Cyber kriminalitet - novo područje za socijalnopedagoške intervencije

Tomić, Matea

Sveučilište u Zagrebu
Edukacijsko-rehabilitacijski fakultet

Diplomski rad

Cyber kriminalitet – novo područje za socijalnopedagoške intervencije

Matea Tomić

Zagreb, lipanj, 2019

Sveučilište u Zagrebu
Edukacijsko-rehabilitacijski fakultet

Diplomski rad

Cyber kriminalitet – novo područje za socijalnopedagoške intervencije

Matea Tomić

Mentor: Prof.dr.sc. Dalibor Doležal

Zagreb, lipanj, 2019

Izjava o autorstvu rada

Potvrđujem da sam osobno napisala rad *Cyber kriminalitet – novo područje za socijalnopedagoške intervencije* i da sam njegova autorica.

Svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima jasno su označeni kao takvi te su adekvatno navedeni u popisu literature.

Ime i prezime: Matea Tomić

Mjesto i datum: Zagreb, lipanj, 2019

SAŽETAK

Naslov rada: Cyber kriminalitet – novo područje za socijalnopedagoške intervencije

Ime i prezime studentice: Matea Tomić

Ime i prezime mentora: Prof.dr.sc. Dalibor Doležal

Program/Modul: Socijalna pedagogija/ Djeca i mladi

Razvoj Interneta je omogućio prijelaz svakodnevnih interakcija te mnogih društvenih fenomena (i problema) u novi – *cyber*-prostor. Pa se tako osim tradicionalnih oblika nezakonitih ponašanja, u *cyber*-prostoru javljaju i novi oblici ponašanja upitne moralnosti. Određena obilježja samog Interneta i digitalne tehnologije olakšavaju činjenje kaznenih djela što može dovesti do rapidnog rasta opsega *cyber*-kriminaliteta. Etiološka objašnjenja uključuju već poznate teorije kriminaliteta i ponašanja poput: teorije učenja, teorije ličnosti i teorije rutinske aktivnosti. No, formiraju se i nove teorije koje se bave isključivo *cyber*-kriminalitetom. Prema tome, jedno od pitanja na koje će se nastojati odgovoriti u radu je: *zašto osobe sudjeluju u aktivnostima cyber-kriminaliteta*. Budući da postoji izražena heterogenost oblika ponašanja koja se smatraju *cyber*-kriminalitetom, kroz rad su opisana ponašanja koja su postojala i u „stvarnom“ prostoru (poput prijevare, krađe, nasilja i dječje pornografije), no koja prelaskom u *cyber*-prostor mijenjaju određena obilježja. Osim navedenog, u radu su opisana i djela „čistog“ *cyber*-kriminaliteta, poput „hakiranja“, „piratstva“ i „spama“. Prema tome, opisana je fenomenologija *cyber*-kriminaliteta te se odgovara na pitanje: *o kakvim aktivnostima se točno radi*. Razvoj kaznenopravnih okvira *cyber*-kriminaliteta se može proučavati na međunarodnoj i nacionalnoj razini, stoga je bitno odgovoriti na pitanje: *kako su države pravno odgovarale na cyber-kriminalitet*. Naposljetku, kako bi se kvalitetno iskoristilo znanje o novom obliku kriminaliteta, potrebno je proučiti i opisati smjernice za prevenciju određenih štetnih ponašanja u *cyber*-prostoru.

Ključne riječi: *cyber*-prostor, *cyber*-kriminalitet, etiologija, fenomenologija, kaznenopravni odgovor, prevencija

ABSTRACT

Thesis: Cybercrime – The New Area for Socio-Pedagogical Interventions

Student: Matea Tomić

Mentor: Prof.dr.sc. Dalibor Doležal

Programme/Module: Social pedagogy/Children and youth

Internet enabled the transition of human interactions and social phenomenons (and issues) from "real world" to cyberspace. So, apart from the traditional forms of illegal behavior, new forms of behavior emerge in cyberspace that are questionably moral. Certain features of the Internet and digital technology make criminal offenses easier to commit, consequently leading to a rapid increase in the scope of cybercrime. Etiological explanations include familiar theories of criminal behavior, such as: learning theories, studies of different personality traits and routine activity approach. But new theories that deal exclusively with cybercrime are also being created. Therefore, one of the issues that will be addressed in this paper is: *Why are people involved in cybercrime activities*. Since there are very different forms of behavior that are considered cybercrimes, this paper describes the crimes that existed in the "real world" (such as fraud, theft, violence and child pornography), but are changing their characteristics in the cyberspace. In addition, paper describes the "pure" cybercrimes, such as hacking, digital piracy and spam. Thus, addressing the issue of: *What activities are considered to be cybercrime.* The development of criminal justice frameworks for cybercrime can be studied at an international and national level, so it is important to address the issue of: *How are different nations legally responding to this form of crime*. Finally, in order to make a good use of studies done in this field, it is necessary to study and describe the guidelines for the prevention of harmful behaviors in the cyberspace.

Key words: cyberspace, cybercrime, etiology, phenomenology, legal response, prevention

SADRŽAJ:

1 Uvod

Internet i digitalna tehnologija uveli su društvo u novo, informacijsko doba. Zbog značajnih tehnoloških dostignuća i jeftinijih uređaja koji imaju mogućnost spajanja na Internet, danas pojedinac može učiti, inspirirati se, upoznavati nove osobe i razvijati svoje vještine unutar *cyber*-prostora, kao i kupovati proizvode koji mu prije nisu bili dostupni. Novonastale mogućnosti stvaraju prilike za psihološko, emocionalno i egzistencijalno zadovoljavanje potreba pojedinca, no i prilike za aktivnosti koje nisu dopuštene ili su upitne prihvatljivosti.

Važnost teme *cyber*-kriminaliteta za područje rada socijalnih pedagoga leži u činjenici da sve više djece i mladih postaje članovima *online*-zajednice, što može rezultirati njihovim češćim sudjelovanjem u kriminalnim aktivnostima, ali i većim rizikom viktimizacije. Stoga, prilikom izučavanja spomenutih aktivnosti ili *cyber*-kriminaliteta potrebno je odgovoriti na sljedeća pitanja kako bi se razumjela priroda istog:

1. Za početak, bitno je odrediti **na što točno se misli kada se govori o *cyber*-kriminalitetu**. Prema tome, u prvom dijelu diplomskog rada bit će opisan povijesni razvoj Interneta, definicija te specifičnosti *cyber*-kriminaliteta u odnosu na tradicionalni.

2. Sljedeći dio rada se odnosi na etiološka objašnjenja *cyber*-kriminaliteta kroz već poznate i novonastale teorije, što odgovara na pitanje **zašto osobe sudjeluju u aktivnostima *cyber*-kriminaliteta**.

3. Kako bi se moglo kvalitetno analizirati *cyber*-kriminalitet, potrebno je razumjeti **o kakvim se aktivnostima točno radi**. Iz tog razloga, kroz rad su opisane različite vrste *cyber*-kriminaliteta te ponašanja potrebna za sudjelovanje u *cyber*-kaznenim djelima.

4. Budući da se rad odnosi na relativno novu vrstu kriminaliteta, bitno je proučiti **kako su države pravno odgovarale na pojavu *cyber*-kriminaliteta**.

