Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru

Protrka, Nikola

SVEUČILIŠTE U ZADRU

POSLIJEDIPLOMSKI SVEUČILIŠNI STUDIJ
MEĐUNARODNI ODNOSI

Nikola Protrka

MEĐUNARODNA SURADNJA I SIGURNOST U SUZBIJANJU KRIMINALITETA U KIBERNETIČKOM PROSTORU

Doktorski rad

Zadar, 2018.

SVEUČILIŠTE U ZADRU

POSLIJEDIPLOMSKI SVEUČILIŠNI STUDIJ
MEĐUNARODNI ODNOSI

Nikola Protrka

MEĐUNARODNA SURADNJA I SIGURNOST U SUZBIJANJU KRIMINALITETA U KIBERNETIČKOM PROSTORU

Doktorski rad

Mentor

doc. dr. sc. Petar Popović

Zadar, 2018.

SVEUČILIŠTE U ZADRU
TEMELJNA DOKUMENTACIJSKA KARTICA

I. Autor i studij

Ime i prezime: Nikola Protrka
Naziv studijskog programa: Zajednički poslijediplomski sveučilišni studij Međunarodni odnosi
Mentor: doc. dr. sc. Petar Popović
Datum obrane: 3.9.2018.
Znanstveno područje i polje u kojem je postignut doktorat znanosti: Društvene znanosti, polje interdisciplinarne društvene znanosti.

II. Doktorski rad

Naslov: Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru
UDK oznaka: 343.85:004
Broj stranica: 202
Broj slika/grafičkih prikaza/tablica: 1/22/32
Broj bilježaka: 149
Broj korištenih bibliografskih jedinica i izvora: 155
Broj priloga: 6
Jezik rada: Hrvatski

III. Stručna povjerenstva

Stručno povjerenstvo za ocjenu doktorskog rada:

1. *izv. prof. dr. sc. Ksenija Butorac, predsjednica*
2. *doc. dr. sc. Petar Popović, član*
3. *doc. dr. sc. Franjo Pehar, član*

Stručno povjerenstvo za obranu doktorskog rada:

1. *izv. prof. dr. sc. Ksenija Butorac, predsjednica*
2. *doc. dr. sc. Petar Popović, član*
3. *doc. dr. sc. Franjo Pehar, član*

UNIVERSITY OF ZADAR
BASIC DOCUMENTATION CARD

I. Author and study

Name and surname: Nikola Protrka
Name of the study programme: Joint postgraduate doctoral study International Relations
Mentor: Petar Popović, PhD
Date of the defence: 3 September 2018
Scientific area and field in which the PhD is obtained: Social Sciences, Field of Interdisciplinary Social Sciences.

II. Doctoral dissertation

Title: International Cooperation and Security in Combating Crime in Cyberspace
UDC mark: 343.85:004
Number of pages: 202
Number of pictures/graphical representations/tables:1/22/32
Number of notes: 149
Number of used bibliographic units and sources: 155
Number of appendices: 6
Language of the doctoral dissertation: Croatian

III. Expert committees

Expert committee for the evaluation of the doctoral dissertation:

1. Associate Professor Ksenija Butorac, PhD, chair
2. Assistant Professor Petar Popović, PhD, member
3. Assistant Professor Franjo Pehar, PhD, member

Expert committee for the defence of the doctoral dissertation:

1. Associate Professor Ksenija Butorac, PhD, chair
2. Assistant Professor Petar Popović, PhD, member
3. Assistant Professor Franjo Pehar, PhD, member

Izjava o akademskoj čestitosti

Ja, **Nikola Protrka,** ovime izjavljujem da je moj **doktorski** rad pod naslovom Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 3. rujna 2018.

Sadržaj:

1. UVOD

Razne međunarodne aktivnosti (diplomatske, ekonomske i sl.) odvijaju se kroz nacionalne pravne norme i stoga su ograničene formalnim granicama, dok kibernetički prostor ili kiberprostor (*cyberspace*), ne poznaje granice ucrtane na političkoj karti svijeta. Tehnološka podjela po internetskim domenama prividno pokazuje matičnu državu kontakta, ali sa sigurnosnog aspekta ova činjenica ukazuje na brojne mogućnosti zloporabe (Goldsmith i Wu, 2006).

Tehnološki razvoj koji se odvija pred našim očima, kao i ekspanzija zloporabe te iste tehnologije, pokazuje da jedno bez drugog jednostavno nije moguće. Globalizacijom i pojavom modernih tehnologija, a u najvećoj mjeri samog interneta, oslabila je jaka pravna linija nacionalne jurisdikcije koja je razgraničavala međunarodnu sferu od nacionalne. (Zekos, 2013). U navedenu raspravu autor ne ulazi dublje od definicije pojmova i prikaza trenutnog stanja jer je navedeno izvan fokusa interesa ovog rada. Znanje i informacije postaju primarnim faktorima razvoja u sveukupnom životu nove zajednice, a zemlja, rad i kapital sekundarnim, te stoga ne iznenađuje interes najrazvijenijih zemalja da ujednače informatičku pismenost i ulože sredstva u istraživanje i razvoj informacijsko-komunikacijskih tehnologija, te obrazovanje informatičkih stručnjaka (Dragičević, 2015, str. 1-2).

U doktorskom radu su prikazani rezultati statističke analize izvornih podataka o pojavnim oblicima i modalitetima kaznenih djela iz domene kibernetičkog kriminala u Republici Hrvatskoj iz godišnjih statističkih izvještaja Ministarstva unutarnjih poslova Republike Hrvatske (dalje u tekstu MUP) i Državnog zavoda za statistiku Republike Hrvatske (dalje u tekstu DZS).

Također se provodi komparativna analiza postojeće međunarodne kaznenopravne regulative i obrazaca međunarodne suradnje za istraživanje i sankcioniranje kaznene domene u kiberprostoru i kaznenih djela kiberkriminala (*eng. Cyberspace* i *Cybercrime*). Nastavno se interpretiraju rezultati istraživanja kvalitativne analize pojmova *Cybercrime* i *Cyberspace* koja uključuje proces analize navedenih pojmova, a u sklopu međunarodnih suradnji i sigurnosnih aspekata u kibernetičkom prostoru, temeljem raznovrsne dokumentacije kao što su strategije, uredbe, direktive i dr., kako država, tako i međunarodnih organizacija.

Uzimajući u obzir današnji napredak tehnologije diljem svijeta, gotovo svugdje možemo vidjeti tehnički uređaj koji ima mogućnost pristupa internetu (nadzorne kamere, mobiteli, automobili, kućanski aparati), tako da je vrijeme pristupa internetu rezervirano samo za računala ostalo iza nas (Verini, 2010).

Globalno povezivanje informacijskih i komunikacijskih tehnologija i njihova međusobna ovisnost pokazuju da pojam računalni kriminal postaje preuzak za potrebno sveobuhvatno određenje, te se pojam kiberkriminal smatra boljim izborom za sva kaznena djela počinjena unutar navedenog kiberprostora uporabom informacijsko-komunikacijskih tehnologija ili na samoj informacijsko-komunikacijskoj infrastrukturi. Kao temeljna infrastruktura za počinjenje ove vrste kaznenih djela u današnjem vremenu koristi se globalna mreža koja povezuje sve uređaje, a to je internet. U posljednjih nekoliko godina sveprisutna je pojava plaćanja određenih dobara ili usluga putem interneta i raznih digitalnih ili kriptovaluta koje ne kontroliraju nacionalne banke i samim time na korisnicima je cjelokupni rizik takvih transakcija. Međutim, na taj način je povećana i mogućnost anonimnosti te plaćanja raznih ilegalnih aktivnosti, kao i izbjegavanje plaćanja poreza. Najpoznatije kriptovalute trenutno su Bitcoin (BTC), Litecoin (LTC) i Etherium (ETH), a o načelima funkcioniranja kriptovaluta detaljno je pisao Nakamoto u *Whitepaperu* još 2008. godine (Nakamoto, 2008).

Radi različitog pristupa nije prihvaćen jedinstven naziv za kriminal vezan uz računalnu i informacijsko-komunikacijsku tehnologiju. Trenutno se u Hrvatskoj koristi nekoliko naziva koji se međusobno ne isključuju, kao što je kibernetički kriminalitet, računalni kriminalitet, kompjutorski kriminalitet i visokotehnološki kriminalitet. Svi navedeni nazivi su vezani uz engleski jezik, a pokušaji prijevoda engleskih naziva i termina na druge jezike često su povezani s nemogućnošću doslovnog i odgovarajućeg prijevoda koji bi u isto vrijeme bio prihvatljiv s leksičkog, gramatičkog i profesionalnog stajališta (Škrtić, 2011, str. 85).

Oblici protuzakonitog djelovanja u kibernetičkom prostoru u zadnje vrijeme ulaze u sferu hibridnog djelovanja, a u nekim publikacijama se izjednačavaju s hibridnim ratovanjem. Napadi putem računalnih sustava u kibernetičkom prostoru od strane neke organizacije ili države mogu se protumačiti hibridnim ratovanjem (Puyvelde, 2017).

1.1 Definicije pojmova

Pojam interneta definira se kao globalna, svima koji imaju tehničke mogućnosti, dostupna računalna mreža (Franjić i Šimundić, 2009, str. 14).

Neki od pojmova, odnosno značenja interneta na engleskom jeziku mogu se pronaći definirani od strane međunarodnih organizacija, primjerice:

- Skup međusobno povezanih (računalnih) mreža pomoću internetskog protokola koji omogućuje da funkcioniraju kao jedna velika virtualna mreža *(eng. "A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network") (International Telecommunication Union, 2000)*
- Globalni sustav međusobno povezanih (računalnih) mreža u javnoj domeni *(eng. "Global system of inter-connected networks in the public domain") (International Organization for Standardization, 2012)*
- Internet je jedini, međusobno povezani, svjetski sustav komercijalnih, vladinih, obrazovnih i drugih računalnih mreža koje dijele (a) paket protokola koji je odredio IAB (RFC 2026) i (b) nazivi i adresni prostori kojima upravlja ICANN *(eng. "The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB (RFC 2026) and (b) the name and address spaces managed by the ICANN") (Internet Engineering Task Force, 2007)*
- Globalna informacijska mreža koja povezuje vrlo značajan dio svjetskih računalnih mreža *(eng. "The global information network that now links a very substantial fraction of the world's computer networks. The Internet is an extraordinary development that stems for the original ARPANET, which was initiated in North America in 1969. In broad terms the Internet does not offer services to end-users, but servers primarily to interconnect other networks on which end-user services are located. It provides basic services for file transfer, electronic mail, and remote login, and high-level services including the World Wide Web and the MBONE. The Internet is global, with connections to nearly every country in the world. It is deliberately nonpolitical and tends to deal with nongovernmental levels within a country. The structure is informal, with a minimal level of governing bodies and with an emphasis in these bodies on technical rather than on administration or revenue generation."*

"Up to the mid-1990s the major users of the Internet were the academic and research communities, but over the last decade, with a growth in home computing, there has been a massive increase in the number of individuals and companies using the World Wide Web and electronic mail. There has also been a large increase in commercial interesting in the exploitation of the Internet.") (Oxford University Dictionary, 2008, str. 269)

Najčešće spominjan pojam u ovom doktorskom radu je *Cyber* i prema Oksfordskom rječniku definira se kao:

- *"Relating to or characteristic of the culture of computers, information technology, and virtual reality." (Oxford University Dictionary, 2008, str. 268)*

Dakle, pojam cyber uključuje obilježja računalne kulture, informacijske tehnologije i virtualne stvarnosti. Također, on se odnosi na prefiksalni morfem koji se koristi za pojmove vezane uz računala, informacijske tehnologije i virtualnu stvarnost.

- *Nacionalna strategija kibernetičke sigurnosti (2015) (dalje u tekstu Strategija) definira pojam "interneta" kao "globalne mreže koja povezuje različite internetske mreže bazirane na TCP/IP protokolu, kao što je primjerice CARNet."*

Pojmovi kibernetički prostor i kibernetički kriminal bit će posebno obrađeni u kasnijem poglavlju, a ovdje je navedeno samo određenje navedenih pojmova iz Strategije:

- ***"kibernetički prostor*** *- prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Strategije obuhvaća internet i sve sustave povezane na njega."*
- ***"kibernetički (računalni) kriminalitet*** *- činjenje kaznenih djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom informacijskih i komunikacijskih tehnologija."*

Raspolaganje potrebnom količinom i kvalitetom informacija predstavljalo je još od drevnih vremena jedan od temeljnih elemenata uspješne vojne, političke ili ekonomske razrade strategije. U posljednja dva stoljeća tradicionalni je oblik prikupljanja informacija (oslonjen na špijunske mreže i diplomatske službe) sve više potiskivan tehnološkim napretkom, počevši od pojave telegrafskih linija i telefona u 19. stoljeću (Popović, 2014, str. 145).

Pravne odrednice Kaznenog zakona, kao i regulativa Zakona o kaznenom postupku Republike Hrvatske *de lege ferenda* bi trebale obuhvaćati i metode pretraga i osiguranja dokaza "podataka u oblacima" (eng. *Cloud Computing*) s obzirom da, primjerice, današnji trend korištenja podataka "u oblaku" nije ništa drugo nego podatak u kibernetičkom prostoru. Svakodnevno se pojavljuju novi uređaji, programi, načini komunikacije, i naravno, novi modaliteti kriminalnih aktivnosti. Izravna posljedica tih promjena je korištenje brojnih termina, pojmova, skraćenih i kolokvijalnih izraza i slično, koji imaju različito lingvističko i/ili semantičko značenje. Brojni pravni i informatički stručnjaci upozoravaju da ključni termini nisu dovoljno jasno i precizno definirani što stvara mogućnost različitog interpretiranja, a za posljedicu konfuziju, redundanciju, odnosno nejasnoće u preciznom definiranju specifičnih kategorija. Iz tih razloga u doktorskom radu bit će sačinjen pregled preciznih određenja ključnih pojmova, termina i izraza u postojećoj teoriji, koji su relevantni za pozitivan učinak međunarodne suradnje.

1.2 Metode znanstvenog istraživanja

Ukoliko se u obzir uzme svrha istraživanja, odnosno postojeća epistemološka baza, možemo reći da se svaki istraživački problem može promatrati multidisciplinarno, ovisno o pitanjima koja postavljamo. Metodološki pristup koji se poduzima je u tome smislu stvar nužnosti, ne istraživačkog opredjeljenja, pogotovo u ovakvoj vrsti istraživanja koja uključuju komponente sigurnosti, međunarodne suradnje, i kažnjivo ponašanje.

Temeljno pitanje ovog doktorskog rada leži u neograničenosti nacionalnih jurisdikcija kibernetičkog prostora, a samim time i nedefiniranoj jurisdikciji rješavanja problema nedopuštenih ponašanja u kibernetičkom prostoru. U ovoj točki od presudne je važnosti međunarodna suradnja, koja ovisi o geopolitičkoj situaciji i položaju, što utječe na sigurnost, kako kibernetičku, tako i nacionalnu. U tom smislu Klemenčić navodi sljedeće: "Geopolitički položaj jedan je od geopolitičkih sadržaja nacionalne sigurnosti. Geopolitički sadržaji obuhvaćaju sve teritorijalno-političke i vojno-geografske ili geostrateške sastavnice povijesno promjenjiva značaja, koje djeluju na stabilnost države u regionalnim, nadregionalnim i globalnim geopolitičkim odnosima.

Na državnoj razini, geopolitički sadržaji nacionalne sigurnosti su: geopolitički položaj, geostrateški položaj, geoprometni položaj, granični i teritorijalni sporovi, veličina teritorija, oblik teritorija, položaj regije jezgre i glavnog grada, ostali aspekti." (Klemenčić, 1997, str. 263-267).

1.3 Struktura doktorskog rada

Doktorski rad podijeljen je u pet osnovnih dijelova. Središnji dio korespondira s pojmovima vezanim uz kibernetički prostor, aspekt nedozvoljenih radnji, utjecaja na sigurnost, kao i međunarodnu suradnju, a posebno je izdvojen dio u kojemu su prikazani rezultati istraživanja. Uz navedeno rad sadrži i uvod i zaključak. S obzirom na fokus problema, istraživački fokus je bio na elementima analize suradnje među državama putem obrazaca navedene suradnje, te njezine specifikacije.

Pojašnjeni su modaliteti činjenja, istraživanja i vještačenja kaznenih djela koja se čine u kibernetičkom prostoru.

Prikazani su konkretni rezultati statističke obrade, kao i trendovi u četverogodišnjem razdoblju za sva kaznena djela iz domene računalnog kriminaliteta koji se odvija u kibernetičkom prostoru, te strukturirani prikaz kvalitativne analize tekstualnih sadržaja obrađenih dokumenata koji određuju definiranje pojmova *Cyberspace* i *Cybercrime* kao domenu sigurnosti i suradnje u kibernetičkom prostoru.

Uvodni dio rada započinje s pregledom utjecaja društvenih fenomena povezanih s trenutnim stanjem "ovisnosti" o kibernetičkom prostoru i elaboriranjem radnih hipoteza, ciljeva istraživanja i znanstvenog doprinosa doktorskog rada. U nastavku je detaljno prikazan problem istraživanja. Prvo su obrazložene karakteristike istraživačkih problema u području kibernetičkog prostora.

U drugom poglavlju rada prikazana je razrada teme s pravnog i istraživačkog aspekta analize kažnjivih ponašanja u kibernetičkom prostoru, pojašnjenja pojmova kriminaliteta u kibernetičkom prostoru. Zatim se naglašava područje pravne regulative unutar koje se ova disertacija razmatra: "Konvencija o kibernetičkom kriminalu", "Nacionalna strategija kibernetičke sigurnosti", "Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti" kao i "Strategija nacionalne sigurnosti Republike Hrvatske".

Treće poglavlje se bavi genezom istraživačkih radnji usmjerenih ka kibernetičkoj sigurnosti. U ovom poglavlju rada prikazane su mogućnosti međunarodne suradnje u suzbijanju kriminaliteta u kibernetičkom prostoru, zatim razrada teme s pravnog i istraživačkog aspekta analize kažnjivih ponašanja u kibernetičkom prostoru, te postupaka kod prijave računalnog kriminaliteta. U nastavku poglavlja analizira se međunarodna suradnja po naprijed rečenim aspektima s osvrtom na institucionalnu suradnju kao i međunarodnopravnu pomoć. Poznavanje prirode analiziranih elemenata kibernetičkog prostora nužno je za razumijevanje istraživanja nedopuštenih aktivnosti u kibernetičkom prostoru. Ovaj dio rada kreće od teorijskog pojašnjenja mogućih kažnjivih radnji sukladno načinu izvršenja, kao i zakonskih opisa kažnjivih ponašanja u Republici Hrvatskoj. Unutar tog teorijskog okvira predstavljen je koncept standardnih operativnih postupaka kod predmetnih istraživačkih radnji te su posebno prikazane ovlasti stalnog sudskog vještaka koji svojim nalazom i mišljenjem pomaže sudu u donošenju presude.

Rezultati istraživanja prikazani su u četvrtom poglavlju rada u kojem su detaljno elaborirani zaključci, kao i usporedni prikaz modela zakonskih rješenja odabranih zemalja.

Posebno mjesto u ovom poglavlju rada zauzimaju analiza statističkog pregleda kaznenih djela iz domene kibernetičkog kriminala za Republiku Hrvatsku u posljednjem četverogodišnjem razdoblju (2013. - 2017.), kao i poredbena analiza pravnih dokumenata iz ove domene određenih država, te kvalitativna i kvantitativna analiza pojmova *Cyberspace i Cybercrime* pomoću softverskog alata NVivo.

U petom poglavlju prikazan je zaključak doktorskog rada u kojemu su konsolidirani doprinosi provedenog istraživanja, dok je literatura navedena u zadnjem, šestom poglavlju.

1.4 Definiranje problema istraživanja

S obzirom na različite percepcije međunarodne suradnje u kibernetičkom prostoru, kao i sigurnosti koja je ugrožena činjenjem kaznenih djela iz ove domene, glavni problem ovog istraživanja je analiza trenutnog stanja različitih aspekata poimanja kibernetičkog prostora, kao i kibernetičke sigurnosti koja je ugrožena činjenjem niza modaliteta kaznenih djela u kibernetičkom prostoru, odnosno kiberkriminala.

Analiziraju se pravna rješenja nekih europskih zemalja, kao i obrasci i institucije međunarodne suradnje. Također, provodi se analiza i daje statistički prikaz pokazatelja za Republiku Hrvatsku u razdoblju od 2013. do 2017. godine prema podacima DZS i MUP-a, koji se odnose na kaznena djela iz domene kibernetičkog kriminala.

U Republici Hrvatskoj je trenutno važeći Kazneni zakon (stupio na snagu 1. siječnja 2013. godine) koji ima posebnu glavu posvećenu kaznenim djelima iz Glave XXV, te su navedena djela iz ovog dijela Zakona korištena radi statističke obrade i pokazatelja stanja i kretanja ove problematike u posljednjih četiri godine. Usporedba s člancima starog Kaznenog zakona (2011) ne bi dala odgovarajući prikaz budući da su pridodani novi članci u ovu grupu kaznenih djela, te je iz navedenog razloga kao referentno odabrano razdoblje od 2013. do 2017., odnosno posljednje četiri godine za koje su statistički podaci bili dostupni. U disertaciji je prikazana i kvalitativna analiza sadržaja postojeće međunarodne kaznenopravne regulative i pojašnjenja pojmova *Cyberspace i Cybercrime*, izrađena uz pomoć softverskog alata NVivo[1].

Razmatranjem "Konvencije o kibernetičkom kriminalitetu Vijeća Europe", "Nacionalne strategije kibernetičke sigurnosti" i "Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti", te "Kaznenog zakona" i "Zakona o kaznenom postupku Republike Hrvatske" elaboriraju se i problematiziraju rješenja koja se odnose na konkretan razlog istraživanja, a koja imaju posredan i izravan doticaj s navedenom problematikom. Temeljem "Konvencije o kibernetičkom kriminalitetu Vijeća Europe", koja je potpisana od Republike Hrvatske 2001. godine, kao i pretpostavke da kaznena djela počinjena u kibernetičkom prostoru uz korištenje računalnih mreža i interneta (*cyberspace*) ne poznaju granice država, prikazuje se sustavan komparativni prikaz zakonodavstava nekih država i njihovih rješenja navedenog problema.

[1] NVivo - QSR International https://www.qsrinternational.com/nvivo/home , stranica posjećena 12. prosinca 2017.

Postojeće teorijske i empirijske spoznaje o suradnji Europske unije na temu kibernetičkog kriminala u ovom se radu nadograđuju sljedećim spoznajama, temeljem pristupa koji do sada nije korišten:

1) *Fokus ovoga istraživanja je prikaz suradnje između država i stanja sigurnosti u kibernetičkom prostoru s motrišta institucija koje provode zakon u slučajevima kibernetičkog kriminala u referentnom razdoblju tijekom kojega kibernetički kriminal uzrokuje sve veći strah i nesigurnost u takav način komunikacije;*
2) *Analizira se vrsta kaznenih djela i daje statistički prikaz s pojašnjenjima;*
3) *Kvalitativno i kvantitativno se analiziraju pojmovi Cyberspace i Cybercrime uz pomoć računalnog softvera NVivo na parametrima koji do sada nisu korišteni, te se prikazuje učestalost (frekvencija) ponavljanja ključnih riječi.*

S obzirom na opasnost i izravne posljedice koje mogu nastupiti uslijed nedostatnog razumijevanja i razmatranja ove problematike, kao i manjakvog poznavanja zakonskih i tehničkih pretpostavki za počinjenje kaznenih djela u kibernetičkom prostoru, ova tema ima za cilj identificirati i elaboriririrati rizike korištenja kibernetičkog prostora, kao i evaluaciju praćenja i suradnje s drugim državama, imajući na umu da elektronički dokazi (koji se pojavljuju kod ove vrste kaznenih djela) ne poznaju državne granice, te se posebno razmatra problem jurisdikcije (Featherstone i Burrows, 2001).

1.5 Radne hipoteze, ciljevi i svrha istraživanja

Prvi cilj istraživanja je steći preciznije razumijevanje pojmova iz domene kibernetičkog prostora i kibernetičkog kriminala (engl. pojmovi *Cyberspace* i *Cybercrime*) te tako provjeriti i odgovoriti na pitanje je li pozitivna pravna regulativa adekvatno odgovorila na zahtjeve modernog doba u kojem živimo i u kojemu smo oslonjeni na putovanje informacija kroz kibernetički prostor.

Sljedeći cilj je identificirati i elaborirati rizike korištenja kibernetičkog prostora, kao i potrebu praćenja i suradnje s drugim državama, imajući na umu da elektronički (digitalni) dokazi (koji se pojavljuju kod ove vrste kaznenih djela) nisu odijeljeni državnim granicama s obzirom na opasnost i izravne posljedice koje mogu nastupiti uslijed nedovoljnog razumijevanja i razmatranja ove problematike, kao i nedovoljno poznavanje zakonskih i tehničkih pretpostavki za počinjenje kaznenih djela u kibernetičkom prostoru. Stoga se posebno razmatra problem jurisdikcije u poredbenom pregledu zakonodavstava određenih država.

Također, cilj ovoga istraživanja je ustanoviti i na novim osnovama analizirati međunarodnu suradnju, te sigurnost u kiberprostoru s motrišta institucija koje provode zakon u slučaju kibekriminala (*Cybercrime*), nadograditi postojeći korpus empirijskog znanja, provjeriti i preispitati dosadašnje teorijsko-normativne postavke, te u konačnici dati doprinos razumijevanju i izradi kibernetičko-sigurnosne politike Europske unije, koja se povezuje s edukacijskim pravcima u obrazovanju.

Osim toga, cilj je da se ukaže i na mogućnosti unaprjeđenja postojeće metodologije međunarodne suradnje svih službi koje se bave ovom problematikom, počevši od istražnih institucija (policije i državnog odvjetništva, Interpol, Europol) do sudstva (međunarodno-pravna pomoć, Ujedinjeni narodi), kao i sudskih vještaka za informatiku, koji u najvećem broju slučajeva razjašnjavaju sudu sve bitne činjenice u kaznenom postupku, uključujući i elektroničke (digitalne) dokaze, a koji su uključeni u međunarodne zajednice eksperata, kroz statističke prikaze kaznenih djela kao relevantnih pokazatelja domene računalnog kriminaliteta DZS i MUP za posljednje četverogodišnje razdoblje po svim dostupnim parametrima, s trendovima i analizom.

Kako je ranije istaknuto, istražuju se mogućnosti primjene modela zakonskih rješenja koje su uvele neke države u svojim zakonodavstvima, te preporuke za standardne operativne postupke kod međunarodne suradnje. Svakodnevno smo svjedoci napretka računalne tehnologije i njenog ulaska u sve pore života. Nastavno, pojavljuju se novi uređaji, programi, načini komunikacije, i sukladno tome, novi modaliteti međunarodne suradnje.

Izravna posljedica tih promjena je korištenje brojnih termina, pojmova, skraćenih i kolokvijalnih izraza i sl., koji imaju različito lingvističko i/ili semantičko značenje. Brojni pravni i informatički stručnjaci upozoravaju da ključni termini nisu dovoljno jasno i precizno definirani (osobito vezano uz pravnu terminologiju), što stvara mogućnost različitog interpretiranja i ima za posljedicu konfuziju, redundanciju, odnosno nejasnoće u preciznom definiranju specifičnih kategorija. Iz tih razloga u disertaciji je dan pregled preciznih određenja ključnih pojmova, termina i izraza u postojećoj teoriji koji su relevantni za uspješnu međunarodnu suradnju.

Daje se i prikaz kvalitativne analize pojmova *Cyber space, Cyberspace, Cyber crime i Cybercrime* korištenjem sadržaja primarnih izvora navedenih zemalja (strategije, zaključci, uredbe, direktive, odluke, preporuke i mišljenja) po navedenim pojmovima.

1.6 Istraživačka pitanja

S obzirom na prethodno elaborirani problem suradnje u kibernetičkom prostoru, kao i sigurnosti koja je ugrožena činjenjem kaznenih djela iz ove domene, glavni problem ovog istraživanja je nekonzistentna aktualna međunarodna kaznenopravna regulativa kao i obrasci međunarodne suradnje za istraživanje i sankcioniranje navedene kategorije kaznenih djela, s analitičkim osvrtom na Republiku Hrvatsku. Razmatranjem "Konvencije o kibernetičkom kriminalitetu Vijeća Europe", "Nacionalne strategije kibernetičke sigurnosti" i "Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti", te "Kaznenog zakona" i "Zakona o kaznenom postupku Republike Hrvatske" specificiraju se problemske točke istraživanja koje imaju doticaj u većoj ili manjoj mjeri s navedenom problematikom te se analiziraju ranija i aktualna rješenja.

Jedan od ciljeva rada je odgovor na pitanje je li pozitivna pravna regulativa primjereno odgovorila na zahtjeve modernog doba u kojem živimo i u kojemu smo oslonjeni na putovanje informacija kroz kibernetički prostor.

Temeljem "Konvencije o kibernetičkom kriminalitetu Vijeća Europe", koju je Republika Hrvatska potpisala 2001. godine, kao i pretpostavke da kaznena djela počinjena u kibernetičkom prostoru (*cybercrime*) uz korištenje računalnih mreža i interneta (*cyberspace*) nisu odijeljena granicama matičnih država, dat će se sustavan komparativni prikaz zakonodavstava određenih država i njihovih rješenja navedenog problema, prikazati analiza i trendovi takvih kaznenih djela i kvalitativno analizirati pojmove *Cyberspace* i *Cybercrime* u izabranim relevantnim dokumentima.

Postojeće teorijske i empirijske spoznaje o suradnji na temu kibernetičkog kriminala u ovom se radu nadograđuju sljedećim spoznajama, temeljem pristupa koji do sada nije korišten:

1) Fokus ovoga istraživanja je analiza međunarodne suradnje i sigurnosti u kibernetičkom prostoru s aspekta tijela za provođenje zakona u borbi protiv kibernetičkog kriminaliteta u recentnom razdoblju, tijekom kojeg kibernetički kriminal uzrokuje sve veći strah i nesigurnost u takav način komunikacije, temeljem komparativnog prikaza zakonskih rješenja, s pojašnjenjem određenih kažnjivih ponašanja i njihovog načina istrage.

2) Analiziraju se vrste dokumenata koji do sada nisu bili obuhvaćeni u takvom opsegu s aspekta pojmova *Cyberspace* i *Cybercrime*. Istraživanje se temelji na kvalitativnoj analizi sadržaja na parametrima koji do sada nisu korišteni uz pomoć softvera NVivo.

3) Istraživanje se temelji i na statističkom prikazu kaznenih djela iz domene računalnog kriminala za recentno razdoblje od četiri godine za Republiku Hrvatsku, odnosno evidentiranih kaznenih djela, broja prijavljenih, optuženih i osuđenih punoljetnih počinitelja tih kaznenih djela.

Istraživačka pitanja su sljedeća:

1. Kakva je dinamika kreiranja obrazaca za oblikovanje kibernetičko-sigurnosne politike s obzirom na endogene i egzogene čimbenike, dinamiku, područje i opseg međunarodne suradnje?

2. Kakav je međuodnos kooperacije, koordinacije, integracije i učinkovitosti u analiziranim dokumentima koji sadrže pojmove Cyberspace i Cybercrime s aspekta sigurnosti u kibernetičkom prostoru?

3. Podupiru li nalazi vezani uz dinamiku promjene opsega i obrazaca međunarodne suradnje i sigurnosti u kibernetičkom prostoru i međuodnos pokazatelja kooperacije, koordinacije i integracije postojeće teorijske paradigme?

1.7 Metodološki okvir istraživanja

Kvalitativnim istraživanjem analiziraju se primarni izvori prikazanih država i međunarodnih organizacija po pitanju pojmova *Cyberspace* i *Cybercrime* (strategije, zaključci, uredbe, direktive, odluke, preporuke i mišljenja, te radni dokumenti institucija EU), kao i pravni dokumenti Republike Hrvatske:

- *"Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu";*
- *"Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava Vijeća Europe";*
- *"Nacionalna strategija kibernetičke sigurnosti";*
- *"Akcijski plani za provedbu Nacionalne strategije kibernetičke sigurnosti";*
- *"Kazneni zakon";*
- *"Zakon o kaznenom postupku Republike Hrvatske";*

Daje se analiza usporednih aktualnih kaznenopravnih rješenja u drugim državama i njihovih pravnih normi. Statistički se prikazuju pokazatelji i trendovi vezano uz problematiku kaznenih djela iz domene računalnog kriminaliteta, korištenjem podataka Ministarstva unutarnjih poslova Republike Hrvatske (Statistika MUP-a - 2013., 2014) (Statistika MUP-a - 2014., 2015) (Statistika MUP-a - 2015., 2016) (Statistika MUP-a - 2016., 2017) i Državnog zavoda za statistiku Republike Hrvatske (Statistička izvješća broj 1528, 2014) (Statistička izvješća broj 1529, 2014) (Statistička izvješća broj 1551, 2015) (Statistička izvješća broj 1552, 2015) (Statistička izvješća broj 1576, 2016) (Statistička izvješća broj 1577, 2016) (Statistička izvješća broj 1605, 2017) (Statistička izvješća broj 1606, 2017) za razdoblje 2013.-2017., otkad je na snazi izmijenjeni Kazneni zakon Republike Hrvatske .

Istražuju se obrasci i trenutni doseg međunarodne suradnje vezano uz sigurnosni aspekt u kibernetičkom prostoru, s pojašnjenjem svih oblika i pojmova takve suradnje, kao i uloge Republike Hrvatske s obzirom na globalni karakter ovog problema.

Predmetno istraživanje polazi od fundamentalne pretpostavke da međunarodna suradnja radi veće sigurnosti kibernetičkog prostora, kao i zloporabe njegovih mogućnosti zahtijeva poznavanje metodologije i rada računalnog sustava, kao i osnovne informatičke pojmove, primarno *Cyberspace i Cybercrime* te procese međunarodne suradnje ustanova koje surađuju na sigurnosti i preveniranju svih oblika kriminala počinjenih u kibernetičkom prostoru i/ili uz pomoć kibernetičkog prostora.

Analiziraju se i načini funkcioniranja određenih nacionalnih ustrojstvenih jedinica zaduženih za međunarodnu suradnju na polju kibernetičkog prostora i kriminala, te njihovih kontakt točaka, koji su dionici navedene suradnje, te prikazuje rad i ustroj takvih institucija.

Istraživanje rezultira smjernicama za poboljšanje prevencije i suzbijanja nedopuštenog ponašanja u kibernetičkom prostoru, te prikazuje nove mogućnosti koje pruža kibernetički prostor po pitanju iskoristivosti mehanizma međunarodne suradnje i edukacije.

Kako je riječ o kvalitativnom istraživanju, za potrebe ovoga rada je neprikladno postavljati hipoteze predikcijskog tipa koje pripadaju kvantitativnom pristupu. Sukladno logici provođenja istraživanja unutar kvalitativnog pristupa, postavljeni su ciljevi istraživanja koji su eksploratornog karaktera. Vezano uz objašnjavanje fenomena u kvalitativnom istraživanju, fundamentalno je pitanje cjelokupne društvene znanosti (Hruška, 2010, str. 178).

Kakav je status objašnjenja koje društvene znanosti mogu ponuditi? Jedna grupa istraživača društvenih fenomena traži objašnjenje društvene interakcije u terminima univerzalno determinističkih odnosa kao što je uobičajeno u prirodnim znanostima, dok druga grupa odbacuje takav pristup. Iako ljudsko ponašanje nije definirano zakonima, ono nije niti kaotično. Pažljivim istraživanjem moguće je pronaći pravilnost u društvenim interakcijama. Kauzalni odnos može biti rezultat kvalitativnog istraživanja, no riječ kauzalnost se ovdje treba uzeti sa zadrškom, na način da je riječ o postavljanju pretpostavki, a ne usko definiranih zakona (Patton, 2002, str. 99).

Hruška (2010) dalje naglašava da se logika objašnjenja fenomena u kvalitativnim istraživanjima može promatrati iz dvije perspektive. Prvo, na kvalitativne podatke može se gledati kao na varijable – entitete, koji mogu biti uniformno prezentirati. Iz drugog kuta promatranja, mogu se odbiti ideje kako kvalitativne varijable imaju direktnu kauzalnost (x vodi do y), a pojedine kategorije pokušavaju se promatrati kroz sistematično grupiranje, prikazivanje i diskusiju (Ritchie i Lewis, 2003, str. 14).

Namjera predloženog istraživanja nije utvrditi odnose između razmatranih koncepata na deterministički način. Cilj je opisati prirodu povezanosti različitih elemenata koji imaju utjecaj na promatrani fenomen (Richards i Richards, 1994, str. 445-462).

Kvalitativno istraživanje može doprinijeti razvoju društvenih teorija kroz istraživanje društvenih procesa i struktura koje formiraju i objašnjavaju dio konteksta za individualno ponašanje ili vjerovanja. Pozicija predloženog istraživanja je kako teorija treba biti utemeljena na empirijskoj stvarnosti jer samo ona omogućava razvoj teorije koja je relevantna i koja se može testirati.

Metoda istraživanja (primjerice statistička korelacija u kvantitativnim istraživanjima ili promatranje u kvalitativnim istraživanjima) sama po sebi nema intrinzičnu vrijednost; vrijednost metode se određuje u ovisnosti o konkretnom predmetu istraživanja. U kvalitativnim istraživanjima afirmirane su četiri temeljne istraživačke metode: (1) promatranje, (2) analiza teksta, (3) intervjui, (4) audio snimke i videosnimke (Silverman, 2001, str. 19).

U provedbi istraživanja koristi se struktura analitičke hijerarhije koja se zasniva na: "(1) obradi podataka, (2) opisu podataka i (3) objašnjenju definiranih kategorija" (Ritchie i Lewis, 2003, str. 199-219). Analitička hijerarhija oblik je konceptualne strukture koja sadrži niz analitičkih zadataka koji osposobljuju istraživača da dobije uvid u podatke i u njima pronađe smisao. Ovaj pristup provedbi kvalitativnog istraživanja zasnovan je na tematskoj analizi koja se fokusira na interpretaciju značenja. Temeljne faze provedbe istraživanja koje se predlažu prikazane su u tablici 1. (Ritchie i Lewis, 2003, str. 212).

Objašnjenje definiranih kategorija	Traganje za primjenom objašnjenja u širem teorijskom okviru
	Razvijanje objašnjenja (odgovaranje na pitanje zašto)
Opis podataka	Utvrđivanje obrazaca
	Postavljanje tipologija
	Identificiranje elemenata i dimenzija, rafiniranje kategorija, klasificiranje podataka
Obrada podataka	Sumiranje ili sintetiziranje podataka
	Sortiranje podataka prema temama ili konceptima
	Povezivanje i označavanje podataka prema temama ili konceptima
	Identificiranje inicijalnih tema i koncepata
	Podatci

Tablica 1 - Opis temeljnih faza predloženog istraživanja Izvor: (Ritchie i Lewis, 2003, str. 212)

Prvi dio analize odnosi se na obradu podataka iz prikupljenih dokumenata i u ovom dijelu analize obuhvaćaju se definicije pojmova *Cyberspace* i *Cybercrime*. Ovaj dio analize prikazuje nam empirijske podatke, a što je od vitalne važnosti za kasnije interpretativne faze analize. Obrada podataka izvršava se uz pomoć NVivo računalne aplikacije.

Nakon što se generira skup tema i koncepata i aplicira na prikupljenu empirijsku građu, sintetizirani podaci upotrebljavaju se za iduću fazu istraživanja - identificiranje ključnih dimenzija fenomena te utvrđivanje raspona i različitosti koje se nalaze unutar pojmova. Kada je većina posla vezanog za opis i razvoj tipologija obavljena slijedi faza objašnjavanja definiranih kategorija i frekvencija ponavljanja. Tranzicija od faze opisivanja prema fazi objašnjavanja odvija se kroz potragu za obrascima unutar pojmova i objašnjenjem pojavljivanja pronađenih obrazaca. Ovo je temeljna faza kvalitativnog istraživanja.

Rafiniranje kategorija, razjašnjavanje dimenzija problema i razvijanje objašnjenja iterativan je proces unutar kojega postoji stalna potreba za uvidom u originalne ili sintetizirane podatke u potrazi za novim tragovima ili u želji da se određene propozicije evaluiraju. U tom smislu ne može se promatrati analitička hijerarhija kao linearan proces nego radije kao fluidna struktura koja omogućava kretanje od podataka do potvrđenih teorijskih koncepata i natrag (Ritchie i Lewis, 2003, str. 213).

Kako je već naglašeno, metodologija kvalitativnog istraživanja nije dizajnirana da bi potvrdila ili opovrgnula hipoteze, nego da omogući opis istraživanog fenomena. Fenomenološko bogatstvo se ostvaruje kroz iskazivanje dokaza koji potkrepljuju nastale teme, usporedbom definicija i prikazom frekvencije ključnih riječi.

2. KRIMINALITET U KIBERNETIČKOM PROSTORU I KIBERNETIČKA SIGURNOST

Kriminalitet koji se povezuje uz računalno-informacijsku tehnologiju doveo je do potrebe definiranja te vrste kriminaliteta. Napredak navedenih tehnologija utječe na nove načine i vrste komunikacije suvremenog društva. Ne tako davno, u prošlosti, više se koristila tradicionalna hijerarhijska, centralizirana i vertikalna struktura, dok je u današnje vrijeme i s uporabom novih tehnologija, došlo do pomaka u radu kriminalnih organizacija, koje sve više koriste mrežnu, decentraliziranu i horizontalnu komunikaciju, a što se u zadnje vrijeme najviše vidjelo na principu organiziranja terorističkih aktivnosti po cijelom svijetu pod nazivom "Globalni džihad" (Božinović, 2016, str. 62).

U takvom globalnom svijetu, suvremeno društvo uvelike ovisi o neometanom funkcioniranju informacijskih i komunikacijskih sustava uz pomoć kojih se upravlja svim bitnim sustavima kao što su policija, vojska, promet, opskrba i druge službe, kao i kritična nacionalna infrastruktura, te uobičajena dnevna komunikacija. Kako se svi ti sustavi međusobno sve više povezuju, tako postoji i sve veća opasnost napada na takve sustave. Široka dostupnost tehnologije omogućuje sve veću automatizaciju napada i korištenja sofisticiranih alata za napade. Razvoj informacijsko-komunikacijske tehnologije, uz sve svoje pozitivne strane, nažalost ima i svoju negativnu stranu - kibernetički kriminal, odnosno kiberkriminal (Dragičević, 2005, str. 150).

2.1 Pojam kriminaliteta u kibernetičkom prostoru

"Konvencijom o kibernetičkom kriminalu" (dalje u tekstu Konvencija) u svakodnevni jezik struke uveden je pojam kibernetički kriminal. O samoj Konvenciji, njenim dosezima i učincima bit će govora u posebnom poglavlju.

Kako bi mogli razlučiti dosege i razjasniti pojmove, problem treba sagledati iz više perspektiva. "Kazneni zakon Republike Hrvatske" (u daljnjem tekstu KZ) sadrži poglavlje koje se bavi isključivo kaznenim djelima proizašlim iz Konvencije.

Ovo poglavlje nosi naziv "*Kaznena djela protiv računalnih sustava, programa i podataka"* i nalazi se u glavi XXV.

"Zakon o kaznenom postupku Republike Hrvatske" (u daljnjem tekstu - ZKP) koristi pojmove iz Kaznenog zakona, ali i definira jedan novi pojam važan za ovu vrstu kriminala a to je pojam elektronički dokaz, dok se u dijelu literature, osobito stranih izvora, koristi pojam digitalni dokaz.

Također vrijedi istaknuti da su trenutnom Uredbom o unutarnjem ustrojstvu Ministarstva unutarnjih poslova Republike Hrvatske[2], te zadnjim izmjenama iz 2017. godine[3] određene službe koje se bave istraživanjem ovih kaznenih djela, ali pod različitim nazivima. Na razini države, odnosno unutar Ravnateljstva policije naziv ove službe je "Služba kibernetičke sigurnosti, unutar Kriminalističko-obavještajnog sektora Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminala" - PNUSKOK, dok je do zadnjih izmjena iz 2017. godine ova služba bila ustrojena kao Odjel za visokotehnološki kriminalitet.

Tijekom kriminalističkih istraga, vještačenje iz ove domene kaznenih djela obavlja se u Centru za forenzična ispitivanja, istraživanja i vještačenja Ivan Vučetić koji se nalazi unutar Ravnateljstva policije.

Na razini policijskih uprava kaznena djela računalnog kriminala svrstavaju se u rad "Odjela za financijske institucije, izvangospodarsku djelatnost, intelektualno vlasništvo i kompjutorski kriminalitet" unutar Sektora kriminalističke policije, a sve ovisno o razini kategorije policijske uprave. Naime, u Republici Hrvatskoj postoje četiri razine ustroja policijskih uprava, sukladno tome organizirani su na sektor, službe, odjeli, odsjeci ili grupe pod čiju ingerenciju spada i policijski službenik koji se bavi ovom problematikom.

U posljednje vrijeme dominira mišljenje da je računalni kriminal dio kibernetičkog kriminala. Kako navodi Bača, kibernetički kriminal je općeniti pojam kojim se označavaju sva kriminalna djela u kojima je kao cilj ili sredstvo bilo uključeno računalo ili računalna mreža, dok valja istaknuti kako se računalni kriminal smatra dijelom kibernetičkog kriminala (Bača, 2004, str. 29)

[2] Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova Republike Hrvatske, Narodne novine 70/2012.
[3] Uredba i izmjenama i dopunama uredbe o unutarnjem ustrojstvu ministarstva unutarnjih poslova, Narodne novine 129/2017.

Kibernetički kriminal je nastajao i razvijao se zadnjih pedesetak godina kada je po prvi put zamijećen kao problem. Pojam kibernetičkog kriminala javlja se krajem prošlog stoljeća, a u posljednje vrijeme koristi se i pojam kiberkriminal.

Donosi se skup novih pojmova vezanih uz kibernetički kriminal od strane Ministarstva pravosuđa SAD-a 1994. godine, a potom i Konvencija o kibernetičkom kriminalu 2001. godine. Pojam kibernetičkog kriminala aktualizirao je i pojam pravno relevantnih činjenica, odnosno dokaza koji se mogu koristiti u dokazivanju računalnog kriminala.

Općenito se koriste četiri kategorije kibernetičkog kriminala. U prvu kategoriju uključena su kaznena djela u kojima je računalo objekt kriminala, kada je kriminal bio povezan sa samim računalima (poput krađe računala ili njegovih komponenti ili uništenje računala i slično).

Druga kategorija opisuje računalo kao cilj, odnosno "subjekt" kriminala, kada računalo predstavlja okolinu u kojoj je kriminal počinjen (poput krađe podataka, provale u računalo i slično).

U treću kategoriju uvrštena su kaznena djela u kojima je računalo alat ili instrument za izvođenje ili planiranje kriminala (kada se npr. računalo koristi za provalu u drugo računalo). Četvrta kategorija opisuje sva kaznena djela u kojima se računalo slučajno pojavljuje u drugima kriminalnim djelima ili se jednostavno koristi kao simbol za zastrašivanje (poput pedofilije, pranja novca i slično) (Bača, 2004, str. 30).

Pojam kibernetičkog kriminala (engl. *cybercrime*) Dragičević definira kao "ukupnost kaznenih djela koja su kroz određeno vrijeme počinjena unutar kibernetičkog prostora ili uz njegovu pomoć korištenjem ili zlorabljenjem resursa ili servisa kibernetičkog prostora ili usluga uz pomoć informacijskih tehnologija koje čine njegovu infrastrukturu. Kako do danas ne postoji opće prihvaćena definicija pojma, tako je bitno naglasiti da termin *cyber,* kao prvi element riječi, u većini rječnika označava nešto vezano uz svijet prividne stvarnosti koji nastaje uporabom računala" (Dragičević, 2004, str. 13).

Doseg kibernetičkog kriminala možemo pokušati objasniti kroz širi pojam, a to je kibernetički prostor ili kiberprostor (engl. Cyberspace), što je i intencija autora ovog doktorskog rada.

Devedesetih godina prošlog stoljeća u Sjedinjenim Američkim Državama (dalje u tekstu SAD) pojavio se pojam *cyberspace* koji je označavao računalnu mrežu, te je jasno distancirao fizički svijet od digitalnog - nevidljivog ljudskom umu. Taj svijet nije ograničen teritorijalnim granicama država, on obuhvaća sva mjesta s kojih se obavlja komunikacija te nema nacionalnih granica i nacionalnih jurisdikcija. (NATO CCDCOE, 2017)[4]

U svojoj knjizi iz 1992. godine Krapac navodi da bi računalni kriminalitet podrazumijevao sve slučajeve zloporabe elektronskog računala (manipulacija na njemu ili s njime) koji su pravno određeni kao kaznena djela. (Krapac, 1992, str. 12) Iako je ovaj pojam definiran s aspekta napretka tehnologije davne 1992. godine, smatramo da je navedena definicija još uvijek aktualna i prihvatljiva.

Bitna obilježja dokazivanja svih kaznenih djela počinjenih u kiberprostoru su elektronički, odnosno digitalni dokazi, a analiza računalnih podataka i računalna forenzika su neizostavni dio prevencije, otkrivanja i procesuiranja kiberkriminaliteta. Istražitelji i forenzičari gotovo svakodnevno otkrivaju nove slučajeve kiberkriminala.

U jednom ranijem radu navodim da "Korištenje ICT[5] tehnologije u nedozvoljene svrhe zahtijeva dodatne metode i tehnike za vođenje kriminalističkog istraživanja. Elektronički dokazi su osjetljivi, lako se brišu, mijenjaju i time se kompromitiraju. Specijalni forenzički alati omogućavaju povrat i analizu obrisanih, skrivenih i privremenih datoteka koje u svakodnevnom uobičajenom radu nisu vidljive. S obzirom da se računalo može koristiti kao oruđe za počinjenje nedopuštenih radnji, ono može, odnosno mora sadržavati dokaze koji se odnose na bilo koje protupravno ponašanje, čak i kaznena djela poput ubojstva ili silovanja. Nije nevažno napomenuti da većina eksperata pohranjuje svoje podatke na računala. Bilo koje kriminalističko istraživanje može koristiti računala ili internet i svi koji sudjeluju u istraživanju mogu izvući korist ako vladaju ovom tehnologijom" (Protrka, 2011, str. 2).

[4] Cyber definitions https://www.ccdcoe.org/cyber-definitions.html, stranica posjećena 12. prosinca 2017.
[5] ICT - eng. "Information and communication technologies"

Ako se podaci prilikom istraživanja prikupe nezakonito, oni se neće moći koristiti u sudskom postupku. Članak 29. stavak 4. Ustava Republike Hrvatske zabranjuje korištenje dokaza u bilo kojem sudskom postupku ako su ovi pribavljeni protivno zakonu, a tako je i u svim promatranim državama.[6]

Prema Caseyu "pojam digitalni ili elektronički dokaz koristi se u američkom zakonodavstvu i označava bilo koji računalni podatak koji može potvrditi da je počinjeno kazneno djelo ili koji može ukazati na povezanost između kaznenog djela i žrtve ili takvog djela i njegovog počinitelja" (Casey, 2011, str. 1-2).

U knjizi Uvod u računalnu sigurnost, Bača opisuje elektroničke dokaze kao "vrlo važne jer predstavljaju kombinaciju različitih informacija poput teksta, slike, audio i videosnimke. Ponekad informacija koja je pohranjena na računalu može biti jedini trag koji će kriminalističko istraživanje dovesti na pravi put.

Postoji cijeli niz elektroničkih dokaza koji nas okružuju u našem svakodnevnom životu, a kojih smo skoro u potpunosti nesvjesni. Forenzika osigurava načela i tehnike koje omogućuju kriminalističko istraživanje i progon počinitelja računalnog kriminaliteta.

Općenito gledajući, forenzika je primjena pravnih znanosti i drugih znanstvenih procesa i tehnika koje se mogu iskoristiti u identifikaciji, povratku, rekonstrukciji ili analizi dokaza tijekom kriminalističke istrage. Forenzičari pokušavaju uz pomoć elektroničkih dokaza rekonstruirati događaj te ga približiti i na taj način pojasniti istražiteljima" (Bača, 2004, str. 262).

[6] Ustav Republike Hrvatske - NN 85/2010. V. članak 29. stavak 4.

2.2 Pojam elektroničkog (digitalnog) dokaza

Elektronički ili digitalni dokazi mogu se naći na različitim uređajima (računalima, mobitelima, tabletima, printerima, digitalnim kamerama, skenerima) ili medijima za pohranjivanje (CD, DVD, SD kartica, USB disk, SSD disk), kao i "na mreži", odnosno udaljenim poslužiteljima (eng. *Server*). Za lakši pronalazak elektroničkih dokaza treba jasno definirati što je elektronički dokaz.

