojske Srbije.

Zakon o tajnosti podataka („Službeni glasnik RS”, broj 104/09) uređuje jedinstven sistem određivanja i zaštite tajnih podataka koji su od interesa za nacionalnu i javnu bezbednost, odbranu, unutrašnje i spoljne poslove Republike Srbije, zaštite stranih tajnih podataka, pristup tajnim podacima i prestanak njihove tajnosti, nadležnost organa i nadzor nad sprovođenjem ovog zakona, kao i odgovornost za neizvršavanje obaveza iz ovog zakona i druga pitanja od značaja za zaštitu tajnosti podataka.

Zakonom o zaštiti podataka o ličnosti („Službeni glasnik RS”, br. 97/08, 104/09 - dr. zakon, 68/12 – US i 107/12) uređuju se uslovi za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka iz Republike Srbije i nadzor nad izvršavanjem ovog zakona.

Zakoni iz oblasti prava intelektualne svojine uređuju za svaku vrstu prava intelektualne svojine posebno predmet i uslove za sticanje zaštite, postupak zaštite, sadržinu, sticanje i obim prava, prestanak prava i građanskopravnu zaštitu. Zakonodavni okvir u oblasti intelektualne svojine čine sledeći zakoni: Zakon o autorskom i srodnim pravima („Službeni glasnik RS”, br. 104/09, 99/11, 119/12 i 29/16 – US), Zakon o patentima („Službeni glasnik RS”, br. 99/11 i 113/17), Zakon o žigovima („Službeni glasnik RS”, br. 104/09, 10/13 i 44/18 – dr. zakon), Zakon o pravnoj zaštiti industrijskog dizajna („Službeni glasnik RS”, br. 104/09, 45/15 i 44/18 - dr. zakon), Zakon o zaštiti topografija poluprovodničkih proizvoda („Službeni glasnik RS”, broj 55/13), Zakon o oznakama geografskog porekla („Službeni glasnik RS”, br. 18/10 i 44/18 – dr. zakon), Zakon o optičkim diskovima („Službeni glasnik RS”, broj 52/11), Zakon o zaštiti poslovne tajne („Službeni glasnik RS”, broj 72/11).

U vezi sa Zakonom o informacionoj bezbednosti značajne su sledeće četiri uredbe: Uredba o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja; Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja; Uredba o utvrđivanju Liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja; Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, kao i Pravilnik o bližim uslovima za upis u Evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima.

Pored navednih uredbi doneta je i Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija, kojom su predviđene preventivne mere za bezbednost i zaštitu dece pri korišćenju informaciono-komunikacionih tehnologija, odnosno bezbednost i zaštitu dece na internetu i postupanje u slučaju narušavanja ili ugrožavanja njihove bezbednosti na internetu.

Na osnovu **Zakona o elektronskim komunikacijama,** Regulatorna agencija za elektronske komunikacije i poštanske usluge je donela Pravilnik o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja. Ovim pravilnikom bliže su propisani opšti uslovi za obavljanje delatnosti i određeni uslovi koji važe za obavljanje svih ili pojedinih delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja i propisan obrazac obaveštenja o obavljanju delatnosti elektronskih komunikacija. Takođe, u članu 127. stav 5. Zakona o elektronskim komunikacijama propisano je da ministarstvo nadležno za poslove telekomunikacija, po pribavljenom mišljenju ministarstva nadležnog za poslove pravosuđa, ministarstva nadležnog za unutrašnje poslove, ministarstva nadležnog za poslove odbrane, Bezbednosno-informativne agencije i organa nadležnog za zaštitu podataka o ličnosti, bliže propisuje zahteve za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija. Na osnovu navedene odredbe Ministarstvo trgovine, turizma i telekomunikacija je donelo Pravilnik o zahtevima za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija i tehničkim zahtevima za ispunjenje obaveze zadržavanja podataka o elektronskim komunikacijama, koji je u primeni od 31. oktobra 2015. godine.

Pored toga, doneti su i sledeći pravilnici: Pravilnik o bližim uslovima za upis u Evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima, nakon uredbi koje su donete na osnovu Zakona o informacionoj bezbednosti („Službeni glasnik RS”, br.6/16 i 94/17), Pravilnik o metodologiji za izvršavanje poslova u skladu sa Zakonom o sprečavanju pranja novca i finansiranja terorizma, Pravilnik o načinu obaveštavanja fizičkih i pravnih lica o promeni na listi označenih lica donetoj od strane Saveta bezbednosti Ujedinjenih nacija i drugih međunarodnih organizacija u kojima je Republika Srbija član.

3.3.2. Aktuelne promene u pravnom okviru

Radi usklađivanja određenih zakonskih propisa sa pravom EU, izrađeni su nacrti zakona čije se usvajanje očekuje u toku 2018. godine ili u prvom delu 2019. godine. U toku 2018. godine, očekuje se usvajanje izmena i dopuna Zakona o autorskom i srodnim pravima, Zakona o patentima, Zakona o žigovima, Zakona o zaštiti topografija poluprovodničkih proizvoda, zatim, uvajanje novog Zakona o oznakama geografskog porekla i Zakona o elektronskim komunikacijama, a u prvom kvartalu 2019. godine i usvajanje novog Zakona o zaštiti poslovne tajne. Pored navedenog, urađen je Nacrt zakona o izmenama i dopunama Zakona o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine.

Takođe, Ministarstvo pravde je osnovalo radne grupe za izmene i dopune Krivičnog zakonika i Zakonika o krivičnom postupku radi daljeg usklađivanja domaćeg krivičnog zakonodavstva sa pozitivnim propisima Evropske Unije. Usvajanje izmena i dopuna Krivičnog zakonika i Zakonika o krivičnom postupku očekuje se do 2020. godine.

Trenutno su u izradi podzakonska akta na osnovu Zakona o elektronskom dokumentu, elektronskom identitetu i uslugama od poverenja u elektronskom poslovanju, a očekuju se i izmene Zakona o informacionoj bezbednosti.

U Nacrtu o kritičnoj infrastrukturi po kome se uspostavlja normativni okvir za identifikaciju, označavanje i zaštitu kritične infrastrukture u Republici Srbiji, shodno Akcionom planu za Poglavlje 24, gde je nosilac zadatka Sektor za vanredne situacije u Ministarstvu unutrašnjih poslova, u članu 2. definisan je pojam kritične infrastrukture.

3.4. Programi i strategije

3.4.1. Programi i projekti u fazi programiranja

1. Program „Izgradnja kapaciteta za predstavnike policije i pravosuđa uključene u borbu protiv sajber kriminala”

Program je namenjen predstavnicima policije i pravosuđa iz regiona Zapadnog Balkana, Istočne Evrope i Centralne Azije. Predviđeno je da projekat traje od 1. maja 2017. godine do 30. aprila 2019. godine, a vrednost je 648.433,80 evra i da se u prvoj godini organizuje pet obuka za predstavnike policije i pravosuđa država Zapadnog Balkana.

2. Projekat za borbu protiv visokotehnološkog kriminala u okviru Fonda za unutrašnju bezbednost – Policija (ISPF)

Projekat ima za cilj borbu protiv sajber kriminala i planira se učešće: forenzičkih eksperata, istražitelja, operativnih analitičara i tužilaca iz zemalja članica EUSDR. Predloženi budžet projekta je okvirno 1,2 miliona evra. Trenutno vodeći partneri projekta čekaju otvaranje odgovarajućeg poziva od strane Evropske komisije u okviru ISFP fonda radi podnošenja predloga projekta. Takođe, vodeći partneri su otvoreni za dodatne predloge i ideje budućih partnera. Radi jednostavnije komunikacije zamolili su da se zainteresovane države članice EUSDR izjasne o zainteresovanosti za partnerstvo u projektu i opredele kontakt osobu odgovornu za predviđeno partnerstvo i odgovarajuću komunikaciju.

3. Tvining projekat na temu borbe protiv sajber kriminala

U okviru programiranja IPA 2017 u pripremi je Tvining projekat, koji predviđa sledeće obuke: Istraživanje „malvera” (zlonamernih softvera); Automatizovana pretraga podataka na Internetu za prikupljanje podataka o izvršenim krivičnim delima u „Online” prostoru; Korišćenje besplatnih alata i tehnika u svrhe sprečavanja visokotehnološkog kriminala (Open sorce inteligence – OSINT); Obuka za prikupljanje podataka sa računara (eng. „first responder”) i forenzika računara u online režimu rada (eng. „live forensic”); Obuka tipa „trening trenera” u oblasti visokotehnološkog kriminala. Osim obuka predviđena je i konferencija o saradnji policije sa privatnim kompanijama, akademskim institucijama, nevladinim sektorom i istaknutim stručnjacima u oblasti informacionih tehnologija. Odeljenje za suzbijanje visokotehnološkog kriminala ima izraženu potrebu za saradnjom sa partnerima iz oblasti državnog i javnog sektora, privatnog sektora i istaknutih stručnjaka u ovoj oblasti. Potreba za ovakvim vidom saradnje nastaje zbog prirode visokotehnološkog kriminala. Znanja, vešine i podaci koja poseduju banke, privatne kompanije, pa i stručnjaci koji se bave informacionom bezbednošću ponekad su daleko ispred veština i tehničkih mogućnosti država koje se suprotstavljaju visokotehnološkom kriminalu. To se posebno odnosi na multinacionalne kompanije. Projektom su predviđene i studijske posete koje bi trebale da omoguće uvid u najbolju praksu vezanu za istraživanje zlonamernih softvera, automatizovanu pretragu podataka na internetu i za prikupljanje podataka sa računara (eng. „first responder”) i forenzika računara u online režimu rada (eng. „live forensic”). U okviru programiranja IPA 2017 u pripremi je i Ugovor o nabavci opreme koji predviđa nabavku IT opreme i softvera namenjenih borbi protiv sajber kriminala.

3.4.2. Projekti u fazi sprovođenja

1. Projekat „Saradnja u borbi protiv kriminala u sajber prostoru: ciljanje imovine stečene kriminalom na internetu u Jugoistočnoj Evropi i Turskoj":

Korisnik ovog projekta je Uprava kriminalističke policije, Služba za borbu protiv organizovanog kriminala (višekorisnička IPA 2014). Ukupna vrednost projekta je 5.560.000 evra (od čega 5.000.000 evra je doprinos EU, a 560.000 evra je kofinansiranje Saveta Evrope). Implementator projekta je Savet Evrope, Kancelarija za borbu protiv kriminala u sajber prostoru u Bukureštu, Rumunija. Ostale zemlje koje učestvuju u projektu su: Republika Albanija, Bosna i Hercegovina, Crna Gora, Republika Srbija, Republika Makedonija, Republika Turska i Kosovo[8*]. Projekat će trajati 42 meseca (od januara 2016. do juna 2019. godine). Opšti cilj projekta je ojačati zakonodavstvo u pogledu traženja, zaplene i oduzimanja prihoda sajber-kriminala i sprečavanje pranja novca na internetu u skladu sa zahtevima za zaštitu podataka.

Rezultati ovog projekta su: doprinos jačanju vladavine prava kroz borbu protiv korupcije i organizovanog kriminala; jačanje kapaciteta institucija za istrage, zaplene i oduzimanje imovine proistekle iz kriminala u sajber prostoru i prevencija pranja novca na internetu; uspostavljanje javnog sistema prijavljivanja prevara; unapređenje zakonskog okvira; saradnja policijskih jedinica; izrada priručnika za finansijski sektor; mehanizmi razmene informacija privatnog i javnog sektora; pravosudni trening i međunarodna saradnja.

U okviru projekta, u toku 2016. i 2017. godine realizovan je veliki broj aktivnosti od kojih su najznačajnije: konferencija u Ohridu, regionalna studija slučaja o kompjuterskom kriminalu i finansijskim istragama „Regional case simulation exercise on cybercrime and financial investigations" u Tbilisiju, međunarodna radionica na temu sajber kriminala u Briselu, radionice o rizicima pranja novca u vezi sa tehnologijama, kao i o onlajn finansijskim prevarama i prevarama u vezi sa platnim i kreditnim karticama, seminar u Bukureštu na temu „Istrage u vezi sa Darknetom i virtuelnim valutama", obuka o istrazi „Darkneta" i virtuelnih valuta i kurs u Zagrebu pod nazivom: „Training on WMD Cyber Crimes Investigations".

2. Naučno-istraživački projekat Advanced Tools for fighting online illegal trafficking - ANITA (787061) u sklopu Horizon 2020

Kriminalističko-policijski univerzitet učestvuje u realizaciji ovog projekata, koji je usmeren na razvoj i usavršavanje softverskih rešenja i obuke pripadnika policije, tužilaštva i drugih organa i organizacija čija je osnovna delatnost u suzbijanju krivičnih dela i prevencije viskotehnološkog kriminala. Projekat je počeo 15. maja 2018. godine i ima za cilj da, preko radnih scenarija, razvije i usavrši, već postojeća, kao i nova, softverska rešenja kojima bi se pratile nezakonite aktivnosti u Darknet i Deep Web[9]. Predviđeno je da se projekat realizuje do 15. maja 2020. godine.

[*] Ovaj naziv je bez prejudiciranja statusa i u skladu je sa Rezolucijom Saveta bezbednosti Ujedinjenih nacija 1244 i mišljenjem Međunarodnog suda pravde o deklaraciji o nezavisnosti Kosova.

[9] Deep weeb (srp. „Duboka mreža") – poznata i kao nevidljiva ili skrivena mreža, označava pretragu koja se odnosi na sadržaj na svetskoj mreži, koja nije indeksirana od strane standardnih pretraživača.

3. Projekat Evropske unije i Saveta Evrope iPROCEEDS@IPA

U projekat su uključene zemlje jugoistočne Evrope i Republika Turska. On ima za cilj osposobljavanje i jačanje kapaciteta državnih organa nadležnih za borbu protiv visokotehnološkog kriminala u Republici Srbiji i zemljama u regionu u postupcima oduzimanja imovine u predmetima visokotehnološkog kriminala. U okviru projekta sprovedene su dve ekspertske misije, kada je održan sastanak o saradnji državnih organa i privatnog sektora u suzbijanju visokotehnološkog kriminala i oduzimanju imovine proistekle iz krivičnih dela iz ove oblasti, dok je druga misija, održana u junu 2017. godine, u cilju izrade vodiča za prevenciju i otkrivanje imovine proistekle iz krivičnih dela učinjenih putem Interneta. U okviru projekta održan je niz radionica i stručnih skupova u kojima su učestvovali predstavnici javnog tužilaštva.

Takođe, predstavnik Posebnog tužilaštva nastavio je učešće u izradi logičke matrice za sektor unutrašnjih poslova IPA 2017 projekta, kojim se planira jačanje administrativnih i tehničkih kapaciteta Posebnog tužilaštva, kroz sprovođenje opremanja tužilaštva i organizovanje specijalizovanih obuka.

U okviru ovog projekta, od 12. do 13. oktobra 2017. godine, predstavnici CERT, Regulatorne agencije za elektronske komunikacije i poštanske usluge i Ministarstva unutrašnjih poslova učestovovali su u studijskoj poseti CERT Rumunije[10], koja je imala za cilj jačanje kapaciteta novoosnovanih CERT kroz razmenu znanja, iskustva i najboljih praksi vezanih za operativno okruženje CERT. Pored toga, 20. decembra 2017. godine u Skoplju je održana Regionalna radionica o razmeni dobrih praksi o mehanizmima izveštavanja u Jugoistočnoj Evropi i Turskoj[11]. Radionica je poslužila kao forum za raspravu za tužioce, istraživače u oblasti sajber kriminala, predstavnike Ministarstva pravde, Ministarstva unutrašnjih poslova i CERT timove u vezi sa funkcionisanjem i korišćenjem mehanizma izveštavanja o sajber kriminalu. Utvrđena je struktura i metode za prikupljanje informacija za izveštaj i doprinos izveštaja kroz deljenje informacija, kao i istraživanje krivičnih predmeta i statističkih razloga. Dogovorena je i razmena dobrih praksi u regionu na online platformama za prijavljivanje sajber kriminala.