5. Na pitanje **koliki je opseg nedozvoljenih *online*-ponašanja,** u radu je odgovoreno putem analize prevalencije prijavljenih, optuženih i osuđenih počinitelja kaznenih djela u Republici Hrvatskoj.

6. Posljednje poglavlje odgovara na pitanje: **kako prevenirati *cyber*-kriminalitet**.

2 Definiranje *cyber*-kriminaliteta

2.1 Definiranje ključnih pojmova

Iako postoji mnoštvo termina kojima autori opisuju pojavu kršenja zakona u *cyber*-prostoru, poput *cyber*-kriminaliteta, zlouporabe računala, kriminala „internetskog doba“, kriminaliteta visoke tehnologije, elektroničkog, virtualnog te digitalnog kriminaliteta (Moise, 2014; Clough, 2010), engleski termin *cybercrime* (hrv. *cyber*-kriminalitet) je postao uobičajen u svakodnevnim interakcijama te je najčešće korišten pojam u medijima (Clough, 2010).

Budući da je većina stručne literature na temu spomenute vrste kriminaliteta originalno napisana na engleskom jeziku u kojem koristi pojam *cybercrime*, potrebno je izabrati hrvatsku inačicu riječi *cyber*- koja vjerno opisuje izučavanu pojavu.

Cambridge Dictionary definira riječ *cyber*- kao prefiks koji opisuje pojavu koja uključuje, koristi ili se povezuje s računalima, posebice s Internetom (Cambridge Dictionary, 2019). *Hrvatski jezični portal* također definira riječ *cyber*- (izg. . sàjber) kao prvi element u riječima koji označava što vezano uza svijet prividne stvarnosti koji nastaje pomoću kompjutera (Hrvatski jezični portal, 2019).

Međutim, Vojković i Štambuk-Sunjić (2005) ukazuju da je u Republici Hrvatskoj nastala mala terminološka zbrka kada je *Convention of Cybercrime* prevedena kao Konvencija o kibernetičkom kriminalu. Naime, „kibernetiku“ *Hrvatski jezični portal* definira kao „*znanost o istraživanju i automatskim sustavima kontrole u strojeva i živih bića, istraživanje procesa upravljanja raznim sustavima (biološkim, tehničkim, ekonomskim i dr.)*“(Hrvatski jezični portal, 2019). Vojković i sur. (2005) smatraju da je ovaj termin korišten u pogrešnom smislu te dodaju da ne postoji mogućnost ni korištenja pojma „računalni kriminal“ jer ne obuhvaća sve oblike društveno neprihvatljivog ponašanja koje regulira Konvencija. Budući da u hrvatskom jeziku ne postoji istoznačnica, u ovom radu će se koristiti engleska riječ *cyber*- kao prefiks za riječi poput kriminalitet ili prostor.

2.2 Razvoj Interneta

Zasluge za početni koncept koji se kasnije razvio u multimedijalni, mrežni uslužni program (u javnosti poznat kao World Wide Web ili WWW/Web) se obično pripisuju Leonardu Kleinrocku koji je 1961. pisao o ARPANET-u, prethodniku Interneta, u radu „Protok informacija u velikim komunikacijskim mrežama“ („Information Flow in Large Communication Nets“). Kleinrock je s J.C.R. Licliderom i drugim inovatorima osigurao kostur za sveprisutno strujanje elektroničkih poruka, medija, Facebook objava i „tweetova“ koji se dijele Internetom na dnevnoj bazi (Zimmermann i Emspak, 2017).

Abbate (1999; prema Castells, 2001) smatra da priča o kreaciji i razvoju Interneta ističe ljudski kapacitet za nadilaženjem institucionalnih ciljeva i birokratskih barijera te za rušenjem utvrđenih vrijednosti u procesu stvaranja „novog svijeta“. Osim toga, podupire stajalište da su suradnja i sloboda informiranja povoljnije za inovaciju i razvoj od tržišnog natjecanja i vlasničkih prava. Jaishankar (2018) dodaje da je Internet doveo do revolucije jer je pojednostavio rutinske poslove i omogućio trgovinu putem Interneta koja je promijenila obrasce marketinga te ponašanje samih potrošača. Dodatno, nastanak društvenih medija povezao je ljude u jedinstvenu zajednicu te je poništio granice i instance (Jaishankar, 2011). Castells (2003; prema Tintor, 2016) navodi da je današnja uloga informacijske tehnologije ekvivalentna otkriću električne energije u industrijskoj revoluciji te uviđa da se gubi klasično viđenje mjesta boravka i mjesta djelovanja. Danas, ono što se odvija u svakodnevnom životu, paralelno se odvija i u *cyber*-prostoru što je, između ostalog, direktan utjecaj na globalno ekonomsko tržište čime počinje uspon umreženog društva (Castells, 2003; prema Tintor, 2016).

Međutim, društvena svijest i entuzijazam za pozitivne promjene koje donosi Internet su pomiješani sa strahom da donosi nove prijetnje i opasnosti koje ugrožavaju našu dobrobit i sigurnost.

2.3 Tradicionalni i *cyber*-kriminalitet

Inicijalno, kriminolozi nisu razumjeli *cyber*-kriminalitet kao novu formu kriminala te je *cyber*-prostor više istraživan od strane drugih stručnjaka poput informatičara te internetskih forenzičara (Jaishankar, 2007). Iako Capeller (2001; prema Yar, 2006) naglašava da pojavom novog društvenog prostora nastaje potreba za razvojem odgovarajućeg kriminološkog vokabulara, ne

slažu se svi stručnjaci s ovakvim stavom. Neki od njih, poput Graboskyja (2001; prema Yar, 2006) koji objašnjava *cyber*-kriminalitet kao „staro vino u novoj boci“, vide isti kao slučaj poznatih kriminalnih aktivnosti provođenih uz korištenje novih alata i tehnika. Ako je navedeno istina, onda bi *cyber*-kriminalitet mogao biti kvalitetno objašnjen, analiziran i shvaćen pomoću već uspostavljenih kriminoloških klasifikacija i etioloških shema (Yar, 2006).

Međutim, prilikom analiziranja *cyber*-kriminaliteta moramo uzeti u obzir prostorne i vremenske dimenzije kriminaliteta i devijacije. S jedne strane, tradicionalni kriminalitet sadrži neke generalne karakteristike, poput statičnog vremena i mjesta. To znači da se tradicionalni počinitelji pojavljuju u određenom trenutku, na određenom mjestu na kojem počine kazneno djelo. Dakle, da bi se neko ponašanje moglo smatrati i prepoznati kao kriminalno mora se odvijati unutar specifičnih vremenskih i prostornih granica u kojima je prepoznato kao zabranjeno (Willams, 2006; prema Moise, 2014). S druge strane, karakteristike *cyber*-kriminaliteta odmiču se od ovakvog poimanja kaznenih djela s obzirom na fluidnost vremena i prostora u kojima se odvija te nepostojanju konsenzusa o dopuštenosti određenih ponašanja.