Zakon o kaznenom postupku definira pojam elektroničkog (digitalnog) dokaza "Elektronički (digitalni) dokaz je podatak koji je kao dokaz u elektroničkom (digitalnom) obliku pribavljen prema ovom Zakonu." [7]

Ne postoje jasne definicije te se vode mnoge rasprave teoretičara o tome što je elektronički dokaz. Tako neki teoretičari tvrde da je elektronički dokaz bilo koji podatak pohranjen ili poslan korištenjem računala koji potvrđuje ili opovrgava teoriju o tome kako se kazneno djelo ili prekršaj dogodio ili u sebi sadrži neki bitni podatak o kaznenom djelu ili prekršaju kao što je namjera ili alibi. (Casey i suradnici, 2004:12)

Međunarodna organizacija za računalne dokaze (IOCE) definira da je elektronički dokaz informacija pohranjena ili poslana u binarnom kodu koja se kasnije može koristiti u sudskom procesu. [8]

Pregledom ovih definicija i kombiniranjem s jasnom, čak i malo pojednostavljenom definicijom materijalnog dokaza (izvori saznanja o tome što se zapravo dogodilo), može se zaključiti da je elektronički dokaz svaki podatak ili informacija o kaznenom djelu ili prekršaju koja se nalazi na elektroničkom (digitalnom) uređaju ili se prenosi posredstvom takvih uređaja.

Elektronički dokaz može biti u tekstualnom obliku ili kao slika, audio ili videozapis, a može se nalaziti i u "pokretu" bilo zrakom ili žičanim putevima (Mason i Seng, 2017, str. 24).

Svojstva elektroničkih dokaza su promjenjivost (podložni su brisanju, oštećenju ili manipulaciji), ne moraju biti dostupni na duže vrijeme (podaci u RAM-u - *Random Access Memory* - memorija se gubi gašenjem ili korištenjem računala) i nevidljivi su okom, teško je potvrditi autentičnost i, u pravilu, zahtijevaju posebne vještine u rukovanju s njima.

---

[7] Zakon o kaznenom postupku, članak 202., st. 33.
[8] FBI - https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm stranica posjećena 31. listopada 2017.

Elektronički dokazi mogu biti pohranjeni na relativno malim uređajima[9] koji su ponekad zanemareni od strane istražitelja osim ako nisu upućeni na njih. Istražitelji koji osiguravaju mjesto zločina kao i tehničari koji kasnije fiksiraju i izuzimaju dokaze, moraju imati na umu krhkost elektroničkih dokaza i biti upoznati u radu s njima jer jednom promijenjeni, teško se mogu povratiti i u pravilu bivaju odbijeni od suda. Pravilno fiksirani i izuzeti, elektronički dokazi mogu se kopirati relativno lako i originalni dokazi se mogu spremiti na puno dulje vrijeme, dok se na preslikama mogu raditi različiti eksperimenti bez ugrožavanja dokaza, što je velika prednost nad klasičnim materijalnim dokazima. Digitalne dokaze teško je obrisati jer postoje razni alati za povratak (eng. *recovery*) podataka u njihovo originalno stanje.

Pregledom računalne arhitekture (građe), koja se može primijeniti na većinu današnjih elektroničkih uređaja, dobivamo uvid u vrste izvora elektroničkih dokaza. To su statični podaci koji su trajno spremljeni u razne vrste *ROM* memorije (npr. tvrdi disk, USB disk, CD/DVD) i predstavljaju pouzdan izvor koji nije podložan gubitku električne energije i može mu se utvrditi izvor. Izvor elektroničkih dokaza su dinamični podaci koji su trenutno spremljeni u RAM, *spool* ili virtualnu memoriju, te su podložni promjeni i brisanju tijekom vremena ili gubitkom električne energije i, na kraju, podaci na mreži ili internetu su izvori elektroničkih dokaza podložni korupciji i propadanju tijekom vremena, veoma ih je teško locirati u fizičkom svijetu i teško je odredit izvor i vlasnika podataka (Mason, 2016, str. 147).

Više o samom načinu prikupljanja, čuvanja i procesuiranja elektroničkih dokaza bit će pojašnjeno u kasnijem poglavlju.

Potencijalni elektronički (digitalni) dokaz može se definirati kao elektronička informacija koja sadrži podatke o počinjenom kaznenom djelu, odnosno informacija u elektroničkom obliku koja ima dokaznu vrijednost.

Informacije i podaci mogu biti pohranjeni ili preneseni putem elektroničkih medija za pohranu i prijenos podataka, a to su onda nositelji dokaza.

[9] Jedna microSD kartica veličine nokta na malom prstu ruke može sadržavati tisuće brojeva bankovnih kartica ili stotine slika dječje pornografije.

Adresari - Address Books	Dijelovi datoteka
Elektronička pošta - e-mail	Datoteke za pohranu - Backup files
Audio/Video datoteke - *.avi, *.mp3	Log datoteke - *.txt
Slikovne/Grafičke datoteke - *.jpg	Datoteke za konfiguraciju - *.ini
Kalendari	Ispisne datoteke za pisače - Printer spool
Baze podataka - Database files	Kolačići - Cookies
Tablične datoteke - *.xlsx	Privremene datoteke - Swap files
Kompresirane datoteke - *.zip, *.rar itd.	Sistemske datoteke - System files
Datoteke sa pogrešnim nazivom	Povijest - History files
Enkriptirane datoteke	Privremene datoteke - Temporary files
Skrivene datoteke	Datoteke dokumenata - *.docx
Datoteke zaštićene lozinkom	Internet favoriti - bookmarks/favorites
Podaci u oblaku (Cloud computing)	WiFi podaci
Skeneri	Zapisi nadzornih kamera (CCTV)

Tablica 2 - Potencijalni elektronički (digitalni) dokazi

Izvor: (Protrka, Računalni podaci kao elektronički (digitalni) dokazi, 2011, str. 3)

Bača je još 2004. godine okarakterizirao elektroničke dokaze kao "vrstu materijalnih dokaza, bez obzira na činjenicu što ih je teže evidentirati" (Bača, 2004, str. 270).

Kazneni zakon definira računalni podatak kao "svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu."[10] Kako su sve informacije, u stvari, interpretirani podaci koji mogu biti od interesa za postupak, tako nam je bitno da sve takve podatke osiguramo. Dokaz u obliku digitalnih videosnimaka, kao što je snimak sigurnosnih-nadzornih kamera (CCTV), također se može prihvatiti uz sudsko preispitivanje o načinu na koji je pribavljen.

Kada je dobiven na način protivan zakonu, primjerice neovlaštenim sredstvima ili bez poštivanja dostojanstva i časti osobe koja je snimljena, tada neće biti dopustiv.[11]

[10] Članak 87. st. 19. Kaznenog zakona.
[11] Članak 8. "Europske konvencija za zaštitu ljudskih prava i temeljnih sloboda, Narodne novine - Međunarodni ugovori 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10."

Računala (stolna, prijenosna, serveri)	Kućni uređaji za grijanje i hlađenje (termostati za bojler i klima uređaj)
Mobiteli (interna memorija, vanjska memorija)	Hladnjaci
Tablet uređaji (Windows, Android, iOS)	TV uređaji
GPS uređaji	Prijenosni tvrdi diskovi (HDD i SSD)
Računala u prijevoznom sredstvu (vozilo, brod, zrakoplov - crne kutije)	Čipovi za označavanje životinja
USB prijenosne memorije	Dokumenti (osobna iskaznica, zdravstvena iskaznica, putovnica)
Optički mediji (CD/DVD/BluRay)	Elektronske brave
Memorijske kartice (SD, MMC, MS…)	Beskontaktne čip kartice
Fotoaparati	SIM kartice
Kamere - kamkorderi	Internet pristupnici (ADSL router)

Tablica 3 - Potencijalni nositelji elektroničkih (digitalnih) dokaza

Kod privremenog oduzimanja elektroničkih dokaza bitno je izvršiti dobru pripremu, odnosno osiguranje mjesta događaja, dokumentiranje mjesta događaja, prikupljanje dokaza, pakiranje, prijevoz i pohranu. Riječ je o "standardnom operativnom postupku" (dalje u tekstu SOP).

Njegova uloga je ispravno usmjeriti postupanje istražitelja i na jednostavan način osigurati ujednačenost, provjerljivost i procesnu valjanost poduzetih radnji, mjera ili postupaka. SOP koji se odnosi na elektroničke (digitalne) dokaze je trenutno u fazi izrade (pod pokroviteljstvom Projekta i u suradnji s policijama EU).[12]

Metodološka razrada kaznenih djela koja se odnose na kažnjiva ponašanja u kiberprostoru bit će prikazana u jednom od sljedećih poglavlja.

U disertaciji se pojašnjavaju neki često korišteni pojmovi koji se mogu naći u pravnim rješenjima zakonodavstava raznih država, konvencijama, uredbama, direktivama, strategijama te definicijama međunarodnih organizacija.

[12] Radna skupina za izradu Standardnih operativnih postupaka za rad s elektroničkim dokazima ispred Republike Hrvatske oformljena je sredinom 2013. godine od predstavnika raznih državnih tijela (ministarstva, akademske institucije, stručnjaci) čiji je član i autor.

Kako su svi pojmovi izvedenice engleskih riječi, autor je preveo na hrvatski jezik za svrhu rada najznačajnije pojmove te dao prikaz ostalih definicija sa izvorima.

Velika baza pojmova nalazi se pojašnjena na nekoliko internet adresa, a jedna od priznatih u akademskim krugovima je i CCDCOE (NATO CCDCOE, 2017).

2.3 Konvencija o kibernetičkom kriminalu

"Konvenciju o kibernetičkom kriminalu" donijelo je Vijeće Europe. Kako navodi Ministarstvo vanjskih i europskih poslova Republike Hrvatske "Vijeće Europe najstarija je europska organizacija sa sjedištem u Strasbourgu. Obuhvaća trenutno 47 država članica (sve europske države osim Bjelorusije), a glavni joj je cilj jačanje suradnje i jedinstva na europskom kontinentu promicanjem ljudskih prava i temeljnih sloboda te demokracije i vladavine prava. Uz ova tri ključna stupa koja predstavljaju njegove temeljne vrijednosti, Vijeće Europe bavi se i nizom specifičnih društvenih tema kao što su socijalna isključenost, rasna, nacionalna i druga netrpeljivost, trgovina ljudima, nasilje nad ženama, prava djece, bioetika, terorizam, zaštita kulturne i prirodne baštine te drugi suvremeni izazovi europskih društava.

Vijeće Europe utemeljilo je 5. svibnja 1949. godine u Londonu deset europskih država, želeći učvrstiti demokraciju, vladavinu prava i zaštitu ljudskih prava na europskom kontinentu. Vijeće Europe se nametnulo kao glavni politički forum za trajni dijalog i suradnju sa zemljama istočne i srednje Europe koje su izabrale demokratski oblik upravljanja državom."[13]

Konvencija o kibernetičkom kriminalu je najopsežniji europski dokument koji se odnosi na sva kaznena djela povezana s kibernetičkom kriminalom.[14]

Konvencija je među prvim međunarodnim ugovorima o kaznenim djelima počinjenima putem interneta i računalnih mreža koji se posebno bavi kaznenim djelima povrede autorskih prava, prijevara putem računala i računalnih mreža, dječjom pornografijom na računalu ili računalnoj mreži i povredama sigurnosti računalnih mreža.

[13] Ministarstvo vanjskih i europskih poslova Republike Hrvatske http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/vijece-europe/, stranica posjećena 5. studenog 2017. http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/vijece-europe/, stranica posjećena 5. studenog 2017.

[14] Konvencija o kibernetičkom kriminalitetu Vijeća Europe, Narodne novine -Međunarodni ugovori 9/02, 4/04.

Konvencija također sadrži niz ovlasti i postupaka kao što su pretraživanja računalnih mreža i računalno presretanje podataka.

Njezin je glavni cilj, kako stoji u preambuli, nastaviti zajedničke kaznene politike usmjerene na zaštitu društva protiv kibernetičkog kriminala, posebice usvajanjem odgovarajućeg zakonodavstva i jačanjem međunarodne suradnje.[15]

Svakodnevno korištenje novih tehnologija daje mogućnost zloporabe, pa je pojam "računalni kriminal" preuzak, kako u Konvenciji, tako i u svakodnevnom govoru se javlja širi pojam "kibernetički kriminal" ili "kiberkriminal" (Jurman, 2006).

Nacrtom Konvencije iz 2000. godine predviđeno je da će zemlje potpisnice uvesti u domaće zakonodavstvo zakonska rješenja koja su nužna za progon počinitelja kaznenih djela iz domene računalnih podataka i sustava. Usvojena su i rješenja koja se odnose na procesni dio postupaka vezanog uz pretragu i pribavljanje dokaza, ovlaštenja istražitelja i obveze davatelja usluge za pristup internetu. [16]

Od zemalja članica Vijeća Europe, Konvencija je potpisana, ratificirana i stupila je na snagu kao što je vidljivo u tablici 4.[17]

Država	**Potpisano**	**Ratificirano**	**U primjeni od**
Albanija	23.11.2001.	20.6.2002.	1.7.2004.
Andora	23.4.2013.	16.11.2016.	1.3.2017.
Armenija	23.11.2001.	12.10.2006.	1.2.2007.
Austrija	23.11.2001.	13.6.2012.	1.10.2012.
Azerbajdžan	30.6.2008.	15.3.2010.	1.7.2010.
Belgija	23.11.2001.	20.8.2012.	1.12.2012.
Bosna i Hercegovina	9.2.2005.	19.5.2006.	1.9.2006.
Bugarska	23.11.2001.	7.4.2005.	1.8.2005.
Cipar	23.11.2001.	19.1.2005.	1.5.2005.
Crna Gora	7.4.2005.	3.3.2010.	1.7.2010.
Češka	9.2.2005.	22.8.2013.	1.12.2013.

[15] Relevantni podaci o konvencijama Vijeća Europe nalaze se na Internetskoj adresi: http://conventions.coe.int, stranica posjećena 7. studenog 2017.
[16] Agenda Vijeća Europe https://wcd.coe.int/ViewDoc.jsp?id=410081&Site=COE, stranica posjećena 12. studenog 2017.
[17] Stanje na dan 12.studenog.2017.

Danska	22.4.2003.	21.6.2005.	1.10.2005.
Estonija	23.11.2001.	12.5.2003.	1.7.2004.
Finska	23.11.2001.	24.5.2007.	1.9.2007.
Francuska	23.11.2001.	10.1.2006.	1.5.2006.
Grčka	23.11.2001.	25.1.2017.	1.5.2017.
Gruzija	1.4.2008.	6.6.2012.	1.10.2012.
Hrvatska	23.11.2001.	17.10.2002.	1.7.2004.
Irska	28.2.2002.		
Island	30.11.2001.	29.1.2007.	1.5.2007.
Italija	23.11.2001.	5.6.2008.	1.10.2008.
Latvija	5.5.2004.	14.2.2007.	1.6.2007.
Lihtenštajn	17.11.2008.	27.1.2016.	1.5.2016.
Litva	23.6.2003.	18.3.2004	1.7.2004.
Luksemburg	28.1.2003.	16.10.2014.	1.2.2015.
Mađarska	23.11.2001.	4.12.2003.	1.7.2004.
Makedonija	23.11.2001.	15.9.2004.	1.1.2005.
Malta	17.1.2002.	12.4.2012.	1.8.2012.
Moldova	23.11.2001.	12.5.2009.	1.9.2009.
Monako	2.5.2013.	17.3.2017.	1.7.2017.
Nizozemska	23.11.2001.	16.11.2006.	1.3.2007.
Norveška	23.11.2001.	30.6.2006.	1.10.2006.
Njemačka	23.11.2001.	9.3.2009.	1.7.2009.
Poljska	23.11.2001.	20.2.2015.	1.6.2015.
Portugal	23.11.2001.	24.3.2010.	1.7.2010.
Rumunjska	23.11.2001.	12.5.2004.	1.9.2004.
Slovačka	4.2.2005.	8.1.2008.	1.5.2008.
Slovenija	24.7.2002.	8.9.2004.	1.1.2005.
Srbija	7.4.2005.	14.4.2009.	1.8.2009.
Španjolska	23.11.2001.	3.6.2010.	1.10.2010.
Švedska	23.11.2001.		
Švicarska	23.11.2001.	21.9.2011.	1.1.2012.

Turska	10.11.2010.	29.9.2014.	1.1.2015.
Ukrajina	23.11.2001.	10.3.2006.	1.7.2006.
Velika Britanija	23.11.2001.	25.5.2011.	1.9.2011.

Tablica 4 - Konvencija o kibernetičkom kriminalu - zemlje članice Vijeća Europe

Izvor: Vijeće Europe

Konvenciju je u vrijeme izrade ovog doktorskog rada potpisalo 56 država, a ažurirani popis se nalazi na internetskoj adresi Vijeća Europe.[18]

Od zemalja koje nisu članice Vijeća Europe, Konvenciju su potpisale sljedeće zemlje navedene u tablici 5.[19]

Država	Potpisano	Ratificirano	U primjeni od
Australija		30.11.2012.	1.3.2013.
Kanada	23.11.2001.	08.07.2015.	1.11.2015.
Čile		20.04.2017.	1.8.2017.
Kostarika		22.09.2017.	1.1.2018.
Dominikanska Republika		07.02.2013.	1.6.2013.
Izrael		09.05.2016.	1.9.2016.
Japan	23.11.2001.	03.07.2012.	1.11.2012.
Mauricius		15.11.2013.	1.3.2014.
Panama		05.03.2014.	1.7.2014.
Senegal		16.12.2016.	1.4.2017.
Šri Lanka		29.05.2015.	1.9.2015.
Tonga		09.05.2017.	1.9.2017.
Sjedinjene Američke Države	23.11.2001.	29.09.2006.	1.1.2007.

Tablica 5 - Konvencija o kibernetičkom kriminalu - zemlje nečlanice Vijeća Europe

Izvor: Vijeće Europe

[18] Internetska adresa Vijeća Europe http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG stranica posjećena 2. studenog 2017.

[19] ibid.

Konvencija se sastoji od ukupno četiri poglavlja. U prvom poglavlju propisuju se kaznena djela, u drugom poglavlju odredbe koje su zemlje potpisnice dužne implementirati u svoju pravnu regulativu, treće je poglavlje koje se odnosi na mehanizme međunarodne suradnje i uzajamne pomoći i četvrto koje sadrži završne odredbe.

U prvom dijelu Konvencije definirani su određeni izrazi koji se u njoj spominju, te se tako *računalni sustav* označava kao "svaka naprava ili skupina međusobno spojenih ili povezanih naprava od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke. Izraz *računalni podaci* označava svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uključujući i program koji je u stanju prouzročiti da računalni sustav izvrši određenu funkciju, a izraz *davatelj usluga* označava svaki javni ili privatni entitet koji korisnicima svojih usluga omogućava komuniciranje uz pomoć računalnog sustava i svaki drugi entitet koji obrađuje ili pohranjuje računalne podatke za takvu komunikacijsku službu ili korisnike te službe."[20]

Kazneni zakon Republike Hrvatske definira navedene pojmove gotovo jednako kao i Konvencija, i to:

- *"Računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja."*[21]
- *"Računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu."*[22]

Iako je Republika Hrvatska u svom Kaznenom zakonu prepoznala računalni kriminalitet još 1997. godine kao kazneno djelo oštećenje i uporaba tuđih podataka, trebalo je doraditi zakonske propise zbog očiglednog napretka tehnologije, a time i ove vrste kriminala.

Vijeće Europe je, naknadno, u cilju zaštite društva objavilo i "*Dodatni protokol uz konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih uz pomoć računalnih sustava"*.

[20] Konvencija, članak 1.
[21] Članak 87., stavak 17. Kaznenog zakona
[22] Članak 87., stavak 18. Kaznenog zakona

2.3.1 Implementirana kažnjiva ponašanja

Kaznena djela koja su implementirana, a izravni utjecaj na implementaciju imaju slijedom potpisivanja i ratificiranja Konvencije, u vrijeme izrade doktorskog rada promijenjena su u dva navrata u Kaznenom zakonu Republike Hrvatske.[23]

U drugom poglavlju Konvencije sadržane se mjere koje bi zemlje potpisnice trebale poduzeti na nacionalnoj razini kako bi se odredbe mogle implementirati u kazneno materijalno i procesno (postupovno) pravo. Navedeno je devet kaznenih djela, a razvrstana su u četiri dijela. Nakon prikaza općih odredbi, Konvencija u člancima od 14. do 21. propisuje procesne odredbe koje se odnose na hitnu zaštitu pohranjenih računalnih podataka kao i podataka o prometu, podataka o pretplatničkim informacijama, pretragu i oduzimanje pohranjenih računalnih podataka, zatim prikupljanje podataka u realnom vremenu i presretanje podataka o sadržaju.

"Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava" navedenih u Konvenciji su:

- Nezakoniti pristup[24]
- Nezakonito presretanje[25]
- Ometanje podataka[26]
- Ometanje sustava[27]
- Zloporaba naprava[28]

Inkriminirana djela temeljem Konvencije koja ulaze u domenu računalnih kaznenih djela su:

- Računalno krivotvorenje [29]
- Računalna prijevara [30]

[23] "Zakon o izmjenama i dopunama Kaznenog zakona" iz 2004. i Kazneni zakon iz 2011.
[24] Konvencija, članak 2
[25] Konvencija, članak 3.
[26] Konvencija, članak 4.
[27] Konvencija, članak 5.
[28] Konvencija, članak 6.
[29] Konvencija, članak 7.
[30] Konvencija, članak 8.

2.4 Nacionalna strategija kibernetičke sigurnosti

Spoznajom o pojavljivanju nove kibernetičke dimenzije društva, kao i pojave novih ugroza za fizičke i pravne osobe te javna i državna tijela, Vlada Republike Hrvatske uvidjela je potrebu za donošenjem Nacionalne strategije kibernetičke sigurnosti[31], a sve u cilju zaštite kibernetičkog prostora. Nacionalna strategija kibernetičke sigurnosti prva je sveobuhvatna strategija zaštite kibernetičkog prostora koja je obuhvatila sve zakonske i podzakonske akte, kao i sve segmente društva nužne za provođenje sigurnosti na kibernetičkom planu.

Temeljna uloga Strategije je povezivanje svih segmenata društva radi boljeg razumijevanja kibernetičke sigurnosti, zato je nužno uspostaviti kvalitetnu koordinaciju i suradnju između tih segmenata društva, kao i svih državnih tijela, pravnih i fizičkih osoba (Standage, 1998). Radi postizanja svoje uloge potrebno je kvalitetno podijeliti nadležnosti, obaveze, zadatke i kontrolne mehanizme ostvarivanja kibernetičke sigurnosti, kao i prepoznati interese i očekivanja svih segmenata društva (Jelenski, 2017, str. 7).

Svrha strategije definirana je kao potreba provođenja aktivnosti radi podizanja sposobnosti Republike Hrvatske u zaštiti kibernetskog prostora te izgradnje sigurnog i kvalitetnog društva u kibernetičkom prostoru. Kako bi se to ostvarilo, potrebno je definirati segmente društva koji će koristi kibernetički prostor (sada i u budućnosti) i potaknuti ih da uslijed korištenja tog prostora budu svjesni njegovih opasnosti i mjera zaštite. Konačan cilj ove strategije definiran je kao provedba zakona i poštovanje ljudskih prava u novoj kibernetičkoj dimenziji društva (Lopez, 2009).

Da bi se postigao ovaj cilj, korisnici kibernetičkog prostora moraju biti svjesni svih zakona i prava osoba koja se mogu narušiti korištenjem tog prostora. To podrazumijeva nužnost obrazovanja (kako općeg, tako i specijalnog) svih segmenata društva o potencijalnim ugrozama koje se mogu pojaviti u kibernetičkom prostoru. Kako bi se ostvarila temeljna uloga, svrha i konačan cilj Strategije definirana su osnovna načela, područja kibernetičke sigurnosti i segmenti društva koji su nadležni za pojedina područja kao i specifični ciljevi koji se imaju ostvariti.

[31] Nacionalna strategija kibernetičke sigurnosti, NN 108/15.

Strategijom su definirani sektori društva nužni za ostvarivanje kibernetičke sigurnosti i opisani su oblici njihove suradnje u zajedničkom nastupu u kibernetičkom prostoru. Kao temeljni sektori društva djeluju:

- *javni sektor;*
- *akademski sektor;*
- *gospodarski sektor i*
- *građanstvo.*

Prema Strategiji u javni sektor se ubrajaju "*državna tijela, jedinice lokalne i regionalne samouprave i pravne osobe s javnim ovlastima"* koji nastupaju u kibernetičkom prostoru te su dužne štiti taj prostor u okvirima svojih ovlasti. Javni sektor predstavlja temeljnu okosnicu kibernetičke sigurnosti jer je njegova zadaća očuvati ljudska prava i osigurati razvitak društva na svim razinama.

Akademski sektor sačinjavaju obrazovne institucije koje provode obrazovanje na teritoriju Republike Hrvatske, bilo da potječu iz javnog ili gospodarskog sektora. Uključenost akademskog sektora je potrebna radi prijenosa stečenih znanja i istraživanje utjecaja novih komunikacijskih i informacijskih tehnologija na čovjekov život.

Gospodarski sektor i građanstvo predstavljaju ukupnost fizičkih i pravnih osoba koji su korisnici kibernetičkog prostora (bilo da su aktivni ili pasivni korisnici) i putem tog prostora ostvaruju svoja prava, ali im se nameću i određene obaveze.

Oblici njihove suradnje kao sudionika kibernetičke sigurnosti su:

- *"koordinacija unutar javnog sektora",*
- *"nacionalna suradnja javnog, akademskog i gospodarskog sektora",*
- *"savjetovanje sa zainteresiranom javnošću i informiranje građanstva",*
- *te "međunarodna suradnja aktera kibernetičke sigurnosti".*

Koordinacija unutar javnog sektora predstavlja zajednički nastup svih javno pravnih tijela u zaštiti kibernetičke dimenzije društva, a podrazumijeva provođenje mjera i aktivnosti nužnih za prevenciju opasnosti i otklanjanje ili umanjivanje šteta nastalih djelovanjem kibernetičkih ugroza. Suradnja akademskog, gospodarskog sektora i građanstva potrebna je radi ostvarivanja sveukupnog cilja ove strategije, odnosno očuvanja temeljnih ljudskih prava i sloboda i provođenja zakona.

Međunarodna suradnja spominje se kao faktor radi međunarodne karakteristike samog kibernetičkog prostora i njegove sigurnosti. Ugroze i rizici koji se pojavljuju u kibernetičkom prostoru imaju međunarodni karakter jer prelaze granice država, a zato je nužna suradnja uže i šire međunarodne zajednice. Kako sam kibernetički prostor ima međunarodni karakter, odnosno širi se izvan granica pojedinih država te korisnici koji djeluju u takvom prostoru djeluju izvan svojih država, potrebno je uspostaviti koordinirano djelovanje na međunarodnoj razini u zaštiti takvog prostora. Dakle, primarno je pojačati suradnju na međunarodnoj razini kao i uspostavu jedinstvenog pravnog okvira u djelovanjima na području kibernetičke sigurnosti te izgradnje povjerenja i razmjenu stečenih znanja.

U sklopu međunarodne suradnje Ministarstvo unutarnjih poslova sudjeluje u stvaranju jedinstvenog sustava zaštite kibernetičkog prostora od raznih kriminalnih ugroza, kao i koordinirano djelovanje s tijelima drugih država u sklopu progona počinitelja kaznenih djela s međunarodnim karakterom, a u slučaju Republike Hrvatske kontakt točka je Služba kibernetičke sigurnosti pozicionirana unutar Ravnateljstva policije.[32]

Temeljem procjene agencije EU - ENISA-e[33], hrvatska strategija nacionalne sigurnosti ispunila je ukupno sedam ciljeva, i to:

- *pojasnila pojam kiberkriminala,*
- *uključena je međunarodna suradnja,*
- *posjeduje mehanizme za prijavu incidenata,*
- *uključuje istraživački dio,*
- *pojašnjava protokole za odgovor na incidente,*
- *uravnotežuje sigurnost i privatnost,*
- *utemeljuje sigurnosne aspekte zaštite.*

[32] Ustroj Ministarstva unutarnjih poslova RH http://stari.mup.hr/159.aspx, stranica posjećena 16. studenog 2017.
[33] ENISA – hrvatska nacionalna strategije kibersigurnosti https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy, stranica posjećena 14.12.2017.

Opći ciljevi Nacionalne strategije kibernetičke sigurnosti predstavljaju aktivnosti koje bi se trebale poduzeti radi ostvarivanja konačnog cilja, svrhe i uloge Strategije. U ostvarivanju ovih ciljeva sudjeluju svi akteri kibernetičke sigurnosti, svaki unutar svojih nadležnosti te zajedničkim djelovanjem pridonose ostvarivanju sigurnosti u ovoj novoj dimenziji društva. Kao opće ciljeve strategije postavljeni su:

- *"sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira",*
- *"provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora",*
- *"uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima",*
- *"jačanje svijesti o sigurnosti kibernetičkog prostora",*
- *"poticanje razvoja usklađenih obrazovnih programa",*
- *"poticanje razvoja e-usluga",*
- *"poticanje istraživanja i razvoja rada akademskog, gospodarskog i javnog sektora",*
- *"sustavni pristup međunarodnoj suradnji".*

Pregledom općih ciljeva ove strategije svakako moramo izdvojiti potrebu razvoja nacionalnog zakonodavnog okvira koji mora biti u skladu s trenutnim svjetskim trendovima i obvezama Republike Hrvatske.

Jedan od važnijih ciljeva je i produbljivanje spoznaje o kibernetičkom prostoru i razvoju obrazovanja jer korisnici današnjih kibernetičkih tehnologija olako shvaćaju ovaj kompleksan problem. Ministarstvo unutarnjih poslova, kao dio državne uprave i kao nositelj i sunositelj ciljeva određenih Strategijom, sudjeluje u ostvarenju cjelokupne zaštite i razvoja Republike Hrvatske na kibernetičkom planu.

Nakon definiranja općih ciljeva Nacionalne strategije kibernetičke sigurnosti i njezinih aktera, odnosno provoditelja, potrebno je definiranje područja kibernetičke sigurnosti na kojima će ti akteri djelovati.

Područja kibernetičke sigurnosti definirana su sukladno vitalnim interesima Republike Hrvatske u trenutku izrade, što nužno znači da te interese treba revidirati periodično. Prema Strategiji definirana su tri cjeline kibersigurnosti:

- *"elektronička komunikacijska i informacijska infrastruktura i usluge",*
- *"kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama" i*
- *"kibernetički kriminal".*

Unutar svakog od ova tri područja kibernetičke sigurnosti postavljeni su specifični ciljevi koje je potrebno ostvariti da bi se ostvarili opći ciljevi ove strategije. Specifični ciljevi usmjereni su na provođenje mjera na području kibernetičke sigurnosti radi poboljšanja usluga koje se pružaju u kibernetičkom prostoru, kao i povećanja otpornosti na rizike i ugroze koji se nalaze u tom prostoru.

Elektronička komunikacijska i informacijska infrastruktura i usluge predstavljaju bitno područje kibernetičke sigurnosti u obliku adekvatnog i brzog pristupa uslugama koje se mogu ostvariti putem kibernetičkog prostora.

Ovo područje kibernetičke sigurnosti podijeljeno je u tri manja područja:

- *"javne elektroničke komunikacije",*
- *"elektronička uprava" i*
- *"elektroničke financijske usluge".*

Javne elektroničke komunikacije podrazumijevaju davanje na korištenje komunikacijskih mreža ili usluga, što podrazumijeva koncepciju, gradnju i razvoj te ustupanje na korištenje mreža i usluga krajnjem korisniku. U ovo područje uključene su i provedba zakonskih odredbi kojima se uređuje područje pružanja komunikacijskih usluga, kao i nadzor nad provođenjem tih odredbi.

Elektronička uprava predstavlja glavni cilj za brzo i sigurno pružanje usluga građanima Republike Hrvatske putem kibernetičkog prostora. Radi ostvarenja ovoga cilja potrebno je definirati odnose, prava i obaveze javnopravnih tijela prema građanima, kao i učiniti dostupnima, ali i sigurnim javne registre i službene podatke tih tijela. Ministarstvo unutarnjih poslova kao dio državne uprave ostvaruje suradnju s drugim institucijama radi poboljšavanja usluge i sigurnosti u radu elektroničke uprave.

Elektroničke financijske usluge naglo su se proširile u posljednjem desetljeću. Pružanje financijskih usluga ovakvog tipa gotovo je zamijenilo rad s gotovim novcem. Elektronička financijska usluga je puno brža, jednostavnija i transparentnija, međutim, državne institucije ju moraju učiniti sigurnom. Uspostavljanjem ovog područja nadležne državne institucije moraju povećati razinu sigurnosti i nadzora nad pružanjem financijskih usluga u kibernetičkom prostoru. Kao jedno od tijela kaznenog progona, Ministarstvo unutarnjih poslova, zaduženo je razmjenjivati podatke s financijskim institucijama radi boljeg rješavanja računalnih sigurnosnih incidenata i pronalaženja počinitelja.

Kritična komunikacijska i informacijska infrastruktura usko je povezana sa Zakonom o kritičnim infrastrukturama, a definirana je odlukom Vlade Republike Hrvatske. Radi postizanja zaštite kritične infrastrukture u kibernetičkom prostoru, potrebno je prvenstveno utvrđivanje mjera zaštite i provođenje tih mjera u stvarnost.

Osim zaštite, nužno je i osiguranje kontinuiranog rada i djelovanja uslijed bilo kakvih predvidivih i nepredvidivih okolnosti, što se postiže procjenama rizika i upravljanjem krizama. Upravljanje krizama počiva na uspostavljanju i radu sustava za upravljanje krizama koji osigurava pravodobnu i kvalitetnu reakciju.

Kao jedno od bitnijih područja kibernetičke sigurnosti, kibernetički kriminalitet također je obuhvaćen Strategijom. Kao što je ranije navedeno, kibernetički kriminalitet predstavlja ukupnost kaznenih djela koje imaju za cilj kibernetičke sustave, podatke ili programe koji se nalaze na takvim sustavima kao i ona kaznena djela koja se čine posredstvom takvih sustava. Zato se, radi ostvarivanja cilja sigurnog informacijskog društva te poštivanja zakona i ljudskih prava, treba uspostaviti niz preventivnih mjera koje će reducirati ovakvu vrstu kriminaliteta, ali i odgovore na eventualne ugroze ovakvoga tipa. MUP, u suradnji s drugim institucijama, ima središnju ulogu u provedbi mjera i ciljeva na ovom području kibernetičke sigurnosti.

U tom pogledu potrebno je razvijati zakonodavni okvir na području kibernetičkog kriminaliteta, pojačati suradnju na nacionalnoj i međunarodnoj razini, pojačati edukacije policijskih službenika i kriminalističkih istražitelja na području elektroničkih dokaza i kibernetičkog kriminaliteta i razvijati kvalitetnu suradnju s gospodarskim sektorom.

Poveznice područja kibernetičke sigurnosti predstavljaju dijelove kibernetičke sigurnosti koji su zajednički većini područja, odnosno aktera kibernetičke sigurnosti. Poveznice su bitne da bi se obuhvatio cjelokupni problem kibernetičke sigurnosti. Kao i područja, poveznice su definirane sukladno trenutnim interesima Republike Hrvatske te ih je potrebno revidirati u nadolazećim godinama.

Za ostvarivanje kibernetičke sigurnosti postavljeni su specifični ciljevi za svaku od sljedećih poveznica:

- *"zaštita podataka",*
- *"tehnička koordinacija u obradi računalnih sigurnosnih incidenata",*
- *"međunarodna suradnja" i*
- *"obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru".*

Zaštitu podataka je nužno spomenuti jer predstavlja značajan problem, osobito kod pravnih osoba, a posebno iz motrišta "Opće uredbe o zaštiti osobnih podataka" (2016) (General Data Protection Regulation - dalje u tekstu GDPR).

Potrebno je steći tzv. sigurnosnu kulturu kada se radi s klasificiranim podacima. Sigurnost podatka u kibernetičkom prostoru poseban je problem jer postoji mnogo ugroza u odnosu na to koji podatak može biti objavljen, izmijenjen, ukraden, izbrisan ili "otet". Zato je nužno specificirati vrste zaštićenih podataka: poput državne tajne, vojne tajne, poslovne tajne i privatne tajne.

Osobe koje rade s podacima moraju biti svjesne o kakvoj vrsti podatka se radi, koje mjere sigurnosti se imaju poduzeti pri radu s takvim podacima i koje prijetnje predstavljaju rizik za taj podatak. Zaštita podataka se sastoji u očuvanju povjerljivosti, dostupnosti i cjelovitosti za vlasnika podatka, odnosno njegovog korisnika.

Kako navodi internetski portal GDPR2018 "Zaštita osobnih podataka jedan je od osnovnih zadataka koje GDPR stavlja pred organizacije bilo da je riječ o osobnim podacima korisnika, klijenata ili zaposlenika.

Organizacije u svakom trenutku moraju znati gdje su koji podaci te u koju svrhu se smiju koristiti. Isto tako, u slučaju da netko odluči povući privolu za korištenje njegovih osobnih podataka, organizacije moraju biti u mogućnosti učiniti to u zadanom roku. Ime, adresa, e-mail adresa, IP i MAC adresa, GPS lokacija, RFID tagova i kolačića na web stranicama, telefonski broj, fotografija, videosnimke pojedinaca, OIB, biometrijski podaci (otisak prsta, snimka šarenice oka), genetski podaci, podaci o obrazovanju i stručnoj spremi, podaci o plaći, podaci o kreditnom zaduženju, podaci o računima u banci, podaci o zdravlju, seksualnoj orijentaciji, glas i mnogi drugi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Dakle svaka tvrtka u Europskoj uniji koja prikuplja neke od navedenih podataka je podložna ovoj Uredbi, te će se od slučaja do slučaja određivati predstavlja li podatak koji prikuplja osobni podatak pojedinca. Sve strane tvrtke koje obrađuju podatke građana EU također podliježu ovoj Uredbi." [34]

"Zakon o pravu na pristup informacijama"[35] donio je Hrvatski sabor na sjednici 15. veljače 2013. godine. U zakonu stoji da je "cilj zakona omogućiti i osigurati ostvarivanje Ustavom Republike Hrvatske zajamčenog prava na pristup informacijama, kao i na ponovnu uporabu informacija fizičkim osobama, ali i pravnim". Njime su uređene obveze tijela javne vlasti i prekršajne odredbe kojima se uvjetuje odgovornost pravnih i fizičkih osoba.

Tehnička koordinacija raznih CERT-ova (eng. *Computer Emergency Response Team*) pri obradi računalnih sigurnosnih incidenata predstavlja nužan uvjet sagledavanja stanja kibernetičke sigurnosti, kako na sektoru pojedinih CERT-ova zaduženih za rješavanje sigurnosnih incidenata, tako i na nacionalnoj razini. Pod koordinacijom se smatra kvalitetna suradnja, razmjena podataka, primjena načela supsidijarnosti i objedinjavanje statističkih pokazatelja rizika na razini kibernetičkog prostora.

Djelovanje MUP-a započinje kada računalni sigurnosni incidenti nastaju kao posljedica nezakonitog i zlonamjernog djelovanja pojedinaca. Ministarstvo ostvaruje suradnju s Hrvatskim nacionalnim CERT-om radi razmjene podataka o novim pojavnim oblicima kibernetičkog kriminaliteta, kao i novim načinima korištenja informacijske i komunikacijske tehnologije za činjenje kaznenih djela koja nisu iz domene kibernetičkog kriminaliteta. S druge strane, Nacionalni CERT dobiva svježe informacije od Ministarstva o trenutnim promjenama zakonodavnog okvira kojim se uređuje kibernetičko-sigurnosno područje.

[34] GDPR2018 Portal https://gdpr2018.eu/sto-je-gdpr/, stranica posjećena 31. listopada 2017.
[35] Zakon o pravu na pristup informacijama, NN 172/2003

Provođenje obrazovanja, istraživanja i razvoja potrebno je za opstanak društva u svakom području njegovog djelovanju, što vrijedi i za kibernetičko područje. Podizanjem svijesti svih građana o sigurnosti u kibernetičkom prostoru predstavlja zahtjevan zadatak za sva tijela akademskog i javnog sektora, posebno zato što naše društvo nema razvijenu sigurnosnu kulturu, a informatička pismenost predstavlja problem srednje i starije populacije.

Prema Strategiji "ciljane skupine na koje je potrebno usmjeriti obrazovne aktivnosti su sljedeće: sudionici formalnog obrazovanja, građani raznih profila, voditelji, primatelji, te izvršitelji obrade podataka, kao i osobe koje dolaze u kontakt s kritičnim infrastrukturama i osjetljivim bazama podataka te stručnjaci koji će se baviti informatičkom sigurnošću". Ministarstvo unutarnjih poslova, zaduženo za obrazovanje policijskih službenika, mora raditi u smjeru pojačanja tečajeva informatičke struke, posebice u polju kibernetičke sigurnosti, elektroničkih dokaza i računalne forenzike.

Ministarstvo unutarnjih poslova mora konstantno podizati svijest građana o sigurnosti u kibernetičkom prostoru, pojavi novih opasnosti i zaštiti na kibernetičkom planu.

2.5 Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti

"Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti" (dalje u tekstu Akcijski plan) predstavlja provedbeni dokument kojim se ostvaruju ciljevi koji su zadani Strategijom. On uključuje provedbene mjere, njihove aktere, odnosno javno-pravna tijela koja ih provode i kontrolne mehanizme koji uključuju i nadzor nad provođenjem mjera. Mjere koje se imaju provesti radi ostvarenja ciljeva zadanih Strategijom raspoređeni su prema područjima kibernetičke sigurnosti, kao i prema njihovim poveznicama.

Uz definiranje nositelja i sunositelja ovih mjera, odnosno državnih i drugih javnih tijela koji su dužni postupati prema Strategiji i Akcijskom planu, uspostavljeno je dodatno tijelo, Nacionalno vijeće za kibernetičku sigurnost, koje će provoditi nadzor nad provedbom Strategije i Akcijskog plana.

Nositelji i sunositelji dužni su podnositi izvješća Vijeću o mogućnostima provođenja, tijeku i ostvarenju pojedinih mjera i ciljeva kako bi se oni u budućnosti mogli revidirati. Zadaće Nacionalnog vijeća za kibernetičku sigurnost su sljedeće:

- *"sustavno praćenje i koordiniranje provedbe Strategije te raspravljanje o svim pitanjima vezanih za kibernetičku sigurnost",*
- *"predlaganje mjera za unaprjeđenje provođenja Strategije i Akcijskog plana za provedbu Strategije",*
- *"predlaganje organiziranja nacionalnih vježbi iz područja kibernetičke sigurnosti",*
- *"izrađivanje preporuka, mišljenja, izvješća i smjernica u vezi s provedbom Strategije i Akcijskog plana",*
- *"predlaganje izmjena i dopuna Strategije i Akcijskog plana odnosno donošenje nove Strategije i Akcijskog plana u skladu s potrebama".*

Osim ovih stalnih zadaća Vijeća, definirane su zadaće prilikom pojave djelovanja kibernetičkih ugroza i rizika, odnosno pojave kibernetičkih kriza. Te zadaće su sljedeće:

- *"razmatranje pitanja bitnih za upravljanje kibernetičkim krizama i predlaganje mjera za veću učinkovitost",*
- *"razmatranje stanja sigurnosti u kibernetičkom prostoru te izvješća o stanju sigurnosti koje mu dostavlja Operativno-tehnička koordinacija za kibernetičku sigurnost",*
- *"izrada periodičnih procjena o stanju sigurnosti",*
- *"utvrđivanje planova postupanja u kibernetičkim krizama",*
- *"izrada planova i programa aktivnosti Operativno-tehničke koordinacije za kibernetičku sigurnost te usmjeravanje njezinog rada".*

Kao podrška Nacionalnom vijeću za kibernetičku sigurnost, bilo je nužno osnovati i tijelo koje će stalno pratiti stanje kibernetičke sigurnosti i osigurati opću koordinaciju između tijela zaduženih za kibernetičku sigurnost u slučaju pojave kibernetičke krize. To tijelo je Operativno-tehnička koordinacija za kibernetičku sigurnost, a njezine zadaće su:

- *"praćenje stanja sigurnosti u nacionalnom kibernetičkom prostoru",*
- *"izrada izvješća o stanju kibernetičke sigurnosti",*
- *"predlaganje planova postupanja u kibernetičkim krizama",*
- *"obavljanje drugih poslova koji su utvrđeni programom i planom aktivnosti".*

Prema Akcijskom planu Ministarstvo unutarnjih poslova djeluje na više područja i poveznica kibernetičke sigurnosti, a ta područja su:

- *"elektronička uprava",*
- *"elektroničke financijske usluge",*
- *"kibernetički kriminalitet",*
- *"tehnička koordinacija u obradi računalnih sigurnosnih incidenata",*
- *"međunarodna suradnja",*
- *"obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru".*

Razvojem i implementacijom elektroničke uprave (e-uprave) u kibernetički prostor, odnosno pružanjem usluga javnih tijela putem informacijskih i komunikacijskih tehnologija, pojavila se potreba za uvođenjem sustava za identifikaciju korisnika takvih usluga kao i potreba za podizanjem razine sigurnosti. U tu svrhu izrađen je Nacionalni identifikacijski i autentifikacijski sustav (NIAS).[36]

Donošenjem Nacionalne strategije kibernetičke sigurnosti utvrđen je strateški cilj koji nalaže "donošenja kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica". U okviru tog cilja bilo je potrebno provesti mjere analize postojećih razina sigurnosti i uvesti jedinstvene kriterije kod korištenja pojedinih razina autentifikacije za pristup uslugama elektroničke uprave.

Ministarstvo unutarnjih poslova kao jedan od pružatelja usluga elektroničke uprave, provelo je nužnu analizu te usuglasilo postupanje s ostalim javnim tijelima koja pružaju usluge elektroničke uprave. Ministarstvo je provelo analizu mogućnosti korištenja elektroničke osobne iskaznice kao najviše razine autentifikacije prilikom pristupa uslugama e-uprave, što je kasnije i implementirano u NIAS. Elektronička osobna iskaznica (eOI) omogućuje, pored fizičke identifikacije (uvidom u osobnu iskaznicu), identifikaciju u kibernetičkom prostoru za potrebe korištenja javnih, financijskih i drugih usluga u kibernetičkom prostoru.

[36] Ministarstvo Uprave , https://uprava.gov.hr/postanite-e-gradjani/867 stranica posjećena 12. prosinca 2017.

Elektronička iskaznica koristi PKI (eng. *Public Key Infrastructure*) certifikat u svrhu identifikacije korisnika prilikom pristupa raznim e-uslugama i predstavlja najvišu razinu sigurnosti u kibernetičkom prostoru.

Temeljem provedbe mjera na području elektroničkih financijskih usluga, Ministarstvo unutarnjih poslova, kao jedno od tijela kaznenog progona, sudjeluje u provedbi strateškog cilja razmjene podataka o nastalim računalnim sigurnosnim incidentima na razini financijskih institucija. Mjerama je nužno osigurati uvjete razmjene podataka radi poboljšanja zaštite i sprječavanja budućih računalnih sigurnosnih incidenata, kao i boljeg rješavanja trenutnih prijetnji. Stoga je potrebno je procijeniti zakonske mogućnosti razmjene podataka vezanih uz informacijske sustave bankarskih institucija s Ministarstvom.

Područje kibernetičke sigurnosti pripada domeni Ministarstva unutarnjih poslova i predstavlja jednu od najopasnijih i najbrže rastućih ugroza kibernetičke sigurnosti. Iz tog razloga Strategija je definirala više ciljeva u svrhu borbe protiv kibernetičkog kriminaliteta: "kontinuirano unaprjeđenje nacionalnog zakonodavnog okvira, imajući u vidu međunarodne obaveze, unaprjeđenje i poticanje međunarodne suradnje u svrhu učinkovite razmjene podataka, kvalitetna međuinstitucionalna suradnja u svrhu učinkovite razmjene informacija na nacionalnoj razini, posebno u slučaju računalnog incidenta, jačanje ljudskih potencijala, adekvatan razvoj kompetencija i tehničkih mogućnosti nadležnih tijela za otkrivanje, kriminalističko istraživanje i procesuiranje kaznenih djela iz domene računalnog kriminaliteta, osiguranje potrebnih financijskih sredstava te poticanje i stalan razvoj suradnje s gospodarskim sektorom".

Ubrzanim razvojem informacijskih i komunikacijskih tehnologija, konstantno se pojavljuju novi oblici kibernetičkog kriminaliteta, koji se po svojem načinu počinjenja razlikuju od dosadašnjih pojavnih oblika. Kako bi se mogao držati korak s kibernetičkim kriminalitetom, nužno je konstantno provoditi analizu i prilagodbu postojećih zakona i podzakonskih akata. Također, kako ne bi dolazilo do razilaženja u nadležnosti, potrebno je uskladiti zakone s međunarodnim obavezama preuzetim iz međunarodnih ugovora i konvencija.

Uzimajući u obzir međunarodni aspekt kibernetičkog kriminaliteta i činjenicu da on ne uvažava državne granice i normativne razlike među državama, potrebna je kvalitetna međunarodna suradnja na području kibernetičke sigurnosti radi identifikacije novih oblika kibernetičkog kriminaliteta i što brže reakcije na takve ugroze.

U tom smislu Ministarstvo unutarnjih poslova, kao nositelj ovih mjera, kontinuirano uspostavlja komunikacijske kanale i razmjenu podataka s nadležnim tijelima drugih država. Suradnja unutar Europske unije moguća je preko kanala Eurojusta i Europola, a izvan Europske unije preko kanala Interpola.

Kako je potrebna međunarodna suradnja između država na međunarodnoj razini, tako je nužna i suradnja između tijela zaduženih za prevenciju i rješavanje kibernetičkih sigurnosnih incidenata na nacionalnoj razini. U tu svrhu uspostavljen je kontakt između Ministarstva unutarnjih poslova, Zavoda za sigurnost informatičkih sustava, Nacionalnog CERT-a, Sigurnosno obavještajne agencije i Državnog odvjetništva Republike Hrvatske. Koordinacija i suradnja između ovih tijela kaznenog progona ključna je radi postizanja učinkovitog kaznenog progona počinitelja kaznenih djela iz domene kibernetičkog kriminaliteta.

Pretpostavka kvalitetne borbe protiv kibernetičkog kriminaliteta jest postojanje adekvatnih tehnoloških mogućnosti, metodologija rada i ljudskih potencijala koji će iskoristiti mogućnosti koje se stavljaju njima na raspolaganje. U tu svrhu Ministarstvo unutarnjih poslova kontinuirano prati i analizira nove pojavne oblike kibernetičkog kriminaliteta i predlaže, uz sunositelje ove mjere ("Operativno-tehnički centar za nadzor telekomunikacija" i "Sigurnosno-obavještajna agencija") promjene u zakonskoj regulativi posebnih dokaznih radnji i prikrivenih policijskih radnji. Nužno je navesti da u sklopu borbe protiv kibernetičkog kriminaliteta imaju veliki potencijal u vidu elektroničkih dokaza.

Kako se razvoj i primjena novih tehnologija događa prvenstveno u gospodarskom sektoru i tek se kasnije te tehnologije implementiraju u javni sektor, nužno je uspostaviti kvalitetan komunikacijski kanal i suradnju radi stjecanja uvida u vrstu i primjenu tih tehnologija.

S druge strane, potrebno je redovito obavještavati gospodarski sektor o novim pojavnim oblicima kibernetičkog kriminaliteta s ciljem samozaštite i prevencije tih kriminalnih pojava.

Kako se niz računalnih sigurnosnih incidenata može povezati sa zlonamjernim radnjama čovjeka, odnosno s kibernetičkim kriminalitetom, Nacionalna strategija kibernetičke sigurnosti predvidjela je potrebu suradnje i razmjene podataka Ministarstva unutarnjih poslova kao tijela kaznenog progona i tijela zaduženih za zaštitu računalnih sustava poput Zavoda za zaštitu računalnih sustava i Nacionalnog CERT-a kao i Ureda vijeća za nacionalnu sigurnost kao krovne provedbene organizacije po pitanju nacionalne sigurnosti.

Prilikom kriminalističkog istraživanja kibernetičkog kriminaliteta dobivaju se uvidi u nove tehnologije i modalitete počinjenja kaznenih djela. Ta znanja uvelike pridonose ukupnoj kibernetičkoj sigurnosti, ali i prevenciji ponovnog činjenja kaznenih djela na isti način ili istom tehnologijom.