3.4.3. Realizovani projekti

1. Projekat „Podrška vladavini zakona kroz jačanje kapaciteta za informacionu bezbednost Ministarstva unutrašnjih poslova”

Projekat finansira Vlada Ujedinjenog Kraljevstva Velike Britanije i Severne Irske (iz Good Governance Fund-a), dok je DCAF bio implementacioni partner. Korisnik projekta je Sektor za analitiku, telekomunikacione i informacione tehnologije, Centar za reagovanje na napade na informacioni sistem (CERT). Pored CERT-a i Odeljenja za informacionu bezbednost, u određenim fazama u projekat su bili uključeni i drugi državni organi od značaja za informacionu bezbednost u Republici Srbiji, od kojih su najviše angažovanja imali Regulatorna agencija za elektronske komunikacije i poštanske usluge - RATEL (kao institucija koja treba da formira Nacionalni CERT), UZZPRO[12] (kao institucija koja treba da formira CERT republičkih organa) i Ministarstvo trgovine, turizma i telekomunikacija (Ministarstvo nadležno za informacionu bezbednost). Svrha projekta je podrška Ministarstvu unutrašnjih poslova u razvijanju održive strukture otporne na pretnje iz sajber

[10] https://www.coe.int/en/web/cybercrime/-/iproceeds-study-visit-on-csirt-cert-regulations-and-operational-environment
[11] https://www.coe.int/en/web/cybercrime/-/iproceeds-regional-workshop-on-sharing-good-practices-on-reporting-mechanisms-in-south-eastern-europe-and-turkey
[12] Trenutno nadležna Kancelarija za informacione tehnologije i elektronsku upravu.

prostora MUP-ovim sistemima i servisima, koja je osposobljena da sarađuje sa svim relevantnim nacionalnim i međunarodnim zainteresovanim stranama i koja doprinosi nacionalnoj i međunarodnoj sajber bezbednosti, a vrednost projekta je 143.720 funti. Projekat je realizovan u periodu od 1. marta 2017. do 31. avgusta 2017. godine.

Jedan od važnijih rezultata prve faze projekta bio je okvir za obuku kadrova koji je planirano da se konkretizuje i sprovede u drugoj fazi projekta tokom 2018. godine, za čiji nastavak su zainteresovani i implementator i donator.

2. Projekat Saveta Evrope i Evropske Unije Global Action on Cyber Crime + (GLACY+)

Posebno tužilaštvo za visokotehnološki kriminal je uključeno u ovaj projekat, čiji je cilj sveobuhvatna, planetarna primena Konvencije o visokotehnološkom kriminalu i pružanje direktne administrativne i tehničke pomoći zemljama koje su obuhvaćene ovim projektom, u okviru kog je Posebni tužilac angažovan na izradi međunarodnih standarda i obuka za postupanje u ovoj oblasti javnih tužilaštva i sudova, kao i izrade procedura za postupanje sa elektronskim dokazima pripadnika nadležnih službi za otkrivanje krivičnih dela i analizu digitalnih dokaza.

Pored navedenih aktivnosti, Republičko javno tužilaštvo i Posebno tužilaštvo za visokotehnološki kriminal učestvuju i u sledećim projektima:

3. Projekat „Unapređenje obuke za kadrove pravosudnih organa u oblasti zaštite dece od nasilja na internetu”

Ovom projektu finansijsku podršku pruža međunarodna organizacija civilnog društva Save the children. Njegov cilj bila je izrada plana i programa obuke za sudije i javne tužioce u oblasti visokotehnološkog kriminala i zaštitite maloletnih lica na internetu. Posebni tužilac je bio član radne grupe za izradu plana i programa obuke. Takođe, u okviru projekta izrađen je priručnik – Vodič za sudije i javne tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republici Srbiji. U sklopu saradnje sa međunarodnom organizacijom civilnog društva Save the children, a u skladu sa Akcionim planom za Poglavlje 24 i aktivnošću 6.2.9.3.1. - Sačiniti i potpisati sporazume o saradnji između državnih organa i organizacija civilnog društva u borbi protiv visokotehnološkog kriminala, razmatra se zaključenje Sporazuma o saradnji.

3.4.4. Strateška dokumenta

1. Strateška procena javne bezbednosti za period od 2017. do 2021. godine i Strateški plan policije 2018-2019. godina

U Strateškoj proceni javne bezbednosti određeni su prioriteti u radu policije za period 2017 – 2021. godine, na osnovu analize stanja i kretanja kriminala. Strateška procena je kao jedan od osam prioriteta odredilo i borbu protiv zloupotreba informaciono-komunikacionih tehnologija na teritoriji Republike Srbije. U okviru Strateškog plana policije konkretizovan je navedeni prioritet kroz definisane aktivnosti, nosioce, rokove i resurse za period 2018 - 2019. godine.

2. Procena pretnji od teškog i organizovanog kriminala u Srbiji (eng. Serious and Organised Crime Threat Assessment - SOCTA) iz 2015. godine

Ova procena je strateški dokument koji ima za cilj stvaranje objektivne osnove za donošenje relevantnih strateških i operativnih odluka kojima će se unaprediti pravni i institucionalni kapaciteti Ministarstva unutrašnjih poslova i drugih organa za sprovođenje zakona i postići veći stepen zaštite osnovnih prava i sloboda građana Srbije.[13] Procena kao bezbednosne pretnje identifikuje različite oblike teškog i organizovanog kriminala, uključujući i visokotehnološki kriminal, a na kojima policija zasniva svoj operativni rad u skladu sa postojećim trendovima.

3. Regionalna procena pretnji od teškog i organizovanog kriminala iz 2016. godine

U pitanju je dokument, izrađen po metodologiji EUROPOL, koji omogućava sveobuhvatno sagledavanje aktuelnog stanja i kretanja, kao i posledica koje prouzrokuju organizovani i teški kriminal uključujući i visokotehnološki kriminal, kao i rano upozoravanje na nove trendove i pretnje po region kako bi se olakšala prevencija i suprotstavljanje navedenim oblicima kriminala. Konkretni ciljevi ovog dokumenta su da se izvrši prikaz aktuelnog stanja na teritoriji Republike Srbije, Crne Gore i Republike Makedonije, ukaže na oblasti koje predstavljaju najveću pretnju u ovom delu regiona (među kojima su i različiti vidovi visokotehnološkog kriminala), da se odrede faktori koji utiču na ove pojave, identifikuju zajedničke karakteristike delovanja kriminalnih grupa, kao i da se daju pretpostavke o razvoju budućih pretnji koje mogu poslužiti kao osnov za donošenje odluka o zajedničkom suprotstavljanju na regionalnom nivou.

4. Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine

Ministarstvo trgovine, turizma i telekomunikacija je bilo nosilac aktivnosti u izradi navedene strategije, koja je usvojena 29. maja 2017. godine. U njoj je kao posebna celina obrađena borba protiv visokotehnološkog kriminala u Republici Srbiji, gde su imenovani najvažniji subjekti u Republici Srbiji u ovoj oblasti. Osnovni cilj je poboljšanje razmene informacija, praćenje aktuelnih rizika i podizanje svesti u ovoj oblasti.

U cilju razvoja i unapređenja informacione bezbednosti u Republici Srbiji utvrđena je, između ostalog, prioritetna oblast borba protiv visokotehnološkog kriminala, što se odnosi na prevenciju i sankcionisanje krivičnih dela koja se zasnivaju na zloupotrebi informaciono-komunikacionih tehnologija;

U oblasti borbe protiv visokotehnološkog kriminala određeni su sledeći strateški ciljevi:

- unapređenje mehanizama za otkrivanje visokotehnološkog kriminala i krivično gonjenje učinilaca;
- podizanje svesti o opasnostima od visokotehnološkog kriminala;
- unapređenje međunarodne saradnje u borbi protiv visokotehnološkog kriminala.

Vlada je donela Akcioni plan za 2018. i 2019. godinu, za sporovođenje Strategije razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine.

5. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine

[13] SOCTA, str. 1.

Ova strategija je akt kojim se na celovit način definišu osnovni ciljevi, načela i prioriteti razvoja informacionog društva i utvrđuju aktivnosti koje treba preduzeti u periodu koji obuhvata ova strategija.[14] Ministarstvo trgovine, turizma i telekomunikacija je bilo nosilac realizacije u izradi ove strategije, u kojoj je borba protiv visokotehnološkog kriminala prepoznata kao jedan od strateških prioriteta u oblasti informacione bezbednosti.

6. Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma

U formulisanju ciljeva Nacionalne strategije u obzir je uzeta i hijerarija ciljeva delotvornog sistema za borbu protiv pranja novca i finansiranja terorizma koja je data u metodologiji FATF. Otuda je i opšti cilj i svrha Nacionalne strategije da u potpunosti zaštiti finansijski sistem i privredu države od opasnosti koje uzrokuju pranje novca i finansiranje terorizma i širenje oružja za masovno uništenje, čime se jača integritet finansijskog sektora i doprinosi bezbednosti i sigurnosti.[15]Ova strategija je od važnosti kada je u pitanju pranje novca stečenog izvršenjem krivičnih dela visokotehnološkog kriminala.

7. Nacionalna strategija za sprečavanje i borbu protiv terorizma za period 2017 – 2021. godina

Ova strategija ima za svrhu zaštitu Republike Srbije od terorističke pretnje po njene građane, vrednosti i interese, uz istovremeno podržavanje međunarodnih napora u borbi protiv terorizma. Između ostalog, navedena svrha biće ostvarena sprovođenjem ciljnih i osmišljenih mera na doktrinarnom planu, kroz razvijanje i podizanje bezbednosne kulture društva i promovisanje određenih vrednosti, kao i na normativnom i institucionalnom planu, kroz unapređenje kapaciteta za prevenciju i borbu protiv terorizma, posebno kapaciteta za suprotstavljanje nasilnom ekstremizmu i radikalizaciji koja vodi u terorizam, kao sve izraženijem fenomenu.[16] Prepoznajući dostupnost savremenih informacionih tehnologija, gde su informacioni resursi objekat napada, Republika Srbija je u postupku izrade Strategije za borbu protiv visokotehnološkog kriminala obuhvatila sve oblasti koje nisu predviđene ovim strateškim dokumentom.

U okviru Strategije je kao Prioritetna oblast 1 određena prevencija terorizma, nasilnog ekstremizma i radikalizacije koji vode u terorizam, dok je strategijski cilj 1.4 – Visokotehnološki sistemi komunikacije i digitalnih mreža otporni na širenje radikalizacije i nasilnog ekstremizma.

Razvoj modernih društava, oličen u snažnom visokotehnološkom, ubrzanom napretku informatičkog društva, učinio je neophodnim pažljivo definisanje politike suprotstavljanja stavljanju ovih sistema u službu terorizma, jer pojedinac može podleći uticaju propagande i steći znanja za izvršenje terorističkog akta bez neposrednog kontakta sa okruženjem.

Ostvarenje ovog cilja biće postignuto kroz nastojanja da se ojača svest u društvu o opasnostima korišćenja visokotehnoloških sistema komunikacije za širenje govora mržnje i na nacionalnom nivou izgrade i implementiraju najbolje politike, zakonska rešenja i praksa suprotstavljanju korišćenja ovih sredstava komuniciranja za širenje nasilnog ekstremizma i

[14] Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine, str 2.
[15] Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma, str. 1
[16] Nacionalna strategija za sprečavanje i borbu protiv terorizma za period 2017 - 2021. godina, str. 1

radikalizacije koji vode u terorizam, uključujući pažljivo definisanje i promovisanje stavova koji predstavljaju protivtežu. [17]

8. Strategija razvoja obrazovanja u Srbiji do 2020. godine

Jedan deo ove strategije odnosi se i na razvoj znanja u vezi sa informaciono-komunikacionim tehnologijama. Nova Strategija za čiju se izradu formira radna grupa, treba da obuhvati i segmente preventivne zaštite neophodne u borbi protiv visokotehnološkog kriminala.

9. Strategija prevencije i suzbijanja trgovine ljudima, posebno ženama i decom i zaštite žrtava 2017 – 2022.

Ova strategija predviđa posebne aktivnosti i zadatke koji će obezbediti da deca u Republici Srbiji, odrastaju u okruženju bezbednom od trgovine ljudima, iskorišćavanja u pornografiji i prostituciji. Otkrivanje i procesuiranje slučajeva trgovine decom i iskorišćavanja u pornografiji i prostituciji će biti u skladu sa proaktivnim pristupom, čiji je cilj da se olakša položaj dece kao žrtava i oštećenih u postupku. Ovo je veoma značajno, s obzirom da se zna da se za ovaj vid iskorišćavanja zloupotrebljavaju savremene tehnologije, mobilni internet i socijalne mreže.

10. Strategija nacionalne bezbednosti Republike Srbije

U okviru politike unutrašnje bezbednosti definiše „Delovanje državnih i ostalih organa i institucija Republike Srbije u oblasti unutrašnje bezbednosti usmereno je na zaštitu ustavnog poretka, života i imovine građana, sprečavanje i suzbijanje svih oblika terorizma, organizovanog, finansijskog, ekonomskog i visokotehnološkog kriminala, korupcije, pranja novca, trgovine ljudima, narkomanije, proliferacije konvencionalnog naoružanja i oružja za masovno uništenje, obaveštajnih i subverzivnih delatnosti, kao i drugih izazova, rizika i pretnji bezbednosti".

11. Nacionalna strategija za borbu protiv organizovanog kriminala

Ova strategija određuje da su „pojavni oblici organizovanog kriminala zastupljeni u Republici Srbiji trgovina narkoticima, iznude, otmice, ucene, trgovina ljudima, krijumčarenje ljudi, korupcija, pranje novca, zloupotreba službenog položaja, falsifikovanje novca i drugih sredstava plaćanja, prostitucija, trgovina oružjem i eksplozivnim materijama, međunarodno krijumčarenje vozila, krijumčarenje akcizne robe i visokotehnološki kriminal".

12. Koncept sajber odbrane Vojske Srbije

Vojska Srbije izradila je Nacrt koncepta sajber odbrane Vojske Srbije, koji još uvek nije usvojen. Dokument predstavlja pogled na pitanje kako se procenjuje odbrambeni, bezbednosni, tehnološki i društveni uticaj koji će u narednom petogodišnjem periodu razvoja i upotrebe Vojske Srbije ostvariti razvoj informaciono-komunikacionih tehnologija, aktivnosti i dejstava u sajber prostoru i upotreba ofanzivnih sajber sposobnosti mogućih protivnika na odbranu Republike Srbije. Pri tome se poseban značaj posvećuje strukturi i međusobnim odnosima organizacionih celina i nosilaca operativnih i funkcionalnih

[17] Nacionalna strategija za sprečavanje i borbu protiv terorizma za period 2017 - 2021. godina

sposobnosti Vojske Srbije, kao i odnos i uticaj koji se ostvaruje u njihovoj interakciji sa spoljnim akterima, sistemima, procedurama i resursima.

Procena je zasnovana na rezultatima predviđanja relevantnih međunarodnih subjekata o očekivanom razvoju informaciono-komunikacionih tehnologija i njihovom kompleksnom uticaju na odbranu i bezbednost Republike Srbije, na identifikovanim pretnjama i rizicima na nacionalnu bezbednosti i odbranu, i dostignutom i očekivanom stepenu razvoja kapaciteta i sposobnosti drugih državnih i nedržavnih subjekata za dejstva i aktivnosti u sajber prostoru ili iz njega, koja mogu biti od uticaja na misije i zadatke Vojske Srbije.