Iako smatra da trenutno ne postoji adekvatna definicija *cyber*-kriminaliteta, Wall (2001; prema Yar, 2005) navodi da je termin postao neizostavan u političkom, kaznenopravnom, medijskom, javnom i akademskom diskursu. Isti autor dodaje da termin može biti korišten za opisivanje širokog opsega nedopuštenih ponašanja čija je poveznica središnja uloga informacijskih i komunikacijskih tehnologija. Slijedom navedenog, Thomas i Loader su 2000. (prema Yar, 2005:409) ponudili radnu definiciju *cyber*-kriminaliteta koja glasi: „*cyber-kriminalitet su aktivnosti, posredovane uporabom računala, koje su ilegalne ili smatrane nedopuštenima od strane određenih grupa i koje mogu biti izvršavane putem globalne internetske mreže*“ (Yar, 2005:409). Dakle, specifičnost *cyber*-kriminaliteta pronalazimo upravo u korištenju novoustanovljenog interaktivnog okruženja u kojem se odvija: *cyber*-prostora.

Termin *cyber*-prostor (eng.*cyberspace*) osmislio je autor romana znanstvene fantastike William Gibson u svom romanu Neuromancer iz 1984. kako bi opisao okružje u kojem „hakeri“ operiraju. Nakon publikacije ovog romana, pojam *cyber*-prostor je prilagođen i korišten na razne načine, od kojih se svi u nekoj mjeri odnose na komunikacijsku tehnologiju te virtualnu stvarnost (Dodge, 2001; prema Chawki, 2005).

Capeller (2001; prema Yar, 2006) prepoznaje da *cyber*-prostor, ključan element *cyber*-kriminaliteta, ima velik utjecaj na oblike socijalnih interakcija (dopuštenih i nedopuštenih) te tako transformira opseg i razmjer kršenja zakona, nepovratno mijenja odnos između počinitelja i žrtve kao i potencijal kaznenopravnog sustava da nudi zadovoljavajuća rješenja. Posebna pozornost se pridaje načinima na koje *cyber*-prostor nadilazi ograničenja prostora i vremena koja utječu na interakcije u „stvarnom svijetu".

Isti autor (2001; prema Yar, 2006:408) definira *cyber*-prostor kao: „*novo i prepoznatljivo društveno okruženje koje se sa svojom vlastitom ontološkom i epistemološkom strukturom, interakcijskim oblicima, ulogama, pravilima, ograničenjima i mogućnostima razlikuje od „stvarnog" ili „fizičkog" prostora*". No, spomenuti prostor, osim online interakcija i razmjena, donosi i široku lepezu mogućnosti za kriminalne i nedozvoljene aktivnosti (Yar, 2006).

Iz navedenog, Yar (2006) zaključuje da obilježja i novine koje Internet donosi čine mogućim stvaranje novih oblika nedopuštenog ponašanja. Isti autor naglašava da upravo razlika između *cyber*- i tradicionalnog kriminaliteta čini *cyber*-kriminalitet specifičnim i originalnim.

Clough (2010) u svom radu Principi *cyber*-kriminaliteta (izv. *Principles of Cybercrime*) navodi neke od ključnih značajki digitalne tehnologije i Interneta koje olakšavaju činjenje kaznenih djela te sprječavaju detekciju od strane zakona:

A. OPSEG

Internet je unaprijedio tradicionalne oblike komunikacije te omogućio svojim korisnicima puno jednostavniji i jeftiniji način za interakciju s mnoštvom ljudi (Clough, 2010). Posljedično, broj internetskih korisnika je u rapidnom porastu te se procjenjuje da danas 56,1% svjetske populacije (oko četiri milijarde ljudi) ima pristup Internetu (Internet World Stats, 2019). Ovakav opseg omogućava bezbroj mogućnosti za činjenje kaznenih djela, posebice kada uzmemo u obzir „lakoću" kršenja zakona u *cyber*-prostoru (Clough, 2010).

B. PRISTUPAČNOST

Internet stvara lak pristup informacijama potrebnim za ilegalne aktivnosti koje bi inače bile izvan mogućnosti pojedinca. Dodatno, počinitelji, koji bi inače bili izolirani u svom kršenju zakona, pronalaze istomišljenike te mogu formirati virtualne zajednice u službi činjenja

kaznenih djela (Morris, 2004; prema Clough, 2010). Dodatno, Stalans i Finn (2016) naglašavaju da Internet olakšava zastranjivanje i kriminalitet kroz dostupnost i vidljivost alternativnih opravdanja i normativnih gledišta o *cyber*-kriminalitetu.

C. ANONIMNOST

Jedna od očitih prednosti Interneta za počinitelja je anonimnost, posebice jer sam Internet nudi mnoštvo mogućnosti u postizanju iste. Počinitelji mogu s namjerom prikriti svoj identitet koristeći dvojnike računala poslužitelja (eng. *proxy servers*; Riječnik internet pojmova, 2019), lažne adrese elektroničke pošte ili *IP* adrese. Dodatno, pristupanje bežičnoj mreži, s ili bez autorizacije, može prikriti identitet stvarnog korisnika čak i ako je lokacija otkrivena (Clough, 2010). Navedeni primjeri su samo nekolicina mogućnosti koje Internet zaista pruža u području prikrivanja identiteta.

D. PRENOSIVOST

Prenosivost se odnosi na mogućnost pohrane ogromnih količina podataka u malen prostor (npr. USB-stick). Dodatno, kopije slika ili zvukova se mogu prenositi milijunima korisnika bez praktički ikakvog troška ili gubitka vremena (Clough, 2010).

E. GLOBALNI DOSEG

Clough (2010) naglašava da je kazneni zakon tradicionalno podređen lokaciji za koju je propisan međutim, moderna tehnologija izaziva ovu paradigmu. Povezanost geografske lokacije i pravnog odgovora na *cyber*-kriminalitet detaljnije je opisana u poglavlju „Kaznenopravni odgovor na *cyber*-kriminalitet“.

F. NEDOSTATAK SPOSOBNIH „ČUVARA“

S obzirom na poteškoće koje digitalna tehnologija predstavlja provedbi zakona, nedostaje bitan faktor koji može utjecati na činjenje kaznenih djela: procijenjeni rizik detekcije i kaznenog progona (Clough, 2010). Budući da ne postoji centralizirano državno tijelo koje bi postavilo norme prikladnog ponašanja i primjenjivalo kazneni zakon pojedinih država, nezakonito ponašanje je u nekim državama tolerirano i zakonito što dozvoljava počiniteljima da biraju čije zakone će poštivati kako bi izbjegli pravne posljedice (Stalans i Finn, 2016).

3 Etiologija *cyber*-kriminaliteta

Kirwan i Power (2012), iz više razloga, naglašavaju važnost teoretskih objašnjenja kriminaliteta. Osim što iste teže razumijevanju uzroka i prirode nedopuštenih aktivnosti, korisne su i u njihovom predviđanju. Posljedično, osnova su razvijanja preventivnih strategija, kao i programiranja uspješnih intervencija za počinitelje.