Kao poveznica područja kibernetičke sigurnosti međunarodna suradnja nužna je za uspostavu kvalitetnog odgovora na rastuće prijetnje koje se pojavljuju u kibernetičkom prostoru. Kao jedan od nositelja ciljeva, Ministarstvo unutarnjih poslova, zaduženo je za "jačanje pravnog okvira, s naglaskom na provedbu i unaprjeđenje Konvencije Vijeća Europe o kibernetičkom kriminalitetu".

Time bi se uskladilo djelovanje Ministarstva s nadležnim tijelima drugih država, radi uspostave kvalitetnih odnosa, razmjene podataka i radi boljeg kaznenog progona, odnosno kažnjavanja počinitelja kaznenih dijela iz domene kibernetičkog kriminaliteta. Bitno je organiziranje i sudjelovanje u civilnim i vojnim vježbama za razvoj i razmjenu znanja o postignućima na području kibernetičke sigurnost. Sa strane Ministarstva unutarnjih poslova to podrazumijeva uvide u nove načine istraživanja kibernetičkog kriminaliteta i sprječavanje njegovog nastanka.

Kao što je već navedeno, obrazovanje, istraživanje i razvoj predstavlja jednu od bitnijih područja kibernetičke sigurnosti jer se njime postiže razvoj ljudskih potencijala i tehnologija potrebnih za postizanje stanja zaštićenosti pred raznim ugrozama koje se nalaze u kibernetičkom prostoru. Ciljevi koje je definirala Nacionalna strategija kibernetičke sigurnosti u ovoj poveznici jesu: "razvoj ljudskih potencijala u području sigurnosti komunikacijsko-informacijskih tehnologija, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru i razvoj nacionalnih sposobnosti, istraživanje i poticanje gospodarstva".

Uloga Ministarstva unutarnjih poslova kao nositelja mjera u ostvarivanju ovih ciljeva očituje se u informiranju javnosti u slučaju nastanka kibernetičkih incidenata koji imaju tendenciju prerastanja u kibernetičke krize, s mogućnošću pogađanja velikog broja korisnika kibernetičkog prostora. Ta informiranja moraju biti pravodobna, točna i kvalitetna da bi se korisnici kibernetičkog prostora, odnosno građani, mogli zaštiti ili u slučaju zahvaćanja smanjiti gubitke uzrokovane tim incidentima.

Ministarstvo mora provesti edukacije policijskih službenika i drugih djelatnika Ministarstva s ciljem usavršavanja ljudskih potencijala u području kibernetičkog kriminaliteta. U sklopu ove mjere veliku ulogu ima Policijska akademija.

2.5.1 Uloga Policijske akademije

Policijska akademija je ustrojstvena jedinica zadužena za provođenje temeljnog, stručnog i specijaliziranog visokoškolskog obrazovanja u području sigurnosti i borbe protiv kriminaliteta.[37] Također sudjeluje u razvoju i usavršavanju metodologije rada u policijskoj i sigurnosnoj struci te postavljanju i ostvarenju strateških ciljeva Ministarstva zajedno s drugim ustrojstvenim jedinicama.

Školovanje se, osim internih tečajeva Ministarstva unutarnjih poslova po liniji rada za policijske službenike, provodi kroz suradnju sa sljedećim međunarodnim policijskim i akademskim organizacijama:

- CEPOL[38] - (fr. "*College Européen de Police"*) "Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva", koja razvija, provodi i organizira osposobljavanje policijskih i drugih službenika odgovornih za izvršavanje zakonodavstva;

- INTERPOL[39] - (eng. "*International police"*) omogućuje policiji u 190 zemalja članica zajednički rad u borbi protiv međunarodnog kriminala;

- EUROPOL[40] - (eng. "*European Police Office"*) je služba podrške agencijama za provedbu zakona zemalja članica EU koja organizira godišnje tečajeve koje nudi EC3 (eng. "*European Cybercrime Centre"*) u području cyber kriminala;

- FBI[41]- (eng. "*Federal Bureau of Investigation"*) Federalna organizacija SAD-a usmjerena na obavještajnu službu i rješavanje obavještajnih prijetnji stranih zemalja;

- OLAF[42] - (fr. "*Office européen de lutte antifraude - European Anti-Fraud Office"*) istražuje prijevare, korupcije i ostala nezakonita ponašanja unutar europskih institucija;

[37] "Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova", NN 70/2012
[38] CEPOL https://www.cepol.europa.eu/ , stranica posjećena 12. prosinca 2017.
[39] Interpol https://www.interpol.int/ , stranica posjećena 12. prosinca 2017.
[40] Europolhttps://www.europol.europa.eu/ , stranica posjećena 12. prosinca 2017.
[41] Federal Bureau of Investigation https://www.fbi.gov/ , (stranica posjećena 12. prosinca 2017.
[42] European Anti-Fraud Office https://ec.europa.eu/anti-fraud//home_en , stranica posjećena 12. prosinca 2017.

- UCD Dublin[43]- (eng. "*University College Dublin"*) jedno od vodećih europskih istraživačkih sveučilišta koje ostvaruje suradnju s agencijama za provođenje zakona preko Europola. Posebno se ističe njihov centar za kibersigurnost i kiber istrage - UCD Centre for Cybersecurity & Cybercrime Investigation;

- ENISA[44] - (eng. *"European Network and Information Security Agency"*) "Agencija Europske unije koja se bavi pitanjima sigurnosti informacija i informacijskih mreža".

2.6 Ured Vijeća za nacionalnu sigurnost

"Ured Vijeća za nacionalnu sigurnost"[45] (dalje u tekstu Ured) središnje je državno tijelo za informacijsku sigurnost. Prema informacijama na službenim web stranicama "Ured usklađuje donošenje te nadzire primjenu mjera i standarda informacijske sigurnosti u okviru područja sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava i sigurnosti poslovne suradnje. Također, izdaje certifikate fizičkim i pravnim osobama za pristup klasificiranim podacima od nacionalne do razine North Atlantic Treaty Organization[46] (u daljnjem tekstu NATO) i Europske unije".

Dalje se navodi da je "u Uredu ustrojen Središnji registar, nadležan za prijam i distribuciju međunarodnih klasificiranih podataka te koordinaciju rada Sustava registara državnih tijela Republike Hrvatske koja primaju međunarodne klasificirane podatke. Ured ostvaruje i koordinira međunarodnu suradnju u području informacijske sigurnosti te odlukom Vlade u ime Republike Hrvatske zaključuje međunarodne sigurnosne ugovore za zaštitu klasificiranih podataka".

[43] University College Dublin http://www.ucd.ie/ stranica posjećena 12. prosinca 2017.
[44] European Network and Information Security Agency https://www.enisa.europa.eu/, stranica posjećena 12. prosinca 2017.
[45] Ured Vijeća za nacionalnu sigurnost http://www.uvns.hr/hr, stranica posjećena 12. prosinca 2017.
[46] North Atlantic Treaty Organization http://www.nato.int/, stranica posjećena 12. prosinca 2017.

2.7 Zavod za sigurnost informacijskih sustava

"Zavod za sigurnost informacijskih sustava" državno je tijelo koje obavlja djelatnosti u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske. Zavod provodi poslove vezane uz sigurnost informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava i upravljanje kripto-materijalima. Djelokrug i zadaće "Zavoda za sigurnost informacijskih sustava" utvrđeni su "Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske"[47], "Zakonom o informacijskoj sigurnosti"[48] te "Uredbom Vlade Republike Hrvatske o mjerama informacijske sigurnosti"[49].

2.8 Strategija nacionalne sigurnosti Republike Hrvatske

"Strategija nacionalne sigurnosti Republike Hrvatske" stupila je na snagu 26. srpnja 2017. godine. Strategijom je razvijen plan sigurnosne politike i sposobnosti djelovanja državnih tijela i građana. U strategiji se navodi da se "Navedenim konceptom sigurnosti jamči bolja koordinacija, strateško planiranje, udruživanje resursa te ujednačeni razvoj sposobnosti s ciljem razvoja sigurnosnih politika što znači da uključuje smjernice, planove i mjere koji će na nacionalnoj razini građanima jamčiti visoku razinu sigurnosti i zaštitu nacionalnih interesa, u suradnji sa saveznicima i partnerima". Strategija nacionalne sigurnosti Republike Hrvatske usko povezuje dijelove s Nacionalnom strategijom kibernetičke sigurnosti, pa iz tog razloga nećemo posebno elaborirati sadržaj.

[47] "Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske" (NN 79/06, 105/06).
[48] "Zakon o informacijskoj sigurnosti" (NN 79/07).
[49] "Uredba o mjerama informacijske sigurnosti" (NN 46/2008).

3. MEĐUNARODNA SURADNJA I KIBERNETIČKI KRIMINAL

Razvoj informacijsko-komunikacijske tehnologije (engl. ICT), uz svoje dobrobiti, nažalost ima za posljedicu i brojne zloporabe kibernetičkog prostora (Cyberspace). Globalni karakter kibernetičkog prostora specifičan je zbog nacionalnih zakonodavstava, te njihovom pogledu na specifičnosti. Neke europske i svjetske zemlje su usvojile preporuke "Konvencije o kibernetičkom kriminalitetu Vijeća Europe (NN-MU 9/02, 4/04)" i uskladile svoja nacionalna zakonodavstva, dok su druge ostale pri kaznenopravnim rješenjima koja ne idu u korak s vremenom i dosegom ove vrste kaznenih djela (Cybercrime) (Loader, 1998). Slijedom navedenog, države su potaknute i neizostavno upućene na međusobnu suradnju i razmjenu informacija o raznolikim modalitetima ovoga kriminala jer je činjenica da počinitelj može biti bilo gdje, a samo djelo može biti počinjeno na velikoj udaljenosti od samog počinitelja. Razne međunarodne aktivnosti (diplomatske, ekonomske i sl.) su prepoznate i uređene kao nacionalne pravne norme jer u stvarnosti postoje formalne granice i nadležnosti, dok je kibernetički prostor difuzan i tih granica nema. Tehnološka podjela po internetskim domenama prividno pokazuje matičnu državu kontakta, ali sa sigurnosnog aspekta ova činjenica upućuje na brojne mogućnosti zloporabe kibernetičkog prostora. (Fialkova i Yelenevskaya, 2005)

Vlada Republike Hrvatske u rujnu 2015. godine, donosi "Nacionalnu strategiju kibernetičke sigurnosti" i "Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti", prvu sveobuhvatnu strategiju u Republici Hrvatskoj u području kibernetičke sigurnosti. Kako tehnološki naprednije zemlje imaju veću stopu kaznenih djela računalnog kriminaliteta, napravit će se i poredbeni prikaz i analiza postojećih zakonodavnih rješenja više zemalja s ciljem uočavanja prednosti i nedostataka pozitivne kaznenopravne regulative u ovom području.

3.1 Međunarodna suradnja u suzbijanju kriminaliteta u kibernetičkom prostoru

Globalni karakter računalnog kriminaliteta specifičan je zbog nacionalnih zakonodavstava. Neke zemlje su usvojile preporuke Konvencije i tome prilagodile svoja nacionalna zakonodavstva, dok su druge ostale pri kaznenopravnim rješenjima koja nisu u korak s vremenom i važnosti ovih vrsta kaznenih djela (Manjikian, 2010).

Slijedom navedenog, države su potaknute na međusobnu suradnju i razmjenu informacija o predmetnom katalogu kaznenih djela jer je činjenica da počinitelj može biti bilo gdje, a samo djelo može biti počinjeno na velikoj udaljenosti od počinitelja (NATO CCDCOE, 2017).

Međunarodna suradnja je na taj način postala nužnost i njene odgovore možemo vidjeti kroz niz specijalističkih, regionalnih, višenacionalnih i globalnih organizacija (Škrtić, 2011, str. 8).

3.1.1 Ujedinjeni narodi

Kako navodi službena web stranica Ministarstva vanjskih i europskih poslova "Ujedinjeni narodi su međunarodna organizacija čiji su članovi suverene države. Ona je gotovo univerzalna po članstvu, nadležnostima i globalnim ciljevima. Okrenuta je, u prvom redu, očuvanju međunarodnog mira i sigurnosti, razvoju prijateljskih odnosa među državama, promicanju međunarodne suradnje na rješavanju problema ekonomskog, socijalnog, kulturnog i humanitarnog karaktera, uključujući zaštitu ljudskih prava i osnovnih sloboda. U tu svrhu stvorena je široka mreža međunarodnih organizacija koje imaju status specijaliziranih agencija Ujedinjenih naroda (dalje u tekstu UN) ili se uklapaju u sustav UN-a. Sjedište Tajništva UN-a je u New Yorku, dok su pojedini dijelovi ove Organizacije locirani po cijelom svijetu npr. u Ženevi, Beču, Rimu, Nairobiju, Haagu, Ateni, Tokyju i Kopenhagenu. Danas UN ima 193 države članice. Na temelju Odluke Opće skupštine Ujedinjenih naroda od 22. svibnja 1992. Republika Hrvatska je postala članicom Ujedinjenih naroda, te na temelju pristupa i stranka Povelje Ujedinjenih naroda te Statuta Međunarodnog suda."[50]

[50] Republika Hrvatska, Ministarstvo vanjskih i europskih poslova, http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/ujedinjeni-narodi/o-un/, stranica posjećena 12. prosinca 2017.

Analiza grupe eksperata navodi da je "Republika Hrvatska u potpunosti posvećena borbi protiv prekograničnog organiziranog kriminala, a osobito protiv trgovanja ljudima, drogom i oružjem, te pranja novca i kiberkriminala. U ovom kontekstu, Hrvatska ključnim drži jačanje međunarodne suradnje na temelju učinkovite provedbe relevantnih međunarodnih i regionalnih ugovora iz tog područja, a osobito Palermo Konvencije o borbi protiv prekograničnog organiziranog kriminala s pripadajućim Protokolima" (Group of Governmental Experts, 2016).

3.1.2 Interpol

Među, svakako, najaktivnijim organizacijama je Interpol, koji trenutno obuhvaća 190 država članica. Unutar svog djelovanja poduzima aktivnosti na području računalne sigurnosti i prevencije računalnog kriminaliteta, kao i edukaciju policijskih istražitelja iz zemalja članica.

Kako navodi službena web stranica Ministarstva unutarnjih poslova "Interpol je druga najveća međunarodna organizacija u svijetu, nakon Ujedinjenih naroda. Financirana je godišnjim prilozima država članica, od kojih godišnje prima oko 40 milijuna € (manje nego Europol, koji prima oko 60 milijuna €). Sjedište organizacije je u Lyonu, Francuska."

Unutar hrvatskog "Ministarstva unutarnjih poslova, Ravnateljstva policije, Uprave kriminalističke policije" ustrojena je i služba Interpol, koja je referentna točka za Republiku Hrvatsku.

3.1.3 Europol

Kako navodi službena web stranica Ministarstva unutarnjih poslova Europol, odnosno Europski policijski ured "osnovan je 1992. godine kako bi se bavio europskim protukriminalnim obavještajnim djelatnostima. Smješten je u Haagu, Nizozemska, a njegovo osoblje uključuje predstavnike agencija za provedbu zakona (policija, carina, imigracijske službe itd.)."[51]

"Cilj je Europola pomoći državama članicama Unije da uže i učinkovitije surađuju u sprečavanju i borbi protiv organiziranoga međunarodnoga kriminala, osobito protiv:

1. krijumčarenja droga,
2. imigracijskih mreža,
3. krijumčarenja ukradenim vozilima,
4. trgovine ljudima, uključujući dječju pornografiju,
5. krivotvorenja novca i drugih sredstava plaćanja,
6. krijumčarenja radioaktivnim i drugim nuklearnim tvarima i
7. terorizma."

Europol podupire države članice putem:

1. "olakšavanja razmjene informacija između Europola i časnika za vezu Europola (ELO). Djelatnici za vezu pridruženi su Europolu od strane država članica Unije kao predstavnici njihovih nacionalnih agencija za provedbu zakona te tako nisu pod izravnom upravom Europola i njegovoga direktora. Oni djeluju u skladu sa svojim nacionalnim zakonodavstvom",

2. "pružanja operativne analize i podupiranja operacija država članica",

3. "pružanja stručnosti i tehničke potpore za istrage i operacije koje se provode u okviru Unije, pod nadzorom i pravnom odgovornošću država članica",

4. "stvaranjem strateških izvješća (npr. procjena rizika) i kriminalističkih analiza na temelju informacija dobivenih od država članica ili prikupljenih iz drugih izvora".

[51] Europska unija, http://delhrv.ec.europa.eu/?lang=hr&content=964, stranica posjećena 12. prosinca 2017.

Unutarnjim ustrojem Ministarstva unutarnjih poslova Republike Hrvatske, pozicionirana je kontakt točka Europola za Republiku Hrvatsku unutar Ravnateljstva policije.

3.1.4 Europski centar za kibernetički kriminal - EC3

Europol je u svom dokumentu o internetom potpomognutom organiziranom kriminalu identificirao da je Europska unija, zbog svoje mrežne infrastrukture i oslanjanja nacija na online usluge, ključna meta kibernetičkog kriminala.

U travnju 2010. godine Vijeće Europske unije dogovorilo je strategiju i akcijski plan vezan za borbu protiv kibernetičkog kriminala, a jedan od bitnijih zaključaka odnosio se na potrebu za stvaranjem posebnog centra koji će se pozicionirati kao vodeća struktura u ovoj borbi. Nakon ekstenzivnog konzultiranja i jednogodišnjih priprema, početkom siječnja 2012. godine otvoren je *European Cybercrime Centre* (EC3) (Kučan, 2014).

Kako je Europol dosad vodio glavnu riječ u operativnim poslovima vezanima za napade utemeljene na novim tehnologijama, Vijeće Europske unije odlučilo je da je najbolji način priključiti jedan dio ove organizacije te da se Europski centar za kibernetički kriminal smjesti unutar Europolove zgrade u Haagu. Po inicijalnim informacijama, u EC3 je zaposleno oko 30 stručnjaka, dok je direktor Europola napomenuo da će, ovisno o potrebama posla, Centru na određeno vrijeme moći omogućiti dodatnih desetak suradnika.[52]

Djelokrug EC3 izravno je vezan za napade na računalnu i mrežnu infrastrukturu te online kriminal. Iz praktične perspektive to znači većinu napada kaznenih djela računalnog kriminaliteta, što uključuje malware (eng. malicious software), upade u sustave, phishing, krađu identiteta, zloporabu kreditnih kartica itd. Zaposlenici Centra aktivno rade na prikupljanju i analiziranju podataka o računalnom kriminalu, edukaciji, podršci istragama u državama Europske unije i stvaranju što boljih odnosa s privatnim sektorom.

Jedan od prvih efekata koji bi se trebao osjetiti u međudržavnoj suradnji biti će kroz tzv. *data fusion* centar kroz koji će EC3 kanalizirati velike količine podataka prikupljenih iz raznih izvora.

[52] European Cybercrime Centre, https://www.europol.europa.eu/ec3, stranica posjećena 12. prosinca 2017.

Prikupljeni podaci, u kombinaciji s policijskim informacijama, bit će spojeni u analitičkom čvorištu koje će postati primarna lokacija za prijavljivanje istraga vezanih za računalni kriminal. Uz to, na ovaj će se način stvoriti platforma za centraliziranu pohranu i obradu podataka koja će omogućiti brzu i učinkovitu suradnju između svih agencija i organizacija koje rade na određenim istragama.

Kontakt točka EC3 centra u Republici Hrvatskoj je Služba kibernetičke sigurnosti, pozicionirana unutar Ravnateljstva policije

3.1.5 ENISA

ENISA (eng. *European Network and Information Security Agency*) je "agencija Europske unije za mrežnu i informacijsku sigurnost, stručni je centar za kibernetičku sigurnost u Europi. ENISA pomaže državama EU da se bolje opreme i pripreme za sprječavanje, otkrivanje i odgovor na probleme informacijske sigurnosti. Djelokrug ENISA-e pruža praktične savjete i rješenja za javni i privatni sektor u državama članicama Europske unije te za institucije Europske unije. To uključuje organizaciju vježbi za slučajeve kibernetičke krize u cijeloj Europi, pomoć u razvoju nacionalnih strategija informatičke sigurnosti, promicanje suradnje među timovima za hitne računalne intervencije i izgradnju kapaciteta" (ENISA - European Network and Information Security Agency, 2017).

Prema dostupnim informacijama na stranicama Europske unije "ENISA također objavljuje izvješća i studije o pitanjima kibernetičke sigurnosti. Do sada je provela studije o sigurnosti računalstva u oblaku, zaštiti podataka, tehnologiji za povećanje privatnosti i osiguravanju privatnosti za nove tehnologije, elektroničkoj identifikaciji i elektroničkim uslugama te prepoznavanju kibernetičkih prijetnji. ENISA pomaže u sastavljanju nacrta politika i prava Europske unije u području mrežne i informacijske sigurnosti. Svakodnevni rad ENISA-e utvrđen je u godišnjem programu rada Agencije koji se sastavlja svake godine nakon opsežnog savjetovanja s ENISA-inim upravnim i izvršnim odborom."

ENISA je razvila i snažnu mrežu dionika u javnom i privatnom sektoru te želi poboljšati:

- *"stručnost: predviđanje i pružanje potpore Europi pri suočavanju s novim izazovima mrežnoj i informacijskoj sigurnosti, uzimajući u obzir razvoj digitalnog okruženja",*
- *"politiku: pomaganje državama članicama i institucijama Europske unije u razvoju i provedbi politika potrebnih za ispunjavanje pravnih i regulatornih zahtjeva u pogledu sigurnosti informacija na nacionalnoj razini",*
- *"kapacitete: potpora Europi u poboljšanju najnovijih kapaciteta za sigurnost mreža i informacija",*
- *"zajednicu: poboljšanje suradnje među državama članicama i među zajednicama koje se bave sigurnošću informacija na nacionalnoj razini".*

Dalje se navodi da "ENISA blisko surađuje s Europolom i Europskim centrom za kibernetički kriminal (EC3) u zajedničkim istraživanjima i razmjeni informacija, te pomaže agencijama Europske unije u problemima kibernetičke sigurnosti:

- *Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva (CEPOL),*
- *tijelu europskih regulatora za elektroničke komunikacije (BEREC),*
- *Europskoj agenciji za operativno upravljanje velikim informatičkim sustavima u području slobode, sigurnosti i pravde (eu-LISA), te*
- *Europskoj agenciji za sigurnost zračnog prometa (EASA)".*

ENISA također savjetuje sve članice Europske unije o implementaciji Nacionalne kibernetičke strategije, te daje preporuke s ciljevima.[53]

[53] ENISA preporuke https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport, stranica posjećena 14.prosinca 2017.

3.1.6 CEPOL

CEPOL - "Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva" je agencija Europske unije koja osposobljavanjem potiče zajedništvo u izvršavanju europskog i međunarodnog zakonodavstva. CEPOL nastoji postati centar svjetske razine i pokretač promjena u osposobljavanju u području izvršavanja zakonodavstva. Prema informacijama na službenoj web stranici "cilj je doprinijeti rješavanju pitanja europske i globalne sigurnosti zbližavanjem zajednica za izvršavanje zakonodavstva radi razmjene dobre prakse, znanja i iskustva". CEPOL spaja stručnjake odgovorne za izvršavanje zakonodavstva radi:

- *omogućavanja osobnog i stručnog napretka osposobljavanjem,*
- *doprinosa učenju rješavanja problema povezanih s europskom sigurnošću,*
- *uspostavljanja mreže ustanova i stručnjaka za osposobljavanje.*

CEPOL doprinosi sigurnijoj Europi pojednostavljivanjem razmjene suradnje i znanja među službenicima za izvršavanje zakona država članica Europske unije-a i, do određene mjere, trećih zemalja o pitanjima proizašlima iz prioriteta Europske unije-a u području sigurnosti, osobito iz ciklusa politika Europske unije-a o teškom i organiziranom kriminalu, a objedinjuje mrežu ustanova za osposobljavanje službenika za izvršavanje zakonodavstva u državama članicama i podupire ih tako što im pruža najpotrebnije osposobljavanje o sigurnosnim prioritetima, suradnji u izvršavanju zakonodavstva i razmjeni informacija. CEPOL također surađuje s institucijama EU kao i međunarodnim organizacijama, te trećim zemljama kako bi osigurao pružanje kolektivnog odgovora na najozbiljnije sigurnosne prijetnje.

Na čelu CEPOL-a je izvršni direktor koji je odgovoran Upravnom odboru. Upravni odbor čine predstavnici država članica Europske unije i Komisije Europske unije. Predsjednik Upravnog odbora predstavnik je jedne od triju država članica koje su zajednički pripremile 18-mjesečni program Vijeća Europske unije. Upravni se odbor sastaje barem dvaput godišnje. Uz to, CEPOL je u svim državama članicama uspostavio posebne nacionalne jedinice (nacionalne jedinice CEPOL-a) za pružanje informacija i pomoći službenicima u području izvršavanja zakonodavstva koji žele sudjelovati u aktivnostima CEPOL-a.

Nacionalne jedinice CEPOL-a pružaju potporu operacijama CEPOL-a. Godišnji program rada Agencije izrađuje se uz pomoć doprinosa ove mreže i drugih dionika, što rezultira tematskim i ciljanim aktivnostima osmišljenima radi ispunjavanja potreba država članica u prioritetnim područjima strategije unutarnje sigurnosti Europske unije-a. CEPOL procjenjuje potrebe za osposobljavanjem kako bi se pružio odgovor na sigurnosne prioritete Europske unije.

CEPOL uvijek nastoji pružiti inovativne napredne aktivnosti osposobljavanja integriranjem relevantnih dostignuća u područjima znanja, istraživanja i tehnologije te stvaranjem sinergije putem osnažene suradnje. Trenutačni portfelj CEPOL-a obuhvaća aktivnosti na licu mjesta, učenje preko interneta (npr. webinari, internetski moduli, tečajevi na internetu itd.), programe razmjene, zajedničke kurikulume, istraživanje i znanost.

Kontakt točka za CEPOL u Republici Hrvatskoj je nacionalna jedinica ustrojena unutar Policijske akademije MUP-a RH u Zagrebu.

3.1.7 Međuinstitucionalna suradnja

Unatoč tome što su mnoge organizacije prepoznale problem kibernetičkog kriminala, suradnja svakako može i mora postati bolja i uspješnija u otkrivanju i preveniranju kaznenih djela računalnog kriminaliteta (Murray, 2008).

Za primjer suradnje referirat ćemo se na podatak da je najveći broj servera koji pohranjuju podatke o mogućim počiniteljima kaznenih djela računalnog kriminaliteta i dalje u Sjedinjenim američkim državama, te da su upiti država članica Interpola koji istražuju takva kaznena djela usmjereni upravo prema zemlji gdje se nalazi takav server.

Provođenjem istražnih radnji u Republici Hrvatskoj i kontaktiranjem s uredom Interpola Washington, SAD, nužno je da zahtjev sadrži sljedeće:

- *zakoni SAD-a zahtijevaju sudski poziv ili nalog za osiguranje/pribavljanje bilo kakvih informacija u vezi s elektroničkim prijenosom podataka koji se odnose na pretplatnika, identificiranje datuma, vremena, korisnika i detaljima internetskih stranica na koje je pristupio korisnik ili druge informacije koje se odnose na pretplatnike ili klijente takvih službi.*

Za pribavljanje takvih informacija potrebno je uputiti Ministarstvu pravosuđa SAD-a zahtjev za međunarodnu pravnu pomoć putem nadležnog Ministarstva u zemlji tražiteljici podataka.

3.1.8 Međunarodna pravna pomoć

Međunarodnu pravnu pomoć Zakon[54] definira kao "sustav pravnih pravila kojima se regulira postupanje u predmetima s tzv. međunarodnim elementom. Navedena pravila rezultat su dugotrajnog razvoja određenog jačanjem međunarodnog organiziranog kriminala, kao regulacijom prava država od dijela svog suvereniteta u području primjene prava i zakona. Razvoj je obilježen napuštanjem ili ograničavanjem dijela tradicionalnih načela međunarodne pravne pomoći te izgradnjom novih načela zasnovanih na visokom stupnju povjerenja u pravne sustave drugih država".

Razvoj međunarodne pravne pomoći u kaznenim pitanjima rezultirao je njezinom promjenom u obliku pravosudne suradnje radi uspješnije međunarodne pravne pomoći (Fuentes-Camacho, 2000).

Međunarodna pravna pomoć ulazi u domenu međunarodnog pravosuđa. No, u određenim slučajevima, kad se radi o hitnom postupanju, odnosno potrebi hitnog očuvanja integriteta podataka, uključuje se Služba kibernetičke sigurnosti Ravnateljstva policije, s obzirom na to da je 24/7 kontakt točka. U tim situacijama traži se čuvanje podataka od strane druge države (na rok od 90+90 dana), a sve kako se podaci ne bi uništili budući da sam postupak međunarodne pravne pomoći traje prilično dugo (Marciuš, 2017, str. 19).

[54] Zakon o međunarodnoj pravnoj pomoći u kaznenim stvarima (NN 178/04).

3.2 Pravna regulativa kriminaliteta u kibernetičkom prostoru Republike Hrvatske

Stupanjem na snagu Kaznenog zakona 1997. godine (Kazneni zakon 1997. - 2012.), prvi je put u pravo Republike Hrvatske uveden računalni kriminal u članku 223. Kaznenog zakona kao kazneno djelo oštećenje i uporaba tuđih podataka.[55] Treba napomenuti da članak 131. sankcionira neovlašteno snimanje i prisluškivanje u računalnom sustavu novčanom kaznom ili kaznom zatvora do jedne godine.[56]

Prema navedenom zakonu "kažnjiva je neovlaštena izrada i prodaja naprava i programa prilagođenih za činjenje kaznenih djela računalnog kriminaliteta, novčanom ili kaznom zatvora do tri godine, te obvezno kažnjavanje za pokušaj". [57]

Kazneno djelo neovlaštenog pristupa podacima ili programima nije u tom trenutku bilo usuglašeno s Konvencijom.[58].

Konvencija u svojim odredbama posjeduje mogućnost kažnjavanja neovlaštenog pristupa. U to vrijeme važeći Kazneni zakon (1997) s Izmjenama i dopunama u spomenutom članku 223. iz 2004. godine sankcionira neovlašteni pristup "unatoč zaštitnim mjerama", a nisu postojala niti jasna pravila jer nije bio uveden standardizirani način zaštite informacijskih sustava sve do 2007. godine.[59]

Temeljem navedenog, informaciju o postojanju takvih zaštitnih mjera morao je davati sud. Počiniteljima ovih kaznenih djela je ostajala izvrsna mogućnost obrane na sudu, što znači da je svaki počinitelj mogao tvrditi da nisu postojale zaštitne mjere (Vjesnik, 2001, str. 30).

Nadalje, temeljem odredbi Konvencije, u zakonodavstvo su implementirana još dva kaznena djela, "računalno krivotvorenje" i "računalna prijevara".

Kod računalnog krivotvorenja inkriminacija se odnosi na počinitelja koji "izradi, unese, izmijeni, izbriše ili učini neuporabljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao pravi ili počinitelj uporabi takve podatke ili programe".[60]

---

[55] Kazneni zakon 1997-2012, "Oštećenje i uporaba tuđih podataka", članak 223.
[56] Kazneni zakon 1997-2012, "Neovlašteno snimanje i prisluškivanje", članak 131.
[57] Kazneni zakon 1997-2012, "Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava", članak 223.
[58] eng. *Hacking* - neovlašteni pristup elektroničkim podacima ili programima.
[59] "Zakon o informacijskoj sigurnosti", Narodne novine 79/07.
[60] Kazneni zakon 1997-2012, Računalno krivotvorenje, članak 223.a

Računalnu prijevaru kao još jedan novi članak odlikuje velika mogućnost pojavnih oblika.[61]

Iako sve razvijene zemlje prate suvremene pravne tokove koji se odnose na kiberkriminal, brzina kojom se ta vrsta kriminala razvija je ponekad ispred zakonskih rješenja.

Republika Hrvatska je Kaznenim zakonom iz 2011. godine (u daljnjem tekstu: Kazneni zakon - u potpunosti stupio na snagu 1. siječnja 2013. godine), uvela sveobuhvatnu Glavu zakona posvećenu "kaznenim djelima protiv računalnih sustava, programa i podataka", te na tom tragu je vidljiva puno veća kompatibilnost i operacionalizacija potpisanih obveza iz Konvencije, kao i prilagodba novim izazovima računalnog kriminaliteta.

Kazneni zakon propisuje sljedeća kaznena djela koja tvore računalni kriminalitet:

- *"neovlašteni pristup" (članak 266.),*
- *"ometanje rada računalnog sustava", (članak 267.),*
- *"oštećenje računalnih podataka", (članak 268.),*
- *"neovlašteno presretanje računalnih podataka" (članak 269.),*
- *"računalno krivotvorenje" (članak 270.),*
- *"računalna prijevara", (članak 271.),*
- *"zloporaba naprava", (članak 272.) i*
- *"teška kaznena djela protiv računalnih sustava, programa i podataka" (članak 273.)."*

Za napomenuti je da počinitelj svih kaznenih djela može biti svaka osoba.

[61] Kazneni zakon 1997-2012, Računalna prijevara, članak 224.a

Kazneni zakon definira, gotovo jednako kao i Konvencija, pojmove koji su prisutni u svim kaznenim djelima računalnog kriminaliteta:

- *"Računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja."*[62]
- *"Računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu."*[63]
- *"Računalni program je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju."*[64]

3.2.1 Ostala dodirna kaznena djela

Osim spomenutih kaznenih djela, u prethodnom poglavlju se nalaze u dvadeset petoj glavi "Kaznenog zakona" pod nazivom "*Kaznena djela protiv računalnih sustava, programa i podataka"*, ali postoje i druga kaznena djela u čijem se opisu spominje računalo kao sredstvo napada ili objekt napada. Takvih kaznenih djela u postojećem Kaznenom zakonu ima nekoliko, a u budućnosti se može očekivati sve više. U sljedećim točkama bit će prikazana kaznena djela protiv privatnosti, časti i ugleda, spolnog zlostavljanja i iskorištavanja djeteta, intelektualnog vlasništva, pa čak i kaznena djela protiv javnog reda.

U skupinu kaznenih djela protiv privatnosti ulazi i kazneno djelo nedozvoljene uporabe osobnih podataka.[65] Iz perspektive Ministarstva unutarnjih poslova, djelatnici policije su korisnici sigurno najveće zbirke osobnih podataka u Republici Hrvatskoj. Sukladno ovlastima i potrebama, svaki djelatnik je osobno odgovoran za etičko korištenje povjerene mu ovlasti korištenja osobnih podataka u službenim evidencijama.

[62] Članak 87., stavak 17. Kaznenog zakona.
[63] Članak 87., stavak 18. Kaznenog zakona.
[64] Članak 87., stavak 19. Kaznenog zakona.
[65] Kazneni zakon, Nedozvoljena uporaba osobnih podataka, članak 146.

U posljednje vrijeme svjedoci smo događanja mnogih društvenih pojava koje u širokom spektru prikupljaju osobne podatke. Jedno od kaznenih djela koje na nedozvoljen način prikuplja naše osobne podatke naziva se *phishing*, ili mrežna krađa identiteta.

3.2.1.1 Kaznena djela protiv časti i ugleda

Kod kaznenih djela protiv časti i ugleda postoje sljedeća kaznena djela: uvreda, sramoćenje i kleveta. Čast se može definirati kao subjektivno pravo svakog čovjeka na osobni osjećaj vrijednosti, a ugled je pravo na priznanje te vrijednosti od strane drugih pripadnika zajednice.

Preuzimanje odgovornosti za javno izrečeno i napisano korištenjem foruma i društvenih mreža, te ostavljanje komentara na portalima donosi sa sobom i razinu odgovornosti budući da su uvrede, sramoćenje i klevete putem računalnog sustava ili mreže tretirane kao kazneno djela za koje su predviđene novčane kazne.[66]

Presuda se mora javno objaviti ukoliko je počinitelj proglašen krivim, a na zahtjev oštećenika.[67]

3.2.1.1.1 Uvreda[68]

Uvredu možemo definirati kao izjavu omalovažavanja koja sadrži negativan vrijednosni sud o nekoj osobi, a mora se odnositi na određenu osobu. Treba napomenuti je da je uvreda moguća i "u četiri oka" i da mora biti prepoznata kao takva jer nerazumljiva, omalovažavajuća izjava koja nije tako percipirana ne predstavlja uvredu. Pokušaj uvrede nije kažnjiv.

[66] Kazneni zakon, "Pokretanje kaznenog postupka za kaznena djela protiv časti i ugleda", članak 150.
[67] Kazneni zakon, "Javno objavljivanje presude za kaznena djela protiv časti i ugleda", članak 151.
[68] Kazneni zakon, "Uvreda", članak 147.

3.2.1.1.2 Sramoćenje[69]

U ovom kaznenom djelu mora se raditi o činjeničnoj tvrdnji, bez obzira bila istinita ili neistinita, dok su vrijednosni sudovi isključeni. Oštećenik može biti fizička ili pravna osoba, a za navedenu izjavu mora saznati treća osoba.

Pokušaj također nije kažnjiv.

3.2.1.1.3 Kleveta[70]

Kazneno djelo klevete spada u najteže kazneno djelo protiv časti i ugleda. Mora se raditi o neistinitoj činjeničnoj tvrdnji i vrijednosni sudovi moraju biti isključeni, a također za difamirajuću izjavu mora saznati treća osoba. Kao kod kaznenog djela sramoćenja, oštećenik može biti i fizička i pravna osoba.

Pokušaj nije kažnjiv.

3.2.1.2 Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta

Autori navode da "sama činjenica da su sadržaji koji prikazuju seksualno zlostavljanje djece na internetu dostupni doslovno jednim klikom miša ne znači da su ti sadržaju legalni" (Cvjetko i Singer, 2013, str. 17). Njihovo gledanje putem interneta, spremanje u memoriju računala ili na bilo koji drugi medij za pohranu podataka, predstavlja radnju kaznenog djela. Do izmjena Kaznenog zakona[71] iz 2011. godine, gledanje takvih sadržaja nije obuhvaćalo opis inkriminacije.

[69] Kazneni zakon, Sramoćenje, članak 148.
[70] Kazneni zakon, Kleveta, članak 149.
[71] Kazneni zakon Republike Hrvatske, Narodne novine 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11

3.2.1.2.1 Iskorištavanje djece za pornografiju[72]

Odredbe ovog članka penaliziraju široki katalog zabrana specifičnih za iskorištavanje djece za pornografiju. S motrišta teme ovog doktorskog rada zanimljiv je stavak 2. koji kaže da *"će se kazniti tko neovlašteno snima, proizvodi, nudi, čini dostupnim, distribuira, širi, uvozi, izvozi, pribavlja za sebe ili drugoga, prodaje, daje, prikazuje ili posjeduje dječju pornografiju ili joj svjesno pristupa putem informacijsko komunikacijskih tehnologija"*, što znači da je inkriminiran već i sam pristup, bez obzira što počinitelj ne pohranjuje materijale kojima je pristupio putem interneta ili nekog drugog medija.

3.2.1.2.2 Iskorištavanje djece za pornografske predstave[73]

Odredbe ovog članka odnose se na "mamljenje djece za zadovoljenje spolnih potreba", što je u internetskim krugovima poznato kao *child grooming*. Kvalificirani oblik odnosi se na imovinsku korist, odnosno zarađivanje od pornografskih predstava u kojima sudjeluje dijete, a zarada je najčešće omogućena prodajom putem interneta, korištenjem računalnih mreža. Sankcijama iz ovog članka namjera je suzbijanje ne samo ponude takvih materijala putem računalnih mreža, nego i potražnja.

3.2.1.2.3 Upoznavanje djece s pornografijom[74]

Kako ističu Cvjetko i Singer, kazneno djelo dovršeno je već samim stvaranjem mogućnosti da se dijete upozna s pornografskim sadržajem predmeta i nije potrebno da se ono s tim sadržajem doista i upoznalo. Dijete ne mora ni prepoznati da je riječ o pornografskom sadržaju, a s obzirom na dob ne mora biti ni kadro prepoznati da je riječ o pornografiji (Cvjetko i Singer, 2013, str. 187-188).

[72] Kazneni zakon, Iskorištavanje djece za pornografiju, članak 163.
[73] Kazneni zakon, Iskorištavanje djece za pornografske predstave, članak 164.
[74] Kazneni zakon, Upoznavanje djece s pornografijom, članak 165.

3.2.1.3 Kaznena djela protiv intelektualnog vlasništva

Sukladno Zakonu o autorskom i srodnim pravima, autorska prava sadržavaju imovinska prava, koja obuhvaćaju:

- *"pravo reproduciranja (pravo umnožavanja),*
- *pravo distribucije (pravo stavljanja u promet),*
- *pravo priopćavanja autorskog djela javnosti,*
- *pravo prerade."*[75]

U Republici Hrvatskoj, interese proizvođača softvera i njihovih partnera zastupa međunarodno udruženje Business Software Aliance (dalje u tekstu: BSA).[76]

Od stupanja na snagu novog Kaznenog zakona zabilježen je značajan pad broja kaznenih djela iz domene povreda prava intelektualnog vlasništva, prema kojem je za postojanje kaznenog djela nužan preduvjet ostvarenje znatne imovinske koristi ili prouzročenje znatne materijalne štete koja, prema novom tumačenju Kaznenog odjela Vrhovnog suda Republike Hrvatske, iznosi najmanje 60 000 kn.

Slijedom navedenog, može se zaključiti da su kaznena djela iz domene povrede prava intelektualnog vlasništva izmjenama Kaznenog zakona dobila novi značaj, budući da su svrstana u zasebnu glavu što do sada nije bio slučaj. No, može se reći da te izmjene nisu doprinijele i boljoj kaznenopravnoj zaštiti, već naprotiv, da je ona u jednom dijelu i smanjena.

3.2.1.3.1 Povreda osobnih prava autora ili umjetnika izvođača[77]

Pod ovim kaznenim djelom spomenut ćemo samo kontekst koji se temelji na dodirnim područjima računalnog kriminaliteta, poznatije kao softversko piratstvo.

[75] Zakon o autorskom i srodnim pravima, članak 18.
[76] Business Software Aliance, http://ww2.bsa.org/country.aspx?sc_lang=hr-HR stranica posjećena 17. studenog 2017.
[77] Kazneni zakon, Povreda osobnih prava autora ili umjetnika izvođača, članak 284.

Pod softverskim piratstvom smatra se neovlašteno kopiranje, korištenje i distribucija zaštićenih računalnih podataka i programa, što se odnosi na one podatke i programe koji uživaju punu autorsko pravnu zaštitu, a ne i na druge kod kojih se autor u cijelosti ili djelomično, privremeno ili trajno odrekao svojih materijalnih prava, odnosno potraživanja.[78]

Počinitelj može biti svaka osoba. Ovaj članak je usklađen s člankom 10. Konvencije.

3.2.1.3.2 Nedozvoljena uporaba autorskog djela[79]

Kako navodi Mladen Vukmir (2005), odvjetnik iz Zagreba, "osim svih prednosti koje nam donose elektronički mediji, pokazuju se vrlo često i nedostaci vezani uz zaštitu sadržaja pohranjenih na njima. Kao što je opće poznato, CD-i i DVD-i su danas uz svoju nisku cijenu, pristupačni širokim masama, te samim time uz posjedovanje odgovarajuće opreme od jednog izvornika autorskog djela u elektroničkom obliku, moguće je proizvesti nebrojeno mnogo kopija bez osjetnog gubitka na njihovoj kakvoći. Zakon, štoviše, sadrži određene iznimke kada je dopušteno umnožavanje, odnosno kopiranje autorskog djela pod strogo ograničenim uvjetima propisanim Zakonom. Takvo bi umnožavanje bilo dopušteno samo fizičkim osobama i samo za vlastite potrebe koje nisu komercijalne naravi, odnosno ova kopija nije pristupačna ili namijenjena javnosti. Dopušteno je fotokopirati dijelove knjige, a cijelu samo ako je ista rasprodana na tržištu dvije godine. Takvo pravo na privatnu kopiju je izričito isključeno kod računalnih programa, kod kojih pak postoji pravo na tzv. sigurnosnu, odnosno backup kopiju. Danas smo sve više svjesni da je internet izvor iznimno jednostavnog načina prenošenja podataka, skidanja zaštićenih sadržaja bez naknade, s relativno malim mogućnostima nadzora takvih povreda. U Hrvatskoj se takve reprodukcije obično obavljaju u kućnoj radinosti, teško se otkrivaju, kao i počinitelji takvih povreda. Također, ako se radi o neznatnim povredama, primjerice, o nekoliko neovlaštenih kopija ili njihovoj maloj vrijednosti, autoru se obično ne isplati pokretanje sudskih postupaka zbog prevelikih troškova u odnosu na visinu naknade koja mu zakonski pripada".[80]

---

[78] Programi tipa: public domain, shareware, freeware, charityware, firmware i cardware.
[79] Kazneni zakon, Nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača, članak 285.
[80] InfoTrend online, http://www.infotrend.hr/clanak/2008/3/pravne-aktivnosti---bsa,15,457.html, stranica posjećena 17. studenog 2017.

3.2.1.4 Kaznena djela protiv javnog reda

Kaznena djela protiv javnog reda u globalnosti karakterizira heterogenost, a napadaju se različiti društveni odnosi.

3.2.1.4.1 Javno poticanje na nasilje i mržnju[81]

Sukladno izmjenama u pravnoj regulativi i sve široj dostupnosti računalne infrastrukture, svjedoci smo uporabe te iste tehnologije u svrhu poticanja i pozivanja na nasilje i mržnju, kao što su forumi, društvene računalne mreže itd.

U spektru kaznenih djela računalnog kriminaliteta usredotočit ćemo se na računalni sustav ili mrežu kao sredstvo počinjenja ovog kaznenog djela.

3.3 Istraživanje nedozvoljenih ponašanja u kibernetičkom prostoru

U većini slučajeva kibernetičkog kriminaliteta počinjenje kaznenih djela se odvija u više zemalja, što zahtijeva niz koordiniranih operacija od strane većeg broja međunarodnih tijela koja su nadležna i kompetentna za rješavanje, odnosno realizaciju operacija u svrhu zaustavljanja počinjenja i hvatanja počinitelja kaznenih djela u domeni kibernetičkog kriminaliteta (Hughes, 2010).

Tijekom 2014. godine od strane "The Hague"[82] objavljeno je izvješće o nizu operacija u 16 zemalja širom svijeta, koordiniranih od strane Eurojusta. Eurojust je tijelo za pružanje pomoći nadležnim tijelima država članica, kada se bave ozbiljnim prekograničnim i organiziranim kriminalom.

[81] Kazneni zakon, Javno poticanje na nasilje i mržnju, članak 325.
[82] EUROJUST http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-05-19.aspx, stranica posjećena 12. prosinca 2017.

U Haagu su, uz podršku Europskog centra za cyber kriminal (EC3) Europola, ciljani programeri, distributeri i korisnici "BlackShadesa" [83], zlonamjernih programa koji su se nalazili na meti pravosudnih i policijskih službenika. Tijekom operacije u svijetu je obavljen nadzor nad 359 kućanstava, dok je više od 80 osoba uhićeno. Zaplijenjeno je preko 1.100 uređaja za pohranu podataka za koje se sumnjalo da su korišteni u ilegalnim aktivnostima, uključujući računala od uhićenih osoba, prijenosna računala, mobilne telefone, vanjske tvrde diskove i USB memorije.

Zaplijenjene su i znatne količine novca, ilegalnog vatrenog oružja i droga. Kao izoliran primjer možemo navesti slučaj u Nizozemskoj gdje je osamnaestogodišnjak koristio "BlackShades" softver kako bi zarazio najmanje 2 000 računala i dobio kontrolu nad web kamerom žrtve u svrhu fotografiranja žena. U istu operaciju uključene su zemlje koje su poduzele korake protiv kiberkriminalaca: Nizozemska, Belgija, Francuska, Njemačka, Velika Britanija, Finska, Austrija, Estonija, Danska, SAD, Kanada, Čile, Hrvatska, Italija, Moldavija i Švicarska. Dakle, može se slobodno zaključiti kako su u operaciju bile uključene zemlje iz skoro cijelog svijeta. Prije nego što je navedena operacija započela, održana su tri koordinacijska sastanka u Eurojustu na kojima je sudjelovala većina uključenih zemalja.

Tijekom koordinacijskih sastanaka od strane Eurojusta uspostavljen je koordinacijski centar koji je pomagao različitim zemljama tako što im je omogućio pregled stanja uključenih zemalja, kao i pružanje pravosudne pomoći, u slučaju potrebe. Koordinaciji su bili prisutni predstavnici Eurojusta, EC3 Europola i FBI-a. Daljnjim tijekom suradnje EC3 Europol bio je prisutan prilikom daljnjih operacija i omogućio je analitičku podršku u stvarnom vremenu. Jedan od važnijih zadataka EC3 bilo je praćenje, identificiranje žrtava i analiza prikupljenih podataka.

Direktor Europskog centra za cyber kriminal (EC3) u Europolu, G. Troels Oerting, naveo je: "Ovaj slučaj još je jedan primjer kritične potrebe za koordiniranim operacijama provođenja zakona protiv sve većeg broja cyber kriminalaca koji djeluju na razini Europske Unije i na globalnoj razini. EC3 će nastaviti - zajedno s Eurojustom i drugim partnerima - neumorno raditi na pružanju podrške našim partnerima u borbi protiv prijevara i drugih cyber kriminalaca koji iskorištavaju internet za počinjenje kaznenih djela.

[83] "Blackshades" - maliciozni trojanski konj.

Djelo je daleko od prošlosti, ali je naša suradnja na zajedničkom radu preko granica povećana, a predmetima se kontinuirano bavimo. "[84]

Marciuš navodi slučaj iz 2017. godine o kojem je izvijestio Europol[85] gdje je poljska nacionalna policija, u suradnji s nadležnim službama u Hrvatskoj, Njemačkoj, Rumunjskoj i Švedskoj, a zajedno s Europolovim Europskim centrom za cyber kriminal (EC3), uništila poljsku mrežu organiziranog kriminala, osumnjičenu za online plaćanje prijevare i pranje novca. Ista operacija rezultirala je s devet uhićenja organizatora kriminalne mreže. Kaznena djela počinjena su na način da je organizirana skupina kupovala male tvrtke preko kojih su oglašavani oglasi na internetu, da bi se dobio kredibilitet. Novac dobiven od žrtava prao se kroz mrežu "novčanih mazgi" koje su ga zatim unovčile na bankomatima u Poljskoj, Hrvatskoj ili Češkoj. Počinitelji su preko interneta oglašavali prodaju automobila, građevinskih ili poljoprivrednih strojeva i vozila, koje nikada nisu isporučili kupcima, dok su plaćanja tražili unaprijed. Oglase su objavljivali na brojnim internetskim stranicama za prodaju vozila i strojeva u različitim državama članicama Europske unije. Tisuće je osoba prevareno i oštećeno, s materijalnom štetom od oko petnaest milijuna kuna. Poljska je policija tijekom konačne racije zaplijenila kartice za bankomate, automobile, prijenosna računala i mobilne telefone. Neki od članova skupine također su bili uključeni u druge oblike organiziranog kriminala poput krijumčarenja alkohola i duhana (Marciuš, 2017, str. 24).

Europska komisija EC3 podržala je operaciju organiziranjem operativnog sastanka krajem travnja 2017. godine u sjedištu u Haagu, gdje su zemlje poput Poljske, Hrvatske, Švedske, Njemačke i Rumunjske razmijenile saznanja i korisne informacije. Poljski i hrvatski istražitelji, kao i ostali službenici za vezu Europola, dogovorili su daljnje moguće operacije, ovisno o kretanju vođa i članova kriminalne skupine.

Europol je koordinirao rješavanje slučaja. Svemu tome bio je nazočan Europolov EC3 stručnjak, s mobilnim uredom, omogućujući izravan pristup bazama podataka Europola za unakrsnu provjeru, analizu i razmjenu obavještajnih podataka u realnom vremenu.

---

[84] EUROJUST http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-05-19.aspx, stranica posjećena 12. prosinca 2017.

[85] EUROPOL https://www.europol.europa.eu/newsroom/news/9-arrested-for-online-payment-scams-in-joint-operation-polish-police-and-europol, stranica posjećena 12. prosinca 2017.

3.3.1 Metode i tehnike istraživanja kriminaliteta u kibernetičkom prostoru

Analiza kriminala u kibernetičkom prostoru još uvijek predstavlja novo poglavlje u kriminalističkim istragama koje provodi policija. Hrestak navodi da su naročito mistificirana istraživanja kažnjivih ponašanja u kibernetičkom prostoru. Osim u policijskim i u redovima državnog odvjetništva istraživanje takvih kažnjivih ponašanja, kao i procesuiranje počinitelja kaznenih djela počinjenih unutar kibernetičkog prostora nije zastupljeno u dovoljnoj mjeri, prvenstveno zato što ni državno odvjetništvo nema dovoljan broj osposobljenih tužitelja sa znanjima potrebnim za takva istraživanja (Hrestak, 2017, str. 1).