Koncept sajber odbrane Vojske Srbije predstavlja osnovni vodič koji služi donosiocima odluka na strategijskom nacionalnom nivou za razvoj odgovarajućih, delotvornih, optimalnih i održivih vojnih kapaciteta i sposobnosti Republike Srbije u sastavu oružanih snaga za izvođenje sveobuhvatnih aktivnosti i dejstava u sajber prostoru u obavljanju svoje ustavne funkcije odbrane.

13. Strategija razvoja intelektualne svojine za period 2018-2022 godine

Izrađen je Predlog strategije, čije se usvajanje očekuje. U Predlogu ove strategije, za realizaciju određenih planiranih aktivnosti kao nosilac realizacije je određen Zavod za intelektualnu svojinu, a za realizaciju drugih aktivnosti zadužen je Zavod u partnerstvu sa ostalim organima odgovornim za sprovođenje zaštite prava intelektualne svojine, a za ostale je zaduženo Koordinaciono telo za efikasnu zaštitu prava intelektualne svojine u Republici Srbiji. Posebno tužilaštvo za visokotehnološki kriminal ima značajnu ulogu u pogledu zaštite prava intelektualne svojine, odnosno nadležno je za gonjenje učinilaca krivičnih dela u oblasti intelektualne svojine, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Pod proizvodima u elektronskom obliku posebno se podrazumevaju računarski programi i autorska dela koja se mogu upotrebiti u elektronskom obliku.

4. INSTITUCIONALNI OKVIR ZA BORBU PROTIV VISOKOTEHNOLOŠKOG KRIMINALA U REPUBLICI SRBIJI

4.1. Institucionalni okvir – trenutno stanje

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala iz 2005. godine, osnovano je **Posebno odeljenje za borbu protiv visokotehnološkog kriminala (Posebno tužilaštvo**), u okviru Višeg javnog tužilaštva u Beogradu. Ovo odeljenje nadležno je za krivično gonjenje učinilaca krivičnih dela visokotehnološkog kriminala i nadležno je da postupa na celoj teritoriji Republike Srbije. Shodno odredbama navedenog zakona, za postupanje u predmetima visokotehnološkog kriminala nadležan je Viši sud u Beogradu za teritoriju Republike Srbije, a za odlučivanje u drugom stepenu nadležan je Apelacioni sud u Beogradu. Trenutno u Posebnom tužilaštvu, kojim rukovodi Posebni tužilac, raspoređena su četiri zamenika javnog tužioca, dva viša tužilačka saradnika, jedan tužilački saradnik i dva administrativna radnika. Obučenost je na zavidnom nivou sa tendencijom konstatnog usavršavanja, koje se ogleda u kontinuiranim pohađanjima specijalističkih programa obuka zamenika javnog tužioca i tužilačkih pomoćnika.

Takođe, odredbom Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, u okviru **Ministarstva unutrašnjih poslova** (MUP), predviđeno je formiranje službe za borbu protiv visokotehnološkog kriminala koja postupa po nalozima Posebnog tužioca za visokotehnoški kriminal. U Ministarstvu unutrašnjih poslova je formirano Odeljenje za borbu protiv visokotehnološkog kriminala koja je postala jedina specijalizovana jedinica MUP zadužena za krivična dela visokotehnološkog kriminala. Ovo odeljenje postupa po zahtevima nadležnog Odeljenja za borbu protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu, koje rukovodi predistražnim postupkom u ovim predmetima, ali zbog prirode posla, ovo odeljenje postupa i po zahtevima drugih tužilaštava u Republici Srbiji, posebno Tužilaštva za organizovani kriminal, te aktivno pruža operativno-tehničku podršku drugim policijskim jedinicama, pre svega odeljenjima u sastavu SBPOK. Odeljenje se bavi sprečavanjem svih oblika krivičnih dela iz oblasti bezbednosti računarskih podataka, seksualne eksploatacije dece na internetu (dečija pornografija), kršenja prava intelektualne svojine na internetu (softverska piraterija, filmska i muzička piraterija), trgovine na internetu, internet bankarstva, prevara i zloupotreba platnih kartica na internetu, širenja štetnih i nedozvoljenih sadržaja (rasne, verske i nacionalne mržnje, propagiranje terorizma i ksenofobije), ugrožavanje sigurnosti putem Interneta i dr. Odeljenje za borbu protiv visokotehnološkog kriminala, od formiranja 2007. godine do sredine juna 2018. godine, u svom sastavu imalo je dva odseka: Odsek za suzbijanje elektronskog kriminala i Odsek za suzbijanje kriminala u oblasti intelektualne svojine**.** Aktom o sistematizaciji predviđeno je formiranje pored navedenih još dva odseka i to Odsek za suzbijanje nedozvoljenih i štetnih sadržaja na internetu i Odsek za suzbijanje zloupotreba u oblasti elektronske trgovine, elektronskog bankarstva i platnih kartica na internetu. Ujedno je promenjen naziv odeljenja u Odeljenje za suzbijanje visokotehnološkog kriminala u kome je sistematizovano 22 radna mesta

U okviru Ministarstva unutrašnjih poslova, Sektora za analitiku, telekomunikacione i informacione tehnologije formiran je Centar za reagovanje na napade na informacioni sistem (CERT) koji, između ostalog, obavlja sledeće poslove: stalno prikupljanje informacija o novim bezbednosnim problemima i merama zaštite, identifikacija kritične informacione infrastrukture u Ministarstvu, predlaganje mera za zaštitu kritične informacione infrastrukture, analiza zahteva koje treba da ispuni informacioni sistem Ministarstva unutrašnjih poslova za povezivanje na informacione sisteme EU, saradnja i razmena informacija sa nacionalnim CERT, CERT timovima drugih državnih institucija i međunarodnim CERT timovima, preventivno reagovanje u slučaju potencijalne opasnosti po informacioni sistem Ministarstva unutrašnjih poslova, pomoć u saniranju posledica napada na informacioni sistem Ministarstva unutrašnjih poslova. CERT preduzima sve mere i postupke protiv počinioca napada sa Interneta kroz saradnju sa Odeljenjem za suzbijanje visokotehnološkog kriminala, Uprave kriminalističke policije, u cilju prikupljanja dokumentacije i obezbeđenja dokaza za pokretanje postupka protiv počinioca napada koji su neophodni Posebnom javnom tužilaštvu za visokotehnološki kriminal, radi podnošenja krivičnih prijava i pokretanja postupka pred sudom da bi se zakonski ispoštovao tzv. lanac nadređenosti postojanja krivičnih dela učinjenih u sajber prostoru - CHAIN OF CUSTODY, tj. lanac kretanja dokaza, odnosno neprekinut lanac koji omogućava praćenje kretanja dokaznog materijala od trenutka kada je pronađen, i to kroz obrazac-formular koji sadrži hronološke podatke o datumu, licu koje je rukovalo dokazom i eventualnim promenama ili radnjama koje su nastupile u vezi sa istim tokom dokaznog postupka (npr. prenos, mesto čuvanja, analiza i dr.), a u svrhu upotrebe dokaza u sudskom postupku.

U cilju inoviranja sistema policijskog obrazovanja, Kriminalističko-policijski univerzitet je u okviru departmana Računarstva i informatike, u saradnji sa Ministarstvom

unutrašnjih poslova, akreditovao studijske programe na sva tri nivoa studija koji stvaraju uslove za obrazovanje u oblastima suprotstavljanja visoko-tehnološkom kriminalu i informatičke bezbednosti, kao i za naučna istraživanja u tim oblastima.

Značajnu ulogu u ovoj oblasti imaju Narodna banka Srbije i Ministarstvo trgovine, turizma i telekomunikacija (MTTT). Narodna banka Srbije nadležna je za kontrolu, odnosno nadzor informaciono-komunikacionih sistema finansijskih institucija koje su pod njenim nadzorom. Ministarstvo trgovine, turizma i telekomunikacija je nadležni organ za informacionu bezbednost, odnosno bezbednost IKT sistema od posebnog značaja u Republici Srbiji. U vršenju ove nadležnosti MTTT obavlja sledeće poslove: izrada propisa i strategija u oblasti informacione bezbednosti; inspekcijski nadzor nad radom IKT sistema od posebnog značaja; prima obaveštenja o incidentima koji značajno ugrožavaju bezbednost IKT sistema od posebnog značaja i preduzima mere u skladu sa zakonom, u saradnji sa Ministarstvom unutrašnjih poslova i tužilaštvom; sprovodi međunarodnu saradnju u oblasti informacione bezbednosti. Februara 2017. godine MTTT je, u skladu sa Uredbom o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija („Službeni glasnik RS", broj 61/16), osnovalo Nacionalni kontakt centar za bezbednost dece na internetu 19833[18]. Putem Nacionalnog kontakt centra vrši se savetovanje i omogućava se prijem prijava štetnog, neprimerenog i nelegalnog sadržaja i ponašanja na internetu, odnosno ugroženosti interesa i prava dece, telefonskim putem i putem elektronskog obrasca na veb sajtu. U skladu sa članom 11. stav 6. Zakona o informacionoj bezbednosti, u slučaju da je incident u IKT sistemu od posebnog značaja povezan sa izvršenjem krivičnih dela koja se gone po službenoj dužnosti, Ministarstvo o tome obaveštava nadležno javno tužilaštvo, odnosno ministarstvo nadležno za unutrašnje poslove.

Imajući u vidu potrebu za pojačanom kontrolom robe koja se naručuje, odnosno prodaje putem interneta, Uprava carina, u okviru Ministarstva finansija, radi na uspostavljanju uslova za formiranje jedinice Sajber carina, koja bi se aktivno borila protiv visokotehnološkog kriminala, sa ciljem identifikacije dela koja su u suprotnosti sa carinskim propisima na internetu. U sklopu Plana razvoja carinske službe, kao i odgovarajućeg Akcionog plana, navodi se obaveza formiranja odgovarajuće organizacione jedinice u okviru Sektora za kontrolu primene carinskih propisa koja bi se isključivo bavila pitanjem tzv. „ilegalne internet trgovine", što je i navedeno u Planu razvoja carinske službe za period 2017-2020. godine i Akcionog plana za sprovođenje navedenog Plana razvoja. Takođe, Uprava za sprečavanje pranja novca je organ uprave u sastavu ministarstva nadležnog za poslove finansija. Uprava obavlja finansijsko-informacione poslove: prikuplja, obrađuje, analizira i prosleđuje nadležnim organima informacije, podatke i dokumentaciju koju pribavlja u skladu sa ovim zakonom i vrši druge poslove koji se odnose na sprečavanje i otkrivanje pranja novca i finansiranja terorizma u skladu sa zakonom. Ako u vezi sa određenim transakcijama ili licima postoje osnovi sumnje da se radi o pranju novca, finansiranju terorizma ili prethodnom krivičnom delu, Uprava za sprečavanje pranja novca može započeti postupak prikupljanja podataka, informacija i dokumentacije u skladu sa ovim zakonom, kao i izvršiti druge radnje i mere iz svoje nadležnosti i na osnovu pismene i obrazložene inicijative nadležnog suda i tužilaštva, Ministarstva unutrašnjih poslova, Bezbednosno-informativne agencije, Vojnobezbednosne agencije, Poreske uprave, Uprave carina, Narodne banke Srbije, Komisije za hartije od vrednosti, nadležnih inspekcija i državnih organa nadležnih za državnu reviziju i borbu protiv korupcije. Ako u vezi sa određenim transakcijama postoje osnovi sumnje da se radi o pranju novca,

[18] http://www.pametnoibezbedno.gov.rs/rs-lat/kontakt-centar

finansiranju terorizma ili prethodnom krivičnom delu, državni organi mogu da traže od Uprave podatke i informacije potrebne za dokazivanje tih krivičnih dela.

U Ministarstvu prosvete, nauke i tehnološkog razvoja, poslednjom sistematizacijom radnih mesta formiran je Sektor za digitalizaciju u prosveti i nauci. Ovaj sektor čine tri niže organizacione jedinice: Grupa za e-prosvetu, Grupa za e-nauku i Grupa za digitalizaciju u obrazovanju (od po tri državna službenika). Pored ovog sektora, u Sekretarijatu Ministarstva postoji Grupa za održavanje kvaliteta u internoj mreži računara (tri državna službenika), kao i radna mesta za informatičke poslove u nekim školskim upravama. Kada je u pitanju sprečavanje nasilja (pa i zloupotreba informaciono-komunikacionih tehnologija), tri osobe su zadužene za zaštitu od nasilja u obrazovno vaspitnim sistemu, odnosno u Ministarstvu i u okviru toga se takođe bave ovom oblašću. Podršku pružaju i prosvetni savetnici iz školskih uprava.

Bezbednosno-informativna agencija (BIA) u skladu sa Zakonom o Bezbednosno-informativnoj agenciji obavlja poslove koji se odnose na: zaštitu bezbednosti Republike Srbije i otkrivanje i sprečavanje delatnosti usmerenih na podrivanje ili rušenje Ustavom utvrđenog poretka Republike Srbije; istraživanje, prikupljanje, obradu i procenu bezbednosno-obaveštajnih podataka i saznanja od značaja za bezbednost Republike Srbije i informisanje nadležnih državnih organa o tim podacima. Terorizam i organizovani kriminal predstavljaju značajnu pretnju po nacionalnu bezbednost, posebno ako se kao objekt ili sredstvo izvršenja javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom smislu. Osim terorizma i organizovanog kriminala, BIA je nadležna za suprotstavljanje i svim drugim vrstama visokotehnološkog kriminala, ako su njegove posledice takve prirode da mogu destabilizovati nacionalnu bezbednost npr. kroz ugrožavanje ustavnog, ekonomskog ili monetarnog sistema.

Suprotstavljanje navedenim bezbednosnim pretnjama vrše operativni radnici koji su raspoređeni u organizacione jedinice za suprotstavljanje svim vidovima terorizma, organizovanog kriminala i kriminala koji ugrožava nacionalnu bezbednost, tako da nije moguće odrediti broj, strukturu i obučenost zaposlenih u BIA samo za ovu oblast. Potrebno je istaći da Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala nije prepoznao Bezbednosno-informativnu agenciju kao jednu od institucija koja se bavi suprostavljanjem ovoj vrsti kriminala, iako je za to nadležna po Zakonu o Bezbednosno- informativnoj agenciji.

Vojnobezbednosna agencija u skladu sa zakonom obavlja poslove bezbednosne i kontraobaveštajne zaštite Ministarstva odbrane i Vojske Srbije i u okviru iste, poslove otkrivanja, sprečavanja i dokazivanja krivičnih dela protiv bezbednosti računarskih podataka. Vojnobezbednosna agencija je ovlašćena da sprovodi bezbednosnu zaštitu IKT sistema. Pored navedenog, Vojnobezbednosna agencija je ovlašćena za otkrivanje, praćenje i onemogućavanje unutrašnjeg i međunarodnog terorizma, ekstremizma i drugih oblika organizovanog nasilja usmerenih protiv Ministarstva odbrane i Vojske Srbije; odnosno otkriva, istražuje i prikuplja dokaze za krivična dela protiv ustavnog uređenja i bezbednosti Republike Srbije, krivična dela protiv čovečnosti i drugih dobara zaštićenih međunarodnim pravom, krivična dela organizovanog kriminala, krivično delo pranje novca kao i krivična dela korupcije (zloupotreba službenog položaja, trgovina uticajem, primanje mita i davanje mita) i ako nisu rezultat delovanja organizovane kriminalne grupe, unutar Ministarstva odbrane i Vojske Srbije. Ove poslove, konkretno, vrše ovlašćena službena lica raspoređena u organizacionim jedinicama Vojnobezbednosne agencije, prema aktu o formaciji.

Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL), osnovana Zakonom o elektronskim komunikacijama, je regulatorno telo u oblasti

elektronskih komunikacija i poštanskih usluga, nadležna je, između ostalog, za saradnju sa regulatornim i stručnim telima država članica Evropske unije i drugih država radi usaglašavanja prakse, primene propisa iz oblasti elektronskih komunikacija i podsticanja razvoja prekograničnih elektronskih komunikacionih mreža i usluga. Takođe, učestvuje u radu međunarodnih organizacija i institucija u oblasti elektronskih komunikacija u svojstvu nacionalnog regulatornog tela u oblasti elektronskih komunikacija. Stupanjem na snagu i početkom primene Zakona o informacionoj bezbednosti utvrđeno je da je RATEL nadležan za koordinaciju i izvršavanje poslova Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni CERT).

Odredbom člana 31. Zakona o ministarstvima propisano je da Zavod za intelektualnu svojinu (ZIS) obavlja stručne poslove i poslove državne uprave koji se odnose na: patent i mali patent, žig, dizajn, oznaku geografskog porekla, topografiju integrisanog kola, autorsko pravo i srodna prava; primenu međunarodnih ugovora iz oblasti zaštite intelektualne svojine i predstavljanje i zastupanje interesa Republike Srbije u specijalizovanim međunarodnim organizacijama za zaštitu intelektualne svojine; nadzor nad radom organizacija za kolektivno ostvarivanje autorskog prava i srodnih prava; razvoj u oblasti zaštite intelektualne svojine; informaciono-obrazovne poslove u oblasti zaštite intelektualne svojine, kao i druge poslove određene zakonom. Predlaganje propisa iz oblasti zaštite i prometa intelektualne svojine u delokrugu je Ministarstva prosvete, nauke i tehnološkog razvoja, kao i vršenje nadzora nad radom Zavoda za intelektualnu svojinu. Zavod sarađuje sa različitim državnim organima nadležnim za efikasno sprovođenje prava intelektualne svojine kroz rad Koordinacionog tela za efikasnu zaštitu prava intelektualne svojine u Republici Srbiji, koje je osnovano Odlukom Vlade („Službeni glasnik RS”, broj 121/14), kao i kroz rad tri radne grupe koje je oformilo ovo telo. Zadatak Koordinacionog tela za efikasnu zaštitu prava intelektualne svojine u Republici Srbiji je da, na polju operativne zaštite prava intelektualne svojine, prati i usmerava pojedine poslove iz delokruga više organa državne uprave radi obezbeđivanja efikasne zaštite prava intelektualne svojine.

Uloga Privredne komore Srbije (PKS) u borbi protiv visokotehnološkog kriminala svodi se na edukaciju privrednika, kao i na povremeno prikupljanje informacija o incidentima, kao i njihova analiza i uticaj na poslovanje. Razmatra se uvođenje tima koji bi se permanentno bavio ovom problematikom.

Udruženje banaka Srbije (UBS) okuplja sve banke koje posluju na teritoriji Republike Srbije, banke u Udruženju formiraju stučne odbore preko kojih se bave različitim oblastima iz svog poslovanja. Odbor za bezbednost koji funkcioniše pri Udruženju banka Srbije okuplja predstavnike većine banka koji se bave poslovima bezbednosti (informacione, fizičko tehničke, prevencijom prevara i dr.). Međusobnom saradnjom kao i uspostavljanjem saradnje sa državnim organima iz oblasti visokotehnološkog kriminala Odbor deluje preventivno i reaktivno u borbi protiv visokotehnološkog kriminala.

4.2. Saradnja državnih organa u okviru borbe protiv visokotehnološkog kriminala

Shodno Zakoniku o krivičnom postupku, svi organi koji učestvuju u predistražnom postupku dužni su da o svakoj radnji preduzetoj u cilju otkrivanja krivičnog dela ili pronalaženja osumnjičenog obaveste nadležnog javnog tužioca. Policija i drugi državni organi nadležni za otkrivanje krivičnih dela dužni su da postupe po svakom zahtevu nadležnog javnog tužioca.

U vezi preduzimanja krivičnog gonjenja učinilaca krivičnih dela visokotehnološkog kriminala, Posebno tužilaštvo za visokotehnološki kriminal najveći deo saradnje ostvaruje sa Ministarstvom unutrašnjih poslova, Službom za borbu protiv organizovanog kriminala,

Odeljenjem za suzbijanje visokotehnološkog kriminala, sa Službom za specijalne istražne metode koja se ogleda u pronalaženju dokaza vezanih za izvršenje krivičnih dela visokotehnološkog kriminala, a izuzetna saradnja je ostvarena i sa Odeljenjem za javni red i mir, Policijske uprave za grad Beograd. Republičko javno tužilaštvo i Posebno tužilaštvo za visokotehnološki kriminal ostvaruju saradnju sa Ministarstvom trgovine, turizma i telekomunikacija u vezi sa primenom Uredbe o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija koja je doneta u junu 2016. godine i Nacionalnim kontakt centrom za bezbednost dece na internetu.

Odeljenje za suzbijanje visokotehnološkog kriminala značajan deo svojih aktivnosti sprovodi u saradnji sa Tužilaštvom za organizovani kriminal. U periodu od 2008. godine do danas, ovo odeljenje je sprovelo ukupno osam samostalnih operativnih obrada. U okviru jedne od operativnih obrada, po prvi put u Republici Srbiji je potpisan Ugovor o osnivanju zajedničkog istražnog tima između Republike Srbije i Kraljevine Holandije. Odeljenje je u istom periodu postupalo po većem broju zamolnica za međunarodnu pravnu pomoć Tužilaštva za organizovani kriminal i to u međunarodnim operacijama „Rico" i „Bug Byte" sa američkim FBI, po zamolnici FBI u vezi međunarodnog krijumčarenja oružja, te u operaciji „Atlantis" (nelegalno „on-line" klađenje) kod koje je predistražni postupak započelo Tužilaštvo za organizovani kriminal, ali je sudski postupak vođen pred Višim sudom u Beogradu, a optužnicu je zastupalo Posebno tužilaštvo za visokotehnološki kriminal.

Pored ovih samostalnih aktivnosti, Odeljenje je učestvovalo u većem broju operativnih obrada Službe za borbu protiv organizovanog kriminala, pružajući operativnu i tehničku podršku drugim odeljenjima. Sprovedeno je preko 25 operativnih obrada, među kojima su i neke od najvećih operativnih obrada Službe.

Radi efikasne koordinacije i saradnje državnih organa u oblasti informacione bezbednosti, Vlada je obrazovala Telo za koordinaciju poslova informacione bezbednosti, kojim predsedava predstavnik Ministarstva trgovine, turizma i telekomunikacija, a u njegovom radu učestvuju predstavnici ministarstava nadležnih za poslove odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Kancelarije za informacione tehnologije i elektronsku upravu i Nacionalnog CERT.

Shodno Odluci o obrazovanju Tela za koordinaciju poslova informacione bezbednosti („Službeni glasnik RS", br. 24/16, 53/17, 79/17 i 112/17) zadatak Tela je da ostvaruje saradnju između organa i usklađuje obavljanje poslova u funkciji unapređenja informacione bezbednosti, inicira i prati preventivne i druge aktivnosti u oblasti informacione bezbednosti, predlaže mere za unapređenje informacione bezbednosti u Republici Srbiji, daje sugestije i predloge koji se odnose na pripremu strateških dokumenata, podzakonskih akata i politika informacione bezbednosti u Republici Srbiji i utvrđuje međusobnu saradnju u slučaju incidenata koji mogu da imaju znatan uticaj na narušavanje informacione bezbednosti u Republici Srbiji.

U oblasti bezbednosti dece na internetu, ovo ministarstvo sarađuje sa organima nadležnim za borbu protiv visokotehnološkog kriminala. Naime, Nacionalni kontakt centar za bezbednost dece na internetu 19833 (veb sajt: www.pametnoibezbedno.gov.rs) vrši savetovanje i omogućava prijem prijava štetnog, neprimerenog i nelegalnog sadržaja i ponašanja na internetu, odnosno ugroženosti interesa i prava dece, telefonskim putem i putem elektronskog obrasca na veb sajtu. U slučaju da navodi iz prijave ukazuju na postojanje krivičnog dela, Ministarstvo prosleđuje prijavu radi daljeg postupanja Republičkom javnom tužilaštvu i, radi informisanja, Ministarstvu unutrašnjih poslova.

Na predlog Ministarstva trgovine, turizma i telekomunikacija Vlada je donela Odluku o obrazovanju Koordinacionog tela u oblasti bezbednosti i zaštite dece pri korišćenju

informaciono-komunikacionih tehnologija („Službeni glasnik RS”, broj 9/18) u čijem sastavu su predstavnici Ministarstva trgovine, turizma i telekomunikacija, Ministarstva za rad, zapošljavanje, boračka i socijalna pitanja, Ministarstva zdravlja, Ministarstva unutrašnjih poslova, Ministarstva kulture i informisanja i Ministarstva prosvete, nauke i tehnološkog razvoja. Zadatak Koordinacionog tela je da ostvaruje saradnju između organa i usklađuje obavljanje poslova u funkciji unapređenja bezbednosti i zaštite dece pri korišćenju informaciono-komunikacionih tehnologija, inicira i prati preventivne i druge aktivnosti u oblasti bezbednosti i zaštite dece na internetu, predlaže mere za unapređenje bezbednosti i zaštiti dece na internetu i utvrđuje međusobnu saradnju.

Uprava carina u ovoj oblasti sarađuje sa Posebnim tužilaštvom u pogledu razmene podataka. Takođe, razvijena je saradnja sa carinskom administracijom Francuske i Austrije, kroz čije je obuke na temu „Cyber customs” u dva navrata već prošao deo carinskih službenika. Pored toga, Uprava carina svakodnevno razmenjuje podatke sa drugim carinskim administracijama, na osnovu potpisanih međunarodnih sporazuma.

U okviru potpisanog Protokola između Ministarstva unutrašnjih poslova i Ministarstva prosvete, nauke i tehnološkog razvoja realizuje se projekat „Osnovi bezbednosti dece”. U okviru ovog projekta obučeni policijski službenici realizuju nastavu u svim četvrtim i šestim razredima osnovnih škola, a između ostalog posebno se obraćuju teme Bezbednost dece na internetu. Određene teme iz oblasti visokotehnološkog kriminala prilagođene su uzrastu dece, a deca se edukuju u oblastima korišćenja interneta u kojima su najranjivija.

Imajući u vidu nadležnost Bezbednosno-informativna agencija u ovoj oblasti, ostvaruje saradnju sa Posebnim odeljenjem za borbu protiv visokotehnološkog kriminala, Višeg javnog tužilaštva u Beogradu i Službom za borbu protiv organizovanog kriminala – Odeljenjem za suzbijanje visokotehnološkog kriminala.

Vojnobezbednosna agencija u ostavrivanju svojih nadležnosti sarađuje sa svim relevantnim državnim organima. Radi se o zakonskoj obavezi, koju ustanovljava odredba člana 3. stav 4. Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji prema kojoj Vojnobezbednosna agencija sarađuje i razmenjuje podatke sa nadležnim organima, organizacijama, službama i telima Republike Srbije, u skladu sa Ustavom, zakonom, drugim propisima i opštim aktima, odnosno utvrđenom bezbednosno-obaveštajnom politikom Republike Srbije.

Odbor za bezbednost koji funkcioniše pri Udruženju banaka Srbije sarađuje sa Narodnom bankom Srbije kao regulatorom. Finansijske institucije, koje su IKT sistemi od posebnog značaja u skladu sa Zakonom o informacionoj bezbednosti, u obavezi su da o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti obaveste Narodnu banku Srbije. Pored redovnih kanala komunikacije ka državnim organima, Odbor je uspostavio i radi na unapređenju saradnje sa Odeljenjem za suzbijanje visokotehnološkog kriminala i Posebnim tužilaštvom za visokotehnološki kriminal u cilju efikasne i pravovremene reakcije na različite oblike visokotehnološkog kriminala.

4.3. Saradnja sa subjektima civilnog društva, stručnom javnošću, medijima i privredom

Oblici saradnje sa subjektima civilnog društva i privredom su na zadovoljavajućem nivou i ostvaruju se kroz potpisivanje odgovarajućih ugovora i protokola o saradnji između zainteresovanih strana, organizovanjem javnih rasprava o nacrtima propisa, kao i održavanjem konferencija, seminara, obuka, radionica.

Posebno tužilaštvo prilikom suzbijanja krivičnih dela visokotehnološkog kriminala ima dobru saradnju sa civilnim društvom i privredom, a pogotovo sa bankarskim sektorom, internet servis provajderima, mobilnim operaterima, Privrednom komorom Srbije i Beograda, medijskim kućama, udruženjima koja zastupaju nosioce autorskih prava, Nacionalnim CERT, a koja se ogleda u razmeni informacija, učestvovanjem u radnim grupama i okruglim stolovima i drugim oblicima saradnje, a sve u cilju uspešne borbe protiv visokotehnološkog kriminala.

Potrebno je istaći i da je Republičko javno tužilaštvo zaključilo 2013. godine Memorandum o saradnji sa Fondom B92 u cilju realizacije projekta „Klikni bezbedno" Centar za bezbedni internet Srbija na suzbijanju i rešavanju problema nezakonitog, neprimerenog i štetnog sadržaja i neprimerenog ponašanja na internetu, kao i na širenju informacija o načinima bezbednog korišćenja interneta.

U okviru projekta formirana je online platforma pod nazivom Net partola u cilju anonimnog prijavljivanja nezakonitog sadržaja na internetu, posebno iskorišćavanja maloletnih lica u pornografske svrhe, kao i izvršenje drugih krivičnih dela putem interneta (npr. maltretiranje u virtuelnom svetu tzv. cyberbullying). Net patrola član je međunarodne organizacije INHOPE – Internation Association of Internet Hotlines, koja koordiniše i pomaže rad mreže ovakvih servisa za prijavu nelegalnog sadržaja na internetu širom sveta.

Pored navedene saradnje, Republičko javno tužilaštvo i Posebno tužilaštvo za visokotehnološki kriminal uspostavili su saradnju sa međunarodnom organizacijom civilnog društva „Save the children", u okviru programa Pravosudne akademije za izradu plana i programa obuke za sudije i javne tužioce u oblasti visokotehnološkog kriminala i zaštite maloletnih lica na internetu. U skladu sa uspostavljenom saradnjom, od januara 2017. godine počele su osnovne i napredne obuke na temu visokotehnološkog kriminala i bezbednosti dece na Internetu. U okviru projekta izrađen je Priručnik za sudije i javne tužioce na temu zaštite dece od nasilja na internetu i razmatra se potpisivanje sporazuma o saradnji sa organizacijom „Save the children".

Organizacija „Save the children" je u saradnji sa Ministarstvom trgovine, turizma i telekomunikacija izradila Mapu puta prevencije onlajn i drugih oblika nasilja nad decom na internetu u Republici Srbiji[19], koja pruža prikaz dobrih praksi i primera drugih zemalja. Navedeni dokument takođe daje smernice na putu kojim bi Republika Srbija trebalo da se kreće u odnosu na sopstvene kapacitete u ovom polju.

Takođe, 26. decembra 2016. godine Republičko javno tužilaštvo, Ministarstvo unutrašnjih poslova, Udruženje novinara Srbije, Nezavisno udruženje novinara Srbije, Udruženje novinara Vojvodine, Nezavisno društvo novinara Vojvodine, Asocijacija nezavisnih elektronskih medija, Asocijacija medija i Asocijacija onlajn medija zaključili su Sporazum o saradnji i merama za podizanje nivoa bezbednosti novinara. Ovim sporazumom predviđene su obuke novinara i vlasnika medija o osnovama informacione bezbednosti informativnih internet portala, uključujući i obuku u pogledu primene osnovnih mera zaštite od napada korišćenjem informacionih tehnologija.