Postoji nekoliko razina proučavanja kriminaliteta. S jedne strane, sociološka (ili makro) razina uključuje proučavanje šire i lokalne zajednice. S druge strane, analiza se može vršiti na osobnijoj razini te uključuje teorije učenja i individualne teorije (Howitt, 2009; prema Kirwan i Power, 2012). Teorija može proučavati problem na više razina, no rijetke su one koje uspijevaju obuhvatiti sve njegove aspekte. Dodatno, Kirwan i Power (2012) naglašavaju da navedene teorije nisu isključive već komplementarne, što znači da se mogu usporedno koristiti u objašnjavanju pojave kriminaliteta.

S obzirom na navedeno, bitno je problematizirati primjenjivost postojećih teorija na fenomen *cyber*-kriminaliteta.

3.1 Socijalna konstrukcija kriminaliteta

Howitt (2009; prema Kirwan i Power, 2012) objašnjava da aktivnost, sama po sebi, nije univerzalno neprihvatljiva. Naime, društvo određuje što predstavlja nezakonito ponašanje. Prema tome, aktivnost može biti definirana kao nedopuštena s obzirom na specifični niz okolnosti, poput povijesnog i kulturološkog konteksta unutar kojeg se odvija.

Proces socijalne konstrukcije je bitan element prilikom izučavanja *cyber*-kriminaliteta. Neka kaznena djela, poput posjedovanja i distribucije dječje pornografije, su već bila okarakterizirana kao nezakonita zbog postojanja njihovih *offline* inačica. Druge aktivnosti, poput proizvodnje i distribucije potencijalno malicioznih programa, pripadaju sivoj zoni. Iako se intuitivno može zaključiti da su nezakonite, ove aktivnosti prvo moraju biti propisane kao takve od strane zakonodavaca. S obzirom na postojeće dileme oko legalnosti određenih *online* aktivnosti, može se zaključiti da je socijalna konstrukcija *cyber*-kriminaliteta još uvijek u fazi evolucije (Kirwan i Power, 2012).

3.2 Biološke teorije kriminaliteta

Iako postoje dokazi da je većina *cyber*-kriminalaca muškog spola (s vrlo malo ženskih počinitelja zabilježenih u znanstvenoj literaturi), ne postoji dovoljno informacija o tome kako biološkim teorijama objasniti *cyber*-kriminalitet. Razlog za navedeno je nedostatak značajnih neuroloških, genetskih i hormonalnih istraživanja na skupini *cyber*-kriminalaca (Kirwan i Power, 2012).

3.3 Teorije učenja

Teorije učenja se koriste u forenzičkoj psihologiji prilikom razvoja intervencija za počinitelje s ciljem promjene ponašanja te zbog objašnjavanja uzročnosti nedozvoljenih aktivnosti. Učenje, u psihologiji, označava: „*relativno stabilnu promjenu u ponašanju ili znanju*“ (Kirwan i Power, 2012:41) te postoji nekoliko metoda postizanja ovakve promjene, poput klasičnog i operantnog uvjetovanja te učenja po modelu.

Klasično uvjetovanje se javlja kada osoba nauči povezivati različite podražaje. Na primjer, postoje argumenti da određeni dio osoba koje sudjeluju u *cyberbullyingu*, ovakva ponašanja ne bi manifestirao u „stvarnom“ svijetu. Budući da se nasilje odvija u *cyber*-prostoru, „nasilnik“ nije izložen uvjetovanom podražaju (žrtvinoj reakciji) pa ne doživljava uvjetovanu reakciju osjećaja krivnje (Kirwan i Power, 2012).

Dok klasično uvjetovanje objašnjava emocionalne i psihološke reakcije pojedinca, operantno uvjetovanje uzima u obzir načine na koje pojedinac uči kontrolirati ponašanje s obzirom na posljedice određenih događaja i aktivnosti. Operantno uvjetovanje predlaže da će potencijalan počinitelj nastaviti sudjelovati u aktivnostima koja su nagrađivana, dok će odustajati od aktivnosti koje predstavljaju prevelik rizik od kažnjavanja. Slijedom navedenog, prilikom činjenja kaznenog djela, percipirani dobici su veći od percipirane potencijalne kazne. Prilikom nekih vrsta *cyber*-kriminaliteta, poput računalne prijevare, percepcija rizika od strane počinitelja je vrlo mala, posebice zbog anonimnosti koje pruža Internet (Kirwan i Power, 2012).

Prilikom učenja po modelu, učenje se odvija indirektno kroz promatranje drugih osoba te imitiranjem njihovih ponašanja u sličnim situacijama. Modeli su često članovi obitelji ili vršnjačke skupine. Prema tome, može se zaključiti da će pojedinac češće sudjelovati u ilegalnim aktivnostima ako u njima sudjeluju njegovi vršnjaci ili bliske osobe. Ovom teorijom možemo

objasniti neke devijantne aktivnosti u *cyber*-prostoru, poput ilegalnog preuzimanja zaštićenih materijala (Kirwan i Power, 2012).

3.4 Teorije ličnosti

Kirwan i Power (2012) navode da je povijest forenzičke psihologije ispunjena pokušajima objašnjavanja kriminalnog ponašanja pojedinaca proučavanjem njihovih obilježja ličnosti. Najpoznatija među ovim teorijama je Eysenckova teorija koja uključuje ispitivanje crta ličnosti poput psihoticizma, neuroticizma i ekstraverzije (1977; prema Kirwan i Power, 2012). Međutim, Kirwan i Power (2012) smatraju da nije pretjerano korisna u širenju znanja o *cyber*-kriminalitetu.

Drugi autori su analizirali povezanost kršenja zakona s karakteristikama ličnosti poput moralnog razvoja, empatije, inteligencije, samokontrole i impulzivnosti (Palmer i Hollin, 1998; Jolliffe i Farrington, 2004; Lopez-Leon i Rosner, 2010; Piquero, Moffitt i Wright, 2007; Shuman i Gold, 2008; prema Kirwan i Power, 2012). Neka od spomenutih obilježja su, kroz empirijska istraživanja, potvrđena kao korelati ili prediktori kriminalnog ponašanja. Tako postoje dokazi da „hakeri“ imaju slabo razvijene interpersonalne vještine, a osobe koje sudjeluju u ilegalnom preuzimanju materijala imaju niske razine samokontrole (Kirwan i Power, 2012).

Ipak, Kirwan i Power (2012) spominju dileme o točnoj uzročnosti ponašanja. Problem proizlazi iz činjenice da je nemoguće odrediti jesu li nedozvoljena ponašanja uzrokovana određenim crtama ličnosti, ili su one razvijene zbog učestalog sudjelovanja u ilegalnim aktivnostima. Drugi nedostatak teorija ličnosti je nemogućnost generalizacije rezultata zbog manjka homogenosti skupine. Gotovo je nemoguće odrediti set psiholoških karakteristika koji objašnjava različita ponašanja poput krađe identiteta, proizvodnje računalnih virusa, distribucije dječje pornografije, *cyber*-terorizma i nasilja (Kirwan i Power, 2012).

Naposljetku, Kirwan i Power (2012) naglašavaju da, unatoč svojim nedostatcima, teorije ličnosti mogu biti korisne prilikom proučavanja psiholoških obilježja počinitelja te pomažu u stvaranju sveobuhvatnijih teorija.