Svjesni smo činjenice da se svakodnevni život pod utjecajem tehnologije i informatike ubrzano mijenja, tako da ga je teško i uspoređivati sa životom od prije 20 - 30 godina. U današnje vrijeme, kada u zapadnom razvijenom svijetu gotovo da i ne postoji čovjek koji nema mobitel, računalo i pristup internetu, teško je mlađim generacijama predočiti kako je svijet funkcionirao kada su tek rijetki imali kućni telefon, a o pristupu internetu mogli su samo sanjati. S tehnološkim napretkom čovječanstva napreduje i kriminal, odnosno kriminalna ponašanja i načini izvršenja kaznenih djela. Činjenica je da kriminalci puno brže prihvaćaju nove tehnologije i u svojim načinima počinjenja kaznenih djela su puno fleksibilniji od snaga reda, koje ih pokušavaju u tome spriječiti i otkriti (Kahin i Nesson, 1998).

Treba priznati da zakonodavstvo kasni s prepoznavanjem i definiranjem novih vrsta kaznenih djela počinjenih preko računalne mreže i računalnih sustava, a ni policija još uvijek ne reagira adekvatno na ubrzani tehnološki razvoj, što za posljedicu ima veliki broj kaznenih djela koja nisu zakonski definirana ili su u tamnoj brojci jer ih policija i državno odvjetništvo ne prepoznaju kao kaznena djela ili se uopće ne bave razrješavanjem takvih kaznenih djela (Kuehl, 2009).

Prema izvješću Hrvatske regulatorne agencije za mrežne djelatnosti (dalje u tekstu HAKOM), u zadnjem tromjesečju 2016. godine u Hrvatskoj je broj priključaka širokopojasnog pristupa internetu putem nepokretnih mreža bio 1 043 795, a broj priključaka putem mobilnih mreža bio je 3 380 741[86]. Ako broj priključaka na širokopojasni internet usporedimo s brojem stanovnika iz posljednjeg popisa stanovništva iz 2011. godine, a koji je iznosio 4 284 889[87] proizlazi da u Hrvatskoj ima 139 647 više internetskih priključaka za pristup širokopojasnom internetu nego stanovnika. Ako uzmemo da je svaki korisnik širokopojasnog interneta potencijalna žrtva nekog od kaznenih djela protiv računalnog sustava, programa i podataka ili kaznenih djela iz domene dječje pornografije kao i da je svaki korisnik i mogući počinitelj takvih kaznenih djela, može se konstatirati da je tamna brojka takvih kaznenih djela značajna i da se 2 049 otkrivenih kaznenih djela ne može smatrati uspjehom.

U kriminalističkom istraživanju počinitelja kaznenih djela u kibernetičkom prostoru u skladu s hrvatskim zakonodavstvom postoje dva moguća scenarija. Prema prvom scenariju policijski službenik može sačiniti izvješće o prikupljenim saznanjima korištenjem otvorenih internetskih izvora u kojem će navesti podatke o datotekama koje je osumnjičeni nudio na dijeljenje, te će to izvješće služiti samo kao osnova za pokretanje kriminalističkog istraživanja i provođenje hitnih dokaznih radnji. Drugi smjer kriminalističkog istraživanja bi bio da policijski službenik u skladu s člankom 12. Zakona o policijskim poslovima i ovlastima, ne otkrivajući svoj identitet, uz pomoć specijaliziranih računalnih programa preuzme datoteke koje je osumnjičeni distribuirao te da se te datoteke u daljnjem kaznenom postupku koriste kao elektronički dokazi (Hrestak, 2017, str. 28).

Konvencijom o kibernetičkom kriminalitetu, u članku 35. definirana je mreža u neprekidnom pogonu, što se direktno odnosi na Službu kibernetičke sigurnosti Ministarstva unutarnjih poslova Republike Hrvatske, odnosno kontakt točka za kaznena djela računalnog kriminaliteta.

[86] HAKOM https://www.hakom.hr/UserDocsImages/2017/e_trziste/Tromjese%C4%8Dni%20usporedni%20podatci%20za%20tr%C5%BEi%C5%A1te%20elektroni%C4%8Dkih%20komunikacija%20RH%20Q42016.pdf, stranica posjećena 12. prosinca 2017.
[87] DZS. Dostupno na: http://www.dzs.hr/, stranica posjećena 12. prosinca 2017.

Bitno je napomenuti da je kazneno djelo računalne prijevare u prvih 9 mjeseci 2017. godine bilo na sedmom mjestu po učestalosti kaznenih djela gospodarskog kriminaliteta u Republici Hrvatskoj, dok u domeni kaznenih djela računalnog kriminaliteta zauzima visoko prvo mjesto.

Pavišić, Modly i Veić, kao autori objedinjuju istraživanje računalnih kaznenih djela s kriminalističkog aspekta, kao posebno poglavlje, te su obrađene morfološke značajke i istraživanja pojedinih kaznenih djela u svezi s kaznenim djelima računalnog kriminaliteta (Pavišić, Veić i Modly, 2012, str. 615-624).

3.3.1.1 Hakiranje

Prema autorima "kada jedna osoba koristi identitet druge osobe kako bi na taj način pristupila računalnoj infrastrukturi, govorimo o lažnom predstavljanju ili maskiranju. Sigurnosne metode koje koriste sustavi zaštite računalne infrastrukture moraju biti dovoljno aktivne kako bi otkrili i spriječili lažno predstavljanje. Kada se govori o lažnom predstavljanju, moramo razlikovati fizičku i elektroničku formu lažnog predstavljanja. O fizičkom predstavljanju govorimo kada počinitelj koristi ovlašteni korisnički identitet ili pristupnu karticu kako bi pristupio povjerljivim područjima i stekao pristup računalnoj infrastrukturi i podacima. Za lažno predstavljanje kažemo da je elektroničko kada počinitelj, u stvari, koristi legalni korisnički identifikacijski broj ili zaporku kako bi se prijavio u računalni sustav te na taj način nelegalno došao u posjed podataka i informacija" (Larry i Lars, 2012).

Istraživanje kojim se može ustanoviti neovlašteno pristupanje podacima ili računalnim sustavima ovise o tipu podataka i računalnih sustava, te načinima na koji se ti podaci i sustavi u prvom redu štite od neovlaštenog pristupa. Dakle kriminalističko istraživanje predstavlja postupke kojima se pronalaze tragovi koji upućuju na odstupanja od mehanizama zaštite podataka i računalnih sustava. Ovisno o veličini i geografskoj i mrežnoj rasprostranjenosti podataka i sustava kriminalističko istraživanje može biti centralizirano ili distribuirano, može obuhvaćati jedan sustav ili cijeli niz sustava i računala.

Ključno je ustanoviti tko i kada je imao pravo pristupa na sustav ili podacima, potom te informacije usporediti s informacijama dobivenim iz sustava koje pokazuju tko je i kada stvarno pristupao sustavu ili podacima.

Ustanovljavanje o kojim se informacijama u sustavu točno radi ovisi o samom računalnom sustavu i njegovom sadržaju, te ih nije moguće jednostavno navesti ili pobrojati, no, ipak mogu se definirati neke osnovne pretpostavke, prema zahtjevima računalne forenzike.

Svako istraživanje u razmatranom području obuhvaća istovjetni pristup. Kao prvo, potrebno je definirati opseg sustava i vlasništva tj. odgovornosti za podatke i komponente sustava koji se istražuje. Na osnovu toga može se odrediti u suradnji sa stručnim osobljem koje skupine podataka i informacija postoje u računalnom sustavu i koje od njih su od važnosti za istragu, te na koji način ih se može pronaći na sustavu i na forenzički ispravan način izuzeti sa sustava i analizirati. S obzirom na to da se računalni sustav danas može prostirati preko više država, bitno je ustanoviti i opseg do kojih se podataka i dijelova sustava može doći bez ulaženja na područje drugih država te, ako je potrebno, definirati načine na koje se može doći do podataka i dijelova sustava koji su izvan države. Izdvajanje podataka sa sustava mora biti brižljivo planirano i provedeno da podaci ne bi bili oštećeni, netočni ili necjeloviti, kako bi se izbjegla netočna slika događaja u kasnijoj analizi.

Planiranje i provođenje dokaznih radnji zahtjeva suradnju stručnjaka raznih područja od pravnih stručnjaka, forenzičara, istražitelja, informatičkih stručnjaka te drugih specijalista. Sve radnje na ovom području zahtijevaju suradnju raznih profila znanja pri čemu je ključno da pravni zahtjevi i ograničenja budu jasni svim stručnjacima koji sudjeluju u procesu istražnih radnji i analiza. Neke od istražnih radnji koje se koriste su standardni postupci administracije računala i računalnih sustava i tu postoji opasnost da rezultati tih radnji budu legalno neprihvatljivi ako postupak nije u skladu sa zakonom i postupcima računalne forenzike.

Može se dogoditi da se određena radnja obavi bez potrebnog dokumentiranja i stoga se rezultati ne mogu legalno prihvatiti iako su tehnički potpuno ispravni.

Ponovljivost rezultata istražnih radnji također može doći u pitanje ako se radi o podacima i sustavima koji nisu pod punom kontrolom lokalnih vlasti, kao što je npr. rad s raznim uslugama elektroničke pošte ili tzv. servisima u oblaku, koji podatke čuvaju na udaljenim lokacijama, a pristup je moguć samo preko korisničkog imena i lozinke. U takvom slučaju potrebno je imati potpuni opis i dnevnik postupaka tokom istražnih radnji, ako je moguće i videozapis i audiozapis postupka koji prikazuje kako su izgledali nalazi na ekranima računala tokom izvođenja određene radnje (Pavišić, Veić i Modly, 2012, str. 616-618).

3.3.1.2 Računalna sabotaža

Računalni podaci u današnje vrijeme predstavljaju iznimno vrijednu imovinu i često se dogodi slučaj u praksi, a pogotovo u IT sektoru, da je vrijednost računalnih podataka mnogo veća nego u fizičkom obliku. Za primjer možemo navesti poredbu da vrijednost programa, aplikacije ili izvornog koda može biti veća od zgrade u kojoj se ti podaci nalaze. Još 2013. godine analitičari su predviđali porast vrijednosti internetskih društvenih mrežnih stranica kao novi način financijskog bogaćenja.

3.3.1.3 Sabotaža računalnih sustava

Dokazne radnje kojima se može ustanoviti sabotaža računalnih sustava ovise primarno o korištenom softveru i hardveru, te mjestu u arhitekturi računalnog sustava gdje se ometanje događa. Potrebno je ustanoviti koja funkcija računalnog sustava je ometana i na koji način, koji je uzrok ometanja te tko je prouzročio ometanje.

Kod ometanja rada računalnog sustava uzroci ometanja mogu biti i neispravna ili nepravilno konfigurirana oprema i računalna podrška, tako da je često moguće da ne postoji namjera ometanja. Mogući izvori ometanja mogu biti i izvan i unutar računalnog sustava pri čemu pronalaženje načina i uzroka ometanja može uključivati i otkrivanje drugih kaznenih djela kao što je i neovlašteni pristup. Iz tog razloga istražne radnje moraju obuhvatiti i druge moguće uzroke.

Za ometanje rada računalnog sustava vrlo često se koriste razni namjenski tzv. napadački alati pa dokazne radnje moraju ako je moguće pronaći o kojem se tipu alata radi te na koji je način korišten (Libicki, 2007).

3.3.1.4 Sabotaža računalnih podataka

Oštećenje računalnih podataka je vrlo teško ustanovljiva situacija koja zahtijeva otkrivanje promjena na podacima. U tom smislu istraživanje mora otkriti je li se dogodila promjena na podacima, na koji se način dogodila, te tko ju je uzrokovao i s kojom namjerom.

Već ustanovljavanje je li se dogodila promjena traži da se na neki način pouzdano ustanovi prethodno stanje tj. stanje prije promjene, s obzirom da bez toga nije moguće ustanoviti je li došlo do bilo kakve promjene podataka. Uzroci promjena podataka su vrlo često tehničke greške ili neispravnosti sustava pa je kriminalističkim istraživanjem potrebno ustanoviti da greška ili kvar nisu uzrok promjene.

3.3.1.5 Računalna špijunaža

Istraživanja kojima je moguće ustanoviti neovlašteno presretanje računalnih podataka su izuzetno kompleksna, što je razlog da se vrlo teško može ustanoviti situacija presretanja podataka. U najvećem dijelu slučajeva radi se o otkrivanju kopija podataka dobivenih presretanjem, a radnje na osnovu tih pronađenih podataka moraju dokazati da je došlo do presretanja podataka. Uz same kopije podataka mogu se pronaći i alati tzv. napadački alati. Postojanje alata nije jednoznačan dokaz budući su vrlo često u uporabi kao pomoćna sredstva za administraciju računalnih sustava, pogotovo bežičnih računalnih mreža.

Pri pronalaženju kopija podataka potrebno je u okviru dokaznih radnji napraviti usporedbu pronađenih podataka s onima iz računalnog sustava, te ustanoviti radi li se o izvornicima ili kopijama te koji je stupanj sličnosti.

Kako svaki elektronički sustav proizvodi određenu elektromagnetsku komunikaciju koju je moguće odgovarajućim uređajem snimiti i kasnije reproducirati, za spomenuti je relativno jednostavnu tehnologiju prisluškivanja CRT ili LCD monitora, koji se mogu pratiti na nekoliko desetaka metara, a riječ je o Van Eck prisluškivanju (Maurer i Morgus, 2014). U današnje vrijeme primjenjuju se mjere zaštite - TEMPEST.

3.3.1.6 Računalno piratstvo

Piratstvo programske podrške posebno je zanimljiv napad. Svojom jednostavnom tehnologijom zapisa koja omogućuje brzo i lako umnažanje, programska podrška postavlja svakog korisnika pred dvojbe koje su vezane uglavnom uz isplativost i cijenu programske podrške.

Ovim se problemom u svijetu bavi veliki broj organizacija od kojih se izdvajaju dvije najveće organizacije koje okupljaju proizvođače programske podrške: Business Software Alliance i Software Publisher's Association (SPA).

Piratstvo programske podrške predstavlja neovlašteno kopiranje i distribuiranje programa koji su zakonski zaštićeni od kopiranja. Sam čin piratizacije programske podrške moguće je promatrati sa aspekta omogućavanja korištenja i kopiranja nelegalne programske podrške svjesnim kopiranjem zaštićene programske podrške i njezinim distribuiranjem, te sa aspekta instaliranja prethodno piratizirane programske podrške na računalo. Piratizacija programske podrške može se izvesti na nekoliko načina od kojih su najčešći:

- kopiranje krajnjeg korisnika,
- kloniranje tvrdog diska,
- "skidanje" softvera s interneta,
- slanje putem elektroničke pošte,
- krivotvorina,
- korištenje programske podrške sa poslužitelja,
- kopiranje posuđene programske podrške

Za počinjenje ovog kaznenog djela nije potrebno veliko tehničko i informatičko znanje jer samo oblik računalnih programa i medij na kojem su pohranjeni omogućava svim korisnicima da jednostavno, brzo i jeftino reproduciraju njihov sadržaj (Shipley i Bowker, 2014). Tome je posebno pridonio razvoj uređaja za povezivanje i komunikaciju putem računala, te razvoj velikih računalnih mreža, posebice interneta.[88]

Ovaj oblik napada može počiniti svatko. Razlikujemo nekoliko tipova počinitelja: amateri, profesionalci i industrijski pirati. Vrlo široka rasprostranjenost programske podrške u svakodnevnom životu vjerojatno je jedan od temeljnih razloga počinjenja ovog kaznenog djela, a sama programska podrška predmetom je zanimanja kako pojedinaca tako i organizacija.

Među najčešće počinitelje ubrajaju se kupci i korisnici komercijalne programske podrške, zatim sami pirati programske podrške te zaposlenici koji ukradu programsku podršku.

Najčešći razlozi piratstva programske podrške su nedostatak novca, laka nabava piratizirane programske podrške, nedostatak adekvatne zaštite programske podrške i velika vjerojatnost da piratizacija programske podrške neće biti sankcionirana.

[88] InfoTrend online, http://www.infotrend.hr/clanak/2008/3/pravne-aktivnosti---bsa,15,457.htm, stranica posjećena 12. prosinca 2017.

Načini otkrivanja ove vrste napada različiti su:

- prikupljanje obavijesti,
- promatranje, zasjeda, racija,
- stručni kriminalističko-tehnički pregled,
- pretraga stana, vozila, osoba i računala,
- privremeno oduzimanje predmeta i
- vještačenje.

Među dokaze ove vrste napada u prvom redu ubrajamo fotografije, odnosno slikovne zapise zaslona monitora iz kojih je vidljivo izvođenje piratske programske podrške, sadržaji memorijskih nosača i kopije medija na kojima je piratska programska podrška nađena, i ispisi koji su rezultat rada piratske programske podrške (Pavišić, Veić i Modly, 2012, str. 620).

3.3.1.7 Računalna prijevara

Računalna prijevara obuhvaća razne vrste manipulacija na podacima, a najčešće financijskim. Do takvih manipulacija može doći tijekom unosa, obrade, pohranjivanja, distribucije podataka i informacija, kao i pri razmjeni podataka unutar računalne mreže ili putem telefonskih i drugih komunikacijskih kanala. Pri tome se podaci mogu nalaziti na bilo kojem digitalnom mediju.

Prema Grgiću "noviji razvoj računalnih mreža i telekomunikacija u velikoj mjeri je pridonio njihovom širenju i pojavi novih oblika prijevara. Razvoj bankomata i njihovo sve šire uvođenje u redovito poslovanje banaka otvorilo je nove mogućnosti manipulacija s računalno pohranjenim podacima na karticama ili unutar sustava. Daljnjim razvojem računalnih mreža te širenjem elektroničkog poslovanja i digitalnog novca, ovakve manipulacije zbog lakoće izvođenja i relativno teškog otkrivanja postaju jedan od najčešćih oblika računalnog kriminala. U tu svrhu počinitelj i se sve češće koriste tuđim podacima i otuđenim programski dobivenim brojevima kreditnih kartica kako bi sebi ili drugome pribavili neku korist (kao što je kupovina raznih proizvoda, plaćanje nekakve usluge i sl.) Do izmjene podataka može doći neposredno, izravnim pristupom podacima, pri čemu se koristi neki od programa za upravljanje radom baza podataka. To se može učiniti na samom sustavu, pristupom s neke druge radne stanice unutar računalne mreže ili daljinskim pristupom putem telefonskih, satelitskih i drugih

komunikacijskih kanala. Nakon što se pristupilo računalnom sustavu, manipulacije se izvode na ulaznim ili izlaznim podacima. Ulazne podatke moguće je neposredno promijeniti, dodati nove ili izbrisati postojeće tijekom unosa ili prije same obrade. Slično je i s izlaznim podacima, s tim da se podacima manipulira nakon provedene obrade, a prije ispisa ili distribucije podataka i informacija. Ovo mogu počiniti osobe unutar sustava kao što su stručnjaci koji su izradili program i/ili osobe koje su zadužene za njegovo održavanje." (Grgić, 2013)

Osim toga, do manipulacije može doći i zbog djelovanja programa kao što je tzv. trojanski konj, računalni program koji, osim svoje vidljive namjene, ima i druge, skrivene i korisniku nepoznate funkcije, u ovom slučaju mijenjanje, brisanje postojećih ili dodavanje novih podataka. Vrlo često takvi programi sadrže i naredbu za samouništenje, tj. brisanje nakon čina izvršenja manipulacije, a moguće je i njihovo aktiviranje tek nakon isteka određenog vremena, što dodatno može otežati otkrivanje takvih nezakonitih radnji.

Prijevare s podacima je vrsta djelovanja koje se čini promjenom podataka prije ili poslije unosa u računalni sustav.

Među počinitelje ovog vida napada ubrajamo:

- programere s detaljnim poznavanjem računalnog programa,
- zaposlenike ili bivše zaposlenike,
- programere financijskih sustava,
- računalne korisnike i
- računalne operatere.

U kontekstu određivanja napadača ne može se ustvrditi da su ovi napadači jedini u stanju izvesti ove napade.

Prema autorima "načini detekcije ove vrste napada različiti su, a kreću se od usporedbe računalnog programskog koda s prijašnjom kopijom, detaljne analize podataka uključujući i analizu programskog koda, nadzor financijskih transakcija potencijalnih počinitelja, ispitivanje sumnjivih računalnih programa, pregled tablica s podacima o pristupanju računalu radi pronalaska računalnog programa ili počinitelja do revizije transakcija. Kvalitetna detekcija napada, posebice u inicijalnoj fazi, može biti vrlo učinkovita, a može rezultirati i kvalitetnijim dokazima o počinjenom napadu ili djelu. Među dokaze ove vrste napada u prvom redu ubrajamo izlazne forme računalnog sustava, nedokumentirane transakcije, analizu rezultata ispitnih računalnih programa i datoteke koje sadrže podatke o pristupu računalnom sustavu" (Pavišić, Veić i Modly, 2012, str. 622).

3.3.1.8 Zloporaba naprava

Za počinjenje kaznenih djela računalnog kriminalitet potreban je ili određeni hardver ili određeni softver ili spoj hardvera i softvera, odnosno računalna oprema.

Mnogo je primjera iz prakse, a globalnošću tržišta ovakve opreme u budućnosti biti će sve više potencijalnih alata za počinjenje kaznenih djela računalnog kriminala (Whittaker, 2004).

3.3.2 Pronalaženje podataka

Hrvatski nacionalni CERT navodi da je "prikupljanje podataka i dokaza najosjetljiviji korak računalne forenzičke analize (dalje RFA). Eventualne pogreške u ovom stupnju mogu značiti nepovratan gubitak dokaza, bilo zbog njihova oštećivanja ili zbog gubitka njihove vjerodostojnosti uslijed neprimjerenih metoda prikupljanja. Zbog toga je potrebno pažljivo isplanirati postupak prikupljanja dokaza, s posebnim naglaskom na ranjive dokaze, te koristiti odgovarajuće programske alate" (Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2006-11-174 , 2006, str. 3).

Dalje se navodi da se "postupci računalne forenzičke analize u mnogo čemu razlikuju od postupaka klasične forenzičke analize. Kod klasične istrage dovoljno je osigurati mjesto zločina kako bi se zaštitili dokazi, za koje se kaže da se pokoravaju tzv. *Dead Body*[89] teoremu" (Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2006-11-174 , 2006, str. 4).

Nhan navodi da "čak i kada su dokazi na neki način ugroženi, moguće ih je zaštititi brzo i bez posebnih znanja, primjerice prekrivanjem otisaka obuće na tlu u slučaju kiše. Kod računalne forenzičke analize situacija je daleko zamršenija. Samo za utvrđivanje prisutnosti dokaza potrebno je provesti sveobuhvatnu analizu sustava, jer na računalu, odnosno mediju za pohranu podataka nema rupa od metaka ili mrlja krvi koje bi ukazale na kazneno djelo" (Nhan, 2010).

[89] Eng. - It's not going anywhere

Lu navodi da su "elektronički dokazi ujedno i mnogo ranjiviji od fizičkih pa je vještom napadaču puno lakše ukloniti tragove svoga djelovanja, a nepažljivo ili nestručno provođenje istrage također, može rezultirati gubitkom ključnih podataka. Prije prikupljanja dokaza potrebno je izvršiti temeljitu procjenu danog slučaja i na temelju toga odrediti smjer daljnjeg djelovanja. U okvir takve procjene ulaze nalog za pretragu, detalji slučaja, vrsta medija , potencijalni dokazi koje se traži, te uvjeti njihovog prikupljanja." (Lu, 2009).

Tijekom pronalaženja podataka potrebno je razmotriti:

- "primjenu ostalih forenzičkih postupaka nad dokazima (analiza DNA, prikupljanje otisaka prstiju, traženje tragova mehaničke obrade i sl.)",
- "važnost opreme pronađene uz računalo",
- "vrstu potencijalnih dokaza (fotografije, tablice, dokumenti, baze podataka, financijski podaci)",
- "ostale informacije vezane uz slučaj (korisnička imena, zaporke, računi elektroničke pošte, mrežne postavke, dnevnički zapisi) koje je možda moguće dobiti u razgovoru s administratorima, korisnicima ili zaposlenicima", te
- "razinu informatičkog znanja korisnika čije se djelovanje ispituje".

Po dolasku na mjesto potencijalnog kaznenog djela potrebno je utvrditi:

- "broj i vrste računala",
- "prisutnost računalne mreže",
- "vrstu i količinu medija za pohranu podataka te dokumentirati gdje su pronađeni",
- "postojanje udaljenih spremišta podataka i/ili udaljenih računala",
- "korištene komercijalne programske pakete",
- "o kojim se operacijskim sustavima radi", te
- "intervjuirati sistemske administratore i korisnike" *(Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2006-11-174 , 2006)*.

3.3.3 Pribavljanje elektroničkih dokaza

S obzirom na svojstva elektroničkih dokaza opisanih u prethodnom poglavlju, potrebno je imati na umu da je posao prikupljanja elektroničkih dokaza vrlo opsežan i ozbiljan.

Izradom točne kopije (slike) elektroničkih podataka za koju možemo pretpostaviti da bi nam kasnije mogla poslužiti kao elektronički dokaz, postoji mogućnost da se kasnije u postupku koristi kao i original.

Alat za prikupljanje dokaza mora zadovoljavati sljedeće kriterije:

1. forenzički integritet ispitivanog digitalnog dokaza mora biti očuvan. To znači da takvom digitalnom dokazu nije dozvoljena daljnja uporaba.
2. alat autonomno izvodi cjelokupno rukovanje dokazima, bez interakcije korisnika. Ovo je potrebno kako bi se dokazi osigurali od nestručnog rukovanja. Time se ujedno osigurava i vjerodostojnost prikupljenih dokaza jer ih korisnik ne može mijenjati (Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2006-11-174 , 2006).

U hrvatskom Zakonu o kaznenom postupku elektronički (digitalni) dokazi su prilično šturo definirani kao "podatak koji je kao dokaz u elektroničkom (digitalnom) obliku pribavljen prema navedenom Zakonu".[90]

Nacionalni CERT navodi da "čak i ako istražitelj nije odgovoran za prikupljanje elektroničkih dokaza s računalne mreže, u određenom slučaju, on mora posjedovati osnovna znanja o elektroničkim dokazima" (Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2006-11-174 , 2006).

Zakon o kaznenom postupku definira i pribavljanje elektroničkih dokaza, ali s obzirom na rasprostranjenost i specifičnost elektroničkih dokaza, treba se pridržavati primjera najbolje prakse do donošenja standardnih operativnih postupaka u radu s elektroničkim dokazima.[91]

Kod pribavljanja elektroničkih dokaza Zakon o kaznenom postupku određuje da se istražiteljima omogući pristup, što je navedeno u članku 257. stavku. 1. Zakona o kaznenom postupku.[92]

[90] Zakon o kaznenom postupku, članak 202.,stavak 33.
[91] Zakon o kaznenom postupku, "članak 331.
[92] Zakon o kaznenom postupku, Pretraga pokretne stvari i bankovnog sefa, članak 257.

U slučaju da osobe koje imaju potrebna znanja i obavijesti ne postupe po naloženom, može im se izreći novčana kaznu do 50 000 kn s napomenom da se odredba o kažnjavanju ne odnosi se okrivljenika.[93]

Zakon propisuje da se može odrediti zaštita i čuvanje svih podataka dok je to potrebno, a najdulje 6 mjeseci, a za kibernetička kaznena djela i druga djela počinjena uz pomoć računalnog sustava i duže od 6 mjeseci.[94]

3.3.4 Osiguranje nepromjenjivosti elektroničkih podataka

Kako bi osigurali nepromjenjivosti elektroničkih podataka, potrebno ih je što prije pohraniti na siguran medij i osigurati njihovu autentičnost.

Da bi utvrdili istovjetnost sadržaja elektroničkih dokaza, forenzičari se koriste alatima za usporedbu sadržaja uz pomoć neke od hash funkcija. Dva najčešće korištena algoritma u svim alatima ove namjene su MD5[95] i SHA1[96].

Svi prikupljeni elektronički dokazi moraju biti autentični, odnosno istovjetni, kao i u trenutku njihovog prikupljanja. Kako bi usporedili istovjetnost dokaza, možemo se koristiti hash funkcijama.

Svi forenzični alati za usporedbu sadržaja elektroničkih dokaza koriste se jednom od hash funkcija. Kako navode autori "termin *message digest* označava sažetak poruke (datoteke). Sažetak poruke dobiva se posebnim tzv. *hash* funkcijama, odnosno funkcijama za izračunavanje sažetka poruke. Ove funkcije zapravo sažimaju niz bitova poruke u niz bitova određene veličine (*hash value*). Kompresija se mora izvršiti na takav način da je zanemarivo mala vjerojatnost od neke druge poruke dobiti istom metodom isti sažetak. Tipična veličina sažetka poruke je 128, 160 ili 256 bita. U svijetu su se već standardizirale neke funkcije koje služe za dobijanje sažetaka. Najpoznatije su one iz skupine MD, a trenutno je u uporabi verzija hash funkcija - MD5. Također, iako se MD5 naširoko koristi ipak se počeo smatrati prilično nesigurnim. Ono što trenutačno još uvijek zauzima vrh sigurnosti su funkcije familija SHA-1

[93] Zakon o kaznenom postupku, članak 259.
[94] Zakon o kaznenom postupku, članak 263.
[95] MD5 algoritam razvio je 1991. godine Ronald L. Rivest s američkog sveučilišta MIT.
[96] Secure Hash Algorithm (SHA-1) je hash algoritam koji se koristi za računanje sažetka.

te RipeMD-160 koje još uvijek odolijevaju svim napadima kriptoanalitičara" (Protrka i Skakavac, 2012, str. 296).

Hash funkcija tada daje autentičnu informaciju o sadržaju za koji je. U računalnoj forenzičkoj analizi takve funkcije se koriste pri usporedbi istovjetnosti sadržaja, odnosno datoteka.

Dva najčešće korištena algoritma u svim alatima ove namjene su MD5 i SHA1, ali to nipošto ne znači da se ne mogu susresti drugi algoritmi kao što su MD2, MD4, Whirlpool, DSA i drugi. 32 bita duži sažetak SHA-1 algoritma je glavna prednost algoritama SHA-1 u odnosu na algoritam MD5.

Oba algoritma su relativno brza na 32-bitnim računalima. Međutim, zbog manjeg broja koraka MD5 se je pokazao za nijansu bržim od ostalih algoritama.

Prema CERT-u "poželjno je analizu dokaznih materijala provesti u kontroliranim uvjetima kakve pruža forenzički laboratorij ili neki drugi radni prostor takve namjene. Ako objektivne okolnosti nameću potrebu analize dokaza na mjestu pronalaska, prije pristupanja analizi, treba razmotriti vrijeme, materijalna sredstva i osoblje potrebno za takvu analizu te utjecaj na poslovanje ustanove u kojoj se provodi istraga" (Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2010-05-301, 2010).

Kako na tržištu postoje specijalizirani alati za ovu namjenu, tako postoje i određeni alati pod freeware licencom. Ukoliko se koristi isti algoritam, svi alati moraju dati isti rezultat hash funkcije, sažetak. Smatra se da nije potrebno objašnjavati kako komercijalni alati nude podršku za njihovo korištenje, te redovitu nadogradnju, dok je kod *freeware* alata namjena većinom usredotočena na samo jedan segment njihove primjene, te većinom ne postoji ažurnost u nadogradnji samog alata.

Za profesionalnu primjenu mnoga ministarstva i sigurnosne službe diljem svijeta koriste alat EnCase proizvođača Guidance Software. NATO koristi EnCase kao softver za forenzičke analize IT sustava.

3.4 Postupak kod prijave računalnog kriminala

Uporaba modernih tehnologija donosi određene sigurnosne rizike. Bez uporabe zaštitnih tehnologija (poput *firewalla* ili antivirusnog softvera), posjedujemo ranjivu opremu.

Ciljevi kriminalističkog istraživanja povodom prijave za računalni kriminal su:

- pribaviti dokaze koji ukazuju na počinjenje kaznenog djela,
- utvrditi identitet počinitelja,
- utvrditi identitet oštećene osobe/žrtve,
- utvrditi identitet eventualno drugih žrtava i počinitelja,
- privesti počinitelja.

Katulić još 2006. navodi da "kako bi olakšali postupanje istražiteljima, preporuča se prikupljanje što je moguće više elektroničkih zapisa, logova, koji će istražnim tijelima poslužiti u otkrivanju počinitelja. Ovdje se u prvom redu misli na firewall logove i druge sistemske zapise koji sadrže podatke o aktivnostima na koje se oštećenik žali. Prema odredbama Konvencije (2001), pružatelji usluga dužni su ustrojiti službe za obradu incidenata odnosno kibernetičkog kriminala. Ovo je samo kodifikacija prakse koju već godinama provodi veliki broj najvećih svjetskih ISP-ova. Isto tako, i hrvatski pružatelji internet usluga, kako komercijalni, tako i oni iz javnog sektora poput CARNeta, imaju organizirane slične službe, često kolokvijalno nazvane *Abuse* službama. Kao što smo naveli ranije, spomenuta Konvencija predviđa i obvezu pružatelja internet usluga da nadležnim tijelima učini dostupnima podatke o svom prometu. Prvi korak svakog korisnika koji sumnja da je postao žrtvom nekog od oblika kibernetičkog kriminala kontakt je s *Abuse* službom svog pružatelja internet usluga. Iako takve službe imaju ograničeno djelovanje, redovito zapošljavaju stručnjake koji će znati procijeniti ozbiljnost incidenta." (Katulić, 2006).

Zbog tehničke prirode interneta, mnoga kaznena djela iz domene računalnog kriminala mogu vrlo lako prerasti u postupke s međunarodnim elementom. Radnje koje treba poduzeti nakon saznanja, su u većini slučajeva:

- osigurati dokaze,
- utvrditi IP adrese ako je to potrebno i provjeriti kome pripadaju,
- izvršiti uvid u zbirke i registre TK operatera (davatelja Internet usluga),
- napraviti analizu dobivenih podataka uspoređujući ih s našim službenim evidencijama, bazama podataka ali i otvorenim izvorima na Internetu,
- ako je to potrebno zatražiti provođenje posebnih dokaznih radnji,
- zatražiti međunarodnu pomoć ukoliko je to potrebno,
- obaviti pretragu (stana, vozila, pokretnih stvari - računala, mobiteli i sl.),
- poduzeti po potrebi i druge radnje (prepoznavanje i sl.) *(Katulić, 2006)*.

3.4.1 Provođenje kriminalističkog istraživanja na temelju izvješća policijskog službenika o prikupljenim saznanjima

Korištenjem opisanih softverskih rješenja, policijski službenik prikuplja podatke koje počinitelj koristi za distribuciju na P2P (eng. *Peer to Peer*) mreži, vrijeme korištenja te IP (eng. *Internet Protocol*) adrese.

Do sada su IP adrese uglavnom bile dodjeljivane fiksnim nepokretnim priključcima zato što je neograničen internetski promet kakav traže P2P mreže bio moguć samo na njima. U posljednje vrijeme situacija na tržištu mobilnih usluga se mijenja pa tako sve više operatera nudi neograničen mobilni internetski promet, što će u budućnosti predstavljati problem, jer će biti teže locirati korisnika, pogotovo ako je riječ o prepaid korisniku. Nakon dobivenog podatka kome je bila dodijeljena IP adresa i izvješća policijskog službenika o prikupljenim saznanjima putem otvorenih javnih izvora, u suradnji s nadležnim Općinskim odvjetništvom od suca istrage traži se nalog za pretragu doma i drugih prostorija radi pronalaženja dokaza o počinjenju kaznenog djela, jer se smatra da se u tom stanu ili kući nalaze računalo i drugi mediji za pohranu digitalnih podataka na kojima se nalaze dokazi o počinjenju kaznenog djela iskorištavanje djece za pornografiju.

Hrestak navodi da "prilikom pretrage, osim oduzimanja računala, posebnu pozornost treba posvetiti traženju i drugih medija za pohranu podataka, poput vanjskih, prijenosnih tvrdih diskova, memorijskih stikova, optičkih medija, memorijskih kartica ali i drugih elektroničkih uređaja koji u sebi imaju ugrađenu mogućnost pohrane podataka. Osim toga potrebno je pažnju obratiti i na pronalaženje zabilješki s korisničkim imenima i lozinkama servisa za pohranu podataka u oblaku. Takvi servisi su vrlo pogodni za čuvanje ilegalnog sadržaja jer se nalaze na serverima koji su locirani diljem svijeta, a moguć im je pristup s bilo kojeg računala i u slučaju potrebe brisanje svih podataka" (Hrestak, 2017, str. 28).

Sve aktivnosti policije prije samog pokretanja kaznenog postupka skrivene su iza izvješća u kojem se samo navodi da je pretraživanjem otvorenih izvora, bez navođenja naziva programskih rješenja i načina funkcioniranja programa, otkriveno kako određena osoba na P2P mreži dijeli datoteke klasificirane kao dječja pornografija te da su toj osobi, tj. njegovom računalu, određenog dana bile dodijeljene određene IP adrese.

Sva ostala postupanja, kao što su pretraga doma i drugih prostorija te pretraga računala i medija za pohranu podataka se nakon toga provode temeljem naloga suca istrage, čime je u kasnijem tijeku postupka smanjen manevarski prostor braniteljima osumnjičenoga koji se više ne mogu pozivati na to da je policija poduzela neke neformalne radnje koje nije smjela poduzeti ili bi se takve radnje mogle pokušati prikazati kao nezakoniti dokazi. Još jedna od prednosti je u tome što policijski službenici s osumnjičenim ne dolaze u nikakav kontakt do samog trenutka provođenja pretrage i uhićenja, tako da osumnjičeni ni u jednom trenutku ne može znati niti posumnjati da su njegove ilegalne aktivnosti pod paskom policije, a samim time smanjuje se i mogućnost da će uništiti ili sakriti ilegalni materijal koji posjeduje.

S obzirom na to da se u ovom trenutku (2018. godina) cijene memorijskih kartica kapaciteta 8 GB do 128 GB kreću od 30 do 350 kuna, a veličinom su kao nokat lako se može predočiti koliko se tisuća fotografija i videozapisa može vrlo jednostavno i jeftino sakriti.

3.4.2 Provođenje kriminalističkog istraživanja na temelju datoteka preuzetih s računala osumnjičenika

Hrestak (2017) pojašnjava da bi drugi način kriminalističkog istraživanja bio "da se iskoriste mogućnosti softvera i da se od počinitelja preuzmu sumnjive datoteke. Sam tijek preuzimanja se postupno dokumentira te se takve datoteke kasnije mogu koristiti na sudu kao dokaz da je počinitelj distribuirao takve datoteke u kibernetičkom prostoru." Za ovakvo postupanje policije postoji zakonsko uporište u članku 12. *Zakona o policijskim poslovima i ovlastima (NN 76/2009)*, u kojem se navodi da "glavni ravnatelj ili osoba koju on ovlasti, u skladu sa zakonom, može pisanim nalogom odrediti prikrivanje policijskog posla." Prikrivanje se može odnositi na pravni posao, pravnu i fizičku osobu, tijelo državne vlasti i *sredstva komuniciranja*. Usprkos tome do sada se nije postupalo na taj način jer je neslužbeni stav Državnog odvjetništva Republike Hrvatske da ne postoji sudska praksa u takvim predmetima i nije do kraja definirano postupanje policije i način fiksiranja takvih dokaza, zbog čega se nastavilo s praksom da se kaznena djela istražuju na prvotno opisani način kojim je popis dijeljenih datoteka dječje pornografije dovoljan za pokretanje izvida i provođenja dokaznih radnji u cilju otkrivanja počinitelja kaznenog djela iskorištavanje djece za pornografiju.

Brnetić navodi da "za razliku od Hrvatske, druge zemlje, prvenstveno Sjedinjene Američke Države, koriste takve načine kriminalističkog istraživanja, te je u presudama njihovih sudova dokumentirano da prihvaćaju preuzete datoteke dječje pornografije kao dokaz u sudskom postupku". (Brnetić, 1996)

Odustajanje od takvog načina kriminalističkog istraživanja, u jednu ruku, ima dobre strane, barem što se tiče policije jer se reduciraju odlasci na sud, svjedočenja o tome kako funkcioniraju programi i dokazivanje da je u preuzimanju datoteka bilo sve legalno te da nisu narušena nikakva prava okrivljenika.

3.5 Vještačenje kibernetičkog kriminala

Iako istražitelji većinom koriste alate koji se primjenjuju u računalnoj forenzici, sva postupanja su u biti klasične pretrage i naknadna izrada analize sadržaja. U slučaju dvojbe o dokaznoj valjanosti pribavljenih dokaza, najčešće slijedi poduzimanje vještačenja na temelju zahtjeva stranke u postupku.

Ranijim osvrtom navedeno je da "rad stalnih sudskih vještaka u Republici Hrvatskoj definiran je Pravilnikom o stalnim sudskim vještacima.[97] Stalni sudski vještak je vrhunski stručnjak kojega odabire sud kako bi pomogao sudu svojim neovisnim i stručnim mišljenjem u skladu sa zadatkom vještačenja. Potrebno je napomenuti kako je rad sudskog vještaka ključni dio sudskog ili istražnog postupka i o njegovom nalazu često ovisi daljnji tijek postupka, njegovo pokretanje, ili, ukoliko se radi o mišljenju koje se traži tijekom postupka, čak i presuda. Nalaz sudskog vještaka mora biti napisan jasno, kako ne bi bilo dvojbi ili nejasnih situacija, te mora biti lišen od pretjerano stručnog jezika koji bi bio nerazumljiv sucu ili tijelu koje je vještačenje naručio. Vještak mora jasno ukazati na sve dvojbe koje je imao tijekom obavljanja vještačenja bez korištenja pretpostavki ili principa subjektivnog mišljenja" (Protrka, 2013, str. 297).

3.5.1 Pojam sudskog vještaka

Pravilnik određuje da je "stalni sudski vještak vrhunski stručnjak odabran od strane suda s liste sudskih vještaka kako bi mu pomogao neovisnim i stručnim mišljenjem u skladu sa zadatkom vještačenja."

[97] Pravilnik o stalnim sudskim vještacima, Narodne novine broj 38/2014.

Pravilnik spominje nekoliko najvažnijih uvjeta kao što s:u (Pravilnik o stalnim sudskim vještacima, 2014):

- "obrazovanje",
- "dokazano višegodišnje iskustvo na poslovima iz područja za koje aplicira",
- "izvršena stručna obuka",
- "stalno usavršavanje",
- "zdravstvena sposobnost",
- "osiguranje od profesionalne odgovornosti obavljanja posla sudskog vještaka",
- "nekažnjavanje".[98]

Stručna obuka kandidata obavlja se pod vodstvom imenovanog mentora, koji mora imati najmanje dva mandata iz određenog područja, što znači da je izradio veći broj vještačkih nalaza.

Pravilnik propisuje da "rad sudskog vještaka mora biti neovisan, visoko stručan, a obavlja se u skladu sa zadatkom vještačenja koji definira nadležno tijelo, najčešće sudac. Sudski vještak podložan je polaganju zakletve prije imenovanja". Temeljnih pet načela sudskog vještaka su:

- "načelo ponašanja - vještak mora obaviti posao stručno, pošteno, istinoljubivo, angažirano - mora biti osoba u koju se možemo potpuno pouzdati";
- "načelo odgovornosti - vještak smije preuzeti samo one poslove za koje smatra da će ih obaviti na stručno besprijekoran način";
- "načelo povjerenja - vještak treba prihvaćati obveze na način koji služi javnom interesu, poštivati povjerenje javnosti i biti predan svojem zanimanju";
- "načelo vjerodostojnosti - vještaci moraju obavljati radne obveze na što vjerodostojniji način kako bi zadržali i dodatno učvrstili javno povjerenje";
- "načelo profesionalne pažnje, odnosno stručnosti - vještak mora poštivati profesionalna i etička načela, standarde, mora neprekidno usavršavati svoje znanje, podizati kvalitetu usluga i ulagati sve svoje snage u obavljanje poslova".

[98] Pravilnik o stalnim sudskim vještacima, čl. 2

Prema pravnim propisima Republike Hrvatske, sudski vještaci se smatraju jednim od dokaznih sredstava. Široko uvriježeni izraz "stručni svjedok" ne prihvaća se u hrvatskoj doktrini jer se stručnjak ne smatra svjedokom. Vještak nije svjedočio činjenici nekim od svojih osjetila, već umjesto toga daje mišljenje temeljem svog stručnog znanja nakon što se činjenica dogodila (ili se navodno dogodila). Ipak, uloga vještaka može biti presudna na sudu, posebno u slučajevima dokazivanja uz pomoć dokaza u digitalnom obliku. To stoga što suci u pravilu nemaju dostatna znanja za procjenu vjerodostojnosti (ako je u pitanju autentičnost) elektroničkih dokaza ili ne razumiju u cijelosti njihov sadržaj. Premda sud nije vezan uz stručno mišljenje vještaka, praksa pokazuje da je ovakvo postupanje široko prihvaćeno (Kunštek i Pavišić, 2008, str. 127).

3.5.2 Djelatnosti i dužnosti sudskog vještaka

Aksentijević navodi da "sudski predmeti koji se tiču računalnog kriminala izrazito su složeni, djelomično zato što je materija takve prirode, djelomično stoga što je samom sucu, odnosno naručitelju vještačenja teško definirati zadatak vještačenja. Ono što je predmetnom stručnjaku vrlo jasno, laiku može biti izrazito nejasno ili kompliciranо. Stoga je temeljna zadaća sudskog vještaka iz područja informatike ili telekomunikacija u suradnji sa sucem jasno razraditi koji je točno zadatak vještačenja, a zatim izraditi cjelovito mišljenje u skladu sa zadatkom, orijentirajući se samo na zadatak i koristeći isključivo zadužene materijale, bez donošenja subjektivnih stavova, špekulacija ili hipotetskog mišljenja. Vještačenja iz područja informatike dijelom mogu postati i multidisciplinarna vještačenja. Zbog širine područja koja pokriva, informatika zadire u informatičku forenziku, telekomunikacije, računalne i mrežne sustave i zasigurno je teško jednoj osobi biti apsolutni stručnjak u svim navedenim područjima." (Aksentijević, 2013).

Iz tih razloga, i radi lakšeg snalaženja prilikom imenovanja vještaka, postoje strukovne sekcije područja djelatnosti sudskih vještaka u tablici 6.

Agronomija	Kompjuterizacija
Aktuaristika	Krivotvoreni novac
Arheologija	Likovna kultura
Arhitektura	Lovstvo
Brodostrojarstvo	Medicina - klinička
Carinsko poslovanje	Medicina - sudska
Defektologija	Pomorstvo
Devizno poslovanje	Promet - vozila - motori
Doziometrija ionizirajućeg zračenja	Psihologija
Drago kamenje, dijamanti - zlatarstvo	Rukopisi
Elektronika - elektrotehnika - automatika	Sanitarna ispitivanja
Elektrotehnika - nautika	Sigurnost na radu
Fizikalna ispitivanja	Stolarstvo
Gemologija	Stomatologija
Geodezija	Strojarstvo - postrojenja
Gospodarstvo	Šumarstvo
Graditeljstvo	Telefonija
Glazbarstvo	Telekomunikacije - informatika
Kemija - toksikologija	Tekstil - koža - obuća
Kemijsko inžinjerstvo	Tisak
Knjigovodstvo - financije – ekonomika	Zaštita na radu
Knjižnički fondovi - izvornost tekstova	Zrakoplovstvo

Tablica 6 - Strukovne sekcije sudskih vještaka

Izvor: (Hrvatsko društvo sudskih vještaka i procjenitelja, 2017)

Vještačenja iz područja računalnog kriminala obavljaju sudski vještaci koji su vještaci za informatiku, a u zadnje vrijeme pojavom računalnog kriminala i multidisciplinarna vještačenja specijalnosti "telekomunikacije" i "informatika".

Aksentijević dalje navodi da "sudac koji je naručio vještačenje zasigurno je laik i traži pojašnjenje. Stoga je vještak pod jakim pritiskom izraditi mišljenje koje će nedvojbeno biti jasno i dati dovoljnu podlogu sucu za nastavak postupka. Pritom je potrebno imati na umu kako se sudski vještak redovito u procesnom postupku poziva na glavnu raspravu kako bi iznio svoje mišljenje. Ovisno o tome kakav je njegov nalaz i kakav je predmet, njegovo mišljenje različitim argumentima mogu propitivati kako sudac, tako i okrivljenik, odnosno njegov odvjetnik. U slučaju da su termini nedovoljno jasno objašnjeni i da je nalaz napisan nedovoljno jasno, te da slijed nalaza nije logički jasan i dobro objašnjen, moguće je pobiti nalaz ili zatražiti novo vještačenje, što sve produžuje sudski proces, utječe na troškove i naposljetku baca sjenu na stručnost vještaka i čitave struke. Dužnost čuvanja tajne obvezuje vještaka da ne daje obavijesti o onom što je saznao prigodom vještačenja iz spisa, na raspravi ili na drugi način, nikome osim naručitelju vještačenja. Nalaz i mišljenje sudskog vještaka mora sadržavati točan i potpun prikaz svih utvrđenih činjenica, primijenjenih metoda u postupku vještačenja, svih rezultata istraživanja i treba biti razumljiv" (Aksentijević, 2013).

3.5.3 Prikupljanje podataka za vještačenje

Izrazito je važno da svi dokazi budu pribavljeni u skladu s relevantnim zakonima, jer će u protivnom istražni sudac dokaze pribavljene nesukladno izuzeti iz spisa i na njima neće biti temeljeno niti vještačenje niti ostale procesne radnje.

Nadležne osobe istražnog centra obavljaju primarnu pretragu opreme i u popratnoj dokumentaciji ukazuju na činjenice od značaja za pokretanje kaznenog postupka. Policijski djelatnici su najčešće prva "stručna linija" koja obrađuje ovakve slučajeve.

Te nadležne osobe nisu ujedno i stručne osobe koje daju konačno meritorno mišljenje o činjenicama vezanim uz način eventualnog počinjenja djela. Istražni sudac ovaj posao prepušta sudskom vještaku iz područja informatike, telekomunikacija i kibernetičkog kriminala, kojega sud uzima kao stručnu osobu od povjerenja, vrhunskog znalca svoje struke, temeljem kojega se mogu donositi sudske odluke.

Tijekom postupka vještačenja, sudski vještak u skladu s nalogom suda mora napraviti nalaz u odnosu na postavljene zadatke vještačenja. Datoteke elektroničkih (digitalnih) dokaza prikazuju stanje u trenutku oduzimanja od potencijalnog okrivljenika, dok se pitanja suca često odnose na povijesne trenutke. Ponekad sudski vještak ne može doći do tragova koji su mu potrebni jer ih nema, nisu dostupni, sakriveni su, uništeni ili organizacije odnosno ustanove koji ih imaju ne žele surađivati.

U tom slučaju, sudski vještak se ne smije upustiti u nagađanje i mišljenje mora temeljiti na činjenicama, čak i kada je iz iskustva, indicija ili akumuliranog stručnog znanja posve siguran u nešto o čemu nema konkretno dokazivih tragova.

Koristeći razne alate i metode koji su sastavni dio njegovog stručnog djelovanja, sudski vještak se mora koncentrirati na postavljeni zadatak vještačenja i nepristrano dati svoje stručno mišljenje.

Prema tome, sudski vještak iz područja informatike ili kibernetičkog kriminala mora se orijentirati primarno na činjenice iz svoje struke i postaviti jasne ograde prema iznošenju bilo kakvih činjenica ili stavova koji nisu nedvojbeno dio njegovog stručnog područja. (Protrka, 2013).

Temeljem nalaza vještaka, sud može pokrenuti ili odbaciti kazneni postupak, stoga je jasno kako je nalaz najvažniji temelj putem kojega sud donosi svoju odluku. Tijekom postupka, vještačenje sudskog vještaka iz područja informatike, telekomunikacija i kibernetičkog kriminala može biti prihvaćeno ukoliko je napravljeno nedvojbeno stručno, čime se štedi novac ali i vrijeme procesnog postupka. Naime, dobro obavljen posao cijelog lanca, od prikupljanja dokaza do vještačenja, je izrazito važan.

Profesionalna je dužnost sudskog vještaka iz područja informatike, telekomunikacija i kibernetičkog kriminala nikada ne kontaminirati dokazni materijal, odnosno oduzete medije, tvrde diskove i opremu svojim forenzičkim radnjama. Ponekad je vještaku vrlo teško obaviti uvid i analizu bez mijenjanja primarnog sadržaja.