Nastupi u medijima kroz proaktivan pristup su veoma značajni za preventivne aktivnosti za sve subjekte na polju borbe protiv visokotehnološkog kriminala. Nastupi u medijima upoznaju građane i podižu svest o opasnostima koje donosi kontinuirani razvoj digitalnog društva, te se na taj način građani edukuju kako bi samostalno mogli da identifikuju opasnosti i preventivno deluju i time ne postanu žrtve nekog krivičnog dela putem interneta, odnosno minimalizuju štetne posledice.

[19] https://nwb.savethechildren.net/sites/nwb.savethechildren.net/files/library/Mapa%20puta-Srbija.pdf

Udruženje banaka Srbije informiše građane o bezbednosnim rizicima posredstvom javnog veb sajta Udruženja i aktivnostima koje organizuje u samom Udruženju (Centar za bankarsku obuku, rad Odbora za bezbednost i dr.). Banke članice informišu bankarske klijente različitim kanalima informisanja.

Ministarstvo trgovine, turizma i telekomunikacija sprovodi informisanje dece, roditelja i nastavnika o opasnostima na internetu i merama prevencije putem veb sajta „Pametno i bezbedno" (www.pametnoibezbedno.gov.rs), kao i putem televizijskih video programa. Naime, Ministarstvo trgovine, turizma i telekomunikacija u okviru navedenog projekta sprovodi na godišnjem nivou kampanju „IT karavan". Prvi „IT karavan" sproveden je od 20. aprila do 3. juna 2016. godine. Školskim prezentacijama prisustvovalo je 5000 učenika starijih razreda osnovnih škola u 15 škola, dok je na gradskim trgovima promociju ovog projekta videlo više hiljada građana. U 2017. godini u okviru „IT karavana" prezentacijama o zaštiti od digitalnog nasilja i drugih oblika zloupotrebe dece na Internetu prisustvovalo je više od 5500 učenika i oko 90 nastavnika iz 17 osnovnih škola iz Srbije. I u 2018. godini, treću godinu za redom, sprovedena je kampanja „IT karavan" za učenike osnovnih škola u Srbiji, njihove roditelje i nastavnike, sa ciljem podsticanja pametnog i bezbednog korišćenja novih tehnologija. Glavni program koji čine edukativna prezentacija o bezbednosti dece na internetu i radionice za učenike i roditelje, predstavljen je za ukupno 26 škola, u regionalnim centrima u Republici Srbiji. Program iz Niša i Novog Pazara pratilo je još oko 800 škola putem direktnog internet prenosa, a na mapi puta IT karavana 03 bili su i Beograd, Subotica i Novi Sad. U okviru kampanje realizovane su i otvorene promocije za građane, kao i dodatne radionice za roditelje u još šest gradova: Sečnju, Zrenjaninu, Leskovcu, Čačku, Kraljevu i Užicu. Stalni partneri Ministarstva u realizaciji ove kampanje su i Ministarstvo prosvete, nauke i tehnološkog razvoja i Kompanija Majkrosoft, a u prve dve godine jedan od partnera je bilo i Ministarstvo unutrašnjih poslova, dok su se u 2018. godini kampanji pridružili Nacionalna asocijacija roditelja i nastavnika Srbije i Fondacija Petlja.

Preventivne aktivnosti Ministarstva finansija, Uprave za sprečavanje pranja novca ogledaju se kroz kontinuirane obuke obveznika i upoznavanje istih sa novim trendovima i tipologijama, u vezi sa pranjem novca i finansiranjem terorizma. Uspostavljena je odgovarajuća saradnja sa relevantim državnim i međunarodnim institucijama kroz veliki broj stručnih skupova, seminara, obuka, kao i tribina u smislu zajedničke edukacije svih zainteresovanih subjekata u cilju podizanja svesti o značaju suzbijanja ove vrste kriminaliteta.

Na Kriminalističko-policijskom univerzitetu u Zemunu, za studente četvrte godine na smeru kriminalistike u okviru predmeta Ekonomski kriminal, predavanje na temu „Sistem zaštite intelektualne svojine", već treću godinu zaredom održavaju predstavnici Zavoda za intelektualnu svojinu. U 2017. godini, za predstavnike Uprave carina održana je radionica o pretraživanju baza podataka industrijske svojine, pre svega žigova i industrijskog dizajna.

4.4. Međunarodna saradnja u oblasti visokotehnološkog kriminala

Međunarodna saradnja se sprovodi kroz različite vidove: međunarodne sajber vežbe, drill, radionice sa ciljem povećanja razumevanja i izgradnje kapaciteta sa težištem na transnacionalnim sajber bezbedonosnim izazovima i pretnjama, kolektivnom pristupu njihovom rešavanju kako bi se poboljšala regionalna i globalna razmena informacija za razvoj sajber strategija i politika sajber bezbednosti u cilju brzog odgovora na sajber pretnje.

Posebno tužilaštvo za visokotehnološki kriminal od 2010. godine u okviru Evropske unije, Saveta Evrope i OEBS i drugih međunarodnih organizacija učestvuje u projektima koji imaju za cilj olakšavanje međunarodne saradnje, njeno ubrzavanje i pravovremeno reagovanje prilikom izvršenja krivičnih dela visokotehnološkog kriminala. Pored toga, Posebni tužilac za visokotehnološki kriminal određen je za kontakt tačku mreže 24/7 propisane Budimpeštanskom konvencijom. Na taj način, uspostavljena je direktna saradnja sa ostalim kontakt tačkama iz zemalja potpisnica Konvencije, u cilju efikasnijeg postupanja u predmetima sa elementom inostranosti.

Odeljenje za suzbijanje visokotehnološkog kriminala je jedna od najaktivnijih organizacionih jedinica Ministarstva unutrašnjih poslova u oblasti međunarodne saradnje. Saradnja se ostvaruje na dnevnoj bazi kroz sve standardne kanale međunarodne policijske saradnje, posredstvom Interpola i Europola, preko oficira za vezu detaširanih u ambasadama u Beogradu (pre svega SAD i Velike Britanije), posredstvom regionalnih organizacija (npr. SECI Center, SELEC,), ali vrlo često i u direktnoj policijskoj saradnji u zajedničkim međunarodnim akcijama. U Odeljenju je uspostavljena međunarodna kontaktna tačka 24/7 za visokotehnološki kriminal u okviru Saveta Evrope, kao i kontaktne tačke u okviru Europol i to „Twins" (dečija pornografija) i „Cyborg" (sajber kriminal).

Takođe, 2016. godine policijski službenici Službe za borbu protiv organizovanog kriminala sprovodeći višegodišnju međunarodnu policijsku akciju „BUGBYTE" na suzbijanju krivičnih dela protiv sajber kriminala, falsifikovanja i zloupotreba platnih kartica koju sprovodi Federalni istražni biro (FBI) iz SAD-a, sarađivali su sa policijskim službama iz: Republike Srbije, Republike Srpske, Kanade, Australije, Republike Indije, Savezne Republike Brazila, Države Izraela, Ujedinjenog Kraljevstva Velike Britanije i Severne Irske, Rumunije, Republike Hrvatske, Republike Makedonije, Kraljevine Danske, Kraljevine Švedske, Republike Letonske Republike, Republike Kostarike, Kiparske Republike, Republike Kolumbije i Savezne Republike Nigerije. Pored toga, 2016. godine, odobreno je povezivanje Ministarstva unutrašnjih poslova na Interpolovu bazu „ICSE" (baza foto i video materijala seksualne eksploatacije dece).

U prostorijama Odeljenja za suzbijanje visokotehnološkog kriminala instalirana je komunikaciona oprema koja je donirana od strane Generalnog Sekretarijata Interpola, te je pristup bazi podataka „ICSE" omogućen. Kada govorimo o rezultatima, ovo je baza koja služi za identifikaciju žrtava kao i informaciji sa kojih mesta se distribuiraju ilegalni snimci. U našoj zemlji ovo još nije tip kriminala koji je u ozbiljnoj meri zaživeo po pitanju proizvodnje ilegalnih snimaka i prodaje te se kod nas neće pronalaziti žrtve putem ove baze u toj meri kao što je to primer u nekim drugim državama. Doprinos će uglavnom biti što će ostale države koje imaju pristup ovoj bazi eventualno dobiti materijal sa novim žrtvama koji je pronađen tokom pretresa u Republici Srbiji. Predstoji realizacija obuke namenjena korišćenju ove baze podataka koju će izvoditi instruktori iz Generalnog Sekretarijata Interpola.

Ministarstvo finansija, Uprava za sprečavanje pranja novca je član Egmont grupe, grupe koja okuplja finansijsko-obaveštajne službe iz 156 država. To joj daje mogućnost da veoma brzo dođe do veoma bitnih finansijsko-obaveštajnih podataka od drugih država, ako u vezi sa određenom transakcijom ili licem postoje osnovi sumnje da se radi o pranju novca ili finansiranju terorizma. Uprava aktivno učestvuje u radu Komiteta Manival, stručnog komiteta Saveta Evrope koji radi po sistemu uzajamnih procena država članica. Još jedan veoma značajan aspekt međunarodne saradnje Uprave za sprečavanje pranja novca je mogućnost za zaključivanje sporazuma o saradnji sa stranim partnerima. Uprava za sprečavanje pranja novca je do sada potpisala sporazume o saradnji sa 44 države.

Uprava carina u skladu sa postojećim zakonskim ovlašćenjima, Protokolom 6 Sporazuma o stabilizaciji i pridruživanju, u međusobnoj administrativnoj saradnji u

carinskim pitanjima između Republike Srbije i EU i postojećim potpisanim bilateralnim sporazumima, razmenjuje podatke sa drugim carinskim administracijama.

Bezbednosno-informativna agencija ostvaruje regionalnu i širu međunarodnu saradnju, prvenstveno sa drugim sigurnosnim ili sigurnosno-obaveštajnim službama i agencijama.

Vojnobezbednosna agencija ostvaruje međunarodnu saradnju u skladu sa odredbom člana 36. stav 1. Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji prema kojoj, Vojnobezbednosna agencija, shodno utvrđenoj bezbednosno-obaveštajnoj politici Republike Srbije, razmenjuje podatke sa organima i službama bezbednosti stranih država i međunarodnih organizacija, u skladu sa Ustavom, zakonom, drugim propisima i opštim aktima i potvrđenim međunarodnim ugovorima.

Zavod za intelektualnu svojinu ima razvijenu saradnju sa Svetskom organizacijom za intelektualnu svojinu (WIPO), Evropskom patentnom organizacijom (EPO) i Zavodom za intelektualnu svojinu Evropske Unije (EUIPO). Predstavnici Zavoda za intelektualnu svojinu prisustvuju sastancima Savetodavnog kominteta WIPO za primenu prava intelektualne svojine koji pruža tehničku pomoć i koordinira u oblasti primene prava intelektualne svojine. Na ovim sastancima se redovno razmatra i „onlajn" povreda prava intelektualne svojine. *EUIPO* organizuje seminare za predstavnike organa nadležnih za primenu prava intelektualne svojine (sudije, tužioce, carinske službenike i predstavnike nacionalnih zavoda za intelektualnu svojinu). Teme koje se obrađuju u okviru ovih obuka obuhvataju ponekad i pitanja povrede prava intelektualne svojine posmatrane sa aspekta krivičnog prava. Predstavnici Zavoda za intelektualnu svojinu su do sada dva puta posetili i Opservatoriju *EUIPO* koja prati povrede prava intelektualne svojine i koja pruža potrebno znanje i informacije svojim članovima. Saradnja sa Evropskom organizacijom za patente odvija se kroz aktivnosti ugovorene Bilateralnim planom saradnje za period 2016. do 2018. godine, koje se odnose na obuku stručnjaka, saradnju u razvoju usaglašenih evropskih informaciono-tehnoloških servisa i alata i saradnju u podizanju svesti o značaju zaštite intelektualne svojine. Međunarodni ugovori iz oblasti intelektualne svojine koje je ratifikovala Republika Srbija, a koji su značajni za uređenje digitalnog okruženje su WIPO Ugovor o autorskom pravu i WIPO Ugovor o interpretacijama i fonogramima, koji su zaključeni 20. decembra 1996. godine u Ženevi („Službeni list SRJ – Međunarodni ugovori", broj 13/02). Ovi ugovori su poznati pod nazivom „Internet ugovori" i sadrže norme koje imaju za cilj sprečavanje neovlašćenog pristupa kreativnim delima i sprečavanje njihovog korišćenja na internetu ili drugoj digitalnoj mreži.

5. KRATAK PREGLED TRENDOVA U OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

5.1. Opšti pokazatelji

Posebno je potrebno naglasiti da je broj korisnika interneta kako na globalnom nivou, tako i u Republici Srbiji u konstantnom porastu. Javno dostupni statistički podaci govore o tome da je u 2007. godini registrovano da je Internet koristilo ukupno 1.365.000.000 korisnika. Dana 31. marta 2017. godine ukupan broj korisnika u celom svetu iznosio je 3.731.973.423. U Republici Srbiji je u toku 2007. godine registrovano 1.270.000 korisnika. Dana 31. marta 2017. godine broj internet korisnika u našoj državi iznosio je ukupno 4.705.141. Od 2007. godine do 31. marta 2017. godine na globalnom nivou broj korisnika se povećao za ukupno 273,40 %. U Republici Srbiji se broj korisnika u navedenom vremenskom periodu povećao za 370%.

Istraživanje Republičkog zavoda za statistiku o upotrebi informaciono-komunikacionih tehnologija u domaćinstvima koje je sprovedeno na uzorku od 2.800 domaćinstava u Republici Srbiji govori o tome da 68,1% domaćinstava u Republici Srbiji poseduje računar, dok je 2007. godine 34% domaćinstava imalo računar. U istom istraživanju koje je sprovedeno utvrđeno je da 68,0% domaćinstava poseduje internet priključak. Broj internet priključaka u domaćinstvima 2007. godine iznosio je ukupno 26,3%. U 2017. godini 61,9% domaćinstava imalo je širokopojasnu internet konekciju. Taj broj je 2007. godine iznosio 7,3%. U 2017. godini u Republici Srbiji u četvrtom kvartalu bilo je 1,49 miliona aktivnih pretplatnika širokopojasnog pristupa Internetu.

Veoma je interesantan podatak da su mobilni telefoni u Republici Srbiji 2017. godine bili kao uređaji zastupljeni sa 90,5%. Zastupljenost upotrebe 3G mreže (internet preko mobilne telefonije) je kod 53,6% korisnika. Mladi uzrasta od 16 do 24 godine starosti koriste mobilne telefone za pristup Internetu u procentu koji se kreće i do 92,6%. Prosečno korišćenje pametnih telefona iznosi pet sati dnevno u Republici Srbiji, naspram prosečnih 3,3 sata u Zapadnoj Evropi.

Istraživanja pokazuju i da se 62% starijih osnovaca i 84% srednjoškolaca bar jednom tokom godinu dana izložilo nekom riziku na Internetu.

Sprovedena istraživanja Republičkog zavoda za statistiku ukazuju i na to da 99,7% anketiranik preduzeća (reprezentativni uzorak je bio 1655 preduzeća) koristi računare, kao i da 99,7% tih preduzeća ima internet konekciju.

Interesantno je da je od 2007. godine pristup širokopojasnom internetu imalo 55% preduzeća, dok je taj broj 2017. godine iznosio čak 98,6%, dakle broj se gotovo udvostručio.