3.5 Psihoanalitička teorija

Budući da mnoštvo *cyber*-kaznenih djela uključuje racionalno razmišljanje i zaključivanje, psihoanalitičke teorije (koje naglašavaju utjecaj podsvjesnog) se ne mogu smatrati prikladnima u objašnjavanju ovakvog ponašanja. Međutim, spomenute teorije mogu biti korisne u razumijevanju

pedofilije te povezanih nedopuštenih *online* ponašanja, poput kontaktiranja i *groominga* djece na Internetu (Kirwan i Power, 2012).

3.6 Teorije ovisnosti i uzbuđenja

McQuade (2006; prema Kirwan i Power, 2012) predlaže teoriju uzbuđenja kao objašnjenje za aktivnosti povezane s *cyber*-kriminalom. Spomenuta teorija nalaže da pojedincu odgovara određena razina uzbuđenja te pribjegava ponašanjima koja održavaju tu razinu. Isti autor povezuje teoriju uzbuđenja s pretjeranim igranjem *video*-igara te zaključuje da aktivnosti poput *cyber*-uhođenja i „hakiranja" mogu izazvati stanje psihološke uzbuđenosti kod počinitelja.

Howitt (2009; prema Kirwan i Power, 2012) predlaže da teorija ovisnosti objašnjava zašto pojedine osobe ustraju u činjenju kaznenih djela kroz cijeli život, dok većina počinitelja prestane s nedozvoljenim ponašanjem tijekom kasne adolescencije i rane odrasle dobi. Isti autor navodi da postoje dokazi da osobe, koje sudjeluju u ilegalnim aktivnostima, često imaju problema s drugim vrstama ovisnosti (poput pretjerane konzumacije droga i alkohola). Iz navedenog se može zaključiti da se radi o osobama koje su sklone ovisnostima, što može ukazivati i na poteškoće u ranom razvoju (Howitt, 2009; prema Kirwan i Power, 2012).

Međutim, ovisnost o kriminalnim aktivnostima ne objašnjava zašto individua počinje sudjelovati u njima. Dok se teorijom uzbuđenja može opisati početni angažman počinitelja, razvoj ovisnosti objašnjava zašto počinitelj ustraje u ovakvim ponašanjima (Kirwan i Power, 2012).

3.7 Teorija neutralizacije

Teorija neutralizacije pojašnjava kako pojedinac opravdava vlastita nemoralna ponašanja (Sykes i Matza, 1957; prema Kirwan i Power, 2012). Koncept neutralizacije se može povezati s procesom stvaranja kognitivnih distorzija, tj. pogrešnih misli koje služe počinitelju pri objašnjavanju aktivnosti u kojima sudjeluje. Na primjer, pojedinci koji sudjeluju u „piratstvu", svoje ponašanje mogu shvatiti kao pomoć u lansiranju nečije glazbene karijere. Dok osobe koje prikupljaju dječju pornografiju često razvijaju kognitivne distorzije vezane za posljedice njihovog ponašanja (Kirwan i Power, 2012).

3.8 Teorija rutinske aktivnosti

Teorija rutinske aktivnosti postavlja hipotezu da: „*kriminalne aktivnosti ovise o usklađivanju vremenskih i prostornih dimenzija potencijalnog počinitelja i prikladne mete te nedostatku sposobnih čuvara*“ (Cohen i Felson, 1979; prema Yar, 2005:413).

Kirwan i Power (2012) navode da se teorija rutinske aktivnosti može primjenjivati prilikom analiziranja gotovo svih oblika *cyber*-kriminaliteta. Prema tome, većina kaznenih djela *cyber*-kriminaliteta se vrlo lako izvode ako počinitelj ima neograničen i nesmetan pristup resursima, poput osobnog računala i besplatnog Interneta. Prikladna meta može biti bilo koje umreženo računalo nad kojim se uspostavi kontrola, a nedostatak sposobnih čuvara se može shvatiti kao nepostojanje *anti*-virusnih programa na računalu žrtve (Kirwan i Power, 2012).

3.9 *Cyber*-kriminologija i teorija prostornog prijelaza

Iako su mnogi akademici pokušavali objasniti uzroke nastajanja *cyber*-kriminaliteta pomoću postojećih teorija, Jaishankar (2018; Yar, 2005) dovodi njihovu uspješnost u pitanje. Isti autor (2007) uočava specifičnosti *cyber*-kriminaliteta te potrebu za akademskom disciplinom koja obuhvaća multidisciplinarno područje zanimanja, uključujući ispitivanje kriminalnog ponašanja i viktimizacije u *cyber*-prostoru iz kriminološke i ponašajno-teoretske perspektive. Lansiranjem novog časopisa s nazivom Internacionalni časopis *cyber*-kriminologije (izv. *The International Journal of Cyber Criminology*), Jaishankar je osnovao i novu granu kriminologije- *cyber*-kriminologiju, koju definira kao: „*studiju uzročnosti kriminala koji se događa u cyber-prostoru te utječe na fizički prostor*“ (Jaishankar, 2007:1).

Kako bi produbio disciplinu *cyber*-kriminologije, te se odvojio od tradicionalnih objašnjenja, Jaishankar je osmislio teoriju prostornog prijelaza (izv. *Space Transition Theory*) koja objašnjava uzročnost kriminaliteta u *cyber*-prostoru. Spomenuta teorija se fokusira na razumijevanje prirode ponašanja pojedinca koji svoja konformistička i nekonformistička ponašanja manifestiraju u fizičkom i *cyber*-prostoru, dok „prostorni prijelaz“ označava pomicanje iz „stvarnog“ u *cyber*-prostor (i obrnuto) (Jaishankar, 2008; prema Jaishankar, 2011).

Postulati teorije prostornog prijelaza su sljedeći (Jaishankar, 2008; prema Jaishankar, 2011):

- Pojedinci s potisnutom željom za sudjelovanjem u kriminalnim aktivnostima u „stvarnom“ svijetu (zbog statusa ili pozicije) će vjerojatnije koristiti *cyber*-prostor za činjenje kaznenih djela
- Fleksibilnost identiteta, disocijativna anonimnost i manjak faktora zastrašivanja u *cyber*-prostoru, omogućavaju počinitelju sredstva potrebna za kriminalne aktivnosti
- Postoji visoka vjerojatnost prijelaza nedopuštenih aktivnosti iz „stvarnog“ u *cyber*-prostor (i obratno)
- Povremena prisutnost počinitelja u *cyber*-prostoru i prostorno-vremenska priroda istog pružaju počinitelju mogućnost bijega, tj. izbjegavanja identifikacije
- Postoji visoka vjerojatnost da će osobe, koje se ne poznaju u „stvarnom“ svijetu, ujediniti u činjenju kaznenih djela u *cyber*-prostoru
- Osobe koje žive u zatvorenim društvima iskazuju veći rizik za počinjenje kaznenih djela u *cyber*-prostoru od osoba koje žive u otvorenim društvima
- Konflikt između normi i vrijednosti „stvarnog“ svijeta i *cyber*-prostora vodi *cyber*-kriminalitetu

Naposljetku, Jaishankar (2011) navodi da još uvijek ne postoji dovoljno empirijskih dokaza da teorija prostornog prijelaza uspješno objašnjava uzročnost *cyber*-kriminaliteta. Međutim, i ona može biti korisna u stvaranju sveobuhvatnijih teorija.