Prema Matijeviću "kako bi vještačenje imalo dobar temelj, u samome sudskom postupku nužno je prikupiti sve potrebne podatke, koji moraju biti na raspolaganju vještaku u cilju izrade potpunog i jasnog nalaza i mišljenja" (Matijević, 2010).

3.5.4 Uloga sudskog vještaka za računalni kriminalitet

Autor je već ranije naveo da je "vještačenje elektroničkih dokaza računalnog kriminala proces koji uključuje analizu i korelaciju više vrsta podataka na različitim razinama. Svrha i vrijednost analize je ta da proučimo različite tipove podataka i zatim ih pretvorimo u korisne informacije. Kod prikupljanja elektroničkih dokaza potrebno je odrediti računala ili medije koja su predmet istraživanja, sačuvati originalne medije i spriječiti bilo kakve izmjene sadržaja medija, ako je računalo uključeno, preuzeti sadržaj radne memorije (Random Access Memory - RAM), isključiti računalo bilo redovnim putem bilo isključivanjem napajanja, napraviti kopiju svih bitnih medija, te obaviti forenzičku analizu na kopijama - slikama medija (*image*)" (Protrka, Računalna forenzička analiza: Istovjetnost sadržaja CD medija - specijalistički rad, 2009, str. 47).

3.5.5 Nalaz i mišljenje sudskog vještaka

Aksentijević navodi da "u uvodnom dijelu vještačkog nalaza i mišljenja navode se neizostavno vrsta i predmet vještačenja, te temeljem koje dokumentacije je ono izvedeno i po čijem nalogu. Tijekom izrade nalaza temeljna je aktivnost prikupljanja relevantnih činjenica koje podrazumijeva nedvojbeno definiranje postupka i zadatka vještačenja, razmatranje predmeta, teme ili procesa vještačenja, prikupljanje i analizu relevantne dokumentacije, razgovor s osobama koje mogu dati važne informacije za pravilno zaključivanje o činjenicama iz zadatka vještačenja i neposredna opažanja vezano uz predmet vještačenja. Taksativno se navode sve primijenjene strukovne metode i postupci. Po izradi nalaza vještačenja, vještak izvodi zaključak u obliku vještačkog mišljenja, koji sintetizira uzroke, djelovanje, posljedice i značaj određenih činjenica, uz dužnu pažnju, savjesno i sukladno pravilima određene znanstvene discipline (struke) ili vještine. Mišljenje vještaka mora biti neovisno, objektivno, potkrijepljeno činjenicama, deskriptivno, nedvojbeno i logički izloženo" (Aksentijević, 2013).

Matijević zaključuje da je "vještak dužan odgovoriti na pitanja suca i stranaka u postupku vezano uz činjenično stanje utvrđeno njegovim nalazom i mišljenjem, ali i na druga pitanja koja sudac dozvoli ili ocijeni potrebnim u cilju utvrđenja stvarnog činjeničnog stanja. Nalaz vještaka mora biti napisan jednostavnim rječnikom kako bi bio razumljiv sucu i strankama u postupku, mora biti jasan, logičan i sveobuhvatan, ne smije sadržati greške, primijenjene metode i postupci moraju biti obrazloženi, a svi dokazi brižljivo i valjano proučeni. U slučaju valjanih žalbenih razloga sudac može odrediti dopunu vještačenja ili povjeriti vještačenje drugom vještaku. Ukoliko je činjenično stanja utvrđeno po drugom vještaku drugačije u svojim bitnim elementima, vještaci svoje nalaze trebaju uskladiti na raspravi i objasniti sudu u čemu su razlike." (Matijević, 2010).

Zaključak koji se navodi je "stoga je obveza, ali i dužnost stalnog sudskog vještaka, biti u stalnom kontaktu sa stručnjacima na navedenim područjima kako bi mogao potražiti dodatno neovisno mišljenje, ali i jasno obavijestiti naručitelja vještačenja o tome" (Protrka, 2013).

Nakon nedovoljno odrađenog ili nepotpunog nalaza i mišljenja, sud traži dopunsko vještačenje ili čak određuje novo vještačenje od strane drugog vještaka, što produžuje rok sudskog postupka i povećava trošak samog postupka (Protrka, 2013, str. 299).

4. REZULTATI ISTRAŽIVANJA I RASPRAVA

Istraživanje je obuhvatilo tri različita područja:

- *Komparativni prikaz pravne regulative u odabranim državama po pitanju kibernetičkog kriminala ("Savezna Republika Njemačka", "Republika Austrija", "Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske", "Kraljevina Švedska", "Rumunjska" i "Republika Slovenija");*
- *Opseg, struktura i kretanje kriminaliteta počinjenog putem računalnih sustava za Republiku Hrvatsku u razdoblju od 2013. do 2017. godine (podaci "Državnog zavoda za statistiku Republike Hrvatske"[99] i "Ministarstva unutarnjih poslova Republike Hrvatske");*
- *Kvalitativna i kvantitativna analiza pojmova Cyberspace i Cybercrime (pomoću računalnog programa NVivo).*

4.1 Komparativni prikaz pravne regulative u odabranim državama po pitanju kibernetičkog kriminala

Uvid u kaznenopravne sustave država prikazuje načine inkriminiranja koja čine kaznena djela računalnog kriminaliteta. Pravni poretci različitih država na različite načine rješavaju slične ili iste nedozvoljene radnje. O'Donnel navodi da "iako inicijative poput *Konvencije* pokušavaju ujednačiti propise zemalja potpisnica, uspjeh gotovo nikad nije stopostotan" (O'Donnell, 2000).

Analiza normi pozitivnog zakonodavstva *de lege lata* prikazuje inkriminacije u užem smislu, kod kojih se unutar bića kaznenog djela pojavljuje računalni sustav, računalni podatak, računalni program i slično jer su upravo ovi pojmovi predmet rasprave (Katulić, 2006).

[99] DZS Republike Hrvatske, Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita, Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude
https://www.dzs.hr/, stranica posjećena 30. kolovoza 2017.

Kao što je definirano i u Konvenciji u članku 35., a vezano za mrežu u neprekidnom pogonu, tako su i sve zemlje potpisnice bile dužne implementirati nacionalne kontakt točke za suzbijanje kaznenih djela računalnog kriminaliteta.

Kako postoji različita pravna regulativa u pojedinoj zemlji, tako je specifičan način suradnje između nacionalnih kontakt točki za borbu protiv računalnog kriminaliteta, a to je najbrži put za suradnju.

Pravne odredbe kaznenih zakona europskih zemalja bit će izvorno prenesene na engleskom ili njemačkom jeziku, a prikaz članaka zemalja iz jugoistočne Europe biti će na jednom od njihovih službenih jezika ili engleskom jeziku.

U ovom dijelu razmatrani su pravni sustavi nekoliko europskih zemalja. Pravni sustav Velike Britanije svakako je važan u poredbenom pregledu stranog prava. (Valeri, Somers, Robinson, Graux i Dumortier, 2006).

Nadalje, uključena je i Švedska, zbog velike rasprostranjenosti interneta, kao i zbog visokog stupnja *e-governmenta*.[100]

Prikazuje se i zakonodavstvo Rumunjske zbog značajnog broja *hackera*, a i zbog nekoliko slučajeva računalnih prijevara, računalnih krivotvorenja, s obzirom na pojavnost vršenja ove vrste kaznenih djela na području Republike Hrvatske od strane rumunjskih državljana.

Valja napomenuti je da su od navedenih zemalja Konvenciju ratificirali Austrija, Njemačka, Velika Britanija, dok je Švedska potpisala, ali je još nije ratificirala.

[100] "Digital agenda for Europe", http://ec.europa.eu/digital-agenda/life-and-work/public-services, stranica posjećena 17. studenog 2017.

4.1.1 Savezna Republika Njemačka

Kazneno pravo u vezi s računalnim kriminalitetom u Njemačkoj se svodi na sljedeće pravne izvore:

- *"Kazneni zakon" (Strafgesetzbuch, StGB) (Bundesrepublik Deutschland - Strafgesetzbuch Deutschland (StGB), 2017);*
- *"Drugi Zakon o sprječavanju gospodarskog kriminaliteta (Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat, 2.WiKG)";*

U njemačkom Kaznenom pravu sadržana su sljedeća kaznena djela povezana s računalnim kriminalitetom:

- *"Ausspähen von Daten" (§ 202a StGB) - krađa podataka;*
- *"Abfangen von Daten" (§ 202b StGB) - neovlašteno presretanje podataka;*
- *"Vorbereiten des Ausspähens und Abfangens von Daten" (§ 202c StGB) - pripremne radnje za krađu i presretanje podataka;*
- *"Computerbetrug" (§ 263a StGB) - računalna prijevara;*
- *"Fälschung beweiserheblicher Daten" (§ 269 StGB) - računalno krivotvorenje;*
- *"Täuschung im Rechtsverkehr bei Datenverarbeitung" (§ 270 StGB) - računalna prijevara u pravnim odnosima;*
- *"Datenveränderung" (§ 303a StGB) - neovlaštena promjena podataka;*
- *"Computersabotage" (§ 303b StGB) - ometanje rada računala.*

Kaznena djela iz § 202a, § 202b, § 202c nalaze se u glavi kaznenih djela protiv privatnosti i tajnosti, a kazneno djelo § 263a u glavi kaznenih djela prijevare i pronevjere, kaznena djela § 269, § 270 u glavi kaznenih djela krivotvorenja, a § 303a i § 303b u glavi kaznenih djela materijalnih šteta. (Katulić, 2006)

Kazneno djelo iz članka *(§ 202a)*[101] odnosi se na onoga tko protupravno prikuplja podatke za sebe ili drugoga, a da nisu bili namijenjeni za njega i bili su posebno zaštićeni od neovlaštenog pristupa, te je zaobiđena zaštita, kaznit će se "kaznom zatvora do tri godine ili novčanom kaznom", dok se kazneno djelo iz članka *(§ 202b)*[102] odnosi na neovlašteno presretanje podataka (*phishing*), koji podaci nisu namijenjeni određenoj osobi, a kazna u tom slučaju je do dvije godine zatvora ili novčana, osim ako za djelo nije propisana veća kazna nekom drugom odredbom.

Pripremne radnje za počinjenje kaznenih djela iz članaka § 202a i § 202b su kažnjive u članku *(§ 202c)*[103] "kaznom zatvora do jedne godine ili novčanom kaznom", a tu spadaju izrade:

- *lozinki i drugih sigurnosnih kodova koji omogućavaju pristup podacima,*
- *softver radi počinjenja tog djela.*

Računalna prijevara iz članka *(§ 263a)*[104] sankcionira onoga tko s namjerom pribavljanja za sebe ili treću osobu, protupravne imovinske koristi, neovlašteno uporabi podatke, neovlašteno utječe na tijek obrade podataka ili pribavi korist korištenjem netočnih ili nepotpunih podataka, bit će kažnjen "kaznom zatvora do pet godina ili novčanom kaznom".

Ista kazna je predviđena i za kazneno djelo *(§ 269)*[105] i za kazneno djelo *Täuschung im (§ 270)*[106], odnosno o računalnoj prijevari pravno relevantnih podataka i prijevari kod pravnih odnosa.

Tekst članka *(§ 303a)*[107] odnosi se na oštećenje računalnih podataka na način da ih počinitelj obriše, sakrije, učini nedostupnima ili ih promijeni, "kaznit će se kaznom zatvora do dvije godine ili novčanom kaznom", dok je sam pokušaj kažnjiv.

[101] § 202a StGB Ausspähen von Daten.
[102] § 202b StGB Abfangen von Daten.
[103] § 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten.
[104] § 263a StGB Computerbetrug.
[105] § 269 StGB Fälschung beweiserheblicher Daten.
[106] § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung.
[107] § 303a Datenveränderung.

Kazneno djelo računalne sabotaže iz članka *(§ 303b)*[108] odnosi se na ometanje rada računalnog sustava i ometanje računalne obrade podataka kada počinitelj:

- *počini kazneno djelo iz § 303a,*
- *počini kazneno djelo iz § 202a, s namjerom nanošenja štete,*
- *uništi, ošteti, učini neupotrebljivima, onemogući u daljnjem radu sustav za obradu podataka ili sam nosač podataka.*

Zapriječena kazna je "kazna zatvora do tri godine ili novčana kazna", a za kvalificirani oblik je propisana "kazna zatvora do pet godina". Pokušaj je kažnjiv.

Predmetna kaznena legislativa Njemačke ne može se doslovno usporediti s kaznenim okvirom Hrvatske, ali može se predložiti okvirna usporedba radi lakšeg poimanja inkriminacije kaznenog djela, kao što je vidljivo u tablici 7.

Hrvatska	**Njemačka**
Neovlašteni pristup (članak 266.)	Ausspähen von Daten (§ 202a StGB)
Ometanje rada računalnog sustava (članak 267.)	Computersabotage (§ 303b StGB)
Oštećenje računalnih podataka (članak 268.)	Datenveränderung (§ 303a StGB)
Neovlašteno presretanje računalnih podataka (članak 269.)	Abfangen von Daten (§ 202b StGB)
Računalno krivotvorenje (članak 270.)	Fälschung beweiserheblicher Daten (§ 269 StGB)
Računalna prijevara (članak 271.)	Computerbetrug (§ 263a StGB)
Zloporaba naprava (članak 272.)	Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)

Tablica 7 - Istoznačnice kaznenih djela kaznenih zakona Hrvatske i Njemačke

[108] § 303b StGB Computersabotage.

4.1.2 Republika Austrija

Sukladno suradnji austrijskih s njemačkim stručnjacima na području kaznenog prava, otprilike u isto vrijeme devedesetih godina prošlog stoljeća načinjene su izmjene kaznenog zakonodavstva u koje su uvrštena i kaznena djela računalnog kriminaliteta.

U austrijskom Kaznenom zakonu se nalaze sljedeće kažnjive odredbe povezane s računalnim kriminalitetom (Republik Österreich - Strafgesetzbuch Österreich (StGB), 2017):

- *Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB) - neovlašteni pristup računalnom sustavu;*
- *Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) - povreda tajnosti komunikacija;*
- *Missbräuchliches Abfangen von Daten (§ 119a StGB) - neovlašteno presretanje podataka;*
- *Datenbeschädigung (§ 126a) - oštećenje podataka;*
- *Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) - ometanje rada računalnog sustava;*
- *Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB) - zloporaba računalnih programa ili podataka;*
- *Betrügerischer Datenverarbeitungsmissbrauch (§ 148a) - prijevarna zloporaba obrade podataka;*
- *Datenfälschung (§ 225a StGB) -računalno krivotvorenje.*

Kaznena djela iz § 118a, § 119, § 119a nalaze se u glavi kaznenih djela protiv privatnosti i tajnosti, a kaznena djela § 126a, § 126b, § 126c i § 148a u glavi kaznenih djela protiv imovine, dok je § 225a u glavi kaznenih djela krivotvorenja (Katulić, 2006).

Kazneno djelo iz članka *(§ 118a)*[109] odnosi se na neovlašteni pristup računalnim podacima u računalnom sustavu koji nisu bili namijenjeni za javno korištenje i na taj način te podatke koristi, čini dostupnima drugome ili sebi za stjecanje imovinske koristi, na način da je zaobišao zaštitu, može se kazniti "kaznom zatvora do šest mjeseci ili novčanom kaznom".

[109] § 118a StGB Widerrechtlicher Zugriff auf ein Computersystem.

Progon se pokreće po prijedlogu, a ukoliko se radi o zločinačkoj organizaciji, onda je predviđena kazna do tri godine zatvora. Ovo kazneno djelo vuče paralelu s njemačkim zakonom i člankom § 202a.

Članak *(§ 119)*[110] i *(§ 119a)*[111] odnosi se na neovlašteno presretanje računalnih podataka, s time da se u § 119 govori o javnoj telekomunikaciji, dok se u § 119a govori o računalnim podacima na računalnom sustavu oštećenika.

Biće kaznenog djela sastoji se u tome da počinitelj neovlašteno prikuplja podatke za sebe ili drugoga, a nisu bili namijenjeni za njega i bili su posebno zaštićeni od neovlaštenog pristupa, te je zaobiđena zaštita. Predviđena kazna je "kazna zatvora do šest mjeseci ili novčana kazna".

Odredba članka *(§ 126a)*[112] je istovjetno kazneno djelo iz Kaznenog zakona Hrvatske iz članka 268. koje se odnosi na oštećenje računalnih podataka, a zapriječena kazna je do šest mjeseci zatvora ili novčana kazna. Kvalificirani oblik se odnosi na materijalnu štetu počinjenu ovim kaznenim djelom ako je veća od 3000 €, te je tada zapriječena kazna zatvora do dvije godine, a ukoliko je kazna preko 50000 € ili je djelo počinjeno u sklopu zločinačke organizacije, tada kazna zatvora može biti od šest mjeseci do pet godina.

Kazneno djelo iz članka *(§ 126b)*[113] odnosi se na ometanje rada računalnog sustava pri čemu je zapriječena "kazna zatvora do šest mjeseci ili novčana kazna". Kvalificirani oblik odnosi se na dugotrajni poremećaj u radu računalnog sustava, a predviđene kazne su iste kao i u kvalificiranom dijelu članka § 126a.

Kazneno djelo *(§ 126c)*[114] izravno kompariramo s kaznenim djelom iz čl. 272. hrvatskog Kaznenog zakona, a radi se o zloporabi naprava kako bi se neovlašteno izvršila kaznena djela § 118a, § 119, § 119a, § 126a, § 126b,§ 148a. U inkriminirane radnje spadaju izrada, uvoz, distribucija, prodaja, prilagodba računalnog programa, lozinki ili sličnih podataka koji omogućuju pristup računalnom sustavu ili računalnim podacima.

Kazneno djelo iz članka *(§ 148a)*[115] možemo usporediti s kaznenim djelom računalne prijevare, s time da se u § 148a govori o imovinskoj koristi kao rezultatu računalne prijevare

[110] § "119 StGB Verletzung des Telekommunikationsgeheimnisses."
[111] § "119a StGB Missbräuchliches Abfangen von Daten."
[112] § "126a StGB Datenbeschädigung."
[113] § "126b StGB Störung der Funktionsfähigkeit eines Computersystems."
[114] § "126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten."
[115] § "148a StGB Betrügerischer Datenverarbeitungsmißbrauch."

kod obrade računalnih podataka. Kvalificirani oblik se kažnjava od jedne do deset godina zatvora.

Računalno krivotvorenje iz članka *(§ 225a)*[116] opisuje klasični način računalnog krivotvorenja mijenjanjem, brisanjem ili promjenom računalnih podataka, a kažnjivo je do godinu dana zatvora.

Komparativna usporedba članaka kaznenog pravnog okvira Austrije ne može se doslovno usporediti s kaznenim okvirom Hrvatske, ali može se predložiti okvirna usporedba radi lakšeg poimanja inkriminacije kaznenog djela, što je vidljivo u tablici 8.

Hrvatska	**Austrija**
Neovlašteni pristup (članak 266.)	Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)
Ometanje rada računalnog sustava (članak 267.)	Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)
Oštećenje računalnih podataka (članak 268.)	Datenbeschädigung (§ 126a)
Neovlašteno presretanje računalnih podataka (članak 269.)	Missbräuchliches Abfangen von Daten (§ 119a StGB)
Računalno krivotvorenje (članak 270.)	Datenfälschung (§ 225a StGB)
Računalna prijevara (članak 271.)	Betrügerischer Datenverarbeitungsmissbrauch (§ 148a);
Zloporaba naprava (članak 272.)	Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)

Tablica 8 - Istoznačnice kaznenih djela kaznenih zakona Hrvatske i Austrije

[116] § "225a StGB Datenfälschung, Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen."

4.1.3 Velika Britanija

Zakonski propis koji je referentan u odnosu na kaznena djela računalnog kriminaliteta za područje Velike Britanije nosi naziv *Computer Misuse Act* koji je donesen 1990. godine (Parliament of the United Kingdom, 2017).

Navedeni zakon sadrži samo tri odredbe koje regulirajusva moguća računalna kaznena djela, budući da se *common law* sustav razlikuje od sustava kontinentalnog prava, što je slučaj i sa Sjedinjenima Američkim Državama i drugim državama Commonwealtha, što znači da konkretni doseg zakonske regulative ovisi o sudovima koji ga primjenjuju i njihovim odlukama (presedanima) koji su bitan, tvorni izvor prava (Katulić, 2006).

Zakon je izmijenjen i dopunjen 1. listopada 2007. godine kako bi se dodatno prilagodio Konvenciji. Iako kaznena djela nisu sistematizirana kao u Konvenciji, način na koji su kaznene radnje inkriminirane u navedenom Zakonu zadovoljava sve potrebe na kaznenopravnoj razini.

S obzirom na specifičnosti suđenja u Velikoj Britaniji, razlikujemo tri vrste kaznenih djela što je uvjetovano povijesnim razvojem nastanka bića pojedinog kaznenog djela i načina suđenja za pojedino kazneno djelo:

a) *optuživa kaznena djela (indictable offences),*
b) *sumarna kaznena djela (summary offences),*
c) *djela sudiva na oba načina (offences triable either way).*

Optuživa kaznena djela su sva djela utvrđena posebnim zakonima ili prema *common lawu*, kojima sude suci uz sudjelovanje porote u redovnom postupku i kad je potrebno podizanje optužnice.

Za kaznena djela propisana parlamentarnim zakonima sudi se bez porote i nije potrebno podizanje formalne optužnice pa se nazivaju sumarnim kaznenim djelima. (Brnetić, 1996, str. 212-216)

Za kaznena djela sudiva na oba načina, propisano je da se mogu suditi u redovnom ili sumarnom postupku zakonom koji propisuje samo djelo i Zakonom o magistratskim (prekršajnim) sudovima (*The Magisters Court Act*), kao što su djela iz zakona naslovljenog kao *Computer Misuse Act.*

U ovakvim slučajevima, nakon saslušanja stranaka, najprije se odlučuje na koji će se način suditi. Kad se optuženik upućuje na sumarni ili skraćeni postupak, od njega se traži privola jer je svakom građaninu općenito zajamčeno pravo na suđenje pred porotom. U slučaju da je magistrat proveo skraćeni postupak u kojem je utvrdio da ne može izreći kaznu jer bi kazna bila veća od ovlasti za kažnjavanje magistrata (12 mjeseci zatvora ili novčana kazna za Englesku i Wales, a 6 mjeseci i novčana kazna za Škotsku), tada će optuženika uputiti u redovni postupak radi izricanja kazne, dakle, u ovim slučajevima magistrat praktično vodi pripremni postupak. Najveći broj kazneneih djela u Velikoj Britaniji vodi se po skraćenom postupku.

U Britanskom zakonu o zlouporabi računala - *Computer Misuse Act* navedeni su sljedeći članci:

1. "*Unauthorised access to computer material"* - neovlašteni pristup računalnim podacima.

2. "Unauthorised access with intent to commit or facilitate commission of further offences" - neovlašteni pristup s namjerom počinjenja ili olakšanja počinjenja kaznenih djela.

3. "Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc." - neovlašteno postupanje u cilju ometanja rada računalnog sustava.

3A. "Making, supplying or obtaining articles for use in offence under section 1 or 3" - izrada, nabavljanje ili omogućavanje izvršenja kaznenih djela 1-3.

Prvi članak pod nazivom *Unauthorised access to computer material*[117] definira kazneno djelo neovlaštenog pristupa računalnom sustavu ili računalnim podacima.

Inkriminacija uključuje klasični hakerski napad koji se može odnositi i na pristup računalnim podacima bez dopuštenja kao što je elektronička pošta. Namjera ne treba nužno biti usmjerena na određeni računalni program.

Neovlašteni pristup računalnim podacima se široko definira u članku 17. navedenog Zakona u kojemu se navodi da neovlašteni pristup podrazumijeva "mijenjanje ili brisanje podataka, njihovo kopiranje ili premještanje na drugi medij za pohranu, korištenje ili ispisivanje s računala, pa čak i sami prikaz na monitoru."[118]

[117] "Computer Misuse Act 1990, Unauthorised access to computer material."
[118] "Computer Misuse Act 1990, Interpretation. Section 17."

Predviđena kazna za počinitelja sumarnog kaznenog djela iz ovog članka je zatvor do godinu dana ili novčana kazna, ukoliko je počinitelj iz Engleske i Walesa, a ako je počinitelj iz Škotske, tada je predviđena "kazna zatvora do šest mjeseci ili novčana kazna", dok je propisana kazna u postupku pred porotom "do dvije godine zatvora ili novčana kazna" ili oboje.

Kaznena djela koja su sadržana u članku broj 2. pod nazivom "*Unauthorised access with intent to commit or facilitate commission of further offences*"[119] govore o kvalificiranim kaznenim djelima iz prvog članka, jer je sam uvjet da postoji počinjeno kazneno djelo iz prvog članka.

Inkriminacija djela uključuje namjeru počinitelja da počini kazneno djelo iz članka 1. ili da izvrši ili pomogne u izvršavanju bilo kojeg kaznenog djela za koje postoji zapriječena kazna.

Najčešći primjer ovog kaznenog djela u Velikoj Britaniji odnosi se na tzv. *keylogger* programe ili naprave, koje, inače, služe kako bi zabilježile koje su tipke pritisnute na tipkovnici (računala ili bankomata), a sve u svrhu kako bi počinitelj došao do lozinke ili PIN broja.[120]

Predviđena kazna za počinitelja sumarnog kaznenog djela iz ovog članka je zatvor do godinu dana ili novčana kazna, ukoliko je počinitelj iz Engleske i Walesa, a ukoliko je počinitelj iz Škotske, predviđena je "kazna zatvora do šest mjeseci ili novčana kazna", dok je kazna u postupku pred porotom do "pet godina zatvora ili novčana kazna" ili oboje.

Treći članak pod nazivom "*Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.*"[121] bitno je promijenjen u izmjenama i dopunama iz 2007. godine, opisuje ometanje rada računalnog sustava i oštećenje računalnih podataka, odnosno računalnu sabotažu, a najčešći primjer je DDoS napad. Namjera počinitelja također ne treba biti usmjerena na određeni računalni program ili računalni podatak.

[119] Computer Misuse Act 1990, Interpretation. Section 2, Unauthorised access with intent to commit or facilitate commission of further offences.
[120] Sun, 03.08.2007. 17 godišnji Luke Bridges postavio je skimmer uređaj (kalkulator) na tipkovnicu bankomata pomoću koje je skupljao PIN brojeve osoba koje su podizale novac s bankomata (ATM). https://www.fightidentitytheft.com/blog/scam/youth-foils-atm-scam-wins-calculator, stranica posjećena 17. studenog 2017.
[121] Computer Misuse Act 1990, Interpretation. Section 3, Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

Predviđena kazna za počinitelja sumarnog kaznenog djela iz ovog članka je zatvor do godinu dana ili novčana kazna ukoliko je počinitelj iz Engleske i Walesa, a ukoliko je počinitelj iz Škotske, propisana je "kazna zatvora do šest mjeseci ili novčana kazna", dok je kazna u postupku pred porotom do deset godina zatvora, ili novčana kazna ili oboje.

Odredbe članka 3A pod nazivom "*Making, supplying or obtaining articles for use in offence under section 1 or 3"*[122] odnose se na zloporabu naprava koje mogu pomoći počinjenju kaznenih djela iz članka 1. - 3. ovog Zakona, na način da počinitelj upotrijebi bilo koji program ili podatke u elektronskom obliku, na način da ih izradi, promijeni ili učini dostupnima trećoj osobi. U praksi ovakva kaznena djela uključuju sve hakerske alate i programe, maliciozne kodove i sl.

Predviđena kazna za počinitelja sumarnog kaznenog djela iz ovog članka je zatvor do godinu dana ili novčana kazna, ukoliko je počinitelj iz Engleske i Walesa, a ukoliko je počinitelj iz Škotske, tada je predviđena "kazna zatvora do šest mjeseci ili novčana kazna", dok je kazna u postupku pred porotom do dvije godine zatvora, ili novčana kazna ili oboje.

Analiza članaka kaznene legislative Velike Britanije ne može se doslovno staviti u odnos s kaznenopravnim rješenjima Hrvatske zbog očitih razlika u pravnom sustavu (kontinentalni naspram *common law*), ali se može prikazati okvirna usporedba radi lakšeg shvaćanja inkriminacije kaznenog djela, što je prikazano u tablici 9.

[122] Computer Misuse Act 1990, Interpretation. Section 3A, Making, supplying or obtaining articles for use in offence under section 1 or 3.

Hrvatska	Velika Britanija
Neovlašteni pristup (članak 266.)	Section 1, Unauthorised access to computer material
Ometanje rada računalnog sustava (članak 267.)	Section 3, Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
Oštećenje računalnih podataka (članak 268.)	Section 3, Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
Neovlašteno presretanje računalnih podataka (članak 269.)	Section 2, Unauthorised access with intent to commit or facilitate commission of further offences
Računalno krivotvorenje (članak 270.)	Section 2, Unauthorised access with intent to commit or facilitate commission of further offences
Računalna prijevara (članak 271.)	Section 2, Unauthorised access with intent to commit or facilitate commission of further offences
Zloporaba naprava (članak 272.)	Section 3A, Making, supplying or obtaining articles for use in offence under section 1 or 3

Tablica 9 - Usporedba članaka kaznenih zakona Hrvatske i Velike Britanije

4.1.4 Kraljevina Švedska

Kazneno pravo u vezi s računalnim kriminalitetom u Švedskoj se svodi na isključivo uopćeno definirane članke Kaznenog zakona donesenog 1962. godine i zadnjim izmjenama 2007. godine (Government Offices of Sweden - The Swedish Penal Code, 2017). Za napomenuti je da je Švedska potpisala Konvenciju, ali kako je još nije ratificirala, tako nije niti napravila dodatne izmjene u kaznenom zakonodavstvu po pitanju kaznenih djela računalnog kriminaliteta (Katulić, 2006).

U švedskom Kaznenom zakonu definirano je nekoliko relevantnih kaznenih djela i to u četvrtom poglavlju, a koja su povezana s računalnim kriminalitetom.

Kazneno djelo iz članka *Chapter 4, Section 8*[123] odnosi se na neovlašteno pribavljanje podataka, što podrazumijeva i podatke iz poštanskih i telekomuniikacijskih usluga, a ne isključivo računalne podatke. Odredbe iz članka *Chapter 4, Section 9*[124] odnose se na počinitelja kaznenog djela ukoliko krivnja nije kažnjiva po odredbi iz članka *Chapter 4, Section 8*, a odnosi se na neovlašteni pristup podacima ili računalnom sustavu.

Kazneno djelo iz članka *Chapter 4, Section 9a*[125] odnosi se na počinitelja kaznenog djela ukoliko krivnja nije kažnjiva po odredbi iz članka *Chapter 4, Section 8*, a odnosi se na neovlašteno presretanje računalnih podataka.

Kazneno djelo iz članka *Chapter 4, Section 9c*[126] obuhvaćaju aktivnosti počinitelja ukoliko krivnja nije kažnjiva po člancima iz *Chapter 4, Section 8, Section 9, Section 9a i Section 9b*. Odredbe članka definiraju kažnjivo ponašanje kao neovlašteni pristup računalnom sustavu i računalnim podacima, kao i njihovo mijenjanje ili brisanje. Posljednjim izmjenama ovog članka iz 2007. godine, kaznena odgovornost je proširena tako da sada obuhvaća aktivnosti kao što je ometanje rada računalnog sustava, dok ranijim pravnim uređenjem takve vrste napada nisu bile uključene u kažnjivo ponašanje. Predviđena kazna za počinjenje svih navedenih kaznenih djela je "novčana kazna ili kazna zatvora do dvije godine".

[123] Swedish Penal Code, Chapter 4, Section 8.
[124] Swedish Penal Code, Chapter 4, Section 9.
[125] Swedish Penal Code, Chapter 4, Section 9a. (Law 1975:239)
[126] Swedish Penal Code, Chapter 4, Section 9c. (Law 2007)

Usporedba članaka kaznenopravnog okvira Švedske je teško izvediva s člancima Kaznenog zakona Republike Hrvatske, jer Kraljevina Švedska još nije ratificirala Konvenciju i uskladila svoju kaznenu legislativu. Kazneno djelo kao što je računalno krivotvorenje ili računalna prijevara u švedskom pravnom okviru definirana su poglavljima 12. i 13., gdje su sadržane klasične kaznenopravne odredbe o kaznenim djelima protiv imovine i kaznenopravnoj odgovornosti za štetu, te ih stoga nije bilo moguće usporediti u tablici 10.

Hrvatska	**Švedska**
Neovlašteni pristup (članak 266.)	Neovlašteni pristup podacima ili računalnom sustavu (Chapter 4, Section 9) i Neovlašteno presretanje računalnih podataka (Chapter 4, Section 9a)
Ometanje rada računalnog sustava (članak 267.)	Neovlašteni pristup računalnom sustavu i računalnim podacima, kao i njihovo mijenjanje ili brisanje (Chapter 4, Section 9c)
Oštećenje računalnih podataka (članak 268.)	Neovlašteni pristup računalnom sustavu i računalnim podacima, kao i njihovo mijenjanje ili brisanje (Chapter 4, Section 9c)
Neovlašteno presretanje računalnih podataka (članak 269.)	Neovlašteno pribavljanje podataka (Chapter 4, Section 8) i i Neovlašteno presretanje računalnih podataka (Chapter 4, Section 9a)
Računalno krivotvorenje (članak 270.)	-
Računalna prijevara (članak 271.)	-
Zloporaba naprava (članak 272.)	-

Tablica 10 - Usporedba članaka kaznenih zakona Hrvatske i Švedske

4.1.5 Rumunjska

Kazneno zakonodavstvo Rumunjske proučit ćemo s posebnim zanimanjem jer u posljednjih nekoliko godina rumunjski hakeri sudjeluju u gotovo svim važnijim hakerskim napadima, a sama otkrivačka djelatnost u Republici Hrvatskoj i ostalim zemljama, rezultirala je čestim uhićenjima rumunjskih državljana koji se bave računalnim kriminalitetom.

Kaznena djela računalnog kriminaliteta se u rumunjskom zakonodavstvu nalaze u posebnim zakonima, a ne u Kaznenom zakonu. Prvi zakon se odnosi na antikorupcijska kaznena djela gdje su izmjenama i dopunama iz 2003. godine obuhvaćena kaznena djela računalnog kriminala, dok se drugi zakon odnosi na kaznena djela elektroničkog poslovanja, odnosno lažnih financijskih aktivnosti. To su sljedeći pravni izvori:

- *Law no. 161 (Romania - The Romanian Parliament, 2003),*
- *Law no. 365 (Romania - The Romanian Parliament, 2002).*

Odredbe zakona Law no. 161, koje se odnose na kaznena djela računalnog kriminaliteta, opisane su u trećem poglavlju pod prevencijom i suzbijanjem kibernetičkog kriminala.

U prvom odjeljku nalazi se šest članaka iz domene kaznenih djela protiv zloporabe povjerljivosti i cjelovitosti računalnih podataka i računalnih sustava, dok je drugi odjeljak posvećen računalnim kaznenim djelima, kao što slijedi:

- *"Section 1, Offences against the confidentiality and integrity of data and computer systems"*
    - *članci 42. - 47.*

- *"Section 2, Computer-related offences"*
    - *članci 48. - 50.*

Članak 42. sankcionira neovlašten pristup računalnom sustavu "kaznom zatvora od šest mjeseci do tri godine", a ukoliko su zaobiđene sigurnosne mjere, tada je predviđena "kazna zatvora od 3 do 12 godina zatvora".[127]

[127] Romanian Anticorruption law no 161/2003, Title III, Art.42.

Neovlašteno presretanje računalnih podataka sankcionira se u čl. 43. kaznom zatvora od 2 do 7 godina.[128]

Odredbe članka 44. odnose se na neovlašteno mijenjanje, brisanje ili ograničavanje pristupa računalnim podacima, te se sankcionira kaznom zatvora od 2 do 7 godina, a ukoliko se vrši neovlašteno presnimavanje ili prijenos računalnih podataka tada je zapriječena "kazna zatvora u trajanju od 3 do 12 godina zatvora".[129]

Ometanje rada računalnog sustva sankcionira se odredbama članka 45. i kažnjava kaznom zatvora od 3 do 15 godina.[130]

Zloporaba naprava za počinjenje kaznenih djela opisanih u člancima 42. - 45. kažnjiva je kaznom zatvora od jedne do šest godina, a obuhvaća proizvodnju, prodaju, uvoz, distribuciju, stavljanje na raspolaganje u bilo kojem obliku, kao i otkrivanje pristupnih podataka u vidu lozinki ili drugih računalnih podataka.[131]

Pokušaj za kaznena djela iz članka 42. i 43. je kažnjiv.[132]

Tekst članka 48. odnosi se na oštećenje računalnih podataka koji se koriste u pravnom prometu, radi prikazivanja netočnih podataka i kažnjivo je kaznom zatvora od 2 do 7 godina.[133]

Ukoliko se radi o imovinskoj koisti ostvarenom kroz unos, izmjenu ili brisanje računalnih podatka ili bi takvo ponašanje uzrokovalo imovinsku štetu, tada je takvo ponašanje kažnjivo po članku 49. kaznom zatvora od 3 do 12 godina zatvora.[134]

Pokušaj za kaznena djela iz članka 48. i 49. je također kažnjiv.[135]

Odredbe zakona Law no. 365, koje se odnose na kaznena djela elektroničkog poslovanja, nalaze se u osmom poglavlju koje se odnosi na krivotvorenje i korištenje elektroničkih instrumenata plaćanja, posjedovanje hardvera i softvera sa svrhom da se počini krivotvorenje elektroničkih instrumenata plaćanja, kao i lažnih financijskih aktivnosti.

[128] Romanian Anticorruption law no 161/2003, Title III, Art.43.
[129] Romanian Anticorruption law no 161/2003, Title III, Art.44.
[130] Romanian Anticorruption law no 161/2003, Title III, Art.45.
[131] Romanian Anticorruption law no 161/2003, Title III, Art.46.
[132] Romanian Anticorruption law no 161/2003, Title III, Art.47.
[133] Romanian Anticorruption law no 161/2003, Title III, Art.48.
[134] Romanian Anticorruption law no 161/2003, Title III, Art.49.
[135] Romanian Anticorruption law no 161/2003, Title III, Art.50.

Pod navedenim poglavljem nalazi se šest članaka koji se mogu svrstati pod domenu računalnog kriminaliteta pod nazivom:

- *"Chapter VIII, Infringements related to the issuing and use of electronic payment means and the use of identity data for financial operations"*
  - *članci 24. - 30.*

Odredbe ovog poglavlja možemo okarakterizirati kao računalne prijevare i računalna krivotvorenja u gospodarskom poslovanju, dok je posjedovanje opreme za počinjenje tih kaznenih djela kažnjivo, u što ulazi i hardver i softver. Iz razloga što se računalna prijevara i računalno krivotvorenje opisuje isključivo u svojstvu elektroničkog instrumenta plaćanja, navedeni članci se ne mogu doslovno komparirati s člancima hrvatskog Kaznenog zakona, pa stoga nećemo pojašnjavati inkriminaciju i propisane kazne. Navedeni članci se nadopunjuju odredbama iz rumunjskog "Kaznenog zakona" i "Zakona o kaznenom postupku", a što je propisano u članku 30.[136]

Valja primijetiti da Rumunjski pravni okvir ima propisane najviše kazne u odnosu na druge promatrane države.

Usporedba članaka kaznenog pravnog okvira Rumunjske može se dosta kvalitetno referirati na srodnu legislativu Hrvatske, ali s naznakom da kaznena djela računalnog kriminaliteta nisu dio Kaznenog zakona Rumunjske, nego posebnog zakona. U skladu s navedenim može se prikazati okvirna usporedba radi lakšeg poimanja inkriminacije kaznenog djela, što je vidljivo u tablici 11.

[136] Romanian Anticorruption law no 365/2003, Chapter VIII, Art.24-30.

Hrvatska	Rumunjska
Neovlašteni pristup (članak 266.)	Neovlašten pristup računalnom sustavu (Law no. 161, Art. 42.)
Ometanje rada računalnog sustava (članak 267.)	Ometanje rada računalnog sustva (Law no. 161, Art. 45.)
Oštećenje računalnih podataka (članak 268.)	Neovlašteno mijenjanje, brisanje ili ograničavanje pristupa računalnim podacima (Law no. 161, Art. 44.)
Neovlašteno presretanje računalnih podataka (članak 269.)	Neovlašteno presretanje računalnih podataka (Law no. 161, Art. 43.)
Računalno krivotvorenje (članak 270.)	Računalno krivotvorenje (Law no. 365, Art. 24., 25. i 26.)
Računalna prijevara (članak 271.)	Računalna prijevara (Law no. 365, Art. 27., 28. i 29.)
Zloporaba naprava (članak 272.)	Zloporaba naprava (Law no. 161, Art. 46.)

Tablica 11 - Istovjetnost članaka kaznenih zakona Hrvatske i Rumunjske

4.1.6 Republika Slovenija

Republika Slovenija, u odnosu na neke druge države, u svom Kaznenom zakonu nema posebnu glavu za računalna kaznena djela, nego su to članci iz Kaznenog zakona sa zadnjim izmjenama i dopunama iz 2008. godine (Republika Slovenija, 2012):

- *221. čl. "napad na informacijski sistem",*
- *237. čl. "zloraba informacijskega sistema",*
- *306. čl. "izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje".*

Kazneno djelo iz čl. 221., koje se odnosi na napade na informacijske sustave, nalazi se u dvadesettrećoj glavi koja se odnosi na kaznena djela protiv imovine, čl. 237 koji sankcionira kaznena djela zloporabe informacijskog sustava, nalazi se u glavi dvadesetčetvrtoj koja se odnosi na gospodarska kaznena djela, a čl. 306 je opisan u dvadesetdevetoj glavi koja regulira kaznena djela protiv javnog reda i mira.

Članak pod nazivom "napad na informacijski sustav" *(čl. 221)*[137] sadržava nekoliko modaliteta kažnjivih djela koja su prikazana u jednom članku, a inkriminacija se odnosi na neovlašteni pristup informacijskom sustavu, kao i na nedozvoljeno presretanje podataka. Stavkom prvim za navedenu inkriminaciju propisana je kazna zatvora do jedne godine.

Ukoliko se radi o neopravdanom korištenju, izmjeni, brisanju, uništenju računalnih podataka ili ometanju rada računalnog sustava unosom računalnih podataka, tada je propisana kazna zatvora do dvije godine.

Pokušaj je kažnjiv, a ukoliko se radi o kvalificiranom kaznenom djelu, tada je predviđena kazna zatvora od 3 mjeseca do pet godina.

Odredba članka "*zloraba informacijskega sistema" (čl. 237.)*[138] je kazneno djelo koje možemo usporediti s kaznenim djelima iz Kaznenog zakona Republike Hrvatske iz članka 266. i 267., s napomenom da se u članku inkriminira neovlašteni pristup računalnom sustavu, zbog imovinske koristi, kao i ometanje rada takvog računalnog sustava, ali i neovlašteno presretanje računalnih podataka, što je specificirano u članku 269. Kaznenog zakona Republike Hrvatske. Propisana kazna je kazna zatvora do tri godine, dok je za kvalificirani oblik predviđena kazna zatvora do pet godina.

Kazneno djelo "*izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje" (čl. 306.)*[139], odnosno samo treći stavak, možemo izravno usporediti s kaznenim djelom iz čl. 272. hrvatskog Kaznenog zakona, a radi se o zloporabi naprava kako bi se neovlašteno izvršila kaznena djela iz članka 221. i 237. slovenskog "Kaznenog zakona". U nedopuštene radnje spada posjedovanje, izrada, prodaja, uporaba, uvoz, izvoz ili na neki drugi način korištenje alata koji omogućuju pristup računalnom sustavu ili računalnim podacima.

[137] Napad na informacijski sistem, 221. člen.
[138] Zloraba informacijskega sistema, 237. člen.
[139] Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje, 306. člen.

Doslovna usporedba članaka kaznenog pravnog okvira Slovenije s kaznenim okvirom Hrvatske nije moguća, zbog raščlanjivanja kaznene odgovornosti u Sloveniji prema počinjenju zbog imovinske koristi, ali može se predložiti okvirna usporedba radi lakšeg poimanja inkriminacije kaznenih djela, kao što je vidljivo u tablici 12.

Hrvatska	**Slovenija**
Neovlašteni pristup (članak 266.)	221. čl. napad na informacijski sistem
Ometanje rada računalnog sustava (članak 267.)	221. čl. napad na informacijski sistem
Oštećenje računalnih podataka (članak 268.)	221. čl. napad na informacijski sistem
Neovlašteno presretanje računalnih podataka (članak 269.)	221. čl. napad na informacijski sistem
Računalno krivotvorenje (članak 270.)	237. čl. zloraba informacijskega sistema
Računalna prijevara (članak 271.)	237. čl. zloraba informacijskega sistema
Zloporaba naprava (članak 272.)	306. čl. izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje

Tablica 12 - Istoznačnice članaka kaznenog zakona Hrvatske i Slovenije

4.2 Opseg, struktura i kretanje kriminaliteta kaznenih djela računalnog kriminala

Dubinsko i detaljno sagledavanje problematike sigurnosti u kibernetičkom prostoru, što uključuje pregled stanja i dinamike kaznenih djela iz ove domene, praćenje i procjenu, imperativno postavlja zahtjeve pred gotovo sve državne institucije, kako u pogledu vlastitog osposobljavanja kadrova koji koriste kibernetički prostor za ispunjavanje svakodnevnih obveza, tako i u pogledu nadzora i kontrole od strane njihovih upravljačkih struktura. Proširenjem i primjenom novih saznanja i pravnih normi (države i Europske unije) te praćenjem fenomenologije i modaliteta zloporabe kibernetičkog prostora stvoriti će se pretpostavke za izgradnju i formalizaciju sustavnog pristupa u međunarodnoj suradnji u kibernetičkom prostoru.

U smislu primjenjivosti očekivani doprinos ogleda se u mogućnostima i indikatorima procjene rizika međunarodnih odnosa u kibernetičkom prostoru.

U Republici Hrvatskoj je od 1. siječnja 2013. godine na snazi Kazneni zakon koji ima posebnu glavu Zakona posvećenu kaznenim djelima protiv računalnih sustava, programa i podataka, a koja je analizirana zbog potrebe statističke obrade i pokazatelja stanja i kretanja ove problematike u posljednjih četiri godine, jer usporedba sa člancima prethodnog Kaznenog zakona ne bi dala odgovarajući prikaz budući da su inovirani i dodani novi zakonski opisi u ovu skupinu kaznenih djela.

Kako bi kvalitetnije interpretirali statističke pokazatelje kaznenih djela kibernetičkog kriminala prema Kaznenom zakonu, a sukladno Konvenciji, u tablici 13 je prikazano usporedno pojašnjenje naziva pojedinih kaznenih djela:

Kazneni zakon Republike Hrvatske	Konvencija
Neovlašteni pristup (članak 266.)	Članak 2. - Nezakoniti pristup
Ometanje rada računalnog sustava (članak 267.)	Članak 5. - Ometanje sustava
Oštećenje računalnih podataka (članak 268.)	Članak 4. - Ometanje podataka
Neovlašteno presretanje računalnih podataka (članak 269.)	Članak 3. - Nezakonito presretanje
Računalno krivotvorenje (članak 270.)	Članak 7. - Računalno krivotvorenje
Računalna prijevara (članak 271.)	Članak 8. - Računalna prijevara
Zloporaba naprava (članak 272.)	Članak 6. - Zloporaba naprava

Tablica 13 - Poredbeni prikaz Kaznenog zakona i Konvencije o kibernetičkom kriminalu

Statistički podaci o broju evidentiranih kaznenih djela pribavljeni su od Ministarstva unutarnjih poslova Republike Hrvatske [140] za razdoblje od 2013. do 2017. godine za sljedeće članke Kaznenog zakona:

- "neovlašteni pristup" (članak 266.),
- "ometanje rada računalnog sustava" (članak 267.),
- "oštećenje računalnih podataka" (članak 268.),
- "neovlašteno presretanje računalnih podataka" (članak 269.),
- "računalno krivotvorenje" (članak 270.),
- "računalna prijevara" (članak 271.),
- "zloporaba naprava" *(članak 272.)*

[140] "Ministarstvo unutarnjih poslova Republike Hrvatske", Publikacije, Statistika http://stari.mup.hr/main.aspx?id=180991, stranica posjećena 30. kolovoza 2017.

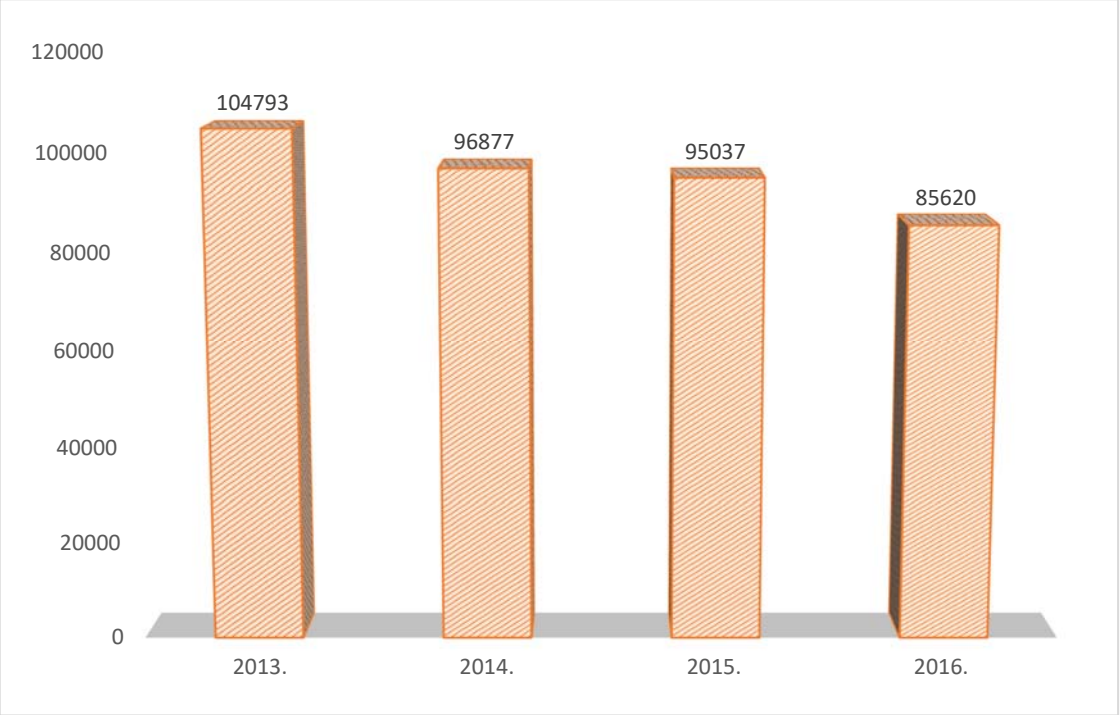
Statistički podaci o broju prijavljenih, osuđenih i optuženih punoljetnih osoba za navedena kaznena djela analizirani su na temelju podataka "Državnog zavoda za statistiku Republike Hrvatske"[141] za referentno razdoblje, osim za teška kaznena djela protiv računalnih sustava, programa i podataka iz članka 273., s obzirom da za navedeno kazneno djelo nema dostupnih podataka u statistici Ministarstva unutarnjih poslova niti Državnog zavoda za statistiku.

4.2.1 Statistički podaci o broju evidentiranih kaznenih djela u Republici Hrvatskoj

Kao što je navedeno u uvodu ove točke, prvotno su analizirani statistički pokazatelji broja evidentiranih kaznenih djela Ministarstva unutarnjih poslova Republike Hrvatske. Statistički pokazatelji, osim ukupnog broja kaznenih djela, pokazuju i broj kaznenih djela od primarnog interesa za ovaj rad (kibernetički kriminalitet) definiranih Konvencijom, te implementiranih u odredbe Kaznenog zakona za vremensko razdoblje od 2013. do 2017. godine.

[141] DZS Republike Hrvatske, Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita, "Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude"
https://www.dzs.hr/, stranica posjećena 30. kolovoza 2017.