Socijalne mreže su, takođe, jako zastupljene. Najpopularniji je „Facebook". U junu 2016. godine, u Republici Srbiji je bilo ukupno 4.758.861. korisnika Interneta (prema podacima Internet live stats; u 2017. godini prema podacima Hootsuite - We are social, je 5,74 miliona) od kojih je ukupno 3.500.000 koristilo „Facebook". I na globalnom nivou broj korisnika socijalne mreže Fejsbuk je u konstantnom porastu od 2008. godine. Ova društvena mreža je jedna od najomiljenijih i za nju je dat prikaz imajući u vidu da krajem 2017. godine ima veći broj korisnika (preko 2,1 milijarde) nego WhatsUp (900.000.000), Twitter (328.000.000) i Instagram (400.000.000) zajedno.

5.2. Statistika i baze podataka

Posebno tužilaštvo vodi evidenciju svih predmeta i postupanja po istim, kroz jedinstveni informacioni sistem javnih tužilaštava, a baza podataka se ažurira na dnevnom nivou.

U Ministarstvu unutrašnjih poslova se podaci o krivičnim delima, uključujući i krivična dela visokotehnološkog kriminala, evidentiraju na mesečnom nivou u programskom sistemu pod nazivom „Krivična dela i učinioci". Radi se o jedinstvenoj elektronskoj evidenciji podataka o krivičnim delima koja se gone po službenoj dužnosti. Ova obimna baza podataka obuhvata, pored navedenog i podatke o učiniocima krivičnih dela i oštećenim licima, kao i o njihovoj starosnoj, polnoj i drugoj strukturi, zatim o načinu izvršenja (vreme, mesto, sredstvo izvršenja krivičnih dela), rasvetljenim i nerasvetljenim krivičnim delima, predmetima krivičnih dela, primenjenim merama prema učiniocima itd. Podaci se u ovoj bazi evidentiraju na osnovu podnetih krivičnih prijava od strane podnosioca, odnosno policijskih službenika organizacionih jedinica nadležnih za poslove suzbijanja kriminala. Podaci se unose na osnovu propisane metodologije i redovno se ažuriraju.

Ministarstvo finansija, Uprava za sprečavanje pranja novca raspolaže bazama podataka o gotovinskim i sumnjivim transakcijama koje prijavljuju obveznici po Zakonu o sprečavanju pranja novca i finansiranja terorizma. Navedene baze se ažuriraju na dnevnom nivou. Uprava carina koristi: Informacioni sistem carinske službe, Obaveštajnu baza podataka, pravo pristupa Poreskoj bazi podataka (JRPO). Pored navedenih, od početka 2015. godine u funkcionalnoj upotrebi je i Novi kompjuterizovani tranzinti sistem (NCTS). Takođe, treba pomenuti i bazu podataka Svetske carinske organizacije (CEN) u koju se unose isključivo podaci (nenominalni) o carinskim prekršajima. Podaci u svim bazama ažuriraju se na dnevnom nivou. Odeljenje za obaveštajne poslove vodi statistiku na: dnevnom, nedeljnom, mesečnom, kvartalnom i godišnjem nivou. Podaci koje Odeljenje za obaveštajne poslove redovno prikuplja su: narkotici, cigarete, duvan lekovi, oružje i municija (sve vrste i količine), zlato, naftni derivati (u količini od najmanje 100 litara), devizni prekršaji (iznosi od 10.000 EUR/USD/CHF pa naviše), prekršaji protiv životne sredine, kulturna dobra, ilegalni migranti, sva druga carinska roba vrednosti preko 3.000 evra.

Ministarstvo trgovine, turizma i telekomunikacija vodi Registar pružalaca kvalifikovanih usluga od poverenja i Registar kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata.

Regulatorna agencija za elektronske komunikacije i poštanske usluge vodi evidenciju o posebnim CERT, koja se ažurira redovno**.**

Na sajtu Zavoda za intelektualnu svojinu pristupačne su sledeće nacionalne baze podataka: Baza podataka žigova i industrijskog dizajna i Baza podataka za patente MIMOSA RS. Takođe, nalazi se link ka nekomercijalnoj svetskoj bazi podataka patentne dokumentacije - Espacenet, koja je dostupna svima preko interneta i koja sadrži podatke od preko 70 miliona objavljenih patentnih prijava i odobrenih patenata iz preko 90 različitih zemalja (i naših) i regiona iz celog sveta, od 1836. godine do danas.

Privredna komora Srbije poseduje Bazu podataka o spoljnotrgovinskoj robnoj razmeni Srbije i spoljnotrgovinskoj robnoj razmeni zemalja (ažuriranje se vrši na mesečnm nivou) i Bazu COMTRADE (preuzimanje preko veb servisa), gde se ažuriranje vrši na godišnjem nivou.

5.3. Statistički trendovi u oblasti visokotehnološkog kriminala[20]

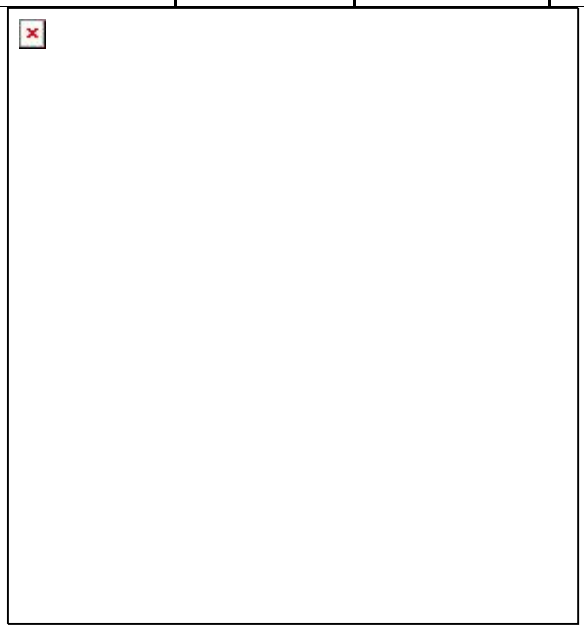
Prema podacima Posebnog odeljenja za borbu protiv visokotehnološkog kriminala u proteklih pet godina na teritoriji Republike Srbije (period 2013-2017. godina) stopa kriminala je u porastu.

Pregled broja predmeta Posebnog tužilaštva za visokotehnološki kriminal zaključno sa 31.12.2017. godine.

	Broj predmeta zavedenih u upisnik poznatih punoletnih učinilaca	**Broj predmeta zavedenih u upisnik nepoznatih učinilaca**	**Broj predmeta zavedenih u upisnik ostalih krivičnih predmeta**	**Ukupno zavedenih predmeta po upisnicima**	**Procenat povećanja/smanjenja broja predmeta u odnosu na prethodnu godinu**

[20] Strateška procena javne bezbednosti, MUP

2006.	19	0	0	19	
2007.	75	11	68	154	+710.53%
2008.	110	14	60	184	+19.48%
2009.	91	42	114	247	+34.24%
2010.	116	13	443	572	+131.58%
2011.	130	28	502	660	+15.38%
2012.	114	65	609	788	+19.39%
2013.	160	243	558	961	+21.95%
2014.	294	770	352	1423	+48,07%
2015.	198	570	1306	2074	+45,74%
2016.	240	580	1237	2057	-0,82%
2017.	213	945	1213	2371	+15,26%



U periodu od 1. januara 2013. godine do 31. decembra 2017. godine, Posebnom tužilaštvu za visokotehnološki kriminal podnete su krivične prijave protiv ukupno 1.318 poznatih punoletnih lica, dok je optužni akt podnet protiv ukupno 280 poznatih punoletnih lica.

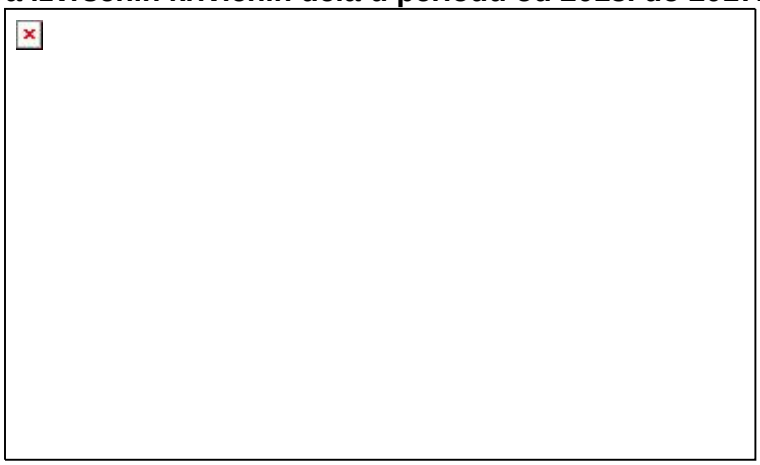
Ministarstvo unutrašnjih poslova je u periodu od 2013. do 2017. godine, podneo krivične prijave zbog izvršenja ukupno 3.824 krivičnih dela visokotehnološkog kriminala. U pitanju su sledeća krivična dela:

- Krivična dela protiv bezbednosti računarskih podataka – ukupno 91 krivično delo i to: oštećenje računarskih podataka i programa iz člana 298. Krivičnog zakonika (5 krivičnih dela ili 5,5% od ukupnog broja), računarska sabotaža iz člana 299. Krivičnog zakonika (7 ili 7,7%), pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika (4 ili 4,4%), računarska prevara iz člana 301. Krivičnog zakonika (40 ili 43,9%), neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302. Krivičnog zakonika (34 ili 37,4%) i sprečavanje i ograničavanje pristupa javnoj računarskoj mreži iz člana 303. Krivičnog zakonika (1 ili 1,1%).

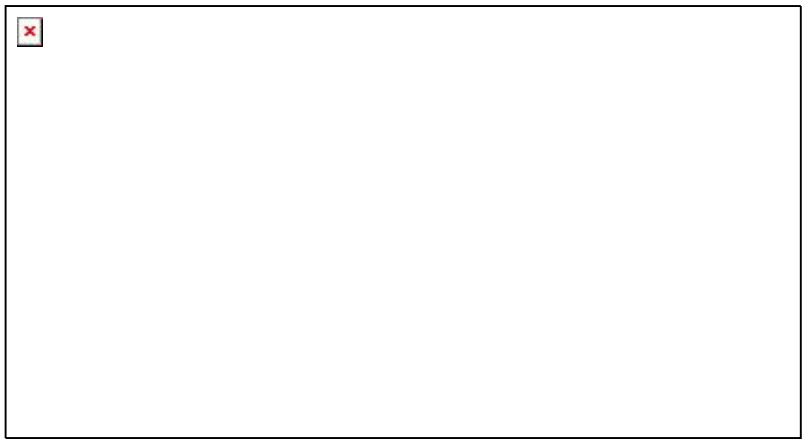
- Krivična dela protiv intelektualne svojine - ukupno 328 krivičnih dela i to: povreda moralnih prava autora i interpretatora iz člana 198. Krivičnog zakonika (1 ili 0,3%), neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199. Krivičnog zakonika (316 ili 96,3%), povreda pronalazačevog prava iz člana 201. Krivičnog zakonika (1 ili 0,3%) i neovlašćeno korišćenje tuđeg dizajna iz člana 202. Krivičnog zakonika (10 ili 3,1%).

- Ostala krivična dela – ukupno 3.405 krivičnih dela i to: prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185. stav 4. Krivičnog zakonika (128 ili 3,8%), iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu iz člana 185b Krivičnog zakonika (14 ili 0,4%), falsifikovanje i zloupotreba platnih kartica iz člana 225. Krivičnog zakonika (2.412 ili 70,8%), pravljenje, nabavljanje i davanje drugom sredstava za falsifikovanje iz člana 227. stav 2. Krivičnog zakonika (18 ili 0,5), neovlašćena upotreba tuđeg poslovnog imena i druge posebne oznake robe ili usluga iz člana 233. Krivičnog zakonika (827 ili 24,3%), odavanje poslovne tajne iz člana 240. Krivičnog zakonika (6 ili 0,2%).

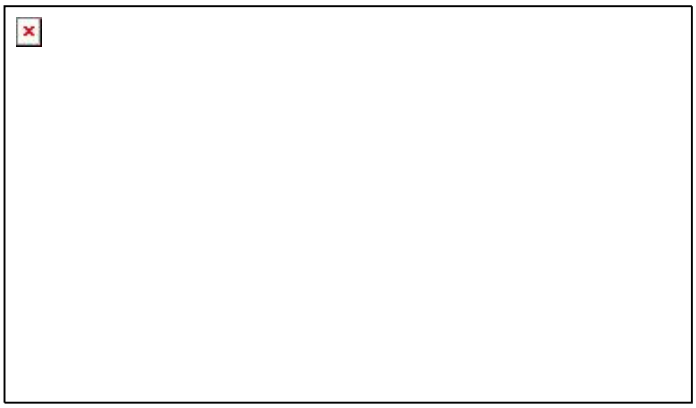
Struktura izvršenih krivičnih dela u periodu od 2013. do 2017. godine



Trend izvršenja krivičnih dela u periodu od 2013. do 2017. godine

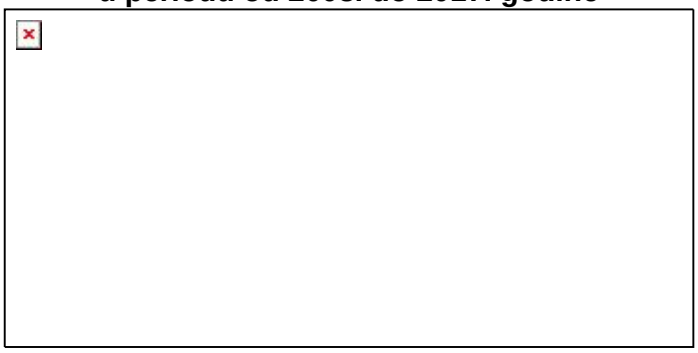


Ukupan broj izvršenih krivičnih dela visokotehnološkog kriminala u periodu od 2013. do 2017. godine



Odeljenje za suzbijanje visokotehnološkog kriminala je u periodu od 2015. do 2017. godine, podnelo krivične prijave protiv 379 osumnjičenih lica za 496 krivičnih dela. Lišena su slobode 164 lica, izvršena su 683 pretresa stambenih i drugih prostorija i privremeno je oduzeto 6.058 predmeta.

Pregled broja predmeta Odeljenja za suzbijanje visokotehnološkog kriminala u periodu od 2008. do 2017. godine



Prema podacima Ministarstva trgovine, turizma i telekomunikacija u okviru kojeg funkcioniše Nacionalni kontakt centar za bezbednost dece na internetu, od februara 2017. godine zaključno sa 15. majom 2018. godine, ukupna registrovana komunikacija koja je ostvarena putem telefonskih poziva, elektronske pošte, prijava putem sajta i društvenih

mreža, iznosi 4.750. Radi unapređenja saradnje i razmene ideja, operateri/edukatori Nacionalnog kontakt centra održali su prezentacije na temu bezbednosti dece na internetu i to: za 150 zaposlenih u domovima zdravlja (direktorima, pedijatrima školskih dispanzera i psiholozima) i za 4.730 učenika i oko 2.500 roditelja u 73 osnovne škole.

5.4. Pojavni oblici visokotehnološkog kriminala

Ministarstvo unutrašnjih poslova je 2017. godine u skladu sa članom 24. Zakona o policiji, izradilo prvu Stratešku procenu javne bezbednosti i Strateški plan policije. Nakon obimne strateške analize stanja u oblasti bezbednosti, definisano je osam bezbednosnih prioriteta u radu policije, od kojih se jedan odnosi na borbu protiv visokotehnološkog kriminala „Borba protiv zloupotreba informaciono-komunikacionih tehnologija na teritoriji Republike Srbije". Analizom je utvrđeno da se krivična dela u kojima se zloupotrebljavaju informaciono-komunikacione tehnologije povećavaju, kao posledica brzog razvoja IKT i to ona koja se odnose na bezbednost računarskih podataka, seksualnu zloupotrebu maloletnih lica i dece u pornografske svrhe na Internetu, prevare putem Interneta, neovlašćeno korišćenje autorskog i srodnog prava, ugrožavanje sigurnosti, terorizam i nasilni ekstremizam koji vodi ka terorizmu.