4 Fenomenologija *cyber*-kriminaliteta

4.1 Tipologije kaznenih djela *cyber*-kriminaliteta

Shinder (2002) naglašava da se *cyber*-kaznena djela, ovisno o prirodi istih, mogu uklopiti u postojeće kategorizacije kriminala. Na primjer, mnoštvo *cyber*-kaznenih djela (poput pronevjere uz pomoć računalne tehnologije) se mogu prepoznati kao kaznena djela „bijelog ovratnika“, a proizvodnja dječje pornografije može pripadati seksualni prijestupima i tretirati se kao kazneno djelo s elementom nasilja. Ovakvi prijelazi između kategorija te raznolikost aktivnosti koje prepoznajemo kao *cyber*-kriminalitet otežavaju razvrstavanje kaznenih djela u uže potkategorije.

Međutim, isti autor (2002) smatra da su ovakve podjele potrebne prilikom detekcije počinitelja. Stoga, slijede različite kategorizacije kaznenih djela koja imaju obilježja *cyber*-kriminaliteta.

Yar (2005) navodi da je moguće, uz korištenje radne definicije *cyber*-kriminaliteta Thomasa i Loadera (2000; prema Yar, 2006), klasificirati *cyber*-kriminalitet s obzirom na ulogu tehnologije. Prema tome, kaznena djela *cyber*-kriminaliteta možemo podijeliti na:

1) Kaznena djela počinjena pomoću računala
2) Kaznena djela s računalom u fokusu

Prva skupina kaznenih djela postojala je i prije izuma Interneta, međutim ista se danas izvršavaju uz pomoć računala i unutar *cyber*-prostora. Primjeri ovakvih kaznenih djela su: prijevara, krađa, pranje novca, seksualno uznemiravanje, govor mržnje te pornografija (Furnell, 2002; prema Yar, 2005). Suprotno navedenom, kaznena djela s računalom u fokusu su nastala s pojavom Interneta i bez istog ne bi mogla postojati. Ova djela su prepoznatljiva i specifična za *cyber*-prostor, na primjer: „hakiranje“, virtualni napadi te oštećenja *web*-stranica (Furnell, 2002; prema Yar, 2005).

Dakle, kada kategoriziramo nedopuštene aktivnosti prema ovoj podjeli, potrebno je ustanoviti je li računalo sporadičan ili neizostavan element u izvršavanju kaznenog djela. Yar (2005) smatra da razlike između ove dvije kategorije mogu biti socio-tehnološki korisne, iako imaju ograničenu kriminološku korist. Stoga je jedna od alternativa mobilizirati postojeće klasifikacije izvedene iz kaznenih zakona u odgovarajuće kategorije kaznenih djela počinjenih uz pomoć računala. Prema tome, Wall (2001; prema Yar, 2005) navodi četiri pravne kategorije kaznenih djela *cyber*-kriminala:

a) **Neovlašteni pristup**: neovlašteni pristup vlasništvu druge osobe i /ili činjenje štete istom (npr. „hakiranje“, računalni virusi, obezličenje *web*-stranica)
b) ***Cyber*-prijevare i krađe**: krađa novca i privatnog vlasništva (npr. prijevare s kreditnim karticama; povrede intelektualnog vlasništva - poput „piratstva”)
c) ***Cyber*-pornografija**: aktivnosti koje krše zakone opscenosti i pristojnosti
d) ***Cyber*-nasilje**: nanošenje psihološke štete ili poticanje fizičkog nasilja, tj. kršenja prava osoba koje su napadnute (npr. govor mržnje; uhođenje).

Navedena klasifikacija je korisna u povezivanju *cyber*-kriminaliteta s postojećim konceptima nedozvoljenih ponašanja. Međutim, Yar (2005) smatra da ne omogućava kvalitativno razlikovanje i izdvajanje *cyber*-kriminaliteta kroz uočavanje specifičnosti istog. Posljedično, većina kriminologa se (posebice oni koji naginju sociološkim objašnjenjima) fokusira na pronalazak noviteta unutar socio-strukturalnih značajki okruženja (*cyber*-prostora) u kojem se takva nedozvoljena ponašanja manifestiraju (Yar, 2005).

McGuire i Dowling (2013) kaznena djela s računalom u fokusu nazivaju „čistim" *cyber*-kriminalom ili djelima koja ovise o računalu. Dakle, radi se o aktivnostima koje se primarno usmjeravaju protiv računala ili računalnih mreža, no isti autori smatraju da mogu postojati sekundarne dobiti ovakvih napada. Na primjer, podatci dobiveni neovlaštenim pristupom određenoj elektroničkoj pošti mogu se koristiti za počinjenje prijevare (McGuire i Dowling, 2013).

Nadalje, McGuire i Dowling (2013) kaznena djela s računalom u fokusu dijele na dvije široke kategorije:

- Neovlašteni pristup računalnim mrežama (npr. „hakiranje")
- Narušavanje ili smanjivanje funkcionalnosti računala i mreže (npr. virusi i DoS napadi- eng. *Distributed Denial-of-service Attack*)

Brenner (2001; prema Schell i Martin, 2004) definira *cyber*-kriminalitet kao kriminalitet počinjen protiv računala ili pomoću računala. Ovakva definicija obuhvaća i kaznena djela počinjena pomoću računala te kaznena djela s računalom u fokusu. Ista autorica dodaje da postoje i politički motivirana kaznena djela, tj. tehnički „ne-prijestupi" u svijetu *cyber*-kriminala.

Slijedom navedenog, Schell i Martin (2004) spominju tri velike kategorije *cyber*-kaznenih dijela s obzirom na počinjenu štetu:

a) Prva kategorija se odnosi na **cyber-kriminalitet koji rezultira imovinskom štetom**. Za činjenje ovakvih kaznenih djela se najčešće koristi tehnika „krekiranja" (neovlašteni pristup računalnom sustavu radi činjenja kaznenog djela) te uključuje sljedeće pojavne oblike: *flooding*, proizvodnju i distribuciju računalnih virusa i crva, *spoofing, phreaking* te povredu prava intelektualnog vlasništva.

b) Druga kategorija obuhvaća **cyber-kriminalitet koji rezultira štetom za osobu** koji se generalno dijeli na *cyber*-uhođenje (eng. *Cyberstalking*) i *cyber*-pornografiju.

c) Naposljetku, treća kategorija se odnosi na djela koja Brenner (2001) naziva **tehničkim „ne-prijestupima“** poput „haktivizma“ (eng. Hacktivism) i „*cyber*-vigilantizma“.

Spomenute aktivnosti bit će detaljnije opisane i razrađene u sljedećem poglavlju.

4.2 Pojavni oblici *cyber*-kriminaliteta

4.2.1 Hakeri

4.2.1.1 Tko su hakeri?

Prije nekoliko desetljeća, pojmovi „haker“ i „hakiranje“ su bili poznati samo nekolicini ljudi kojima je svijet računalstva bio izuzetno blizak (Yar, 2006). Thomas (2002) navodi da je termin neraskidivo povezan s kulturnom, društvenom i političkom povijesti računala. No, ona je vrlo složena i često kontradiktorna, posebno zbog utjecaja koji na nju ima medijska prezentacija te društvena tjeskoba uzrokovana brzim razvojem tehnologije (Thomas, 2002).