Grafikon 1 - Pregled sigurnosnih pokazatelja ukupnog broja evidentiranih kaznenih djela u Republici Hrvatskoj



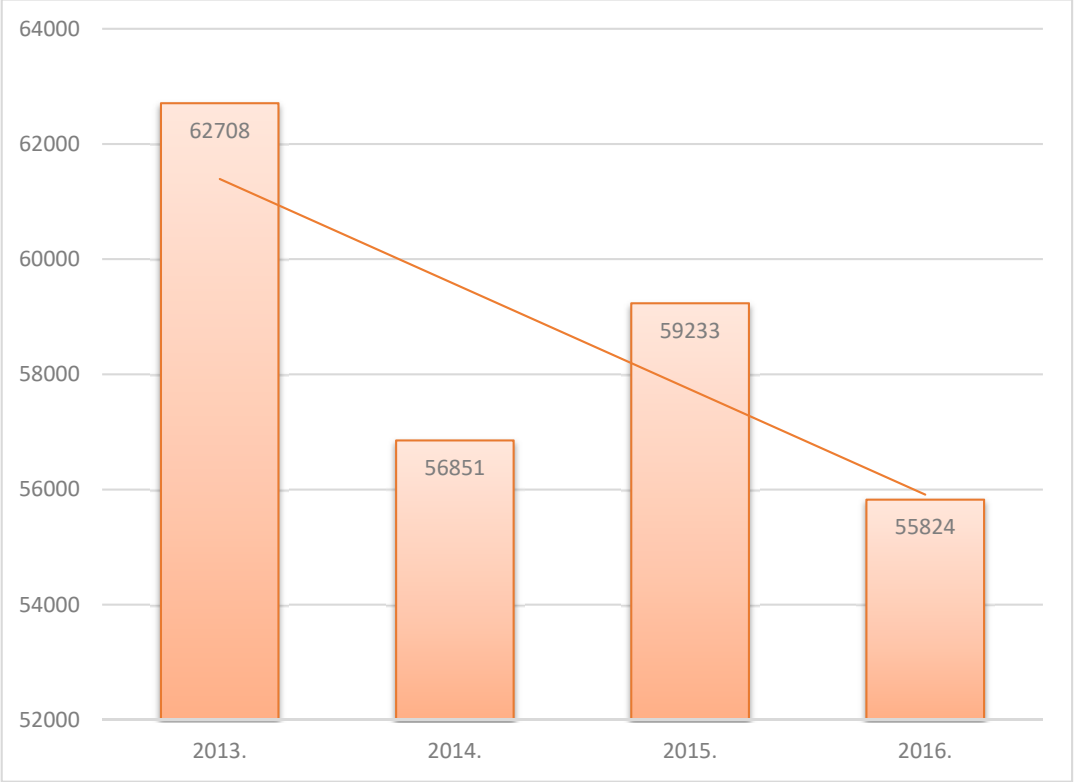
Izvor: Statistički pokazatelji o broju evidentiranih kaznenih djela Ministarstva unutarnjih poslova Republike Hrvatske, 2013.-2017.

Grafikon 1 prikazuje ukupan broj svih evidentiranih kaznenih djela i to:

- "kaznena djela za koja se progoni po službenoj dužnosti",
- "kaznena djela za koja se ne progoni - izostanak prijedloga",
- "kaznena djela za koja se progoni po privatnoj tužbi".

Kontinuirano smanjenje ukupnog broja prijavljenih kaznenih djela evidentirano je kroz cijelo promatrano razdoblje.

Grafikon 2 - Ukupan broj evidentiranih kaznenih djela u Republici Hrvatskoj koja se progone po službenoj dužnosti



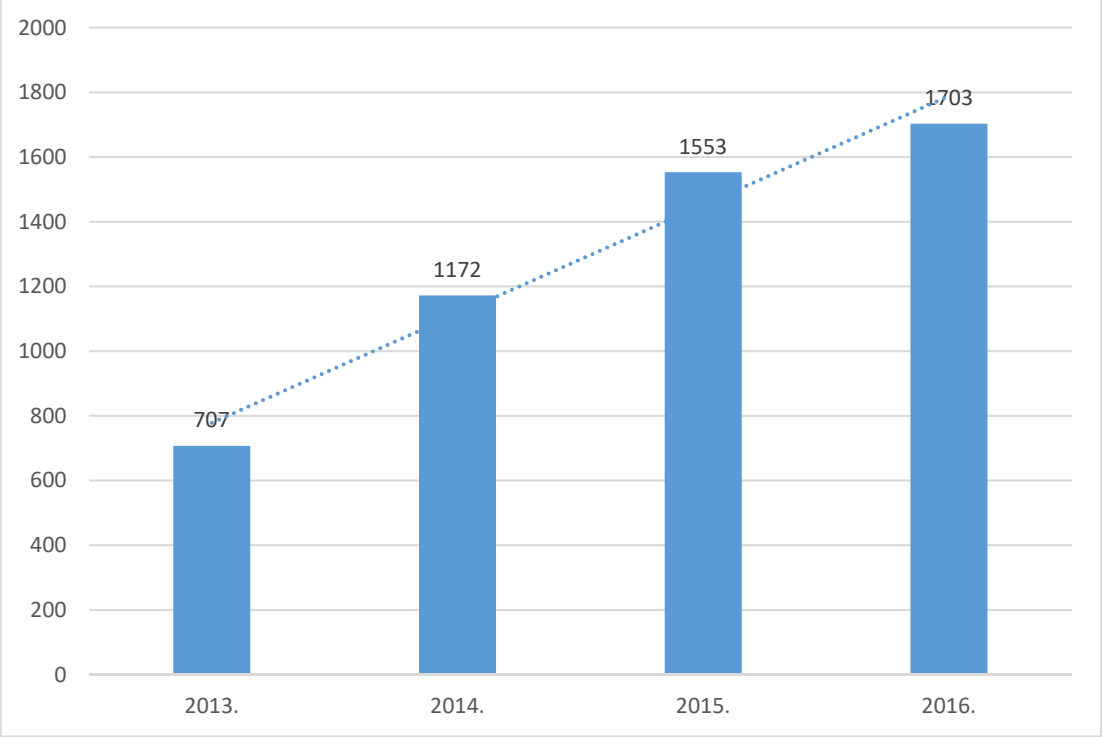
Izvor: Statistički pokazatelji o broju evidentiranih kaznenih djela Ministarstva unutarnjih poslova Republike Hrvatske, 2013.-2017.

Trend kretanja kriminaliteta pokazuje kontinuirano smanjenje broja prijavljenih kaznenih djela koja se progone po službenoj dužnosti i to drastično u 2014. i 2016. godini.

Temeljem novih odredbi Kaznenog zakona i usklađivanja rada policije i državnih odvjetništava, nameće se zaključak da je s vremenom edukacija svih tijela za provođenje zakona, ali i prevencija dala svoj doprinos u znatno smanjenom broju otkrivenih i procesuiranih kaznenih djela, što se vidi u tendenciji pada od gotovo 7 000 kaznenih djela u 2016. godini u odnosu na prvu godinu promatranog razdoblja.

Jednako tako, važno je upozoriti na mogućnost tzv. tamne brojke ove vrste kriminala koja se odnosi na realno počinjena kaznena djela koja nisu otkrivena, ali i počinitelje koji su ostali nepoznati.

Grafikon 3 - Ukupan broj evidentiranih kaznenih djela u Republici Hrvatskoj protiv računalnih sustava, programa i podataka



Izvor: Statistički pokazatelji o broju evidentiranih kaznenih djela Ministarstva unutarnjih poslova Republike Hrvatske, 2013.-2017.

Iako po svojoj inkriminaciji posjeduju obilježja iz domene ove teme, u navedeni prikaz nisu uključena kaznena djela u čijem se opisu spominje računalo kao sredstvo napada ili objekt napada.

Takvih kaznenih djela u postojećem Kaznenom zakonu ima nekoliko, a u budućnosti se može očekivati sve više. To su kaznena djela protiv privatnosti, časti i ugleda, spolnog zlostavljanja i iskorištavanja djeteta, intelektualnog vlasništva, pa čak i kaznena djela protiv javnog reda.

Analizirajući statističke pokazatelje, očito je da je broj evidentiranih kaznenih djela iz grafikona 3 relativno neznatan u udjelu ukupno evidentiranih kaznenih djela koja se progone po službenoj dužnosti, ne prelazi niti 3% u ukupnoj strukturi broja kaznenih djela, ali se može primijetiti trend stabilnog porasta ukupnog broja evidentiranih kaznenih djela iz glave XXV Kaznenog zakona.

4.2.2 Statistički podaci o broju prijavljenih, optuženih i osuđenih osoba

Za prikaz podataka o broju prijavljenih, optuženih i osuđenih osoba za kaznena djela korišteni su podaci Državnog zavoda za statistiku Republike Hrvatske, iz kojih je vidljiv broj prijavljenih, optuženih i osuđenih osoba, struktura i vrste odluka, struktura razloga odbačaja, struktura razloga obustave istraga za navedena kaznena djela, struktura osoba po županijama i struktura osuđenih osoba po dobi, spolu i školskoj spremi, za razdoblje od 2013. do 2017. godine, iz razloga što se za 2017. godinu podaci objavljuju tek u drugoj polovici 2018. godine. 2012. godina nije razmatrana zbog izmjena Kaznenog zakona i nove nomenklature kaznenih djela koja su od interesa za ovu disertaciju.

DZS navodi u svojim izvješćima da "statističke izvještaje ispunjavaju nadležna županijska i općinska državna odvjetništva nakon donošenja konačne odluke te nadležni županijski i općinski sudovi koji sude u prvom stupnju kad je postupak pravomoćno završen. Jedinice promatranja su punoljetni i maloljetni počinitelji kaznenih djela, koji mogu biti počinitelji, supočinitelji, poticatelji ili pomagatelji. Ako jedna osoba počini nekoliko kaznenih djela (stjecaj), kao glavno djelo uzima se najteže kazneno djelo. Kad nekoliko osoba sudjeluje u počinjenju jednoga kaznenog djela, svaki se sudionik (počinitelj) smatra jedinicom promatranja. U tom slučaju svako će se djelo evidentirati kao obilježje kod svakog sudionika, s tim što se odgovorom na posebno pitanje utvrđuje je li riječ o sudioništvu".

U odnosu na ranije podatke Ministarstva unutarnjih poslova Republike Hrvatske, podaci Državnog zavoda za statistiku Republike Hrvatske pružaju potpuniji pregled prijavljenih kaznenih djela jer, pored podataka o članku Kaznenog zakona, može se vidjeti i podatak o stavku određenog članka, što posebno dolazi do izražaja u člancima koji pružaju objašnjenje što svaki od stavaka predviđa sukladno implementaciji odredbi Konvencije.

Statistički podaci u prikazu obuhvaćaju sve punoljetne počinitelje kaznenih djela, prijavljene, optužene i osuđene.

"Punoljetni počinitelji kaznenih djela su osobe koje su u vrijeme počinjenja kaznenog djela imale navršenih 18 godina života, protiv kojih je postupak po kaznenoj prijavi i prethodni postupak završen i optužene osobe (uključujući osobe protiv kojih se progon poduzima privatnom tužbom) protiv kojih je kazneni postupak pravomoćno završen.

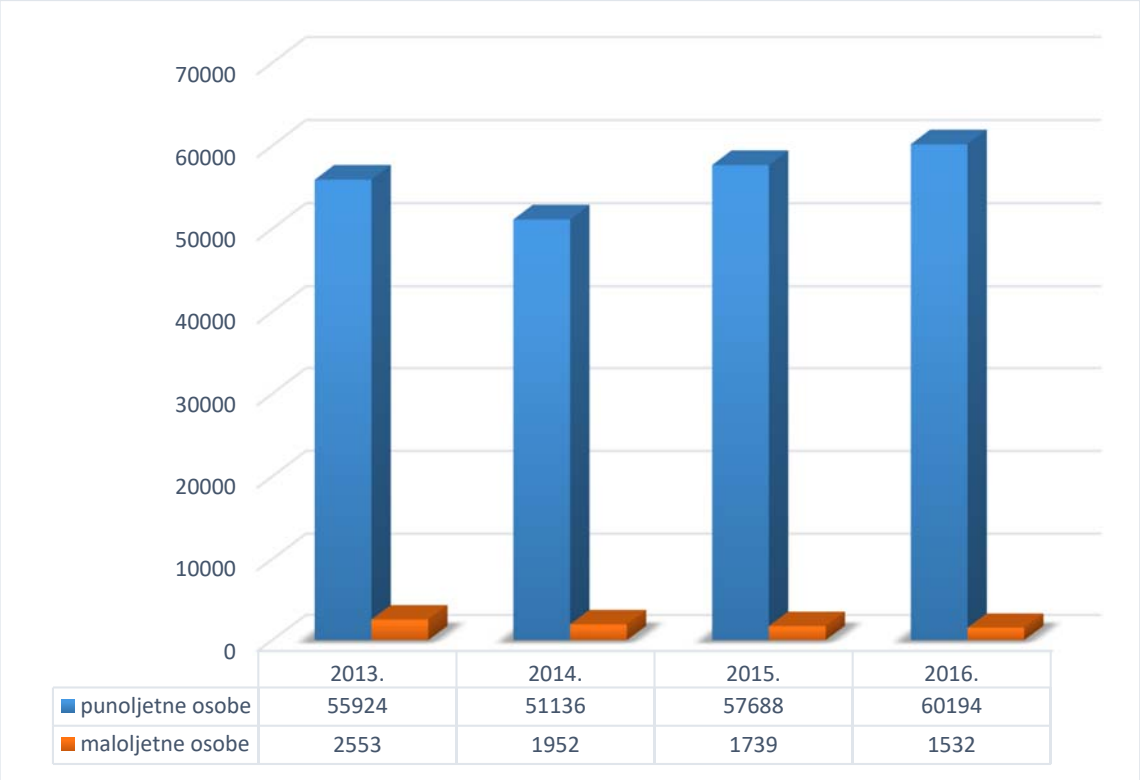
Prijavljena osoba, poznati počinitelj, jest punoljetni počinitelj kaznenog djela protiv kojega je postupak po kaznenoj prijavi i prethodni postupak završen odlukom kojom je odbačena prijava, prekinuta istraga, obustavljena istraga ili podnesena optužnica.

Prijavljena osoba, nepoznati počinitelj jest, počevši od 2015. obradne godine, nepoznata osoba protiv koje je podnesena kaznena prijava državnom odvjetništvu za počinjeno kazneno djelo. Zaključno s 2014. godinom, nepoznati počinitelj definiran je kao nepoznata osoba protiv koje je podnesena kaznena prijava državnom odvjetništvu, a koja i nakon isteka godine dana od dana podnošenja kaznene prijave nije otkrivena. Ta izmjena imat će ograničen utjecaj na podatke o ukupno prijavljenim počiniteljima te prijavljenim nepoznatim počiniteljima kaznenih djela jer se može očekivati da će se dijelu nepoznatih počinitelja iste godine otkriti identitet te će u tim slučajevima doći do dvostrukog uračunavanja u istoj godini.

Optužena osoba jest punoljetna osoba protiv koje je sudu podnesena optužnica ili privatna tužba, protiv koje je kazneni postupak pravomoćno završen odlukom suda kojom se obustavlja kazneni postupak, optužba odbacuje, donosi oslobađajuća ili odbijajuća presuda, određuje prisilni smještaj za neubrojivu osobu ili se počinitelj proglašava krivim.

Mlađa punoljetna osoba je osoba koja je u vrijeme počinjenja djela navršila 18, a nije navršila 21 godinu života i kojoj sud može izreći odgojnu mjeru posebnih obveza, odgojnu mjeru pojačanog nadzora i kaznu maloljetničkog zatvora, ako počinitelj u vrijeme suđenja nije navršio 21 godinu života, odgojnu mjeru upućivanja u disciplinski centar i zavodsku mjeru. Počinitelju koji je u vrijeme suđenja navršio 21 godinu života, sud može umjesto maloljetničkog zatvora izreći kaznu zatvora, u granicama koje se primjenjuju za vremensko trajanje maloljetničkog zatvora. Osuđena osoba je punoljetna osoba proglašena krivom prema kojoj je izrečena kazna ili druga mjera: zatvor, novčana kazna, odgojne mjere, sudska opomena i osoba proglašena krivom, a oslobođena od kazne." (Statistička izvješća broj 1605, 2017, str. 7).

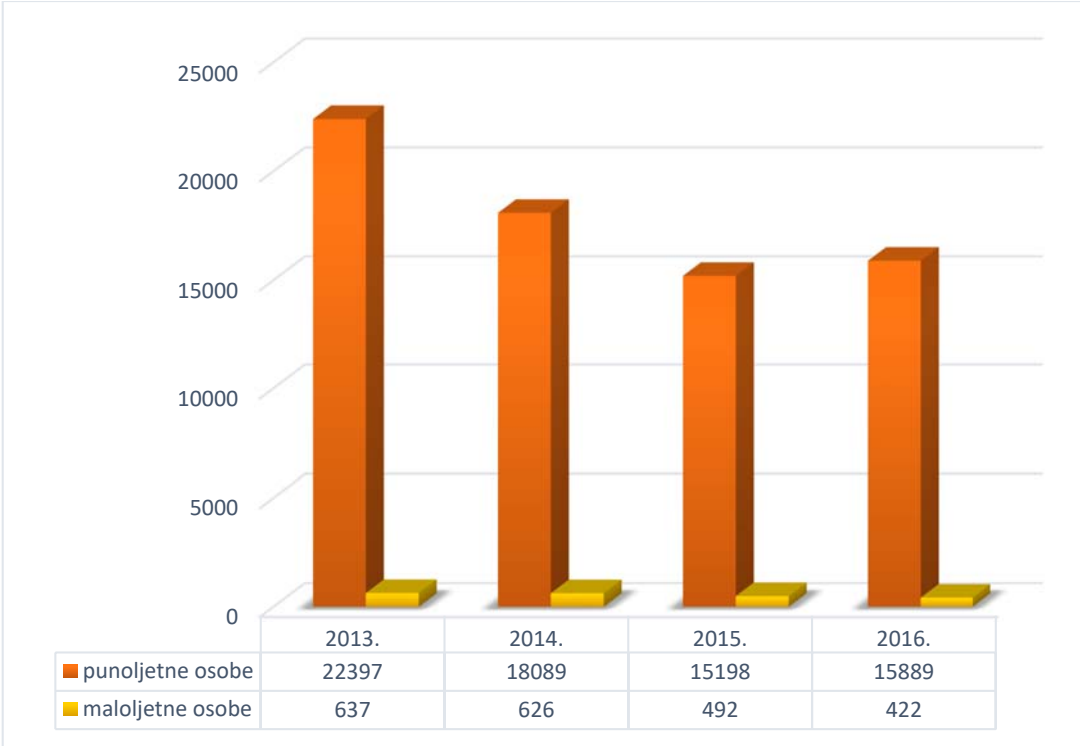
Grafikon 4 - Ukupan broj prijavljenih punoljetnih i maloljetnih osoba od 2013.-2017. godine



	2013.	2014.	2015.	2016.
punoljetne osobe	55924	51136	57688	60194
maloljetne osobe	2553	1952	1739	1532

Izvor: DZS Republike Hrvatske, 2013.-2017.

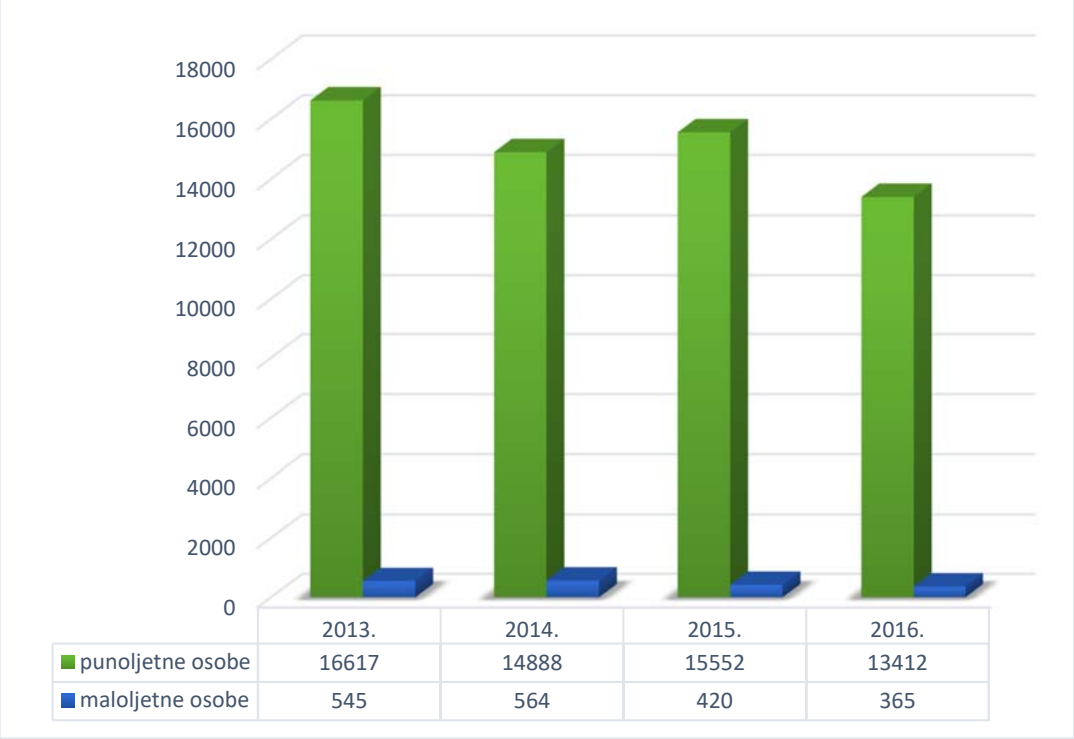
Grafikon 5 - Ukupan broj optuženih punoljetnih i maloljetnih osoba od 2013.-2017. godine



	2013.	2014.	2015.	2016.
punoljetne osobe	22397	18089	15198	15889
maloljetne osobe	637	626	492	422

Izvor: DZS Republike Hrvatske, 2013.-2017.

Grafikon 6 - Ukupan broj osuđenih punoljetnih i maloljetnih osoba od 2013.-2017. godine



	2013.	2014.	2015.	2016.
punoljetne osobe	16617	14888	15552	13412
maloljetne osobe	545	564	420	365

Izvor: DZS Republike Hrvatske, 2013.-2017.

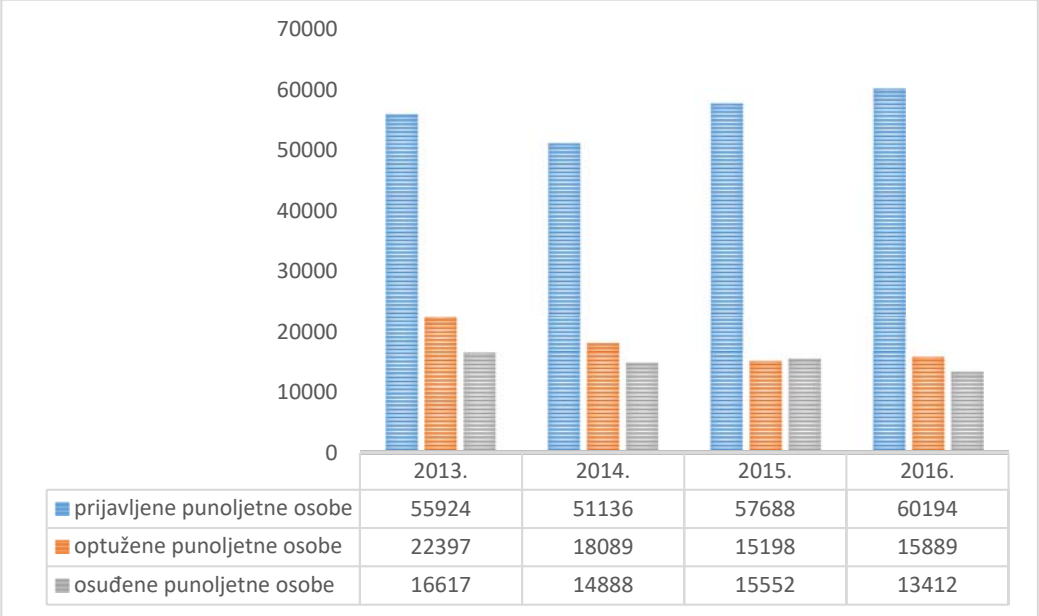
U grafikonima 4, 5 i 6 prikazan je ukupan broj prijavljenih, optuženih i osuđenih punoljetnih i maloljetnih osoba u razdoblju 2013.-2017. Vidljiv je trend povećanja kod prijavljenih punoljetnih osoba, dok je broj prijavljenih maloljetnih osoba u silaznom trendu. Kod broja optuženih osoba primjećuje se tendencija smanjenja i kod punoljetnih i kod maloljetnih osoba, s malim porastom u 2016. godini ukupnog broja optuženih punoljetnih osoba. Kod osuđenih maloljetnih osoba uočava se trend pada, dok je kod punoljetnih osoba silazna tendencija u odnosu na 2013. godinu, s neznatnim porastom 2016. u odnosu na 2015. godinu.

Kod prikaza ukupnog broja prijavljenih, optuženih i osuđenih punoljetnih ili maloljetnih osoba mora se uzeti u obzir da prijava podnesena u određenoj godini ne mora rezultirati pravomoćnom sudskom odlukom te iste godine, odnosno pravomoćna sudska odluka ne mora se odnositi na prijavu ili optužnicu podnesenu iste godine.

To je informacija koju je bitno imati u vidu kada se razmatraju podaci o prijavljenim, optuženim i osuđenim maloljetnim ili punoljetnim osobama za svaku referentnu godinu.

Zbog izrazito malog broja prijavljenih, optuženih i osuđenih maloljetnih osoba i specifičnosti daljnjeg sudskog postupka, u sljedećim grafikonima biti će prikazne prijavljene, optužene i osuđene punoljetne osobe.

Grafikon 7 - Prijavljene, optužene i osuđene punoljetne osobe od 2013.-2017. godine



	2013.	2014.	2015.	2016.
prijavljene punoljetne osobe	55924	51136	57688	60194
optužene punoljetne osobe	22397	18089	15198	15889
osuđene punoljetne osobe	16617	14888	15552	13412

Izvor: DZS Republike Hrvatske, 2013.-2017.

Grafikon 7 prikazuje broj prijavljenih, optuženih i osuđenih punoljetnih osoba za sva kaznena djela za vremensko razdoblje od 2013. do 2017. godine.

Uvidom u ukupan broj prijavljenih, optuženih i osuđenih punoljetnih osoba u promatranom razdoblju uočava se trend porasta prijavljenih punoljetnih osoba, s naznakom da je broj prijavljenih osoba gotovo trostruko, a u zadnjoj godini i četverostruko veći od broja optuženih, odnosno osuđenih, dok se kod broja optuženih, odnosno osuđenih osoba očituje tendencija smanjenja.

4.2.3 Statistički podaci o broju prijavljenih punoljetnih osoba

Kao što je navedeno u prethodnoj točki, statistički podaci o broju prijavljenih punoljetnih osoba za kaznena djela iz članka 266. do 272. Kaznenog zakona uključujući sve stavke, za vremensko razdoblje od 2013. do 2017. godine, temelje se na podacima Državnog zavoda za statistiku (tablica 14).

	2013.	**2014.**	**2015.**	**2016.**	**UKUPNO**
Neovlašteni pristup (članak 266.)	16	16	29	115	**176**
Ometanje rada računalnog sustava (članak 267.)	4	1	2	4	**11**
Oštećenje računalnih podataka (članak 268.)	2	4	7	6	**19**
Neovlašteno presretanje računalnih podataka (članak 269.)	4	3	5	1	**13**
Računalno krivotvorenje (članak 270.)	86	169	80	52	**387**
Računalna prijevara (članak 271.)	583	960	1361	1365	**4269**
Zloporaba naprava (članak 272.)	12	19	69	160	**260**
UKUPNO	**707**	**1172**	**1553**	**1703**	

Tablica 14 - Broj prijavljenih punoljetnih osoba od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

Udio prijavljenih navedenih kaznenih djela u ukupnoj strukturi prijavljenih kaznenih djela naveden je u tablici 15, s napomenom da je broj prijavljenih osoba prikazan za godinu u kojoj je osoba prijavljena, a ne u kojoj je prijavljeno kazneno djelo.

	2013.	**2014.**	**2015.**	**2016.**
Prijavljena kaznena djela (po sl.d.)	62708	56851	59233	55824
čl. 266. - 272. KZ-a	707	1172	1553	1703
Udio	1,13%	2,06%	2,62%	3,05%

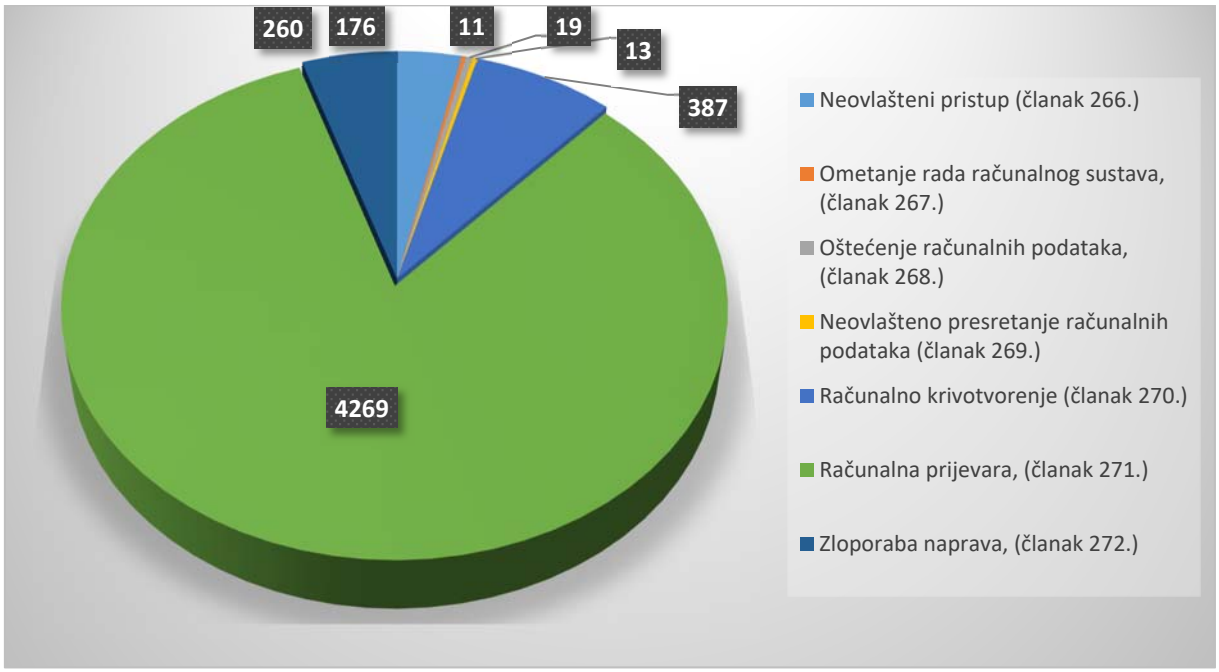
Tablica 15 - Udio prijavljenih promatranih kaznenih djela u ukupnoj strukturi od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

Najveći udio u ukupnom broju kaznenih djela iz glave XXV Kaznenog zakona se odnosi na kazneno djelo računalne prijevare, a ovo kazneno djelo je drugo po broju izvršenja kaznenih djela iz glave gospodarskog kriminaliteta, gdje su uvrštena i računalna kaznena djela.

U grafikonu 8 vidljiv je broj prijavljenih osoba po udjelu promatranih kaznenih djela iz članka 266. - 272. Kaznenog zakona za promatrano razdoblje.

Grafikon 8 - Broj prijavljenih osoba po odabranim člancima KZ-a za od 2013. do 2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Statistički podaci o broju prijavljenih osoba sadrže i podatke o broju prijavljenih poznatih i nepoznatih počinitelja kaznenih djela iz članaka 266. - 272. KZ-a.

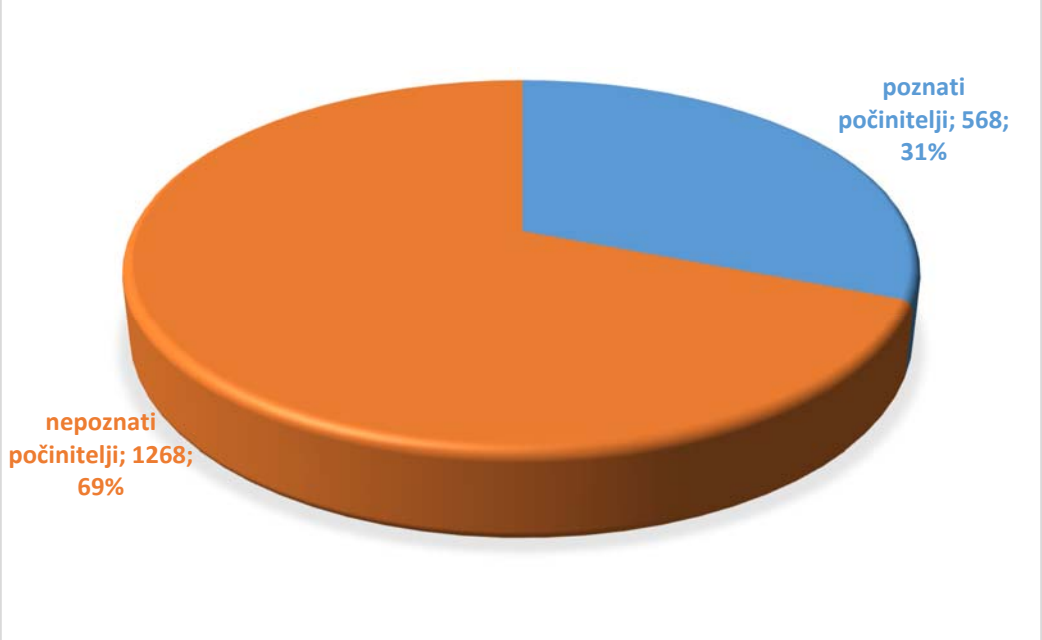
Glava XXV KZ-a	2013.	2014.	2015.	2016.	**UKUPNO**
poznati počinitelji	128	121	154	165	568
nepoznati počinitelji	132	169	526	441	1268

Tablica 16 - Prijavljeni poznati i nepoznati počinitelji kaznenih djela iz članaka 266. - 272. KZ-a od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

Iz tablice 16 i grafikona 9 evidentno je kako je u promatranom vremenskom razdoblju ukupno prijavljeno 568 poznatih počinitelja i 1.268 nepoznatih počinitelja kaznenih djela iz članaka 266. - 272. KZ-a, što ukazuje na više nego dvostruko smanjenu otkrivenost nepoznatih počinitelja ukazujući na relativnu podkapacitiranost policije u kriminalističkom istraživanju .

Grafikon 9 - Odnos prijavljenih poznatih i nepoznatih počinitelji kaznenih djela iz članka 266. - 272. KZ-a



Izvor: DZS Republike Hrvatske, 2013.-2017.

Glava XXV KZ-a	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
Podnesena optužnica ili optužni prijedlog	108	95	103	108	414
Odbačena prijava	20	26	50	57	153

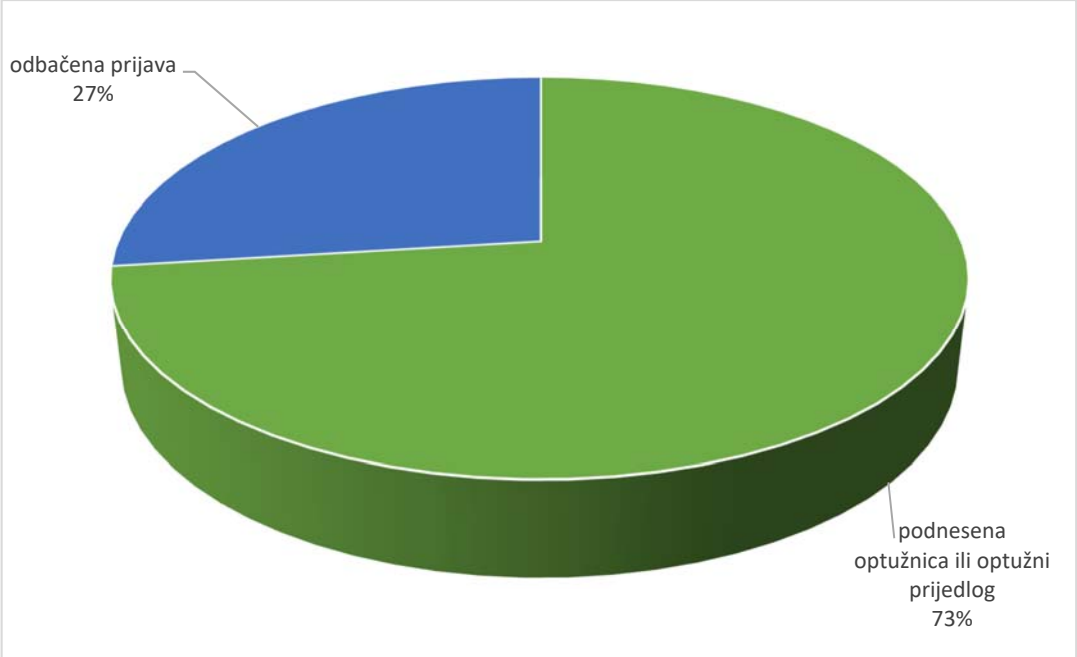
Tablica 17 - Struktura vrste odluka za prijavljene osobe od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

Iz tablice 17 i grafikona 10 uočava se relativno solidan trend podnesenih optužnica. Prijave su za promatrano razdoblje odbačene, prosječno, u jednoj trećini slučajeva.

U izvješćima Državnog zavoda za statistiku struktura vrste odluka za koje se mogu dobiti podaci su odbačena prijava, prekinuta istraga te obustavljena istraga. Kako su za promatrane članke Kaznenog zakona podatci o prekinutim istragama i obustavljenim istragama vezano za ove članke ništavni, tako u pregled strukture vrsta odluka nisu uvršteni podaci o prekinutim i obustavljenim istragama, jer ih nije niti bilo za referentno razdoblje.

Grafikon 10 - Udio vrste odluka u strukturi prijavljenih osoba



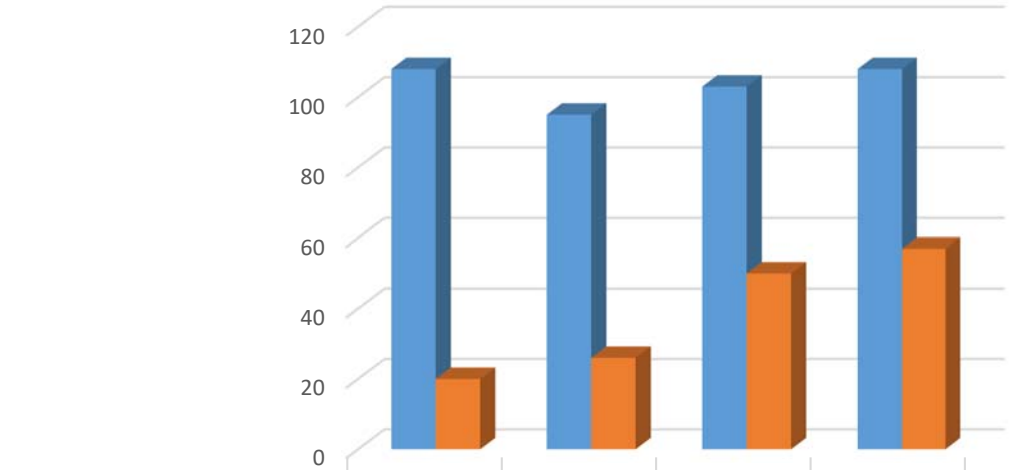
Izvor: DZS Republike Hrvatske, 2013.-2017.

Za promatrano četverogodišnje razdoblje vidljivo je da su državna odvjetništva odbacila skoro svaku četvrtu prijavu ili 27%, odnosno 153 kaznenih prijava, dok je za 73% prijavljenih osoba podignuta optužnica ili optužni prijedlog.[142]

Iz prikazanih podataka je, također, očito da postoji tendencija povećanja udjela odbačenih prijava naspram broja podignutih optužnica.

[142] DZS navodi da se "optužni prijedlog se podnosi za kaznena djela za koja je zapriječena kazna zatvora do 5 godina, za koje se sudi u tzv. skraćenom postupku pred općinskim sudom. Ne treba joj ptrethoditi istraga već eventualno pojedine istražne radnje, a optužnica se podiže za kaznena djela sa zapriječenom kaznom preko 5 godina i mora joj prethoditi istraga. Ova napomena vrijedi za promatrano vremensko razdoblje i odredbe Kaznenog zakona i Zakona o kaznenom postupku u navedeno vrijeme."

Grafikon 11 - Vrste odluka u strukturi prijavljenih osoba od 2013.-2017. godine

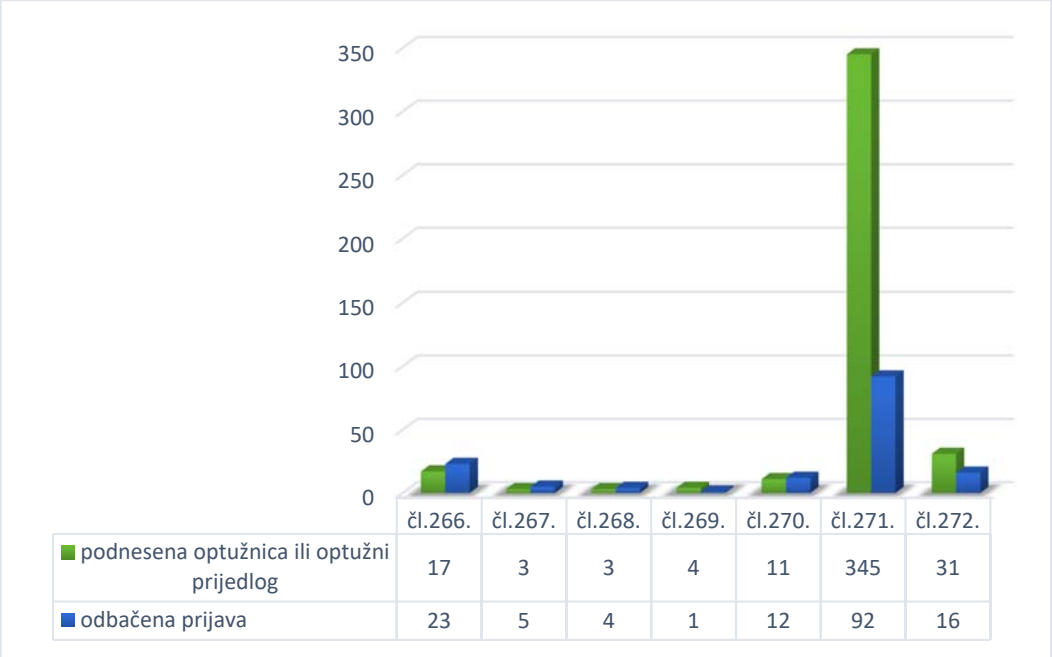


	2013.	2014.	2015.	2016.
podnesena optužnica ili optužni prijedlog	108	95	103	108
odbačena prijava	20	26	50	57

Izvor: DZS Republike Hrvatske, 2013.-2017.

S obzirom na povećanje broja odbačaja u odnosu na broj podnesenih optužnica ili optužnih prijedloga, može se ustvrditi kako su kaznene prijave nedovoljno kvalitetne, odnosno da nije prikupljeno dovoljno dokaza ili dokazi nisu prikupljeni sukladno postojećem zakonodavstvu.

Grafikon 12 - Vrste odluka u strukturi prijavljenih osoba po promatranim člancima



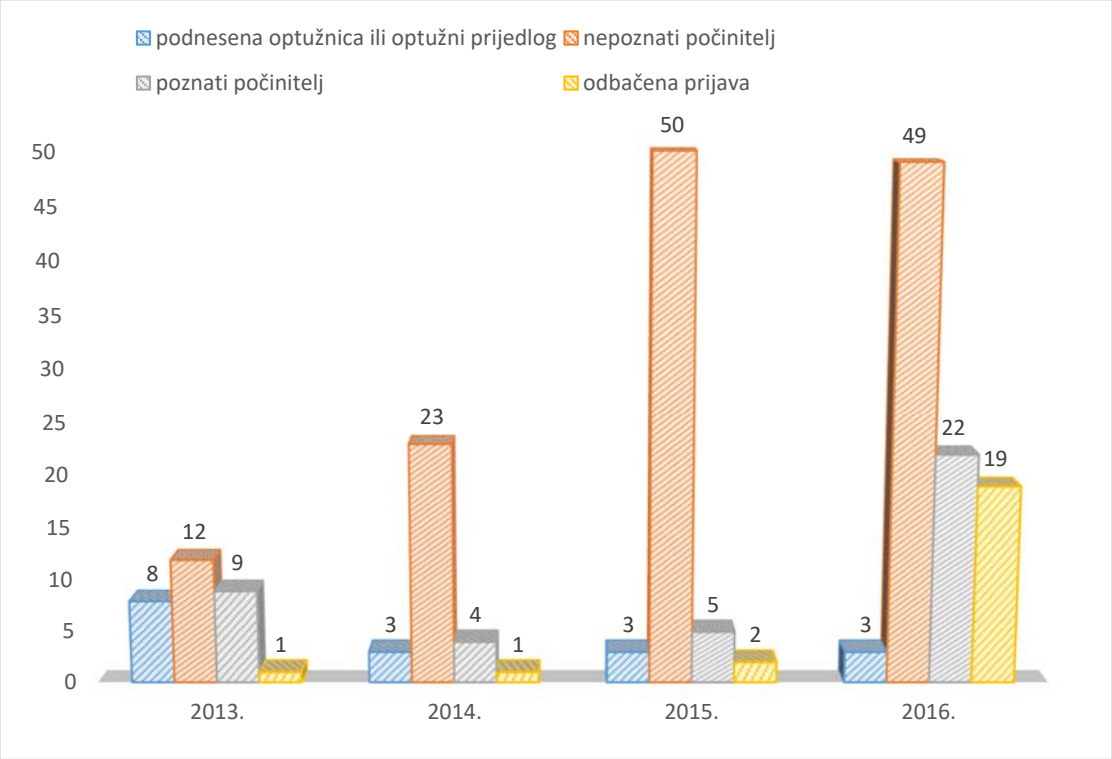
	čl.266.	čl.267.	čl.268.	čl.269.	čl.270.	čl.271.	čl.272.
podnesena optužnica ili optužni prijedlog	17	3	3	4	11	345	31
odbačena prijava	23	5	4	1	12	92	16

Izvor: DZS Republike Hrvatske, 2013.-2017.

Daljnjim prikazom izvršena je detaljna analiza svakog od stavaka promatranih članaka 266. - 272. Kaznenog zakona prema broju odbačaja kaznenih prijava, broju optuženih osoba i broju prijavljenih nepoznatih počinitelja kako bi mogli analizirati stavke navedenih članaka, sukladno implementaciji odredaba Konvencije.

4.2.3.1 Statistički podaci za kazneno djelo neovlaštenog pristupa

Grafikon 13 - Vrste odluka u strukturi prijavljenih osoba iz čl. 266. od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Iz grafikona 13 može se uočiti da je prijavljen višestruko veći udio nepoznatih počinitelja kaznenih djela u odnosu na ukupan broj prijavljenih osoba za ovo kazneno djelo. Broj odbačenih prijava je 2016. godine bio najveći s trendom porasta, što znači da državna odvjetništva nisu imala dovoljno kvalitetnih dokaza za procesuiranje ovih kaznenih djela. Valja napomenuti je da nepoznati počinitelji čine udio od gotovo 77%, što pokazuje složenost i sofisticiranost u počinjenju ovog kaznenog djela te potrebu dodatnog usavršavanja istražitelja.

Neovlašteni pristup (članak 266.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	8	3	3	3	**17**
nepoznati počinitelj	12	23	50	49	**134**
poznati počinitelj	9	4	5	22	**40**
odbačena prijava	1	1	2	19	**23**
UKUPNO	**30**	**31**	**60**	**93**	**214**

Tablica 18 - Vrste odluka u strukturi prijavljenih osoba iz čl. 266. KZ-a od 2013.-2017. godine

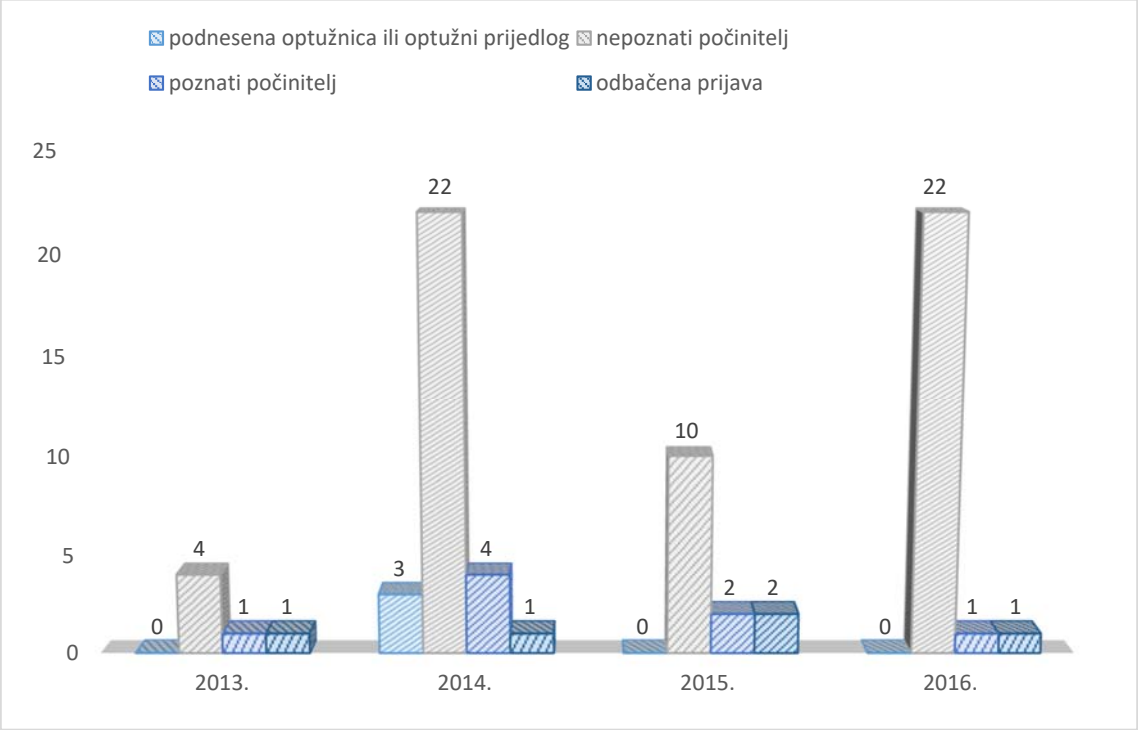
Izvor: DZS Republike Hrvatske, 2013.-2017.

U statističkim podacima nije evidentiran niti jedna prekinuta ili obustavljena istraga za ovo kazneno djelo. Valja ustvrditi kako nepoznati počinitelji čine više od 50% od ukupnog broja prijavljenih osoba (tablica 18) što ponovo ukazuje na nedostatnu stručno-kadrovsku kapacitiranost, možebitno nedosljedno provođenje zakonski odredbi ili manjkav normativni okvir.

4.2.3.2 Statistički podaci za kazneno djelo ometanje rada računalnog sustava

Nastavno prikazani podaci odnose se na broj podnesenih optužnica ili optužnih prijedloga, odbačenih prijava, kao i podatke o broju nepoznatih i poznatih počinitelja za sve stavke kaznenog djela ometanje rada računalnog sustava iz čl. 267. KZ-a.

Grafikon 14 - Vrste odluka u strukturi prijavljenih osoba iz čl. 267. KZ-a od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Analizom podataka grafikona 14 vidljivo je da gotovo i nema optužnica ili optužnih prijedloga osim 2014. godine, a razvidne se oscilacije 2016. godine u kojoj se ističe izrazito veliki broj nepoznatih počinitelja u odnosu na broj poznatih počinitelja ovog kaznenog djela.