Prevare putem Interneta najčešće se dešavaju na različitim aukcijskim sajtovima kao i sajtovima na kojima se vrši oglašavanje. Izvršioci krivičnih dela objavljuju lažne elektronske oglase na kojima oglašavaju prodaju različite robe (automobili, poljoprivredne mašine, mobilni telefoni, satovi i dr). Kada žrtva naruči robu i uplati određeni novčani iznos na ime kupovine, izvršilac krivičnog dela koji je objavio potpuno lažan oglas, zadržava novac kod sebe i održava žrtvu u zabludi da će dobiti robu.

Javljaju se i prevare sa „emotivnim odnosima" na Internetu gde se žrtve od strane izvršilaca krivičnih dela kontaktiraju i započinje komunikacija i razvijanje emocionalnog i partnerskog odnosa. Nakon što se žrtve dovedu u zabludu nudi im se npr. sklapanje braka. Za navedeno, žrtve trebaju da uplate određeni novčani iznos za administrativne troškove (takse, sudski i advokatski troškovi i slično). Slična je situacija i u krivičnim delima, gde se za određeni iznos novca koji se kreće od 10% do 20%, žrtvama nudi da na ime transfera novca na svoj račun uplate određene takse na napred opisani način. Žrtve se dovode najčešće u zabludu da su novac nasledili od dalekih rođaka koji su preminuli u inostranstvu. Vrlo često dolazi i do kombinacije prva dva slučaja kada se prvo žrtva emocionalno dovodi u vezu sa lažnim partnerom, a zatim se traži od nje da otvori račun i da za izvršioca koji stoji iza „emotivnog odnosa" podigne novac koji navodno u državi gde se partner nalazi nije moguće podići iz određenih razloga. Uplate se najčešće vrše preko Western Union-a i MoneyGram-a. Destinacije gde se novac upućuje najčešće su države sa područja Afrike, ali i Velike Britanije, Španije i dr.

Na teritoriji naše države sve su češća i krivična dela na štetu pravnih lica koja se nazivaju „Bussiness Compromised Email", i „Ransomware". Pojavile su se i „CEO Frauds" prevare. Navedena prevara se vrši putem elektronskih poruka u kojima se izvršioci predstavljaju lažno kao nadređeni (šefovi, rukovodioci ili direktori) i dovode u zabludu žrtve (zaposlena lica) u privrednim subjektima da izvrše uplatu na njihov račun. Broj oštećenih privrednih subjekata prevarom tipa „Bussiness Compromised Email" sve je veći. Zloupotrebom komunikacije izvršioci krivičnih dela lažno se predstavljaju u ime strane kompanije sa kojom pravni subjekat iz naše zemlje već ima poslovnu saradnju i nakon ugovorenog posla u prevarnim porukama odmah nakon legitimno prosleđene poruke od strane legitimne kompanije u kojoj se nalaze instrukcije za uplatu, šalju nove poruke sa izmenjenim dispozicijama za plaćanje (IBAN broj). Imajući u vidu da se radi o elektronskom transferu novca izvršioci krivičnog dela novac podižu u inostranstvu veoma

brzo, ponekad i u roku od 24 časa. Za to vreme oštećeno preduzeće je u ubeđenju da je uplatilo novac stranoj kompaniji, a strana kompanija čeka uplatu za npr. određenu robu. Da su prevareni oštećeni saznaju tek nakon što kontaktiraju stranu kompaniju. Navedenim radnjama izvršilaca krivičnog dela prevare najviše su ugrožena mala i srednja preduzeća sa teritorije Republike Srbije.

Izvršioci krivičnih dela na računare oštećenih privrednih lica, ali i građana Republike Srbije, šalju zlonamerne računarske programe - viruse poznatije kao *ransomware* koji enkriptuju elektronske podatke na računarima oštećenih lica, a potom služe za ucenjivanje oštećenih lica kako bi im se iznudio određeni novčani iznos za vraćanje važnih podataka tj. njihovu dekripciju.

U Republici Srbiji vrše se zloupotrebe elektronskih podataka o platnim karticama na Internetu *(card not present).* Izvršioci su elektronske podatke sa platnih kartica koristili za nabavljanje skupocene robe putem Internet sajtova. Podatke o platnim karticama pribaljali su putem karderskih foruma. Uglavnom se radilo o platnim karticama stranih državljana koje su zloupotrebljavane od strane izvršilaca sa teritorije Republike Srbije. U svetu je bilo slučajeva zloupotreba elektronskih novčanika, beskontaktnog načina plaćanja i dr.

Dolaskom Pay-Pal-a u Republiku Srbiju, višestruko se povećalo naručivanje robe putem interneta. Isporuka tako naručene robe najčešće se vrši poštanskim saobraćajem, često i ekspresnim pošiljkama. Međutim, pored robe koja je legalno na tržištu, putem interneta se prodaje i roba (lekovi i razna medicinska sredstva, elektronske cigarete, kozmetika, konditorski proizvodi itd.) koja nije ispitana i za koja se ne poseduju sve propisane dozvole. Poseban problem predstavlja mogućnost da se ne radi o originalnim proizvodima u kom slučaju neće biti samo povređena prava intelektualne svojine, već ti proizvodi mogu ozbiljno ugroziti život i zdravlje stanovništva.

Preko interneta se najčešće prodaje roba od strane fizičkih lica koja nemaju registrovano privredno društvo i nisu preduzetnici. Pri tome, radi se o robi koja se nelegalno nalazi na tržištu (ne poseduju se potrebne dozvole i sertifikati, nisu plaćene dažbine – carina i PDV). Ukoliko postoji konstantno snabdevanje tržišta ovom robom, to može izazvati nelojalnu konkurenciju i porast sive ekonomije.

Uprava carina, kao i carinske administracije drugih država, pored fiskalne uloge, ima i bezbednosnu, odnosno sugurnosnu tj. zaštitnu ulogu. Imajući u vidu potrebe za pojačanom kontrolom robe koja se naručuje, odnosno prodaje putem interneta, carinske administracije EU (Francuska Republika, Holandija, Republika Austrija i dr.) formirale su posebne organizacione jedinice za borbu protiv visokotehnološkog kriminala sa ciljem identifikacije dela koja su u suprotnosti sa carinskim propisima, a koja su učinjena korišćenjem kompjutera i informacionih sistema.

S obzirom na napred navedeno, Uprava carina nalazi da postoji potreba pojačane kontrole robe koja se prodaje preko interneta i u vezi s tim, povećanje uloge koju trenutno Uprava carina ima.

Kada je reč o krivičnim delima protiv bezbednosti računarskih podataka, može se konstatovati da se najčešće vrše krivična dela Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, zatim Pravljenje i unošenje računarskih virusa, kao i računarske prevare i računarske sabotaže. Ova krivična dela vrše se od strane izvršilaca koji poseduju specifična tehnička znanja. Pojačano je i korišćenje specijalizovanih foruma na kojima izvršioci krivičnih dela razmenjuju svoja znanja i pronalaze saizvršioce, kao i alate za vršenje krivičnih dela. Prisutna je i pojava zloupotrebe novih tehnologija za vršenje krivičnih dela. Jedan od takvih primera je i zloupotreba koncepta Interneta stvari (*Internet of Things-IoT*) gde se uređaji koji su mrežno povezani, nakon što su zaraženi računarskim virusom, pojavljuju kao deo DDoS mreže, tako da su ovi vidovi napada jači po svom intenzitetu.

Nove tehnologije kao što su *IoT*, *Cloud* računarstvo, *BYOD* sve su prisutnije i izvršioci krivičnih dela uviđaju prednost ovih tehnologija širom sveta. Zloupotreba ovih tehnologija utiče na intenzitet napada i njihov obim, kao i na nastalu štetu. Računarstvo u *cloud* okruženju takođe predstavlja rizik zbog širokog spektra mogućih zloupotreba ukoliko dođe do kompromitovanja zaštite i platformi. Koncept BYOD (Bring Your Own Device) se odnosi na mogućnost da zaposleni donesu svoje mobilne uređaje, kao što su laptopovi, tableti i mobilni telefoni i koriste ih na svom radnom mestu u poslovne svrhe. Rizik korišćenja ovog koncepta je u tome što je potrebna adekvatna primena bezbednosnih mera u sistemu u kome zaposleni donose svoje uređaje i povezuju ih u korporativnu mrežu. Propusti mogu povećati rizik od uticaja izvršilaca krivičnih dela na korporativno okruženje u kome se nalazi uređaj i samim tim postoji mogućnost za vršenje krivičnih dela na štetu poslovnih subjekata.

Napredne uporne pretnje (*Advance Persistent Threat*-APT) svake godine u sve većoj meri pogađaju privredne subjekte širom sveta. Očekuje se da akcenat više neće biti samo na upornim pretnjama, već da će izvršioci krivičnih dela iz ove oblasti kreirati i otpornije pretnje ili malver programe bez fajlova, smanjujući na taj način tragove u inficiranom sistemu i izbegavajući detekciju.

Izvršioci krivičnih dela vezanih za seksualnu zloupotrebu maloletnih lica u pornografske svrhe, na Internetu koriste P2P (Peer to Peer) mreže kako bi pribavljali i/ili razmenjivali nezakonite audio-vizuelne materijale nastale seksualnom zloupotrebom. Nezakoniti audio-vizuelni materijali pribavljaju se na takav način što se koristeći Peer to Peer mreže, ukucavanjem traženog pojma, pronalazi određeni sadržaj, a zatim se preuzima i skladišti na memoriji svojih računara. Takvi sadržaji mogu se deliti sa drugim izvršiocima krivičnih dela širom sveta koji su u isto vreme tražili materijal koji je preuzimao izvršilac u našoj zemlji i koji je dopustio deljenje u mreži.

U manjem broju slučajeva izvršioci krivičnih dela koriste i različite forume kako bi razmenjivali navedene nezakonite materijale i kako bi pronašli saizvršioce. Za pribavljanje i razmenu materijala nastalog seksualnom zloupotrebom maloletnih lica u pornografske svrhe na Internetu, koriste se i socijalne mreže. Pored preuzimanja, posedovanja i razmene tih sadržaja, socijalne mreže se koriste i kako bi se stupilo u kontakt sa maloletnim licima. Uglavnom se koriste lažni profili koji se prilagođavaju uzrastu dece i njihovim interesovanjima, pokušavajući da zadobiju njihovu pažnju i poverenje. Nakon što ostvare kontakt i zadobiju poverenje izvršioci krivičnih dela iz ove oblasti traže od dece da izvrše određenu radnju (snimanje određenog dela tela ili pokazivanje intimnih delova tela *online* i dr.) i nakon toga materijal koji dobiju koriste za dalje ucene prema žrtvi kako bi produžili vršenje krivičnog dela.

Pored toga, u operativnoj akciji na suzbijanju seksualne eksploatacije maloletnih lica u pornografke svrhe putem interneta „Armagedon", od 2010. do 2018. godine podnete su krivične prijave protiv 181 osumnjičenog lica za 189 krivičnih dela, dok je 163 lica lišeno slobode. Informacije na kojima se zasniva akcija „Armagedon" prikupljaju se operativnim policijskim radom, prijavama građana, kao i na informacijama dobijenim putem međunarodne operativne policijske saradnje (Interpol, Evropol, FBI, NCA i dr.). Odeljenje za suzbijanje visokotehnološkog kriminala i pored ovih značajnih rezultata uopšte nema sistematizovana radna mesta za istrage seksualne eksploatacije dece na Internetu.

Napredak informacionih tehnologija dovodi do konstantnog porasta broja krivičnih dela u oblasti autorskog i drugog srodnog prava. Predmet „piraterisanja" nisu samo dela stranih već i domaćih autora. Veliki problem u ovom smislu predstavljaju najnoviji filmovi, kao i serije ili filmovi domaće proizvodnje čija je proizvodnja često subvencionisana od strane države. Preduzete su konkretne aktivnosti u dogovoru sa pojedinim aukcijskim sajtovima koji oglase na kojima se nude različita autorska prava (filmovi, muzika, igre,

softveri), koji nemaju atribute originalnosti ne postavljaju na svoje veb strane, već da omogućavaju prodaju originalnih proizvoda u elektronskoj formi (na CD-u). U oblasti industrijske svojine na teritoriji Republike Srbije najčešće se putem Internet sajtova prodaju falsifikovana farmaceutska sredstva, kao i garderoba različitih robnih marki i dr.

Ugrožavanje sigurnosti pretnjom da će se napasti na život ili telo žrtve ili njoj bliskog lica izvršioci su vršili kako prema građanima tako i prema nosiocima javnih funkcija. Krivična dela vrše se svim sredstvima komunikacije na Internetu, a najčešći oblici se odnose na korišćenje besplatnih servisa za elektronsku poštu, socijalnih mreža, foruma, komentara ispod određenih tekstova objavljenih u elektronskim medijima.

Zloupotreba informaciono-komunikacionih tehnologija vezana za terorizam i nasilni ekstremizam koji vodi ka terorizmu odvija se za vrbovanje novih sledbenika, davanje uputstava o načinu vršenja krivičnih dela, a pomoću Internet sajtova, foruma, socijalnih mreža i drugih formi namenjenih razmeni multimedijalnih sadržaja vrši se i propaganda ideologije povezane sa terorizmom. Servisi se koriste i za međusobnu komunikaciju, prikrivanje identiteta i anonimnost. Najčešće je korišćenje *VoIP* servisa i zaštićenih foruma. Sa terorizmom i nasilnim ekstremizmom koji vodi ka terorizmu povezano je vršenje krivičnih dela Neovlašćen pristup zaštićenim računarima, računarskim mrežama i elektronskoj obradi podataka (primer: *defacement* ciljanih Internet sajtova), ali i sprečavanja i ograničavanja pristupa i elektronske obrade računarskih podataka (primer: *DDoS* napadi uz upotrebu *CaaS* servisa). Prisutno je i korišćenje virtuelnih valuta kao što je *Bitcoin* za pribavljanje protivpravne imovinske koristi koja se može upotrebiti za finansiranje terorističkih aktivosti.