Danas se ovi termini raznoliko tumače, pa tako Žižek (1996; prema Thomas, 2002) smatra da se „hakeri“ izoliraju iz svakodnevnog života kako bi se u potpunosti fokusirali na korištenje računala, dok Stone (1996; prema Thomas, 2002) naglašava da su neizostavni u bilo kakvoj raspravi o složenosti i dosegu tehnologije. Neki ljudi ih doživljavaju kao osobe koje uživaju u proučavanju računalnih sustava, dok drugi smatraju da se radi o zlonamjernim pojedincima ili znatiželjnim „nametljivcima“ koji traže korist putem obmane ili ilegalnih sredstava (Schell i Martin, 2004).

Termini „haker“ i „hakiranje“ postali su opće poznati te predstavljaju jedan od najčešće analiziranih i raspravljanih oblika *cyber*-kriminaliteta (Yar, 2006). Trenutne rasprave stručnjaka o „hakiranju“ su dovele do zajedničke definicije koja glasi: *„hakiranje je neovlašteni pristup i naknadna uporaba tuđeg računalnog sustava“* (Taylor, 1999; prema Yar, 2006:22). Yar (2006) smatra da se, prema ovoj definiciji, „hakiranje“ može tumačiti kao računalna provala, što bi obilježilo „hakera“ kao provalnika. Iz navedenog se može zaključiti da je „hakiranje“ jedan od ključnih, ako ne i neizostavnih elemenata *cyber*-kriminala koji rezultira imovinskom štetom (Schell i Martin, 2004).

Međutim, kada se termin „haker“ počeo koristiti 1960-ih među računalnim programerima, nije imao ovakvu konotaciju. Među njima je termin bio pozitivan te je opisivao osobu s iznadprosječnim vještinama u razvijanju kreativnih, elegantnih te djelotvornih rješenja računalnih problema. Dodatno, „hack“ je sam po sebi označavao inovativno korištenje tehnologije koje je dovelo do pozitivnih rezultata i prednosti (Yar, 2006). Posljedično, osobe koje su pristup Internetu omogućile širokim masama ljudi te proizvođači novih i uzbudljivih računalnih aplikacija (poput videoigara) su svi smatrani „hakerima“ te hrabrim pionirima u računalnoj revoluciji (Levy, 1984; Naughton, 2000; prema Yar, 2006).

Zbog uvriježenog stava da novinari u krivom kontekstu koriste njihov naziv, „hakeri“ su 1985. osmislili termin „*cracker*“ koji opisuje osobu koja ruši sigurnosne postavke računalnog sustava. Razlika između „hakera“ i „*crackera*“ leži u motivaciji njihovog ponašanja te ih Schell i Martin (2004) dijele u dvije kategorije: „hakeri bijelog šešira“ i „hakeri crnog šešira“. Prva skupina je motivirana kreativnim mogućnostima *cyber*-prostora, poput prikupljanja znanja ili pronalaženja propusta u zaštiti računala. Isti autori ovu skupinu nazivaju „dobrim momcima“ računalnog podzemlja. Suprotno navedenom, druga skupina „hakera“ (izv. Black Hat hacker) ili „*crackera*“ čini kaznena djela pomoću računala. Njihovi motivi variraju od osvete i sabotiranja konkurencije do krađe informacija i teroriziranja određenih meta (Schell i Martin, 2004).

Yar (2006) naglašava da razliku između „hakera“ i „*crackera*“ ,iz kriminoloških razloga, vrijedi imati na umu. Isti autor navodi da je spor o karakteriziranju „hakera“ i „hakiranja“ odličan primjer onoga što sociolozi, poput Beckera (1963; prema Yar, 2006), nazivaju „procesom etiketiranja“. Radi se o procesu kroz koji se kreiraju kategorije kriminalnih i devijantnih aktivnosti i identiteta od strane društva. Posljedično, reakcije na „hakiranje“ i „hakere“ ne mogu se shvatiti odvojeno od činjenice da je značenje ovih termina društveno raspravljano i stvoreno (Yar, 2006).

Kao što su termini „haker“ i „hakiranje“ raznoliko shvaćeni, tako su i interpretacije ovog problema podijeljene. S jedne strane, pri opisivanju rizika koji „hakeri“ predstavljaju, pribjegava se hiperbolama poput izjednačavanja posljedica „hakiranja“ s onima nakon napada na Pearl Harbor (Taylor, 1999; prema Yar, 2006). Takvi nadomak apokaliptični prikazi „hakiranja“ su povezani s već poznatim strahovima da će tehnologija izmaknuti našoj kontroli te uzrokovati neizmjernu štetu. Osim toga, javnost je kroz razne filmove i novinske članke stvorila sliku „hakera“ kao izoliranih i disfunkcionalnih pojedinaca koji učinkovito mogu komunicirati samo sa svojim

računalom (Yar, 2006). Međutim, javno mišljenje o „hakerima“ i „hakiranju“ nije isključivo negativno. Yar (2006) uočava ambivalentnost stavova te navodi da „hakeri“ u nekim slučajevima izazivaju očaranost te čak i divljenje. Isti autor dodaje da studije društvenih stavova pokazuju da značajni dio populacije, posebice mlađa populacija, vidi „hakere“ u pozitivnom svijetlu.

Razlike među generacijama primjećujemo i unutar same „hakerske“ kulture. S jedne strane, „stari hakeri“ su skoro pa uvijek bili visokoobrazovani članovi zajednice. S druge strane, današnji „hakeri“ su sve češće adolescenti koji svoje vještine „hakiranja“ koriste u svrhu neslanih šala (Thomas, 2002). Bez obzira na raznolikost u motivaciji i u korištenim tehnikama, Thomas (2002) smatra da u današnjoj skupini „hakera“ vlada „dječačka kultura“. Ova kultura (Rotundo, 1998; prema Thomas, 2002) ima tri značajke: vještinu vladanja tehnologijom, neovisnost i prkos starijoj generaciji. Budući da je demografija „hakera“ sastavljena prvenstveno (ali ne isključivo) od bijelih adolescenata koji žive u predgrađu, istog autora povezanost s „dječačkom kulturom“ ne iznenađuje.

Rodgers je (2000; prema McGuire i Dowling, 2013) ponudio svoju tipologiju koja razlikuje „hakere“ s obzirom na razvijenost „hakerskih“ vještina te motivaciju u pozadini nedopuštenih aktivnosti:

a) „*Newbie*“ (osobe sa slabo razvijenim vještinama i iskustvom; ovise o alatima koje su drugi kreirali; poznati i kao „*script-kiddies*“)
b) „*Cyberpunks*“ (osobe koje s namjerom napadaju i vandaliziraju)
c) „*Internals“* (*insajderi* s povlaštenim pristupom; često nezadovoljni zaposlenici)
d) *„Coders*“ (pojedinci s visoko razvijenim vještinama)
e) „*Old guard hackers*“ (nemaju kriminalne stavove; visoko razvijene vještine; „hakeri bijelog šešira“)
f) Profesionalni kriminalci
g) *Cyber*-teroristi

4.2.1.2 Što rade hakeri?