Ometanje rada računalnog sustava, (članak 267.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	0	3	0	0	**3**
nepoznati počinitelj	4	22	10	22	**58**
poznati počinitelj	1	4	2	1	**8**
odbačena prijava	1	1	2	1	**5**
UKUPNO	**6**	**30**	**14**	**24**	**74**

Tablica 19 - Vrste odluka u strukturi prijavljenih osoba iz čl. 267. KZ-a od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

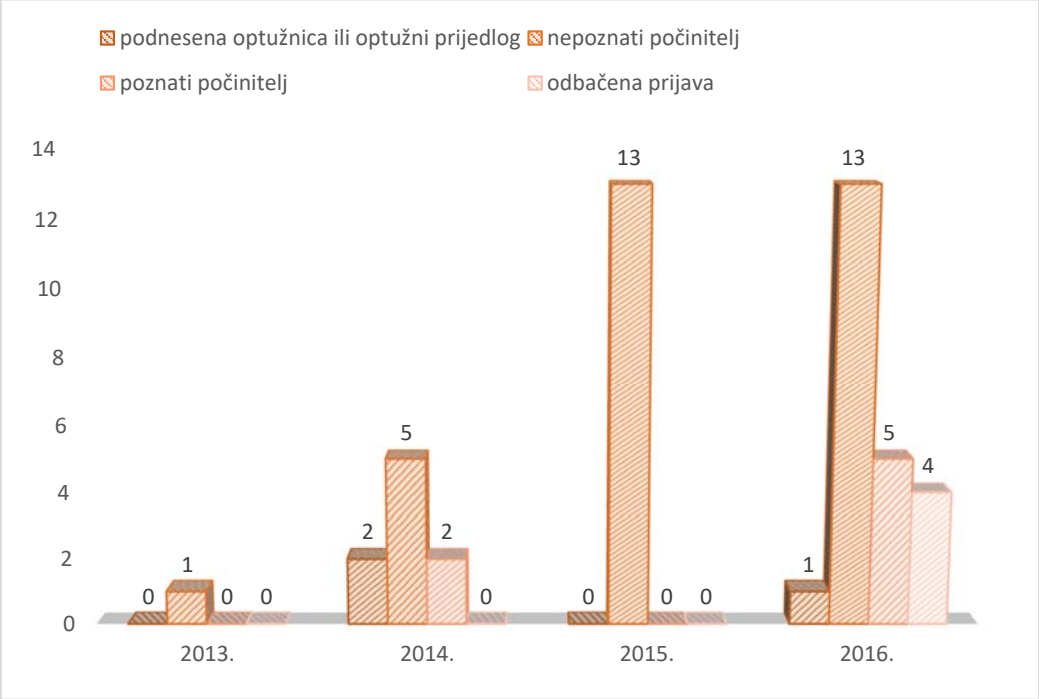
Podaci iz tablice 19 prikazuju da je kod kaznenog djela ometanja rada računalnog sustava udio nepoznatih počinitelja neusporedivo višestruko veći od broja poznatih počinitelja, što je uočljivo i kod prijašnjih modaliteta kaznenih djela u ovoj domeni. Broj odbačaja prijava je gotovo razmjeran broju podnesenih optužnica ili optužnih prijedloga, što pokazuje da se za ovo kazneno djelo gotovo i ne pokreću kazneni postupci.

U statističkim podacima nije evidentirana niti jedna prekinuta ili obustavljena istraga za ovo kazneno djelo.

4.2.3.3 Statistički podaci za kazneno djelo oštećenje računalnih podataka

Uvidom u podatke prikazane u grafikonu 15 stječe se uvid u strukturu podnesenih optužnica ili optužnih prijedloga, odbačenih prijava, kao i podatke o broju nepoznatih i poznatih počinitelja za sve stavke kaznenog djela računalne prijevare iz članka 268. Kaznenog zakona u vremenskom razdoblju 2013. do 2017.

Grafikon 15 - Vrste odluka u strukturi prijavljenih osoba iz čl. 268. KZ-a od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Uvidom u podatke vidljivo je da broj kaznenih prijava protiv nepoznatih počinitelja kontinuirano raste, te da je broj odbačenih prijava veći u odnosu na broj ukupno podnesenih optužnica ili optužnih prijedloga u promatranom razdoblju.

Oštećenje računalnih podataka, (članak 268.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	0	2	0	1	**3**
nepoznati počinitelj	1	5	13	13	**32**
poznati počinitelj	0	2	0	5	**7**
odbačena prijava	0	0	0	4	**4**
UKUPNO	**1**	**9**	**13**	**23**	**46**

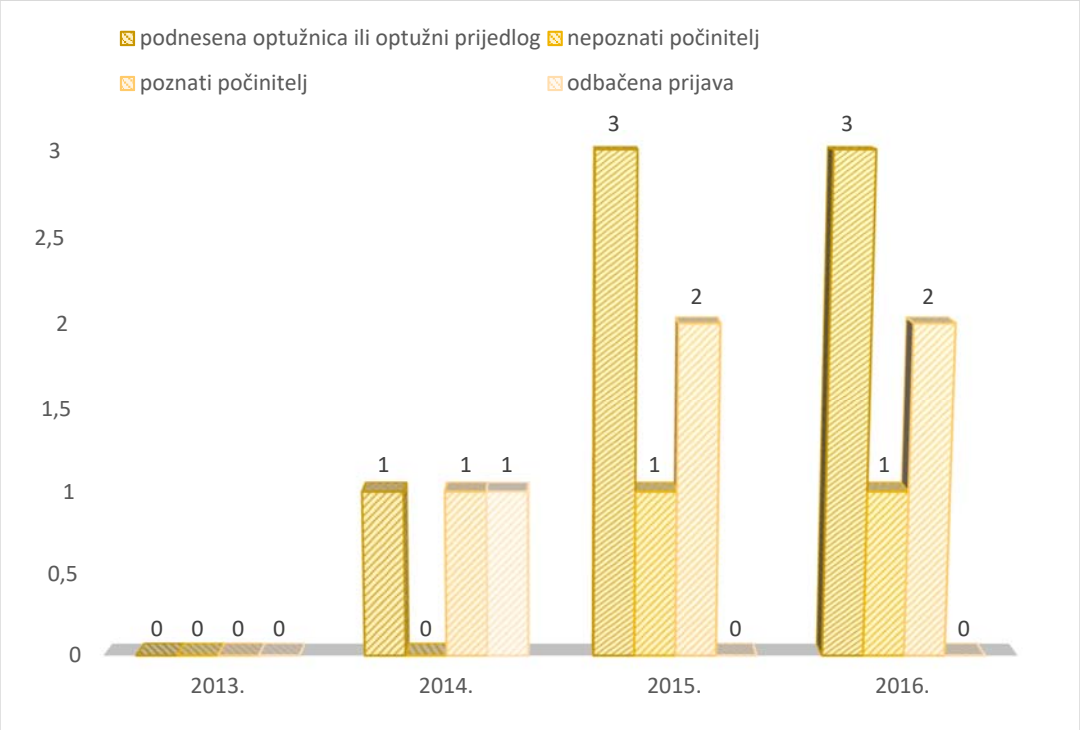
Tablica 20 - Struktura vrste odluka za prijavljene osobe iz čl. 268. od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

Broj nepoznatih počinitelja predstavlja 82% što je zajedničko u usporedbi s kaznenim djelima iz članka 266. i 267. KZ-a, što znači da je otkrivačka djelatnost značajno manja u slučajevima ovog kaznenog djela. U statističkim podacima nije evidentirana niti jedna prekinuta ili obustavljena istraga za ovo kazneno djelo.

4.2.3.4 Statistički podaci za kazneno djelo neovlaštenog presretanja računalnih podataka

Grafikon 16 - Vrste odluka u strukturi prijavljenih osoba iz čl. 269. KZ-a od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Iz grafikona 16 može se uočiti da je prijavljen zanemariv broj nepoznatih počinitelja kaznenih djela (tablica 21) u odnosu na ukupan broj prijavljenih osoba za ovo kazneno djelo. Broj odbačenih prijava je u 2015. do 2016. iznosi 66% od ukupno podnesenih optužnica ili optužnih prijedloga. Temeljem ovog pokazatelja, kao što je već više puta navedeno i ranije, može se ustvrditi da državna odvjetništva nisu imala dovoljno kvalitetnih dokaza za procesuiranje ovih kaznenih djela. Kompleksnost ovog kaznenog djela te, općenito, kaznenih djela iz domene kiberkriminala, zaslužuje puno veću pozornost prilikom postupanja zbog trenutno još uvijek velikog jaza između stanja u praksi i stupnja obrazovanosti istražitelja. Iz tablice 21 razvidan je neznatan broj podnesenih optužnica što izravno ukazuje na smanjeni opseg kriminalističkog istraživanja predmetnih kaznenih djela. Kao što je već ranije naglašeno, potrebno je inzistirati na primjerenoj kriminalističkoj obuci u ovom području suzbijanja kriminala i cjeloživotnom stručnom usavršavanju istražitelja u ovoj domeni.

Neovlašteno presretanje računalnih podataka (članak 269.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	0	1	3	3	**7**
nepoznati počinitelj	0	0	1	1	**2**
poznati počinitelj	0	1	2	2	**5**
odbačena prijava	0	1	0	0	**1**
UKUPNO	**0**	**3**	**6**	**6**	**15**

Tablica 21 - Vrste odluka u strukturi prijavljenih osoba iz čl. 269. KZ-a od 2013.-2017. godine

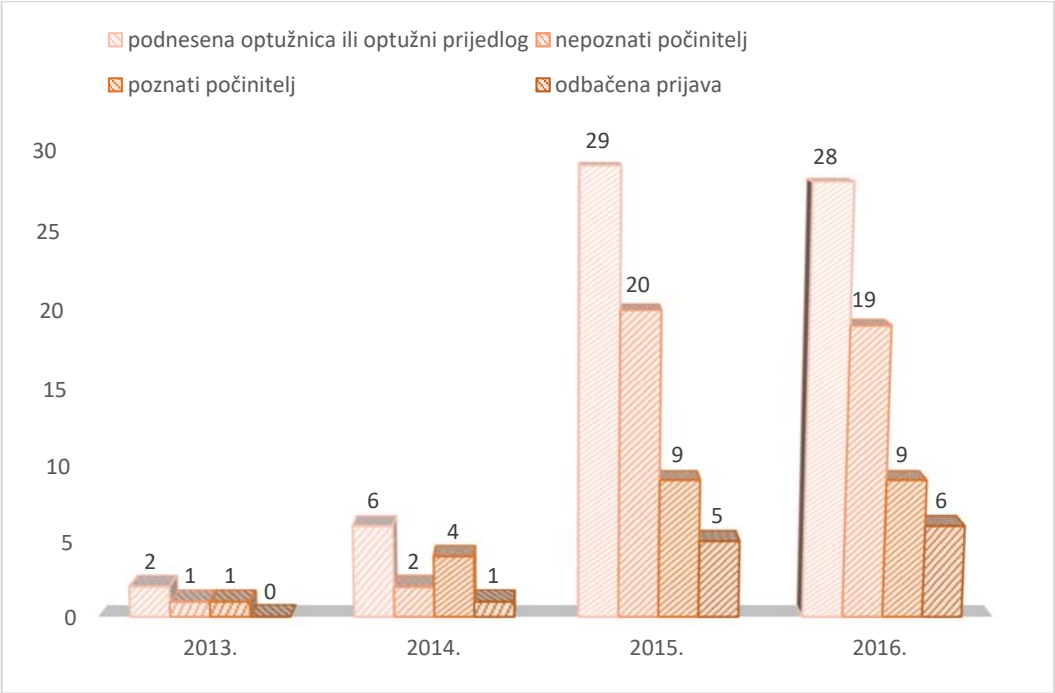
Izvor: DZS Republike Hrvatske, 2013.-2017.

U statističkim podacima nije evidentiran niti jedna prekinuta ili obustavljena istraga za ovo kazneno djelo.

4.2.3.5 Statistički podaci za kazneno djelo računalnog krivotvorenja

Sljedeći podaci odnose se na udio i dinamiku podnesenih optužnica ili optužnih prijedloga, odbačenih prijava, kao i podatke o broju nepoznatih i poznatih počinitelja za sve stavke kaznenog djela računalno krivotvorenje iz čl. 270.

Grafikon 17 - Vrste odluka u strukturi prijavljenih osoba iz čl. 270. KZ-a od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Iz grafikona 17 može se uočiti da je prijavljen relativno velik broj nepoznatih počinitelja kaznenih djela u odnosu na ukupan broj prijavljenih osoba za ovo kazneno djelo. Broj odbačenih prijava je 2016. godine bio najveći, što znači, kao što je i ranije navedeno, da državna odvjetništva nisu imala dovoljno kvalitetnih dokaza za procesuiranje ovih kaznenih djela.

Računalno krivotvorenje (članak 270.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	2	6	29	28	**65**
nepoznati počinitelj	1	2	20	19	**42**
poznati počinitelj	1	4	9	9	**23**
odbačena prijava	0	1	5	6	**12**
UKUPNO	**4**	**13**	**63**	**62**	**142**

Tablica 22 - Vrste odluka u strukturi prijavljenih osoba iz čl. 270. KZ-a od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

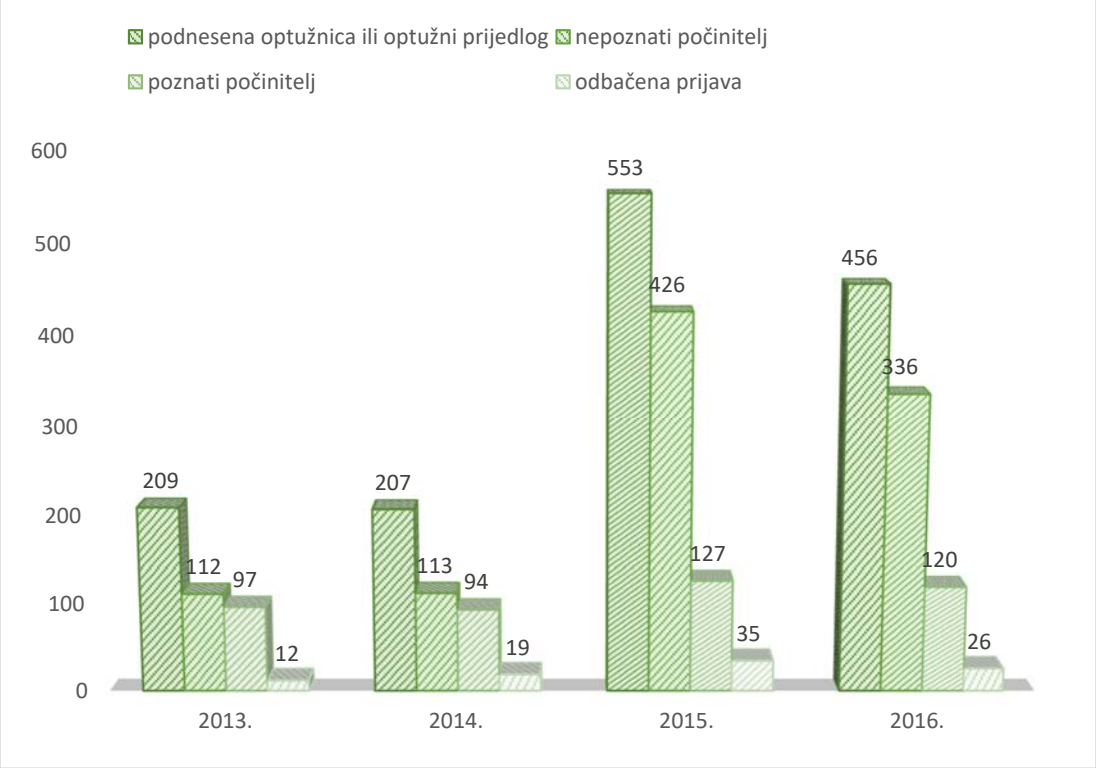
Podaci iz tablice 22 ukazuju na relativno velik udio nepoznatih počinitelja koji je dvostruko veći od broja poznatih počinitelja.

U statističkim podacima nije evidentirana niti jedna prekinuta ili obustavljena istraga za ovo kazneno djelo.

4.2.3.6 Statistički podaci za kazneno djelo računalna prijevara

Grafikon 18 daje uvid u podatke koji se odnose na broj podnesenih optužnica ili optužnih prijedloga, odbačenih prijava, kao i podatke o broju nepoznatih i poznatih počinitelja za sve stavke kaznenog djela računalne prijevare iz članka 271. Kaznenog zakona u vremenskom razdoblju 2013. do 2017., koje predstavlja najveći udio u ukupnom broju kaznenih djela iz domene kaznenih djela protiv računalnih sustava, programa i podataka, a drugo je po broju izvršenja kaznenih djela iz glave gospodarskog kriminaliteta gdje spadaju i računalna kaznena djela. Otkrivačka djelatnost i učinkovitost kriminalističkog istraživanja ove vrste kaznenog djela je više nego dvostruko veća u 2015. i 2016. godini vjerojatno stoga što je ova domena suzbijanja kriminala ojačana novim kadrovskim i tehničkim resursima.

Grafikon 18 - Vrste odluka u strukturi prijavljenih osoba iz čl. 271. KZ-a od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Uvidom u tablicu 23 vidljivo je kako broj kaznenih prijava protiv nepoznatih počinitelja kontinuirano raste, te da je broj odbačenih prijava u opadanju.

Računalna prijevara, (članak 271.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	209	207	553	456	**1425**
nepoznati počinitelj	112	113	426	336	**987**
poznati počinitelj	97	94	127	120	**438**
odbačena prijava	12	19	35	26	**92**
UKUPNO	**430**	**433**	**1141**	**938**	**2942**

Tablica 23 - Vrste odluka u strukturi prijavljenih osoba iz čl. 271. KZ-a od 2013.-2017. godine

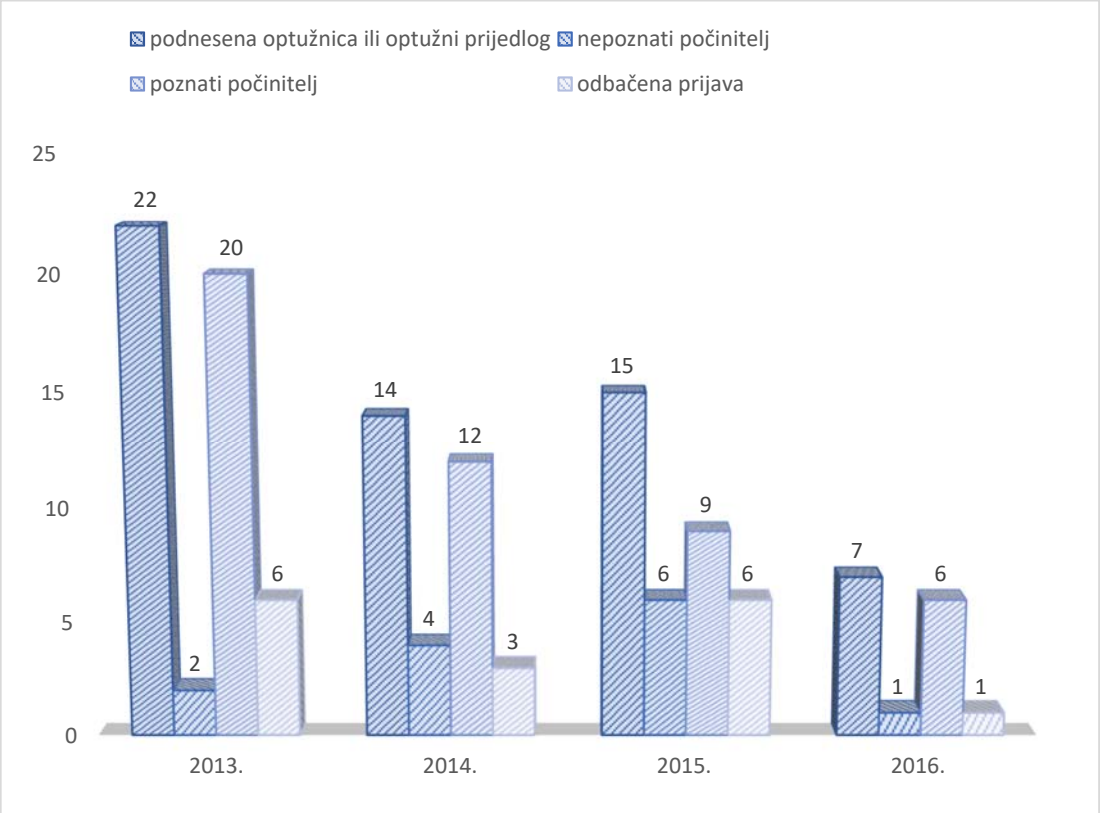
Izvor: DZS Republike Hrvatske, 2013.-2017.

Broj nepoznatih počinitelja čini 69% što je zajednička karakteristika u odnosu na kaznena djela iz članka 266. i 267., što znači da je učinkovitost policije relativno slaba u otkrivanju počinitelja ovog kaznenog djela.

4.2.3.7 Statistički podaci za kazneno djelo zloporabe naprava

Grafikon 19 pruža uvid u podatke koji se odnose na broj podnesenih optužnica ili optužnih prijedloga, odbačenih prijava, kao i podatke o broju nepoznatih i poznatih počinitelja za sve stavke kaznenog djela računalne prijevare iz članka 272. Kaznenog zakona u vremenskom razdoblju od 2013. do 2017. godine.

Grafikon 19 - Vrste odluka u strukturi prijavljenih osoba iz čl. 272. KZ-a od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Uvidom u grafikon 19 i tablicu 24 vidljivo je da je riječ o minornom broju slučajeva sudeći po broju podnesenih optužnica ili optužnih prijedloga koji, pored toga, kontinuirano pada, što je slučaj i kad je riječ o broju otkrivenih počinitelja.

Zloporaba naprava, (članak 272.)	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
podnesena optužnica ili optužni prijedlog	22	14	15	7	**58**
nepoznati počinitelj	2	4	6	1	**13**
poznati počinitelj	20	12	9	6	**47**
odbačena prijava	6	3	6	1	**16**
UKUPNO	**50**	**33**	**36**	**15**	**134**

Tablica 24 - Vrste odluka u strukturi prijavljenih osoba iz čl. 272. KZ-a od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

Broj nepoznatih počinitelja predstavlja 82%, što je slično u usporedbi s kaznenim djelima iz članka 266. i 267., što znači da je otkrivačka djelatnost daleko slabija u slučajevima ovog kaznenog djela.

U statističkim podacima nije evidentirana niti jedna prekinuta ili obustavljena istraga za ovo kazneno djelo.

4.2.4 Statistički podaci o broju optuženih punoljetnih osoba

DZS definira u svojim napomenama da je "optužena osoba punoljetna osoba protiv koje je sudu podnesena optužnica ili privatna tužba, protiv koje je kazneni postupak pravomoćno završen odlukom suda kojom se obustavlja kazneni postupak, optužba odbacuje, donosi oslobađajuća ili odbijajuća presuda, određuje prisilni smještaj za neubrojivu osobu ili se počinitelj proglašava krivim".[143]

[143] Statistička izvješća broj 1504, Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude, DZS, Zagreb, 2012., stranica 8.

Broj optuženih osoba prikazan je u tablici 25 za godinu u kojoj je osoba optužena.

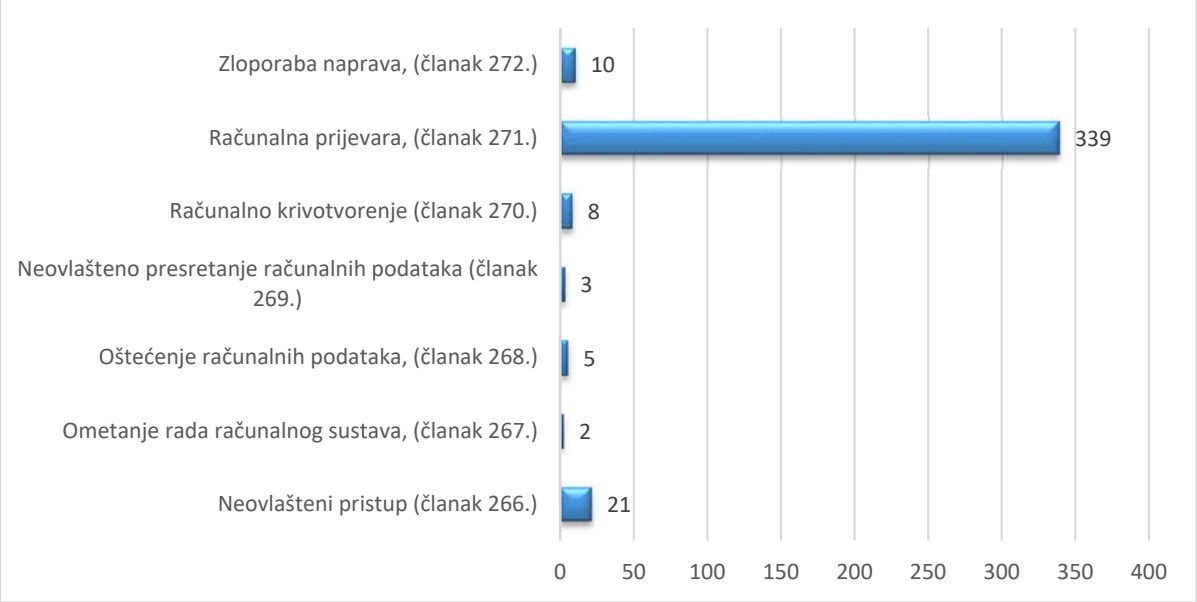
Glava XXV KZ-a	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
Neovlašteni pristup (članak 266.)	9	4	3	5	21
Ometanje rada računalnog sustava, (članak 267.)	0	0	1	1	2
Oštećenje računalnih podataka (članak 268.)	2	1	1	1	5
Neovlašteno presretanje računalnih podataka (članak 269.)	0	0	0	3	3
Računalno krivotvorenje (članak 270.)	2	2	1	3	8
Računalna prijevara (članak 271.)	100	81	65	93	339
Zloporaba naprava (članak 272.)	0	2	7	1	10
UKUPNO	113	90	78	107	388

Tablica 25 - Broj optuženih punoljetnih osoba od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

U grafikonu 20 prikazan je broj optuženih punoljetnih osoba za kaznena djela iz članka 266.-272. sa svim stavcima, za vremensko razdoblje od 2013. do 2017. godine, koji se temelje na podacima Državnog zavoda za statistiku.

Grafikon 20 – Vrste kaznenih djela računalnog kriminaliteta u strukturi optuženih punoljetnih osoba od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

Podaci u tablici 26 pokazuju da se broj podignutih optužnica ili optužnih prijedloga u gotovo 87% slučajeva odnosi na kazneno djelo računalna prijevara.

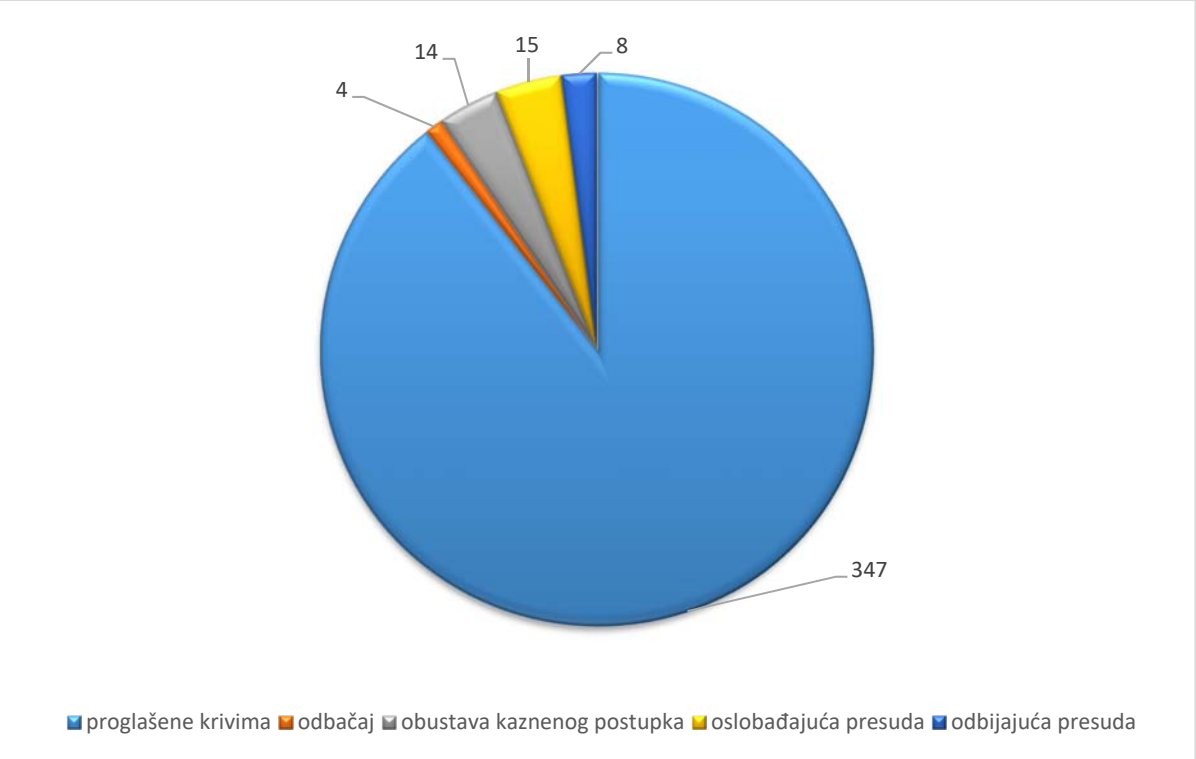
	2013.	**2014.**	**2015.**	**2016.**	**UKUPNO**
proglašene krivima	97	83	68	99	347
odbačaj	3	0	0	1	4
obustava kaznenog postupka	3	5	2	4	14
oslobađajuća presuda	7	0	5	3	15
odbijajuća presuda	3	2	3	0	8
UKUPNO	113	90	78	107	388

Tablica 26 - Vrste odluka u strukturi optuženih punoljetnih osoba od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

U grafikonu 21 prikazane su vrste odluka u strukturi optuženih punoljetnih osoba za kaznena djela iz članka 266. - 272. sa svim stavcima u tablici 26, koji se temelje na podacima Državnog zavoda za statistiku te je vidljivo da je bilo svega 4 odbačaja, odnosno oko 1%.

Grafikon 21 - Vrste odluka u strukturi optuženih punoljetnih osoba od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

U najvećem broju slučajeva radi se o pravomoćnim presudama za počinjenje promatranih kaznenih djela, dok je obustava i odbačaj prisutno u svega 4%, a oslobađajuća presuda u svega 3,8% optuženih punoljetnih osoba. Osobe koje su proglašene krivima sudjeluju s gotovo 90%.

4.2.5 Statistički podaci o broju osuđenih punoljetnih osoba

DZS također definira u svojim napomenama da je "osuđena osoba punoljetna osoba proglašena krivom prema kojoj su izrečene kaznene sankcije: zatvor, novčana kazna, odgojne mjere, sudska opomena i osoba proglašena krivom, a oslobođena od kazne".[144]

Glava XXV KZ-a	**2013.**	**2014.**	**2015.**	**2016.**	**UKUPNO**
Neovlašteni pristup (članak 266.)	8	2	2	5	17
Ometanje rada računalnog sustava (članak 267.)	0	0	1	1	2
Oštećenje računalnih podataka, (članak 268.)	1	1	0	0	2
Neovlašteno presretanje računalnih podataka (članak 269.)	0	0	0	3	3
Računalno krivotvorenje (članak 270.)	2	1	1	3	7
Računalna prijevara (članak 271.)	86	78	59	86	309
Zloporaba naprava (članak 272.)	0	1	5	1	7
UKUPNO	97	83	68	99	347

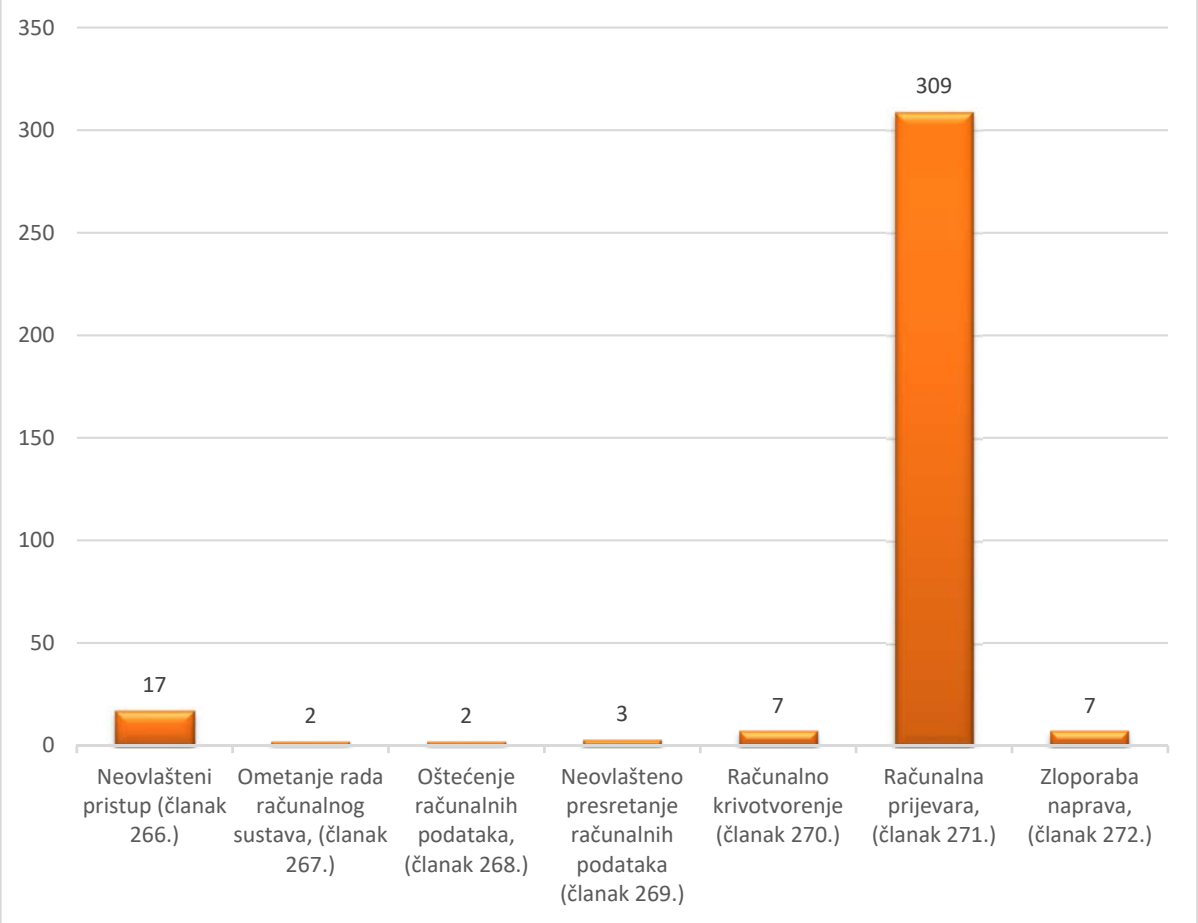
Tablica 27 – Vrste kaznenih djela računalnog kriminaliteta u odnosu na broj osuđenih punoljetnih osoba od 2013.-2017. godine

Izvor: DZS Republike Hrvatske, 2013.-2017.

U tablici 27 je prikazan broj osuđenih punoljetnih osoba za kaznena djela iz članka 266. - 272. sa svim stavcima, za vremensko razdoblje od 2013. do 2017. godine, koji se temelje na podacima Državnog zavoda za statistiku.

[144] Statistička izvješća broj 1504, Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude, DZS, Zagreb, 2012., stranica 8.

Grafikon 22 – Vrste kaznenih djela računalnog kriminaliteta u strukturi osuđenih punoljetnih osoba od 2013.-2017. godine



Izvor: DZS Republike Hrvatske, 2013.-2017.

U promatranom razdoblju vidljivo je da je i nadalje najzastupljenije kazneno djelo iz čl. 271. u odnosu na promatrane članke, a to je kazneno djelo računalne prijevare.

U ukupnom broju osuđenih osoba preko 89% slučajeva se odnosi na kazneno djelo računalne prijevare. Kao što je vidljivo iz grafikona 22, kazneno djelo računalne prijevare je dominantno prema broju prijavljenih kaznenih djela u katalogu kaznenih djela koja se odnose na računalni kriminalitet. Može se ustanoviti kako je otkrivačka djelatnost policije u referentnom razdoblju neujednačena najvjerojatnije zbog novih modaliteta počinjenja kaznenog djela računalne prijevare, kao i sve veće infiltracije i utjecaja različitih svakodnevnih aktivnosti građana koji se koriste modernijim tehnologijama za počinjenje inkriminiranih radnji.

To mogu biti plaćanja računa putem internet bankarstva, sklapanje raznih ugovora na daljinu i slično, a poseban problem u ovom segmentu predstavlja nedostatak potrebnih specijalista u ovom sektoru, poglavito iz područja tijela za izvršenje zakonodavstava, što se primarno odnosi na nedostatno educirane stručnjake u ovom području., Ova tema se posebno elaborira u poglavlju koje razmatra Akcijski plan i ulogu Policijske akademije kao kontakt točke iz Strategije kibernetičke sigurnosti. Za napomenuti je da su Akcijski plan i Strategija doneseni tek 2016. godine, a za pretpostaviti je da je počinjenje ovog kaznenog djela imalo značajan utjecaj u njihovu stvaranju. Uočljiv je, također, nerazmjerno mali udio optuženih u odnosu na prijavljene osobe što indicira na needuciranost kako istražitelja, tako i sudaca za kompetentno i uspješno otkrivanje ove vrste kriminala.

4.3 Kvalitativna analiza pojmova *Cyberspace* i *Cybercrime*

Izvor podataka za ovo istraživanje čine dokumenti odabranih država, ali i nekih drugih zemalja (u pravilu, strategije borbe protiv kiberkriminala) koji sadrže obrasce suradnje institucija koje se bore protiv kiberkriminala, kao i međunarodnih organizacija i istraživačkih institucija. U navedenim dokumentima pojašnjeni su pojmovi *Cyber space, Cyberspace, Cyber crime i Cybercrime*, te smo analizirali iste i njihove međuodnose. Istraživanje uključuje provođenje kvalitativne analize sadržaja odabranih izvora, a osim strategija, obuhvaćeni su zaključci, uredbe, direktive, odluke, preporuke i mišljenja.

Prema Mayringu "kvalitativna analiza sadržaja je empirijski i metodološki kontrolirana analiza tekstova unutar komunikacijskog konteksta" (Mayring, 2000). Prema Halperin i Heath "analiza sadržaja kao kvalitativna istraživačka metoda ima u fokusu proučavanje latentnog sadržaja te pretpostavlja da je moguće otkriti značenja, motive i svrhu unutar teksta te izvesti valjane, skrivene ili inherentne zaključke koji su značajni za istraživača. Ovom se metodom može istražiti kontekst unutar kojeg su dokumenti nastali te predstavlja interpretativni oblik analize u svrhu otkrivanja značenja, vrijednosti, motiva i svrhe teksta". (Halperin i Heath, 2012, str. 319) Ova metoda istraživanja ne zahtijeva stabilno i nepromjenjivo značenje riječi, već je karakterizira osjetljivost na uporabu riječi i kontekst unutar kojeg se koristi.

Dokumenti su odabrani prema kriterijima usmjerenosti na konceptualizaciju kibernetičkog kriminala – *Cybercrime* i kibernetičkog prostora – *Cyberspace* (kiberkriminal i kiberprostor). Riječ je o dokumentima koji su izravno u funkciji provođenjem zakona i mjera u borbi protiv kibernetičkog kriminaliteta i/ili razmatraju "unutarnje" ili "vanjske" aspekte sigurnosnih politika, a usvojeni su ili odobreni od strane nadležnih institucija te na taj način predstavljaju službenu politiku te zemlje. Svi analizirani dokumenti su javni i kao takvi dostupni na web stranicama državnih institucija. Dio dokumenata je službeno preveden na hrvatski jezik (kao što je Konvencija o kibernetičkom kriminalu ili Oxfordski rječnik) ali će se za kvalitativnu analizu koristiti engleski jezik, dok se hrvatski pravni okvir spominje isključivo u poglavlju o usporedbi pravnih rješenja.

Drugi dio istraživanja odnosi se na opis podataka tako da se identificiraju i kodiraju najčešće korištene riječi (frekvencije) koji oblikuju pojmove kiberprostor i kiberkriminal, odnosno borbu protiv kibernetičkog kriminala. Za potrebe ovog doktorskog rada analizirana su ukupno 64 dokumenata u kojima se spominju definicije pojmova *Cyber space, Cyberspace, Cyber crime i Cybercrime*, kao što je vidljivo u tablici 28.

	Broj analiziranih definicija
Cyberspace	41
Cybercrime	23
Ukupno dokumenata	**64**

Tablica 28 - Analizirane definicije

Izvor – vlastita izrada

Pojmovi *Cyber space i Cyberspace* analizirani su kao istovjetni i koristit će se samo pojam *Cyberspace* budući da se radi o istom značenju. Naime, različiti autori koriste različiti standard pisanja, a istoznačnica u hrvatskom književnom jeziku se odnosi na kibernetički prostor ili kiberprostor. Ista situacija odnosi se na pojmove *Cyber crime i Cybercrime* te će se koristiti samo pojam *Cybercrime,* a istoznačnica u hrvatskom književnom jeziku se odnosi na kibernetički kriminal (računalni kriminal) ili kiberkriminal.

Iz gore navedenog proizlazi da je za pojam *Cyberspace* analizirano ukupno 41 odabrani dokument unutar kojeg je izdvojena definicija za traženi pojam, dok je za pojam *Cybercrime* analizirano 23 odabrana dokumenata.

Analiza pojmova obavljena je na način da su prikupljani dokumenti iz sljedećih izvora i po sljedećem redoslijedu:

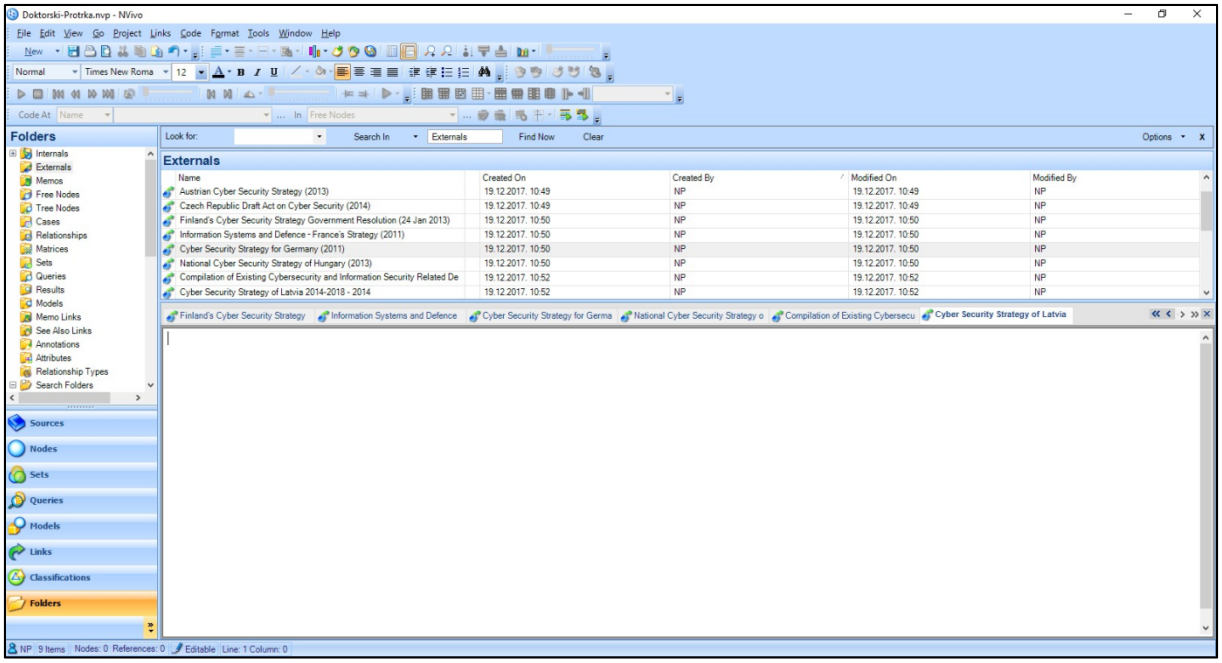
- stalne članice Vijeća sigurnosti UN-a, P5[145],
- države koje nisu članice skupine P5, ali pripadaju u radnu skupinu UN-a:, UNGGE4[146],
- ostale države,
- međunarodne organizacije,
- Vijeće Europe,
- Europska Unija,
- NATO - *North Atlantic Treaty Organization*,
- Rječnik engleskog jezika Oxford - *Oxford English Dictionary.*

Analizirani dokumenti se odnose u najvećem dijelu na nacionalne strategije kibernetičke sigurnosti, dokumente UN-a, dokumente međunarodnih organizacija, kao i odabrane rječnike. Analizi su pomogli i izvori europske agencije ENISA[147], kao i NATO CCDCOE[148]. Ispitivanjem i analizom dokumentacije koja je službeno dostupna na engleskom jeziku obuhvaćeni su niže navedeni dokumenti (NATO CCDCOE, 2017).

Naprijed navedeni postupak izvršen je uz pomoć softvera NVivo koji je omogućio organiziranje i izvještavanje o velikoj količini definicija. Budući da su svi pribavljeni dokumenti objavljeni na engleskom jeziku, svi su dokumenti obrađeni u NVivo softveru na engleskom jeziku.

[145] Kina, Rusija, Velika Britanija, SAD i Francuska.
[146] "UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications": Bjelorusija, Brazil, Kina, Kolumbija, Egipat, Estionija, Francuska, Njemačka, Gana, Izrael, Japan, Kenija, Malezija, Meksiko, Pakistan, Rusija, Južna Koreja, Španjolska, Velika Britanija i SAD.
[147] "European Union. European Union Agency for Network and Information Security", "National Cyber Security Strategies in the World," ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world stranica posjećena 22. prosinca 2017.
[148] "North Atlantic Treaty Organization, NATO Cooperative Cyber Defence Center of Excellence", "Strategies & Policies," NATO CCDCOE, https://www.ccdcoe.org/strategies-policies.html stranica posjećena 22. prosinca 2017.

Slika 1 - Softver NVivo



Za pojam *Cyberspace* analizirano je ukupno 41 odabrana definicija koje sadrže ukupno 60 rečenica, odnosno 1 420 riječi, a one se nalaze u prilogu doktorskog rada.

Red. br.	Element	Broj ponavljanja	Učestalost ponavljanja %	Pozicija
1.	*information*	37	4,2%	1
2.	*cyberspace*	33	3,7%	2
3.	*networks*	31	3,5%	3
4.	*systems*	28	3,2%	4
5.	*data*	21	2,4%	5
6.	*computer*	20	2,3%	6
7.	*internet*	16	1,8%	7
8.	*global*	14	1,6%	8
9.	*environment*	13	1,5%	9
10.	*space*	11	1,2%	10

Tablica 29 - Rezultati kvantitativne tekstualne analize obrađenih pojmova *Cyber space* i *Cyberspace*

Izvor: softver NVivo

Analizirajući glavne elemente navedene 41 definicije pojma Cyberspace prikazane u tablici 29, razvidno je da se riječ *information (*hrv. informacija*)* spominje u 37 ponavljanja od ukupnog fonda analiziranih riječi, dok je slijedi riječ *Cyberspace (hrv. k*ibernetički prostor*)*, na trećem mjestu se nalazi riječ *networks (*hrv. mreže - ekvivalent kontekstu računalne mreže*)*, a na četvrtom mjestu riječ *systems* (hrv. sustavi - ekvivalent kontekstu računalni sustavi*)*, dok je riječ *data (*hrv. podaci*)* na petom mjestu.

Red. br.	Element	Broj ponavljanja	Učestalost ponavljanja %	Istaknutost
1.	*and*	99	7%	50.6
2.	*the*	83	5,8%	51.6
3.	*of*	60	4,2%	55.7
4.	*information*	37	2,6%	53.7
5.	*cyberspace*	33	2,3%	52.7
6.	*networks*	31	2,2%	49.6
7.	*systems*	28	2%	52.7
8.	*to*	27	1,9%	38.4
9.	*is*	24	1,7%	53.9
10.	*a*	24	1,7%	54.2
11.	*in*	22	1,5%	43.7
12.	*data*	20	1,4%	49.2
13.	*by*	19	1,3%	41.6
14.	*computer*	19	1,3%	48.9
15.	*internet*	16	1,1%	56.7
16.	*global*	14	1%	57.5
17.	*which*	13	0,9%	40.2
18.	*environment*	13	0,9%	42.5
19.	*all*	12	0,8%	40.3
20.	*as*	12	0,8%	46.4

Tablica 30 - Rezultati kvantitativne tekstualne analize nefiltriranih riječi definicija pojma *Cyberspace*

Izvor: softver NVivo

U tablici 30 prikazani su rezultati kvantitativne tekstualne analize nefiltriranih riječi definicija pojma *Cyberspace*, a od svih pojmova posebno značajno se ističe pojam Internet, kao temeljna infrastruktura kiberprostora i kiberkriminala, jer se nalazi tek na petnaestom mjestu, i ukupno se ponavlja samo 16 puta, odnosno u 0,7% od analiziranih 1 420 riječi, koji definiraju pojam *Cyberspace*.

Za pojam *Cybercrime* analizirano je ukupno 23 odabrane definicije (u prilogu doktorskog rada), koje se sastoje od 44 rečenice, odnosno 922 riječi.

Red. Br.	Element	Broj ponavljanja	Učestalost ponavljanja %	Pozicija
1.	*information*	20	3,7%	1
2.	*crime*	13	2,4%	2
3.	*criminal*	12	2,2%	3
4.	*cybercrime*	11	2%	4
5.	*systems*	10	1,8%	5
6.	*offences*	10	1,8%	5
7.	*cyberspace*	10	1,8%	5
8.	*committed*	9	1,7%	6
9.	*data*	8	1,5%	7
10.	*computer*	7	1,3%	8

Tablica 31 - Rezultati kvantitativne tekstualne analize obrađenih pojmova *Cyber crime* i *Cybercrime*

Izvor: softver NVivo

Analizirajući glavne elemente ukupno 23 odabrane definicije pojma Cybercrime, iz tablice 31 je razvidno da se riječ *information* (hrv. informacija) spominje u 20 ponavljanja od ukupnog fonda analiziranih riječi iz prikazanih definicija, dok je slijedi riječ *crime (*hrv. kriminalitet), na trećem mjestu se nalazi riječ *criminal* (hrv. kriminal), a na četvrtom mjestu riječ *Cybercrime* (hrv. kibernetički kriminalitet).

Red. br.	Element	Broj ponavljanja	Učestalost ponavljanja %	Istaknutost
1.	*the*	62	6,8%	55
2.	*of*	51	5,6%	50.7
3.	*and*	38	4,2%	50.3
4.	*or*	35	3,8%	50
5.	*information*	20	2,2%	49.2
6.	*to*	19	2,1%	55.8
7.	*a*	18	2%	38.6
8.	*in*	17	1,9%	54.1
9.	*are*	16	1,8%	48.5
10.	*crime*	13	1,4%	41.4
11.	*criminal*	12	1,3%	41.6
12.	*cybercrime*	11	1,2%	43.8
13.	*offences*	10	1,1%	43.3
14.	*cyberspace*	10	1,1%	49.8
15.	*systems*	10	1,1%	58.9
16.	*as*	9	1%	31
17.	*which*	9	1%	62.4
18.	*on*	8	0,9%	47.1
19.	*committed*	8	0,9%	65.7
20.	*data*	8	0,9%	74.1

Tablica 32 - Rezultati kvantitativne tekstualne analize nefiltriranih riječi definicija pojma *Cybercrime*

Izvor: softver NVivo

U tablici 32 prikazani su rezultati kvantitativne tekstualne analize nefiltriranih riječi definicija pojma *Cybercrime*, a od svih pojmova posebno se ističe pojam Internet, kao temeljna infrastruktura kiberkriminala, jer se nalazi tek na dvadesetšestom mjestu i ukupno se ponavlja samo 6 puta, odnosno u 0,7% od analiziranih 922 riječi, koji definiraju pojam *Cybercrime*.

Temeljem rezultata iz tablica 29 i 31, a koje prikazuju tekstualnu analizu prvih deset riječi iz odabranih definicija pojmova *Cyberspace* i *Cybercrime* (u prilogu 8.1. i 8.2. doktorskog rada), a isključenjem članova i veznika (a, the, all, at, or, and, to, in, is, by), vidljivo je da autori definicija najčešće koriste riječ *information* i to kod definicije pojma *Cyberspace* u 37 ponavljanja od ukupno 41 definicije, a istu riječ u 20 od ukupno odabrane 23 definicije pojma *Cybercrime,* što rezultira s gotovo 90%. Kod pojma *Cyberspace* druga najčešće korištena riječ je očekivana- *cyberspace,* a kod pojma *Cybercrime* druga najčešće korištena riječ je *crime,* dok se riječ *cybercrime* nalazi na četvrtom mjestu iza riječi *crime.* Nefiltrirani rezultati svih riječi nalaze se u tablicama 30 i 32.

Rezultati tekstualne analize nefiltriranih definicija pojmova *Cyberspace* i *Cybercrime* iz tablice 30 i 32, prikazuju frekvenciju najčešće pojavljivanih različitih riječi u odabranim definicijama temeljem analize odnosa ukupnog broja riječi. Pojam Internet se navodi kao temeljna infrastruktura proučavanih pojmova *Cyberspace* i *Cybercrime* u neznatnom broju od svega 0,7% .