6. IDENTIFIKOVANjE PROBLEMA, UZROKA I POSLEDICA

Sveobuhvatna strateška analiza bazirana na primarnim i sekundarnim izvorima informacija u oblasti borbe protiv visokotehnološkog kriminala, korišćenjem savremenih metoda i tehnika strateške analize, identifikovala je veći broj problema koje je neophodno otkloniti u cilju efikasnijeg suprostavljanja ovom vidu kriminala. Imajući u vidu povećanja broja krivičnih dela u kojima se informaciono-komunikacione tehnologije zloupotrebljavaju, u kontekstu tendencije brzog razvoja i korišćenja informaciono-komunikacionih tehnologija neophodno je, u državnim organima koji su prepoznati kao nosioci borbe protiv visokotehnološkog kriminala, unaprediti normativni i institucionalni okvir, poboljšati uslove za rad u pogledu povećanja broja zaposlenih, tehničke opremljenosti i operativnih kapaciteta i omogućiti uspostavljanja efikasnije saradnje kako na nacionalnom tako i na međunarodnom nivou:

- Analiza domaćeg i međunarodnog normativnog okvira (pre svega prelaznog merila u okviru Poglavlja 24, zatim direktiva, konvencija i strategija) je pokazala da je neophodno usaglašavanje Krivičnog zakonika i Zakonika o krivičnom postupku sa pravnim tekovinama EU. Takođe je potrebno dopuniti i izmeniti postojeće zakone koji definišu nadležnosti državnih organa u delu koji se odnosi na oblast visokotehnološkog kriminala. Pored toga, podzakonskim aktima je neophodno bliže urediti ovu oblast;

- U okviru uspostavljanja kapaciteta policije i tužilaštva koja su definisana u prelaznom merilu u okviru Poglavlja 24 neophodno je primeniti odredbe Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Pored toga, potrebno je izvršiti izmenu i dopunu navedenog zakona, u

cilju povećanja institucionalnih kapaciteta tužilaštva i policije, ali i drugih državnih organa koji su nosioci borbe protiv visokotehnološkog kriminala. S tim u vezi neophodno je izmeniti akte o unutrašnjem uređenju i sitematizaciji radnih mesta u organima državne uprave;

- U okviru poboljšanja operativnih procedura za rad neophodno je obezbediti ujednačeno postupanje nosilaca borbe protiv visokotehnološkog kriminala, ulagati u specijalističke obuke kadrova, tehničku opremljenost, nove softverske alate, uspostaviti definiciju kritične infrastrukture, uvesti mogućnosti sprovođenja jednostavnije digitalne forenzike itd.;

- Veoma je značajno unaprediti saradnju u ovoj oblasti, kako između organa državne uprave, tako i sa privatnim sektorom i organizacijama civilnog društva. Posebno je važno unaprediti regionalnu i međunarodnu saradnju, pre svega sa Interpolom;

- Od presudnog je značaja sprovoditi preventivne aktivnosti koje se odnose na jačanje svesti građana i građanki, kao i organa vlasti o mogućnostima zloupotrebe informaciono-komunikacionih tehnologija, mobilnih telefona, Interneta i društvenih mreža. S tim u vezi, neophodno je unaprediti proaktivni pristup u kojem će učestvovati svi akteri prepoznati kao nosioci borbe protiv visokotehnološkog kriminala, pre svega Posebno tužilaštvo i Ministarstvo unutrašnjih poslova, Odeljenje za suzbijanje visokotehnološkog kriminala;

- Potrebno je pripremiti se za uspostavljanje jedinstvenog centralizovanog krivičnog obaveštajnog sistema i sigurne platforme za komunikaciju među organima za sprovođenje zakona. Obezbediti bolju povezanost relevantnih baza podataka (uključujući analizu troškova, administrativnih resursa, budžeta i potreba za obukom) i poboljšati prikupljanje objedinjenih statističkih podataka o krivičnim delima (Preporuka 6.2.2.iz AP 24).

S obzirom na obim analizirane problematike i tendenciju porasta krivičnih dela u oblasti visokotehnološkog kriminala, radi otklanjanja problema, a u cilju jačanja kapaciteta Ministarstva unutrašnjih poslova planirano je, donošenjem novog Pravilnika o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu unutrašnjih poslova, koji je stupio na snagu 15. juna 2018. godine, popunjavanje specijalizovanog Odseka za suzbijanje i zloupotrebu u oblasti elektronske trgovine, elektronskog bankarstva i platnih kartica na Internetu i Odseka za suzbijanje nedozvoljenih i štetnih sadržaja na Internetu.

U pogledu institucionalnog okvira za borbu protiv visokotehnološkog kriminala, kada je reč o Javnom tužilaštvu, potrebno je istaći da Posebno tužilaštvo za visokotehnološki kriminal, prema važećim normama, funkcioniše kao deo - odeljenje Višeg javnog tužilaštva u Beogradu. Za razliku od Višeg javnog tužilaštva, koje prati stvarnu i mesnu nadležnost Višeg suda u Beogradu, Posebno tužilaštvo nadležno je za postupanje na čitavoj teritoriji Republike Srbije. Ovakvo rešenje u praksi dovodi do otežanog rada, jer je Više javno tužilaštvo Beogradu organizaciono, funkcionalno i mesno prilagođeno isključivo za postupanje, odnosno, krivično gonjenje učinilaca krivičnih dela i njihovo procesuiranje pred Višim sudom u Beogradu. Specifičnost visokotehnološkog kriminala ogleda se, između ostalog, i u činjenici da se najčešće mesto izvršenja krivičnog dela iz oblasti visokotehnološkog kriminala i mesto nastupanja štetne posledice ne poklapaju, zbog čega je i sam zakonodavac dao republičku nadležnost tužilaštvu za visokotehnološki kriminal.

U pogledu normativnog okvira, radi efikasnog postupanja državnih organa u borbi protiv visokotehnološkog kriminala neophodno je dopuniti i izmeniti set zakona iz ove oblasti, u cilju usklađivanja sa zakonodavstvom EU i to:

- Krivični zakonik potrebno je uskladiti sa međunarodnim standardima, detaljnije i preciznije opisati krivična dela i propisati strožije krivične sankcije. Pored toga, u pojmovima definisati šta predstavljaju podaci o pretplatniku, podaci o saobraćaju i podaci o sadržini saobraćaja.

- Kada je reč o izmeni Zakonika o krivičnom postupku, potrebno je propisati sledeće posebne dokazne radnje:

- Hitno čuvanje pohranjenih računarskih podataka - odnosi se na omogućavanje izdavanje naredbe od strane nadležnog organa, poželjno javnog tužilaštva, kojim će već pohranjeni podaci, uključujući i podatke o saobraćaju, biti dodatno sačuvani od strane držaoca u obaveznom roku od 90 dana koji može biti produžen za još 90.
- Hitno čuvanje i delimično otkrivanje podataka o saobraćaju - odnosi se na hitno čuvanje podataka o sabraćaju, bez obzira na to da li je u prenosu tih podataka uključeno više subjekata (ISP) i otkrivanje ograničene, ali dovoljne količine podataka koje mogu da posluže nadležnom organu za identifikaciju subjekta prenosa podataka, kao i putanje kojom su podaci emitovani.
- Naredba o dostavljanju podataka - odnosi se na izdavanje naredbe fizičkom ili pravnom licu da dostavi/preda nadležnom organu računarske podatke koji se nalaze u posedu ili pod kontrolom tog lica, a koji podaci su pohranjeni u računaru ili na računarskom medijumu, kao i naredbu ISP da dostavi/preda nadležnom organu podatke o pretplatniku određene usluge koje poseduje ili se nalaze pod njegovom kontrolom.
- Naredba o pretrazi i oduzimanju podataka - obuhvata modifikaciju postojećih naredbi o pretresu stvari i posebne dokazne radnje automatske obrade podataka.
- Naredba o prikupljanju podataka o saobraćaju u realnom vremenu - odnosi se na donošenje naredbe kojom bi se upotrebom tehničkih metoda navedeni podaci prikupljali u realnom vremenu, kao i naredbu ISP da u okviru postojećih tehničkih mogućnosti sprovede ovu naredbu sam ili da sarađuje sa nadležnim organom.
- Naredba o presretanju podataka o sadržini saobraćaja - odnosi se na istu materiju kao prethodna naredba, samo je predmet naredbe sadržina saobraćaja, umesto podataka o saobraćaju.

- U okviru međunarodne krivično-pravne pomoći i saradnje potrebno je omogućiti razmenu spontanih informacija, kao i primenu naredbi u vezi hitnog čuvanja pohranjenih podataka, hitnog čuvanja i delimičnog otkrivanja podataka o saobraćaju, pristup pohranjenim podacima, prekogranični pristup pohranjenim podacima uz saglasnost ili kada su javno dostupni, međunarodnu pravnu pomoć koja se odnosi na prikupljanje podataka o saobraćaju u realnom vremenu, te presretanju podataka o sadržini saobraćaja, kao i zakonski konkretizovano uspostavljanje tačaka 24/7 za hitnu policijsku saradnju, kao i druge tačke za 24/7 pružanje međunarodne pravne pomoći, koja bi u ovom kontekstu morala biti pri Republičkom javnom tužilaštvu, imajući u vidu nadležnosti.

Bolja povezanost relevantnih baza podataka i poboljšano prikupljanje objedinjenih statističkih podataka o krivičnim delima će biti predviđena revizijom Akcionog plana za Poglavlje 24.

7. VIZIJA

Vizija ove strategije je:

Stvoreno bezbedno društveno okruženje kroz adekvatan odgovor Republike Srbije na sve pojavne oblike visokotehnološkog kriminala.

8. OPŠTI CILj STRATEGIJE

Republika Srbija poseduje efikasan i održiv sistem zajedničkog delovanja svih subjekata u borbi protiv visokotehnološkog kriminala.

Ovakav opšti cilj Strategije bi trebalo da dovede do boljeg povezivanja svih subjekata Strategije, u borbi protiv visokotehnološkog kriminala, kao i do bolje iskorišćenosti resursa u rešavanju problema.

9. SPECIFIČNI CILjEVI STRATEGIJE

Specifični ciljevi su usmereni u pravcu rešavanja prepoznatih problema u suprotstavljanju visokotehnološkom kriminalu.

Kroz Analizu su prepoznata četiri specifična cilja i definisane mere u okiru njih:

1. Unapređeno i usaglašeno zakonodavstvo Republike Srbije sa pravnim tekovinama i standardima Evropske unije u oblasti borbe protiv visokotehnološkog kriminala

1.1. Izraditi predloge izmena i dopuna pravnih propisa Republike Srbije sa pravnim tekovinama Evropske unije

2. Unapređeni organizacioni, kadrovski, tehnički i operativni kapaciteti nosilaca borbe protiv visokotehnološkog kriminala

2.1. Reorganizovati Odeljenje za suzbijanje visokotehnološkog kriminala
2.2. Formirati posebne organizacione jedinice u organima i organizacijama u skladu sa njihovim nadležnostima i potrebama
2.3. Unapređenje kadrovskih, stručnih, tehničkih i organizacionih kapaciteta nadležnih institucija za razmenu podataka o incidentima i reagovanje na incidente
2.4. Realizovati potrebne obuke različitih nivoa
2.5. Nabaviti savremenu elektronsku opremu i softverske alate
2.6. Usaglašavanje standardnih operativnih procedura nosilaca borbe protiv visokotehnološkog kriminala

3. Unapređen preventivni i proaktivni pristup društvu u borbi protiv visokotehnološkog kriminala

3.1.Podizanje nivoa svesti javnosti po pitanju visokotehnološkog kriminala
3.2.Podizanje nivoa svesti među organima javne vlasti po pitanju visokotehnološkog kriminala

4. Unapređena saradnja na nacionalnom, regionalnom i međunarodnom nivou

4.1.Unaprediti saradnju između privatnog, javnog sektora i civilnog društva
4.2.Unaprediti saradnju na sprečavanju seksualne eksploatacije dece i maloletnih lica
4.3.Unaprediti međunarodnu i regionalnu policijsku saradnju

10. SPROVOĐENjE, PRAĆENjE, OCENjIVANjE I IZVEŠTAVANjE

10.1. Organi nadležni za sprovođenje Strategije

Strategiju za borbu protiv visokotehnološkog kriminala sprovode ministarstva i drugi državni organi, u okviru svojih nadležnosti. Aktivnosti mogu biti u nadležnosti samo jednog ili više ministarstava, odnosno državnih organa. Ako je za neku aktivnost potrebna saradnja više ministarstava ili državnih organa, vođenje aktivnosti preuzima ministarstvo ili državni organ u čijoj je pretežnoj nadležnosti aktivnost, a na nivou Saveta za borbu protiv visokotehnološkog kriminala obezbeđuje se saradnja i koordinisano delovanje sa drugim ministarstvima i državnim organima.

Savet za borbu protiv visokotehnološkog kriminala će predložiti formiranje Stručnog tima za implementaciju Strategije za sprovođenje konkretnih aktivnosti, koji bi bio sastavljen od zaposlenih čije su organizacione jedinice nosioci aktivnosti u Akcionom planu.

Stručni tim za implementaciju Strategije je odgovoran za praćenje uspešnosti primene ove strategije i pratećeg akcionog plana. Ovaj stručni tim će uspostaviti mehanizam kontinuiranog prikupljanja podataka za izveštaj od svih odgovornih organa javne vlasti. Institucije odgovorne za primenu strategije i akcionog plana dostavljaće Stručnom timu za implementaciju izveštaje o sprovedenim aktivnostima. Po potrebi i po zahtevu Stručnog tima odgovorne institucije će dostavljati i dodatne izveštaje i podatke. Kontinuirano će se prikupljati i drugi relevantni podaci, kao što su javno dostupne stručne analize o ovoj oblasti. Konkretne aktivnosti koje će ministarstva, odnosno drugi državni organi sprovoditi, odrediće se Akcionim planom.

10.2. Savet za borbu protiv visokotehnološkog kriminala

Savet za borbu protiv visokotehnološkog kriminala je radno telo koje obrazuje Vlada i nadležan je za analiziranje sprovođenja svih planiranih aktivnosti i u tu svrhu podnosi periodične izveštaje Vladi o napretku u sprovođenju Strategije i Akcionog plana. Savet za borbu protiv visokotehnološkog kriminala može inicirati usklađivanje, izmenu ili dopunu Strategije i Akcionog plana, usaglašavanje zakonodavnih i normativnih akata sa međunarodnim propisima i standardima koji su od značaja za Republiku Srbiju.

10.3. Nacionalni koordinator za borbu protiv visokotehnološkog kriminala

Nacionalni koordinator za borbu visokotehnološkog kriminala informiše Savet o svim aspektima sprovođenja Strategije i Akcionog plana i koordinira radom Stručnog tima za implementaciju Strategije. Uspostavlja saradnju sa međunarodnim organizacijama i sektorom civilnog društva radi uspešnog sprovođenja Strategije i Akcionog plana.

Nacionalnom koordinatoru, članovi Stručnog tima za implementaciju Strategije dostavljaju informacije i podatake u vezi sa visokotehnološkim kriminalom radi efikasnije realizacije ciljeva Strategije.

Nacionalnog koordinatora za borbu protiv visokotehnološkog kriminala imenuje Vlada na predlog Saveta.

Nacionalni koordinator za borbu protiv visokotehnološkog kriminala i Stručni tim za implementaciju Strategije su odgovorni za praćenje uspešnosti primene ove strategije i pratećeg akcionog plana. Oni će uspostaviti mehanizam kontinuiranog prikupljanja pojedinačnih izveštaja svih odgovornih organa javne vlasti u cilju izrade zajedničkog izveštaja.

Nacionalni koordinator za borbu protiv visokotehnološkog kriminala i Stručni tim za implementaciju Strategije će se sastajati tromesečno, a prema potrebi i češće. Nacionalni koordinator će sa ovim timom pripremati šestomesečne izveštaje sa ocenom uspešnosti primene Strategije i dostavljati ih Savetu, a Savet Vladi.

Da bi se ocenili efekti primene strategije i u skladu sa tim korigovala njena primena, biće urađene dve evaluacije: jedna na kraju druge godine sprovođenja i jedna krajem 2023. godine. Nacionalni koordinator sa Stručnim timom za implementaciju strategije pripremiće konačni izveštaj sa ocenom uspešnosti primene ove strategije i dostaviti ga Vladi najkasnije do početka 2024. godine.

11. FINANSIJSKI EFEKTI STRATEGIJE I AKCIONOG PLANA

Sredstva neophodna za sprovođenje aktivnosti planiranih ovom strategijom, koje će se izvršavati u narednom periodu, biće obuhvaćena finansijskim planovima nosilaca aktivnosti i obezbeđivaće se u budžetu Republike Srbije u skladu sa bilansnim mogućnostima, a u skladu sa potrebama dodatna sredstva će se obezbediti iz donacija, projekata, pomoći, kao i iz drugih izvora.

12. ZAVRŠNA ODREDBA

Ovu strategiju objaviti u „Službenom glasniku Republike Srbije”.

05 Broj: 23-8630/2018
U Beogradu, 14. septembra 2018. godine

V L A D A

PREDSEDNIK

Ana Brnabić