Analiza dva zadana pojma *Cyberspace i Cybercrime* ukazuje da, iako se radi o dva povezana pojma, gotovo dvostruko više definicija odnosi se na pojam *Cyberspace*.

5. ZAKLJUČAK

Glavni problem ovog istraživanja bio je analizirati trenutno stanje različitih aspekata poimanja kibernetičkog prostora, kao i kibernetičke sigurnosti koja je ugrožena činjenjem niza modaliteta kaznenih djela u kibernetičkom prostoru, odnosno kiberkriminala. Stoga je cilj doktorskog rada bio prikazati i na novim osnovama analizirati modalitete činjenja, istraživanja i vještačenja kaznenih djela koja se čine u kibernetičkom prostoru kroz konkretne rezultate statističke obrade, kao i trendove u četverogodišnjem razdoblju za sva kaznena djela iz domene računalnog kriminaliteta, te uz upotrebu kvalitativne analize tekstualnih sadržaja obrađenih dokumenata prikazati relevantne pojmovne definicije koje impliciraju domenu sigurnosti i suradnje u međunarodnom kibernetičkom prostoru. U tu svrhu istraživanje je dalo odgovore na sljedeća istraživačka pitanja: 1. Kakva je dinamika kreiranja obrazaca za oblikovanje kibernetičko-sigurnosne politike s obzirom na endogene i egzogene čimbenike, dinamiku, područje i opseg međunarodne suradnje? 2. Kakav je međuodnos kooperacije, koordinacije, integracije i učinkovitosti u analiziranim dokumentima koji sadrže pojmove Cyberspace i Cybercrime s aspekta sigurnosti u kibernetičkom prostoru? 3. Podupiru li nalazi vezani uz dinamiku promjene opsega i obrazaca međunarodne suradnje i sigurnosti u kibernetičkom prostoru i međuodnos pokazatelja kooperacije, koordinacije i integracije postojeće teorijske paradigme? Temeljno pitanje ove disertacije odnosi se na neograničenost nacionalnih jurisdikcija kibernetičkog prostora, a samim time i nedefiniranu jurisdikciju rješavanja problema nedopuštenih ponašanja u kibernetičkom prostoru.

U okviru prvoga istraživačkog pitanja rezultati istraživanja analize kaznenopravnih specifičnosti su pokazali kako rješenja nekih stranih država, uzimajući u obzir razlike između civilnog pravnog sustava zemalja srednje Europe i anglosaksonskog sustava Velike Britanije i vremenski aspekt donošenja pravnih rješenja, na ekvivalentan način donose zakonski opis i klasifikaciju kaznenih djela iz domene kiberkriminala u obliku inkriminacija kiberkriminaliteta. Kako od odabranih zemalja jedino Švedska nije ratificirala Konvenciju, važno je ustvrditi da unutar opisa navedenih kaznenih djela jedino ova država nema usklađeno definirane istovjetne članke za najraširenije kazneno djelo računalne prijevare i kazneno djelo računalnog krivotvorenja. Ostale analizirane zemlje, bez obzira na vrstu pravnog sustava, sadrže gotovo istovjetne članke kaznenih zakona kojima uređuju navedenu problematiku.

Slovenija i Rumunjska su potpuno usporedive hrvatskom zakonodavstvu, dok su rješenja Austrije i Njemačke gotovo identična te usporediva s hrvatskim pravnim određenjima. Analiza poredbenih kaznenopravnih rješenja u prikazanim državama pokazala je da je većina njih dosljedno implementirala međunarodne norme koje reguliraju ovu problematiku, što olakšava međunarodnu policijsku i pravosudnu suradnju, kao i djelovanje zajedničkih istražnih timova (JIT). Rumunjska je sustavno i detaljno normirala nezakonite radnje glede kaznenih djela računalnog kriminaliteta u posebnom zakonu (*lex specialis)* u kojem se navode kaznena djela elektroničkog poslovanja, i navedene norme pokrivaju i problematiku prevencije i suzbijanja kibernetičkog kriminala, što kod nas nije slučaj. Stoga predlažemo da se predmetni sadržaj i metodologija ovog Zakona nomotehnički razmotre te da se suštinske prednosti ovog Zakona inkorporiraju i u hrvatsko zakonodavstvo.

Dinamika kreiranja obrazaca za oblikovanje kibernetičko-sigurnosne politike s obzirom na endogene i egzogene čimbenike, dinamiku, područje i opseg međunarodne suradnje prikazuje ugroze i rizike koji se pojavljuju u kibernetičkom prostoru, a imaju međunarodni karakter jer nisu omeđeni granicama država, što se razmatra u okviru drugog istraživačkog pitanja. Naime, kibernetički prostor ima međunarodni karakter, širi se izvan granica pojedinih država te korisnici u takvom prostoru djeluju na globalnoj razini. Iz navedenih razloga potrebno je uspostaviti koordinirano djelovanje i pojačati suradnju na međunarodnoj razini u zaštiti takvog prostora, kao i uspostavu jedinstvenog pravnog okvira u aktivnostima na području kibernetičke sigurnosti, te izgradnji povjerenja i razmjeni stečenih znanja. Analizirani relevantni dokumenti se odnose u najvećem dijelu na nacionalne strategije kibernetičke sigurnosti, dokumente UN-a, međunarodnih organizacija, kao i rječnike u ovom specifičnom području koje se stalno razvija i poprima nove oblike.

Za provođenje istraživanja, korišten je softver NVivo koji je omogućio organiziranje i izvještavanje iz prikupljenih dokumenata. Temeljem provedene analize navedenih dokumenata prikazanih u ovoj disertaciji i ekstrakcijom frekvencija ključnih riječi vidljivo je da je normativni okvir definiranja pojmova gotovo identičan i naslonjen na engleske pojmove *Cybercrime* i C*yberspace* bez prevođenja na matični jezik države ili organizacije.

Identificirani su i elaborirani rizici korištenja kibernetičkog prostora, kao i potreba praćenja i suradnje s drugim državama, imajući na umu da elektronički (digitalni) dokazi, koji se pojavljuju kod ove vrste kaznenih djela, nisu odijeljeni državnim granicama s obzirom na opasnost i izravne posljedice koje mogu nastupiti uslijed nedovoljnog razumijevanja i razmatranja ove problematike, kao i nedovoljnog poznavanja zakonskih i tehničkih pretpostavki za počinjenje kaznenih djela u kibernetičkom prostoru.

U okviru drugog istraživačkog pitanja također je provedena analiza statističkih pokazatelja DZS i MUP RH u razdoblju od 2013. do 2017. koji se odnose na kaznena djela iz glave XXV Kaznenog zakona te su prikazani trendovi u promatranoj problematici. Dobiveni rezultati ukazuju kako indikatori prijavljenih poznatih i nepoznatih počinitelja navedenih kaznenih djela iz članaka 266. - 272. KZ-a ukazuju na više nego dvostruko manju otkrivenost nepoznatih počinitelja ukazujući stoga na relativnu stručno-tehničku podkapacitiranost policije u kriminalističkom istraživanju. Vidljiv je trend porasta prijavljenih punoljetnih osoba, s naznakom da je broj prijavljenih osoba gotovo trostruko, a u zadnjoj godini i četverostruko veći od broja optuženih, odnosno osuđenih, stoga se posredno može ustvrditi da je takvoj nepovoljnoj slici pridonio značajan nedostatak elektroničkih dokaza u stadiju kriminalističkog istraživanja koji utječe na nemogućnost podizanja optužnice, odnosno donošenja pravomoćne presude koja se izriče prosječno samo u četvrtini slučajeva. Valja ustvrditi kako nepoznati počinitelji čine više od 50% od ukupnog broja prijavljenih osoba što opetovano ukazuje na nedostatnu stručno-kadrovsku kapacitiranost, možebitno nedosljedno provođenje zakonskih odredbi ili manjkav normativni okvir.

Najučestalije kazneno djelo je računalna prijevara, a zamjetan je udio nepoznatih počinitelja, nizak udio procesuiranih počinitelja od strane državnog odvjetništva i indikativno mali broj pravomoćno osuđenih počinitelja. U slučajevima počinjenja kaznenog djela oštećenja računalnih podataka nema niti jednu osuđujuće presude u posljednjem dvogodišnjem razdoblju. Stoga je nužno pojačati obuku svih dionika u procesu istraživanja, dokazivanja, vještačenja, kao i presuđivanja navedenog kaznenog djela.

Navedeni agregacijski podaci izravno ukazuju ne samo na kadrovsko-tehnički deficit, nego i na podkapacitiranost stručnjaka za kiberkriminal, što nadalje indicira neizostavnu potrebu educiranja i usavršavanja stručnjaka u ovoj domeni kaznenog pravosuđa. Tom trendu svakako pridonosi i potreba obvezne sustavne edukacije s obzirom na specifičnosti tehnologije koja se razvija velikom brzinom.

U tom pogledu Akcijskim planom obuhvaćena je i planirana edukacija te se preporuča plan obuke tijela za provođenje zakona. Informatizacija društva i pojava kibernetičke dimenzije otvara prostor daljnjem usavršavanju službenika za provođenje zakona. To usavršavanje potrebno je provoditi kontinuirano jer se promjene na području kibernetike odvijaju veoma brzo te je potrebno usklađivanje i prilagodba na nove izazove.

Temeljem aktualne Strategije i Akcijskog plana, uloga Policijske akademije u stručnom usavršavanju službenika za provođenje zakona u području kibernetičke sigurnosti mora biti višestruka i stoga navodimo sljedeće preporuke:

- u sklopu temeljnog obrazovanja za zanimanje policajac treba uvrstiti i temeljno poznavanje rada s računalom i osiguranja mjesta za kaznena djela kibernetičkog kriminaliteta,
- u okviru visokoškolskog obrazovanja za zanimanje kriminaliste treba uvrstiti više obveznih kolegija iz područja kibernetike i kibernetičke sigurnosti,
- provoditi periodične kolegije o novim pojavnim oblicima i načinima počinjenja kaznenih djela iz domene kibernetičkog kriminaliteta,
- provoditi specijalizirane tečajeve policijskih službenika zaduženih za kibernetičku sigurnost unutar Ministarstva unutarnjih poslova,
- razvijati nove metode i metodologije rada na slučajevima kaznenih djela iz domene kibernetičkog kriminaliteta,
- pratiti stanje, i u suradnji s nadležnim tijelima predlagati promjene zakonodavnog okvira koji se odnosi na kibernetički kriminalitet.

Istraživački rezultati vezani uz dinamiku promjene opsega i obrazaca međunarodne suradnje i sigurnosti u kibernetičkom prostoru i međuodnosa pokazatelja kooperacije, koordinacije i integracije postojeće teorijske paradigme, a temeljem kvalitativne i statističke analize podupiru globalnu integraciju ovog problema na svjetskoj razini, što je vidljivo iz opisa i analize različitih međunarodnih dokumenata država i međunarodnih organizacija. U okviru odgovora na treće istraživačko pitanje, iz dokumenata analiziranih država i međunarodnih organizacija, kao i pravnih dokumenata Republike Hrvatske, rezultati tekstualne analize nefiltriranih definicija obrađenih pojmova ukazuju da autori navedenih definicija nisu imali intenciju pojasniti tehnički aspekt.

Ovu činjenicu smatramo izuzetno praktičnom i logičnom jer bit definicije navedenih pojmova nije ulaziti u tehničku domenu, već isključivo prikazati međuodnos kažnjivog ponašanja i nacionalne jurisdikcije sukladno međunarodnim normama. U tom kontekstu odabrane definicije su vrlo slične i prepoznatljive populaciji korisnika te funkcionalno definiraju potrebe tijela za provođenje zakona.

Na temelju kvantitativne analize i frekvencije pojmova *Cyberspace* i *Cybercrime* u obrađenim dokumentima (strategije, zaključci, uredbe, direktive, odluke, preporuke i mišljenja, te radnih dokumenata institucija EU) najistaknutijim se pokazao pojam *Information* i to kod definicije pojma *Cyberspace* što koincidira s trendom modernog doba u kojem je prema mnogim autorima najvrjednija imovina upravo informacija, u ovom kontekstu pohranjena u elektroničkom obliku. U konačnici, preporuke se odnose na potrebu unaprjeđenja i revidiranja postojećih edukativnih aktivnosti na domaćoj i inozemnoj razini po pitanju problematike sigurnosti u kibernetičkom prostoru, umrežavanja svih dionika koji sudjeluju u razvoju i nadzoru kibernetičkog prostora (tijela za provođenje zakona, akademskog i tehničkog sektora), te sistematizaciji i jasnom definiranju ujednačenog kataloga općeprihvaćenih pojmova koji omogućuju operacionalizaciju kibernetičke sigurnosti i međunarodnu suradnju.

6. POPIS KORIŠTENIH IZVORA I LITERATURE

Aksentijević, S. (2013). *Vještačenja*. Preuzeto 13. 12 2017 iz Vještačenja: http://vjestak-informatika.com

Australija, Cyber Security Strategy. (2009).

Austrija, Austrian Cyber Security Strategy. (2013).

Bača, M. (2004). *Uvod u računalnu sigurnost.* Zagreb: Narodne novine.

Bazeley, P. i Richards, L. (2000). *The NVivo – Qualitative Project Book.* London-Thousand Oaks-New Delhi: SAGE Publications.

Belgija, Cyber Security Strategy. (2012).

Božinović, D. (2016). *Globalna sigurnost.* Zagreb: Narodne novine.

Brnetić, D. (1996). Temelji engleskog pravnog sustava (Common Law). *Policija i sigurnost, 2*, 212-216.

Bundesrepublik Deutschland - Strafgesetzbuch Deutschland (StGB). (20. 12 2017). *Strafgesetzbuch Deutschland (StGB).* Dohvaćeno iz Bundesministerium der Justiz und für Verbraucherschutz: http://www.jusline.de/Strafgesetzbuch_%28StGB%29.html

CARNet CERT i Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike iračunarstva Sveučilišta u Zagrebu. (2006). *Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2006-11-174* . Dohvaćeno iz Osnove računalne forenzičke analize: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2006-11-174.pdf

CARNet CERT i Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike iračunarstva Sveučilišta u Zagrebu. (2010). *Hrvatska akademska i istraživačka mreža, CCERT-PUBDOC-2010-05-301.* Dohvaćeno iz Računalna forenzika: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-05-301.pdf

Casey, E. (2011). *Digital evidence and computer crime 3rd Edition.* Cambridge: Academic press Cambridge University.

Council of Europe - Chart of signatures and ratifications of Treaty 185. (12. 12 2017). *Council of Europe*. Dohvaćeno iz Chart of signatures and ratifications of Treaty 185: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Crna Gora, National Cyber Security Strategy for Montenegro 2013-2017. (2013).

Cvjetko, B. i Singer, M. (2013). *Kaznenopravna zaštita djece.* Zagreb: Nakladni zavod Globus.

Dragičević, D. (2004). *Kompjuterski kriminalitet i informacijski sustavi.* Zagreb: IBS.

Dragičević, D. (7 2005). Novi izazovi kibernetičkog kriminala. *Hrvatska pravna revija, srpanj-kolovoz*, 150.

Dragičević, D. (2015). *Pravna informatika i pravo informacijskih tehnologija.* Zagreb: Narodne novine.

EastWest Institute / Information Security Institute, Moscow State University, Critical Terminology Foundations 2. (2011).

Ekvador, A66/152/Add.1. (2011).

ENISA - European Network and Information Security Agency. (5. 12 2017). *europa.eu*. Preuzeto 12. 12 2017 iz https://europa.eu/european-union/about-eu/agencies/enisa_hr

Estonija, Cybersecurity Strategy. (2008).

Europska Unija, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013).

Featherstone, M. i Burrows, R. (2001). *Kiberprostor, kibertijela, cyberpunk : kulture tehnološke tjelesnosti ; [prijevod Ognjen Strpić].* Zagreb: Naklada Jesenski i Turk.

Fialkova, L. i Yelenevskaya, M. N. (2005). Incipient Soviet diaspora : encounters in cyberspace. *Challenges of migration to the nation-state* (str. 83-99). Haifa: Narodna umjetnost : hrvatski časopis za etnologiju i folkloristiku, 42(1).

Filipini, Submission to the United Nations General Assembly Resolution A/56/164. (2001).

Francuska: Information Systems Defence and Security: France's strategy. (2011).

Franjić, S. i Šimundić, S. (2009). *Računalni kriminalitet.* Split: Pravni fakultet u Splitu.

Fuentes-Camacho, T. (2000). *The international dimensions of cyberspace law.* Aldershot : Ashgate/Darthmouth : UNESCO.

Goldsmith, J. i Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press.

Government Offices of Sweden - The Swedish Penal Code. (16. 12 2017). *Svensk författningssamling.* Dohvaćeno iz Den svenska brottsbalken - The Swedish Penal Code: http://www.government.se/contentassets/5315d27076c942019828d6c36521696e/swedish-penal-code.pdf

Grgić, S. (2013). Strategija "An open, safe and secure cyberspace". *25. konferencija Razvoj poslovnih i informatičkih sustava (CASE 25), Zagreb, 10.-12.6.2013.* (str. 203-205). Zagreb: CASE Rijeka.

Group of Governmental Experts. (10. 8 2016). *United Nations.* Preuzeto 12. 12 2017 iz Developments in the Field of Information and Telecommunications in the Context of International Security: http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201

Halperin, S. i Heath, O. (2012). *Political Research: Methods and Practical Skills.* Oxford: Oxford University Press.

Hrestak, D. (2017). *Kriminalističko istraživanje kažnjivih ponašanja korištenjem P2P mreža.* Zagreb: Visoka policijska škola.

Hruška, D. (2010). *Donošenje radikalnih odluka u velikim organizacijama - doktorska disertacija.* Zagreb: Sveučilište u Zagrebu, ekonomski fakultet.

Hrvatsko društvo sudskih vještaka i procjenitelja. (12. 12 2017). *Hrvatsko društvo sudskih vještaka i procjenitelja*. Dohvaćeno iz Popis strukovnih sekcija: http://www.sudski-vjestaci.hr/

Hughes, R. (2010). A Treaty for cyberspace, International Affairs 86 (2): 523-41. *International Affairs 86, 86*(2), 523-541.

Indija, National Cyber Security Policy – 2013 (NCSP-2013). (2013).

International Organization for Standardization. (2012). *ISO/IEC 27032:2012, 4.29.*

International Telecommunication Union. (2000). *ITU-T, Y.101.*

Internet Engineering Task Force. (2007). Internet Security Glossary. U *Version 2.*

Italija, 2013 National Strategic Framework for cyberspace security. (2013).

Izrael, Resolution No. 3611: Advancing National Cyberspace Capabilities. (2011).

Japan, Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace. (2013).

Japan, National Security Strategy. (2013).

Jelenski, M. (2017). *Uloga Ministarstva unutarnjih poslova u Akcijskom planu za provedbu Nacionalne strategije kibernetičke sigurnosti.* Zagreb: Visoka policijska škola.

Jurman, D. (2006). *Internet - Kibernetički kriminal*. Preuzeto 12. 12 2017 iz Drazen Jurman Web: http://www.djurman.com/tekst/net/cybercrime.htm

Južnoafrička Republika, Notice of Intention to make South African National Cybersecurity Policy. (2010).

Južnoafrička Republika, South African Defence Review 2012. (2012).

Kahin, B. i Nesson, C. (1998). *Borders in cyberspace : information policy and the global information infrastructure.* Cambridge: The MIT Press.

Kanada, Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada. (2010).

Katulić, T. (2006). *Hrvatska akademska i istraživačka mreža, CCERT-DOC-2006-03-1.* Preuzeto 12. 12 2017 iz Usporedni prikaz kaznenog zakonodavstva Republike Hrvatske i stranih izvora u pogledu računalnog kriminaliteta, Hrvatska akademska i istraživačka mreža: http://www.cert.hr/sites/default/files/CCERT-DOC-2006-03-1.pdf

Kazahstan, Submission to the United Nations General Assembly Resolution A/64/129. (2012).

Kenija, Cybersecurity Strategy. (2014).

Klemenčić, M. (1997). *Atlas Europe.* Zagreb: Leksikografski zavod Miroslav Krleža.

Kolumbija, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa). (2011).

Kolumbija, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa). (2011).

Krapac, D. (1992). *Kompjuterski kriminalitet.* Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

Kučan, B. (2014). Europski centar za kibernetički kriminal. *Mreža 02*.

Kuehl, D. T. (2009). *From Cyberspace Cyberpower: Defining the Problem u F.D. Kramer, S. Starr i L. K. Wentz (ur.), Cyberpower and National Security.* Washington DC: National Defence University.

Kunštek, E. i Pavišić, B. (2008). International Electronical Evidence: Croatia - Stephen Mason ur. *International Electronical Evidence*, 127-147.

Larry, D. i Lars, D. (2012). *Digital Forensics for Legal Professionals.* Waltham: Syngress.

Libanon, Submission to the United Nations General Assembly Resolution A/62/98. (2012).

Libicki, M. (2007). *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge: Cambridge University Press.

Litva, Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019. (2011).

Loader, B. D. (1998). *The governance of cyberspace : politics, technology and global restructuring.* London, New York: Routledge.

Lopez, C. T. (27. 2 2009). *Next war will begin in cyberspace, experts predict*. Preuzeto 12. 12 2017 iz US Army: https://www.army.mil/article/17561/next_war_will_begin_in_cyberspace_experts_predict

Lu, Y. (2009). Internet Manhunts. *The World Today, 65*(8/9), str. 16-17.

Mađarska, Annex 1 to Government Decision No. 1139/2013 National Cyber Security Strategy of Hungary. (2013).

Manjikian, M. M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly, 54*(2), str. 381-401.

Marciuš, M. (2017). *Međunarodna suradnja u otkrivanju kaznenih djela počinjenih u kibernetičkom prostoru.* Zagreb: Visoka policijska škola.

Mason, S. (2016). *Electronic signature in Law, Fourth edition.* London: University of London, School of Advanced Study.

Mason, S. i Seng, D. (2017). *Electronic Evidence: Fourth Edition.* London: University of London, School of Advanced Study.

Matijević, B. (2010). *Pravna datoteka.* Preuzeto 13. 12 2017 iz Vještaci: http://www.pravnadatoteka.hr/pdf/vjestaci.pdf

Maurer, T. i Morgus, R. (2014). *Compilation of Existing Cybersecurity and Information Security Related Definitions.* Washington: Federal Department of Foreign Affairs, Switzerland & New America.

Mayring, P. (2000). Qualitative Content Analysis. *Forum: Qualitative Social Research, 1*(2), str. 20. Preuzeto 12. 12 2017 iz http://www.qualitative-research.net/index.php/fqs/article/view/1089/2385

Murray, A. D. (2008). *The regulation of cyberspace : control in the online environment.* Abingdon, New York: Routledge-Cavendish.

Nakamoto, S. (31. 8 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Dohvaćeno iz Satoshi Nakamoto Institute: http://nakamotoinstitute.org/bitcoin/

NATO CCDCOE. (2013). NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare.

NATO CCDCOE. (12. 12 2017). *NATO Cooperative Cyber Defence Centre of Excellence*. Dohvaćeno iz NATO CCDCOE Cyber Definitions: https://www.ccdcoe.org/cyber-definitions.html

NATO CCDCOE. (12. 12 2017). *NATO Cooperative Cyber Defence Centre of Excellence*. Dohvaćeno iz Cyber Security Strategy Documents: https://ccdcoe.org/cyber-security-strategy-documents.html

Nhan, J. (2010). *Policing cyberspace : a structural and cultural analysis.* El Paso: LFB Scholarly Publishing LLC.

Nizozemska, The Defence Cyber Strategy. (2012).

Novi Zeland, New Zealand's Cyber Security Strategy. (2012).

Njemačka, Cyber Security Strategy for Germany. (2011).

Njemačka, Federal Criminal Police Office, Federal Overview Cybercrime 2013. (2013).

Njemačka, Federal Office for Information Security (BSI): Glossary/Terminology. (2017).

Njemačka, Submission to the United Nations General Assembly Resolution A/68/156, 7; A/68/152, 9. (2013).

O'Donnell, J. J. (2000). *Avatars of the word : from papyrus to cyberspace.* London : Harvard University Press.

Oxford English Dictionary. (2017). Oxford University Press. Dohvaćeno iz http://www.oed.com/

Oxford University Dictionary. (2008). *A Dictionary of Computing.* Oxford University Press.

Parliament of the United Kingdom. (15. 12 2017). *Computer Misuse Act 1990.* Dohvaćeno iz Legislation.gov.uk: https://www.legislation.gov.uk/ukpga/1990/18/contents

Patton, M. Q. (2002). *Qualitative Research and Evaluation Methods.* Thousand Oaks: Sage Publications.

Pavišić, B., Veić, P. i Modly, D. (2012). *Kriminalistika 2, Protrka, N. Glava XXVII.* Zagreb: DUŠEVIĆ I KRŠOVNIK.

Poljska, Cyberspace Protection Policy of the Republic of Poland. (2013).

Popović, P. (2014). *Kriza međunarodnog poretka 21. stoljeća.* Zagreb: Nacionalna zajednica Crnogoraca Hrvatske.

Protrka, N. (2009). *Računalna forenzička analiza: Istovjetnost sadržaja CD medija - specijalistički rad.* Varaždin: Fakultet organizacije i informatike - Sveučilište Zagrebu.

Protrka, N. (2011). Računalni podaci kao elektronički (digitalni) dokazi. *Policija i sigurnost, 1*, 1-13.

Protrka, N. (2013). Uloga sudskih vještaka u sudskom postupku u Republici Hrvatskoj s osvrtom na kibernetički kriminal. *Zbornik radova međunarodnog znanstvenog skupa "Pravo i izazovi XXI vijeka"*, 271-291.

Protrka, N. (2014). Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj. *Policija i sigurnost, 4*, 509-522.

Protrka, N. i Skakavac, Z. (2012). Utvrđivanje istovjetnosti digitalnih dokaza pomoću HASH funkcija. *Zbornik radova međunarodno naučno-stručne konferencije "Kriminalističko-krivično procesne karakteristike istrage prema Zakonu o krivičnom postupku u protekloj deceniji"*, 293-300.

Puyvelde, D. V. (10. 12 2017). *NATO Review magazin*. Dohvaćeno iz Hybrid war – does it even exist?: https://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/

Republik Österreich - Strafgesetzbuch Österreich (StGB). (13. 12 2017). *Strafgesetzbuch Österreich (StGB).* Dohvaćeno iz JUSLINE Österreich: http://www.jusline.at/Strafgesetzbuch_(StGB).html

Republika Češka, Draft Act on Cyber Security. (2014).

Republika Hrvatska - Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava Vijeća Europe NN 4/2008. (2008). *Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava Vijeća Europe.* Zagreb: Narodne Novine.

Republika Hrvatska - Kazneni zakon Republike Hrvatske NN- 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11. (2011). *Kazneni zakon Republike Hrvatske.* Zagreb: Narodne novine.

Republika Hrvatska - Kazneni zakon Republike Hrvatske NN 125/11, 144/12, 56/15, 61/15, 101/17. (2017). *Kazneni zakon Republike Hrvatske.* Zagreb: Narodne novine.

Republika Hrvatska - Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti - NN 108/2015. (2015). *Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti.* Zagreb: Narodne Novine.

Republika Hrvatska - Pravilnik o stalnim sudskim vještacima NN 38/2014. (2014). *Pravilnik o stalnim sudskim vještacima.* Zagreb: Narodne novine.

Republika Hrvatska - Zakon o kaznenom postupku Republike Hrvatske - NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17. (2017). *Zakon o kaznenom postupku Republike Hrvatske.* Zagreb: Narodne novine .

Republika Hrvatska - Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu - NN 9/2002. (2002). *Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu.* Zagreb: Narodne Novine.

Republika Hrvatska, Nacionalna strategija kibernetičke sigurnosti. (2015). Narodne novine 108/2015.

Republika Slovenija. (29. 6 2012). *2065. Kazenski zakonik (KZ-1-UPB2) .* Dohvaćeno iz Uradni list Republike Slovenije, Številka 50/2012: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/109161

Richards, T. J. i Richards, L. (1994). *Using computers in qualitative research In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of Qualitative Research.* Thousand Oaks: Sage Publishing.

Ritchie, J. i Lewis, J. (2003). *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* Thousand Oaks: Sage Publication.

Romania - The Romanian Parliament. (7. 6 2002). *Law 365/2002.* Dohvaćeno iz Law on electronic commerce: http://www.legi-internet.ro/en/e-commerce.htm

Romania - The Romanian Parliament. (21. 4 2003). *Law 161/2003.* Dohvaćeno iz Provisions on preventing and fighting cybercrime: http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN012620.pdf

Rumunjska, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de secur. (2013).

Rumunjska, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică. (2013).

Rusija, Concept Strategy for Cybersecurity of the Russian Federation (Концепция Стратегии Кибербезопасности Российской Федерации). (2015).

Shipley, T. G. i Bowker, A. (2014). *Investigating Internet crimes.* Waltham: Syngress.

Silverman, D. (2001). *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction (2nd ed.).* Thousands Oaks: Sage Publishing.

Sjedinjene Američke Države, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. (2009).

Sjedinjene Američke Države, Department of Defense Dictionary of Military and Associated Terms. (2014).

Sjedinjene Američke Države, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology. (12. 12 2017). *Official website of the Department of Homeland Security*. Dohvaćeno iz Adapted from: NSPD 54/HSPD -23, CNSSI 4009, NIST SP 800-53 Rev 4: https://niccs.us-cert.gov/glossary#C

Sjedinjene Američke Države, NIST Glossary of Key Information Security Terms. (2013).

Sjedinjene Američke Države, The National Strategy to Secure Cyberspace. (2003).

Sjedinjene Američke Države, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028. (2010).

Standage, T. (1998). *The Victorian Internet.* New York: Walker.

Statistička izvješća broj 1528. (31. 10. 2014). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2013.: https://www.dzs.hr/Hrv_Eng/publication/2014/SI-1528.pdf

Statistička izvješća broj 1529. (31. 10. 2014). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Maloljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2013.: https://www.dzs.hr/Hrv_Eng/publication/2014/SI-1529.pdf

Statistička izvješća broj 1551. (30. 10. 2015). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2014.: https://www.dzs.hr/Hrv_Eng/publication/2015/SI-1551.pdf

Statistička izvješća broj 1552. (30. 10. 2015). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Maloljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2013.: https://www.dzs.hr/Hrv_Eng/publication/2015/SI-1552.pdf

Statistička izvješća broj 1576. (29. 7. 2016). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2015.: https://www.dzs.hr/Hrv_Eng/publication/2016/SI-1576.pdf

Statistička izvješća broj 1577. (31. 8. 2016). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Maloljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2015.: https://www.dzs.hr/Hrv_Eng/publication/2016/SI-1577.pdf

Statistička izvješća broj 1605. (31. 7. 2017). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2016.: https://www.dzs.hr/Hrv_Eng/publication/2017/SI-1605.pdf

Statistička izvješća broj 1606. (31. 8. 2017). *Objavljeni podaci, Publikacije, Kazneno pravosuđe i socijalna zaštita (metodologija ESSPROS).* Dohvaćeno iz Maloljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2016.: https://www.dzs.hr/Hrv_Eng/publication/2017/SI-1606.pdf

Statistika MUP-a - 2013. (3 2014). *Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2013. godini.* Dohvaćeno iz Statistika MUP-a - Pregled sigurnosnih pokazatelja u 2013. godini: https://www.mup.hr/UserDocsImages/statistika/2014/Statisticki%20preg2013_konacni%20prom_WEB.pdf

Statistika MUP-a - 2014. (3 2015). *Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2014. godini.* Dohvaćeno iz Statistika MUP-a - Pregled sigurnosnih pokazatelja u 2014. godini: http://stari.mup.hr/UserDocsImages/statistika/2014/Statisticki_pregled_2014.pdf

Statistika MUP-a - 2015. (3 2016). *Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini.* Dohvaćeno iz Statistika MUP-a - Pregled sigurnosnih pokazatelja u 2015. godini: http://www.mup.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf

Statistika MUP-a - 2016. (3 2017). *Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2016. godini.* Dohvaćeno iz Statistika MUP-a - Pregled sigurnosnih pokazatelja u 2016. godini: http://stari.mup.hr/UserDocsImages/statistika/2017/Statisticki%20pregled_2016_2.pdf

Škrtić, D. (2011). *Kaznenopravna zaštita informatičkih sadržaja - doktorska disertacija.* Zagreb: Sveučilište u Zagrebu, Pravni fakultet.

Španjolska, National Cyber Security Strategy. (2013).

Švicarska, National strategy for the protection of Switzerland against cyber risks. (2012).

Turska, National Cyber Security Strategy and 2013-2014 Action Plan. (2013).

Valeri, L., Somers, G., Robinson, N., Graux, H. i Dumortier, J. (2006). *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries.* Brussels: RAND Corporation.

Velika Britanija, A Detica report in partnership with the Office of cyber security and information assurance in the Cabinet office. (2011). *The Cost of Cyber Crime.*

Velika Britanija, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space. (2009).

Velika Britanija, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. (2011).

Verini, J. (10. 11 2010). *The New York Times Magazine*. Preuzeto 12. 12 2017 iz The Great Cyberheist: http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=0

Vjesnik, N. (2001). DDOS napad, 29.04.2001. *Nedjeljni Vjesnik*, 30.

Vukmir, M. (6 2005). *Edupoint časopis*. Preuzeto 12. 12 2017 iz Intervju s mr.sc. Mladenom Vukmirom: http://edupoint.carnet.hr/casopis/36/clanci/3.html

Whittaker, J. (2004). *The cyberspace handbook.* London, New York: Routledge.

Zekos, G. I. (2013). *Corporate governance and MNES in globalization & cyberspace.* New York: Nova Publishers.

7. SAŽETAK

Temeljem različite percepcije međunarodne suradnje u kibernetičkom prostoru, kao i sigurnosti koja je ugrožena činjenjem kaznenih djela iz ove domene, autor je istražio i analizirao trenutno stanje aspekta poimanja kibernetičkog prostora, kao i kibernetičke sigurnosti koja je ugrožena činjenjem raznih kaznenih djela u kibernetičkom prostoru, odnosno kiberkriminala. Autor komparativno analizira pravna rješenja nekih europskih zemalja kao i obrasce te institucije međunarodne suradnje. U radu se provodi analiza i prikazuje statistički prikaz za Republiku Hrvatsku za razdoblje 2013. do 2017. godine po svim podacima Državnog zavoda za statistiku i podacima Ministarstva unutarnjih poslova Republike Hrvatske, a koji se odnose na kaznena djela iz domene kibernetičkog kriminala. Za kvalitativnu analizu autor analizira pojmove *Cyberspace* i *Cybercrime*, izrađene uz pomoć softverskog alata NVivo koja uključuje proces kodiranja u svrhu apstrahiranja i analize navedenih pojmova u sklopu međunarodne suradnje i sigurnosti u kibernetičkom prostoru s aspekta tijela za provođenje zakona, temeljem razne dokumentacije kao što su strategije, uredbe, direktive itd., kako država, tako i međunarodnih organizacija.

Ključne riječi: Cyberspace, Cybercrime, kibernetički prostor, kibernetički kriminal, kibernetička sigurnost

ABSTRACT:

Based on the different perceptions of international co-operation in the cyberspace and the security threatened by the crime of this domain, the author explored and analysed the current state of the cyberspace as well as the cybersecurity endangered by the fact of various criminal offenses in the cyberspac. The author analyses comparatively the legal solutions of some European countries as well as the forms of this institution of international cooperation. The paper analyses and presents statistical data for the Republic of Croatia for the period 2013 - 2017 on all data of the Central Bureau of Statistics and data of the Ministry of the Interior of the Republic of Croatia related to criminal offenses in cyberspace. For qualitative analysis, the author analyses the concepts of Cyberspace and Cybercrime, created using the software tool NVivo, which includes the coding process for the purpose of abstracting and analysing the terms under international cooperation and cybersecurity in the field of law enforcement, based on various documentation such as strategies, regulations, directives etc., both state and international organizations.

Keywords: Cyberspace, Cybercrime, Cybersecurity, Cyber, Digital Evidence

8. PRILOZI

8.1 Analizirane odabrane definicije kibernetičkog prostora - Cyberspace

1. "The communication space created by the worldwide interconnection of automated digital data processing equipment." (Francuska: Information Systems Defence and Security: France's strategy, 2011, str. 21)

2. "A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them (individual, organizational, state)." (Rusija, Concept Strategy for Cybersecurity of the Russian Federation (Концепция Стратегии Кибербезопасности Российской Федерации), 2015, str. 2)

3. "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services." (Velika Britanija, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011, str. 11)

4. "Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks." (Velika Britanija, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space, 2009, str. 7)

5. "Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work." (Sjedinjene Američke Države, The National Strategy to Secure Cyberspace, 2003, str. 7)

6. "The globally-interconnected digital information and communications infrastructure known as cyberspace underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security." (Sjedinjene Američke Države, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009, str. 3)

7. "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (Sjedinjene Američke Države, Department of Defense Dictionary of Military and Associated Terms, 2014, str. 64)

8. "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (Sjedinjene Američke Države, Department of Defense Dictionary of Military and Associated Terms, 2014, str. 92) (Sjedinjene Američke Države, NIST Glossary of Key Information Security Terms, 2013, str. 58) (Sjedinjene Američke Države, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 2010, str. 6)

9. "The interdependent network of information technology infrastructures, that includes the Internet, telecommunications network, computer systems, and embedded processors and controllers." (Sjedinjene Američke Države, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology, 2017)

10. "Cyberspace is both the physical and virtual environment consisting of computers, computer systems, computer programs (software), telecommunications networks, data and information which is used for the interaction between users." (Kolumbija, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, str. 38)

11. "Cyberspace is a public good and a public space. As such, we have to consider cyberspace security in terms of the resilience of infrastructure and the integrity and failure safety of systems and its contained data. Being a public space, States have to promote security in cyberspace, particularly regarding security against crime and malicious activities, by protecting those who choose to use authenticity tools against identity theft and securing the integrity and confidentiality of networks and data. Cyberspace is global by nature. Ensuring cyber security, enforcing rights and protecting critical information infrastructures requires major efforts by the State at the national level and in cooperation with international partners." (Njemačka, Submission to the United Nations General Assembly Resolution A/68/156, 7; A/68/152, 9, 2013, str. 6)

12. "Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace." (Njemačka, Cyber Security Strategy for Germany, 2011, str. 9)

13. "The physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data." (Izrael, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, str. 1)

14. "Cyberspace, global virtual spaces such as the internet, composed of information systems, information communications networks and similar systems and which circulate large quantities of a large variety of information, have rapidly expanded and begun permeating real-space." (Japan, Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace, 2013, str. 5)

15. "Cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities." (Japan, National Security Strategy, 2013, str. 9)

16. "The notional environment in which communication over computer networks occurs." (Kenija, Cybersecurity Strategy, 2014, str. 12)

17. "The notional environment in which communication over computer networks occurs" *(Oxford English Dictionary, 2017)*

18. "Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology - including the Internet - networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalisation that provides new opportunities but also entails new challenges, risks and threats." (Španjolska, National Cyber Security Strategy, 2013, str. 9)

19. "Cyber space is the virtual space of all IT systems interconnected at data level on a global scale. The basis for cyber space is the Internet as a universal and publicly accessible connection and transport network, which may be supplemented and expanded through other data networks. In common parlance, cyber space also refers to the global network of different independent IC infrastructures, telecommunication networks and computer systems. In the

social sphere the use of this global network allows individuals to interact, exchange ideas, disseminate information, give social support, engage in business, control action, create art and media works, play games, participate in political discussions and a lot more. Cyber space has become an umbrella term for all things related to the Internet and for different Internet cultures. Many countries regard networked ICT and independent networks operating through this medium as components of their national critical infrastructures." (Austrija, Austrian Cyber Security Strategy, 2013, str. 21)

20. "Cyberspace is the global environment for the interconnection of information and communication systems. Cyberspace is wider than the computer world and also contains computer networks, computer systems, digital media and digital data, whether physical or virtual." (Belgija, Cyber Security Strategy, 2012, str. 12)

21. "Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship." (Kanada, Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada, 2010, str. 2)

22. "Space in which communication among information systems takes place. In the context of the Strategy, it encompasses the Internet and all the systems connected to it." (Republika Hrvatska, Nacionalna strategija kibernetičke sigurnosti, 2015, str. 29)

23. "Cyber space means digital environment, enabling to create, process, and exchange information, created by information systems and services and electronic communication networks." (Republika Češka, Draft Act on Cyber Security, 2014, str. 2)

24. "Cyberspace means the combined phenomenon of globally interconnected, decentralised and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information." (Mađarska, Annex 1 to Government Decision No. 1139/2013 National Cyber Security Strategy of Hungary, 2013, str. 3)

25. "Cyberspace is a man-made domain essentially composed of ICT nodes and networks, hosting and processing an ever-increasing wealth of data of strategic importance for States, firms, and citizens alike, and for all political, social and economic decision-makers." (Italija, 2013 National Strategic Framework for cyberspace security, 2013, str. 9)

26. "Cyberspace is a global space which has no national boundaries, hence, the rapid spread of threats across cyberspace. " (Litva, Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019, 2011, str. 3)

27. "Cyberspace is more than Internet; it includes not only hardware, software and information systems, but also the people, social interaction within these networks." (Crna Gora, National Cyber Security Strategy for Montenegro 2013-2017, 2013, str. 5)

28. "For the purposes of this strategy, cyberspace is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data." (source code, information, etc) present in this domain. (Nizozemska, The Defence Cyber Strategy, 2012, str. 4)

29. "A space of processing and exchanging information created by the ICT systems, together with links between them and the relations with users." (Poljska, Cyberspace Protection Policy of the Republic of Poland, 2013, str. 5)

30. "Cyberspace is characterized by the absence of borders, dynamism, and autonomy, creating opportunities to develop both knowledge-based information society and risks to its operation." (Rumunjska, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de secur, 2013)

31. "The virtual environment generated by cyber infrastructure, including content information processed, stored, or transmitted, and the actions performed by users in it." (Rumunjska, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, str. 7)

32. "The state, the private sector and society make use of information and communication infrastructure and access to cyberspace (Internet, mobile networks and applications, e-business, e-government, computer- based control programmes). " (Švicarska, National strategy for the protection of Switzerland against cyber risks, 2012, str. 5)

33. "The environment which consists of information systems that span across the world including the networks that interconnect these systems." (Turska, National Cyber Security Strategy and 2013-2014 Action Plan, 2013, str. 8)

34. "Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks." (Indija, National Cyber Security Policy – 2013 (NCSP-2013), 2013, str. 1)

35. "Cyberspace, as a network using the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocol, has shown itself to be a fragile and insecure environment which has allowed criminal groups to attack and, on occasion, destroy it, because priority has been given to commercial and marketing objectives." (Libanon, Submission to the United Nations General Assembly Resolution A/62/98, 2012, str. 12)

36. "The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place." (Novi Zeland, New Zealand's Cyber Security Strategy, 2012, str. 12)

37. "Cyberspace means a physical and non-physical terrain created by and/or composed of some or all of the following; computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users." (Južnoafrička Republika, Notice of Intention to make South African National Cybersecurity Policy, 2010, str. 12)

38. "The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify, and exchange data using computer networks." (NATO CCDCOE, 2013, str. 258)

39. "Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed and deleted." (EastWest Institute / Information Security Institute, Moscow State University, Critical Terminology Foundations 2, 2011, str. 17)

40. "The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form." (International Organization for Standardization, 2012)

41. "An informal word first thought to have been used by novelist William Gibson to refer to the total data on all computers on all the networks in the world. The word has passed into common use as a way of referring to any large collection of network-accessible computer-based data." *(Oxford University Dictionary, 2008, str. 121)*

8.2 Analizirane odabrane definicije kibernetičkog (računalnog) kriminala – Cybercrime

1. "Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime." (Francuska: Information Systems Defence and Security: France's strategy, 2011, str. 21)

2. "For the purposes of this study, we are using the term 'cyber crime' to mean the illegal activities undertaken by criminals for financial gain. Such activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government." (Velika Britanija, A Detica report in partnership with the Office of cyber security and information assurance in the Cabinet office, 2011, str. 1)

3. "Illicit actions which are committed through the utilization of a computer service or good. Criminal or abusive activities on computers or communication networks, either because the computer is used as the tool of the crime, or because the computer system (or data) is the objective of the crime." (Ministry of Defense of Colombia) (Kolumbija, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, str. 38)

4. "Criminal offences against computer systems, software support and data; committed in cyberspace using information and communication technologies." (Republika Hrvatska, Nacionalna strategija kibernetičke sigurnosti, 2015, str. 16)

5. "The majority of attacks against information systems and the data stored therein are crimes committed for financial gain. These crimes may manifest themselves in a disruption to a particular financial service or in a violation of the confidentiality, integrity or availability of financial data. Other forms of cyber crime include harassment, fraud, the distribution of illegal materials or

the violation of intellectual property rights. To the criminal, the use of cyberspace for securing material profit might seem attractive because of the simplicity and remoteness with which such crimes can be committed. Other factors which lend to the appeal of cyber crime are: anonymity, deficiencies in international regulation of the use of cyberspace and the negligence of information system owners and end-users in ensuring the security of cyberspace." (Estonija, Cybersecurity Strategy, 2008)

6. "Cybercrime encompasses offenses that are directed against the Internet, data networks, information technology systems or their data, that are committed by means of information technology." (Njemačka, Federal Criminal Police Office, Federal Overview Cybercrime 2013, 2013)

7. "Criminal activity through which services or applications in cyberspace are being used to carry out crime or are targets of crime. In the process, cyberspace can be origin, target or the environment of the attack." (Njemačka, Federal Office for Information Security (BSI): Glossary/Terminology, 2017)

8. "Cyber crime comprises illegal attacks from cyber space on or through ICT systems, which are defined in penal or administrative laws. The term therefore covers all criminal offences committed with the aid of information technologies and communications networks and also encompasses Internet crime." (Austrija, Austrian Cyber Security Strategy, 2013, str. 21)

9. "Cybercrime is an offense abusing, in terms of medium, the automation and automated data and also being applicable to information systems or data stored on them." (Belgija, Cyber Security Strategy, 2012, str. 12)

10. "These offences can be roughly divided into three categories: a) Universal, State and public offences, which represent a threat to national and public security (including calls to overthrow the existing order, attempts to devalue sovereignty or to undermine independence and national interests, terrorist propaganda, chauvinism, xenophobia, all forms of extremism, and discrimination on ethnic, racial, religious, gender and other grounds); b) Universal civil offences, which constitute a threat to individual rights and freedoms (including violations of individual rights and freedoms, the use of compromising material, the exertion of pressure on individuals, the discrediting of individuals, the dissemination of confidential information, the use of another person's Internet services, the forgery of documents and copyright infringement); c) Traditional offences, which threaten the foundations of morality and decency (including pornography, pedophilia, other forms of sexual perversion, drug addiction and alcoholism)." (Kazahstan, Submission to the United Nations General Assembly Resolution A/64/129, 2012, str. 4)

11. "An offence committed in cyberspace." (Poljska, Cyberspace Protection Policy of the Republic of Poland, 2013, str. 5)

12. "The Australian Government defines cyber crime as those computer offences under the Commonwealth Criminal Code Act 1995 (Part 10.7) which involve the unauthorised access to, modification or impairment of electronic communications." (Australija, Cyber Security Strategy, 2009, str. 23)

13. "Information and communication technologies have been widely adopted in societies and are considered to be the foundations that support the current globalized world; however, this widespread usage, among other things, has exposed the information generated, published and stored using information and communication technologies to a wide range of threats, known as cybercrime, that can have a serious impact on such areas as the confidentiality, integrity and availability of the information." (Ekvador, A66/152/Add.1, 2011, str. 5)

14. "Any crime where information and communications technology is: 1. used as a tool in the commission of an offence; 2. the target of an offence; 3. a storage device in the commission of an offence." (Novi Zeland, New Zealand's Cyber Security Strategy, 2012, str. 12)

15. "Cybercrime means cyber crimes as defined in chapter XIII of the ECT Act (no.25 of 2002)." (Južnoafrička Republika, Notice of Intention to make South African National Cybersecurity Policy, 2010, str. 12)

16. "Cyber-crime involving inter alia malware, viruses, identity theft and attacks on financial institutions." (Južnoafrička Republika, South African Defence Review 2012, 2012, str. 79)

17. "Criminal acts involving elements of information security; (ii) acts of malicious intent directed at information resources (e.g. techno-vandalism, techno-trespass and superzapping); (iii) all unauthorized interference or unsanctioned penetration." (Filipini, Submission to the United Nations General Assembly Resolution A/56/164, 2001, str. 4)

18. "All actions under criminal law or other special law that present a social threat and the guilty actions are committed through or over cyber infrastructure." (Rumunjska, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, str. 8)

19. "Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)." (Europska Unija, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, str. 3)

20. "Criminal activity where services or applications in the Cyberspace are used for or are the target of crime, or where the Cyberspace is the source, tool, target, or place of a crime." (International Organization for Standardization, 2012)

21. "Criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime." (International Organization for Standardization, 2012)

22. "Cyber crime is the use of cyberspace for criminal purposes as defined by national or international law." (EastWest Institute / Information Security Institute, Moscow State University, Critical Terminology Foundations 2, 2011, str. 29)

23. "Crime committed on or using a computer or computer network." (Oxford University Dictionary, 2008, str. 120)

8.3 Kratice za literaturu (po abecednom redoslijedu)

Akcijski plan	Akcijski plan za provedbu nacionalne strategije kibernetičke sigurnosti, Narodne novine 108/2015
CERT	engl. Computer Emergency Response Team
Dodatni protokol	Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava Vijeća Europe, Narodne novine 4/2008
DZS	DZS Republike Hrvatske
GDPR	engl. General Data Protection Regulation
Kazneni zakon	Kazneni zakon Republike Hrvatske, Narodne novine, 125/11, 144/12, 56/15, 61/15, 101/17
Kazneni zakon 1997-2012	Kazneni zakon Republike Hrvatske, Narodne novine 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11
Konvencija	Konvencija o kibernetičkom kriminalu Vijeća Europe, NN-MU 9/02, 4/04.
MUP	Ministarstvo unutarnjih poslova Republike Hrvatske
Narodne novine	Narodne novine Republike Hrvatske
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
NIAS	Nacionalni identifikacijski i autentifikacijski sustav
Okvirna odluka	Okvirna odluka 2005/222/JHA, od 24. veljače 2005.
StGB	Strafgesetzbuch, Kazneni zakon Republike Njemačke ili Republike Austrije
Strategija	Nacionalna strategija kibernetičke sigurnosti, Narodne novine 108/2015
Zakon o kaznenom postupku	Zakon o kaznenom postupku Republike Hrvatske, Narodne novine 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17.

8.4 Popis Tablica

8.5 Popis grafikona

8.6 Popis slika

9. KRATKI ŽIVOTOPIS AUTORA

Nikola Protrka rođen je u Zagrebu. Nakon završene matematičke gimnazije upisuje i završava Fakultet kriminalističkih znanosti, danas Visoka policijska škola. Završio je poslijediplomski sveučilišni studij na Sveučilištu u Zagrebu, Fakultetu organizacije i informatike. Zaposlen je u Ministarstvu unutarnjih poslova Republike Hrvatske od 1998. gdje radi na poslovima kriminalističke policije, poslovima općeg i gospodarskog kriminaliteta, kriminalističke analitike, kompjuterskog kriminaliteta, te kao voditelj operativno-komunikacijskog centra policije. Trenutno radi na Visokoj policijskoj školi te je nositelj nekoliko predmeta na temu računalne forenzike, elektroničkih dokaza i kibernetičke sigurnosti. Kao gost predavač sudjeluje u nastavi na Sveučilištu u Zagrebu, Pravnom fakultetu, Fakultetu elektrotehnike i računarstva, Filozofskom fakultetu, Sveučilištu Libertas i Visokom učilištu Algebra.

Redovno sudjeluje u međunarodnim znanstveno-stručnim skupovima kao predstavnik Ministarstva unutarnjih poslova Republike Hrvatske ili kao stalni sudski vještak za informatiku. Međunarodnim odnosima bavi se svakodnevno kao član nacionalne kontakt točke agencije Europske unije CEPOL (European Union Agency for Law Enforcement Training) čije su osnovne zadaće razvoj, provođenje i koordinacija osposobljavanja službenika za izvršavanje zakonodavstva. Rješenjem Županijskog suda u Zagrebu imenovan stalnim sudskim vještakom za informatiku.

Do sada objavio više članaka u znanstveno-stručnim časopisima i knjigama u području elektroničkih (digitalnih) dokaza, kibernetičkog kriminaliteta (*cybercrime*), računalnog kriminaliteta, kibernetičke sigurnosti, zaštite osobnih i poslovnih podataka i informacijskih sustava te raznih vrsta ICT vještačenja.