Kako bismo mogli prepoznati motivaciju za „hakiranje“ bitno je razumjeti načine na koje „hakeri“ operiraju. Yar (2006) smatra da aktivnosti u kojima sudjeluju gotovo uvijek uključuju neku vrstu manipulacije, remećenja i upada u računalni sustav. Stoga, isti autor navodi da su ključni elementi „hakiranja“: a) dobivanje pristupa i b) kontrola nad računalnim sustavom. Jednom kada se kontrola nad računalom uspostavi, široka lepeza ilegalnih aktivnosti postaje moguća:

a) KRAĐA RAČUNALNIH RESURSA/OSOBNIH I POVJERLJIVIH INFORMACIJA

Objekt krađe može biti resurs (npr. glazba, film, transkript i sl.) ili informacija (npr. poslovna tajna, osobni podatci, detalji kreditnih kartica). Furnell (2002; prema Yar, 2006) spominje slučaj švedskog „hakera“ koji je preuzeo ogromnu količinu glazbe te ju dijelio putem Interneta. Međutim, otuđeni podatci se mogu koristiti i u kaznenim djelima s mnogo značajnijim posljedicama (Yar, 2006).

Riem (2001; prema Yar, 2006) navodi incident kada su „hakeri“ ukrali detalje nekoliko tisuća kreditnih kartica te ove informacije iskoristili (kroz manipulaciju bankovnog sustava) za prisvajanje sredstava. Dodatno, zabilježen je slučaj ruskih „hakera“ koji su uspjeli napraviti transfer sredstava, s računa korisnika američke banke, u vrijednosti od 10 milijuna dolara (Grabosky i Smith, 2001; prema Yar, 2006).

b) IZMJENA, SABOTAŽA I UNIŠTAVANJE RAČUNALNOG SUSTAVA

Jednom kada uspiju ući u računalni sustav, „hakeri“ mogu učiniti značajnu štetu. Dok je uništavanje sadržaja relativno rijetko (Furnell, 2002; prema Yar, 2006), postoji nekoliko zabilježenih slučajeva nezadovoljnih korisnika koji su sabotirali svoje nekadašnje poslodavce brisanjem bitnih informacija (Philippsohn, 2001; prema Yar, 2006). Češći oblik je selektivna izmjena podataka unutar računalnog sustava. „Hakeri“ ovu metodu koriste kako bi prikrili dokaze svojih aktivnosti te si tako omogućavaju nesmetani upad u sustav u budućnosti. Dodatno, osoba koja je uspostavila kontrolu nad računalnim sustavom može mijenjati podatke unutar sustava za vlastitu korist. Na primjer, zabilježen je slučaj studenata koji su, nakon upada u računalni sustav sveučilišta, mijenjali svoje ocjene. Posebno je zanimljiv slučaj zatvorenika koji je promijenio vlastiti datum otpusta iz kaznionice, kako bi do Božića stigao kući (Denning, 1999; prema Yar, 2006).

c) „OBEZLIČENJE“ *WEB*-STRANICA I „*SPOOFING*“

Prilikom „obezličenja“ *web*-stranice, za razliku od ranije navedenih aktivnosti, nije potrebno upasti u tuđi računalni sustav. „Haker“ (putem Interneta) može preuzeti kontrolu nad *web*-stranicom te mijenjati sadržaj iste. Motiv za ovakva ponašanja može biti želja da „zabavi“ posjetitelje stranice uz pomoć neslane šale, može se raditi o treniranju vještina „hakiranja“ ili o ideološki i politički motiviranim oblicima prosvjeda protiv država ili korporacija (Vegh, 2002; Woo i sur., 2004; prema Yar, 2006).

Drugi oblik „hakiranja“ *web*-stranica je „*spoofing*“ (hrv. podvala). Radi se o prisvajanju identiteta legitimnog korisnika unutar *cyber*-prostora od strane neovlaštene osobe (Schell i Martin, 2004). Prilikom ove aktivnosti, „haker“ ne upada u *web*-stranicu legitimnog korisnika, već kreira vlastitu inačicu koja podsjeća na originalnu. Posljedice ovakvih aktivnosti mogu biti relativno bezopasne, npr. neugodnosti za pravog vlasnika stranice (budući da promjene *web*-stranice često uključuju prikazivanje pornografskog sadržaja i sl.), no mogu imati i ozbiljnije posljedice za velik broj ljudi. U slučaju da korisnik pristupi lažnoj stranici, misleći da je legitimna, osobne podatke koje unese (poput detalja kreditne kartice) predaje direktno tvorcu stranice. Posljedično, ova metoda prisvajanja povjerljivih informacija se često koristi u slijedu aktivnosti potrebnih za računalnu prijevaru (Philippsohn, 2001; prema Yar, 2006).

Kao dodatak navedenom, Yar (2006) spominje i one nedopuštene aktivnosti koje ne zahtijevaju upadanje u tuđi računalni sustav, već koriste druge pristupe poput elektroničke pošte i umreženosti računala:

a) NAPAD USKRAĆIVANJEM RESURSA („*FLOODING*“)

DoS-napadi (eng. *Denial of Service Attack*) mogu rezultirati prisilnim resetiranjem napadnutog računala, no mogu se koristiti i za iskorištavanje njegovih resursa (poput rada procesora, memorije ili mreže). Rezultat je nemogućnost korištenja računala od strane legitimnog vlasnika (Yu, 2014).

„Haker“ koji je na ovaj način pridobio mnogo publiciteta je 15-godišnji Kanađanin sa pseudonimom „Mafiaboy“. On je uspio ugasiti pristup bitnim *web*-lokacijama, poput Amazona, eBay-a i CNN-a te prouzročiti procijenjenih 1,7 milijardi dolara štete (*BBC News*, 2001; prema Yar, 2006).

b) DISTRIBUCIJA MALICIOZNOG SOFTVERA

Maliciozni softver ili kod (izv. *Malware*) je program koji je tajno implementiran u drugi program ili računalni sustav s ciljem: „*uništavanja podataka, pokretanja razornih programa, ugrožavanja povjerljivosti, integriteta ili dostupnosti podataka, aplikacija i operacijskog sustava legitimnom korisniku*“ (Souppaya i Scarfone, 2013:9). Souppaya i Scarfone (2013) navode da je maliciozni softver jedan od najizvjesnijih prijetnji većini korisnika te uzrokuje rasprostranjenu štetu i nemir unutar većine organizacija. Isti autori (2013) navode sljedeće kategorije i opise spomenutih zlonamjernih programa:

a) **Računalni virus** je program koji kreira svoje kopije te ih implementira u postojeće programe ili datoteke. Često se aktivira putem interakcije s računalom poput otvaranja datoteke ili pokretanja programa.

b) **Crv** također stvara vlastite kopije te je samostalan program koji se aktivira bez interakcije s računalom. Može se širiti putem Interneta ili elektroničke pošte.

c) **Trojanski konj** je samostalan program koji, premda izgleda bezazleno, ima skrivenu malicioznu namjenu. Trojanski konj može zamijeniti postojeće datoteke sa „zaraženima“, ili dodavati takve datoteke u računalni sustav.

d) **Mobilni maliciozni kod** (izv. *Malicious Mobile Code*) je zlonamjerni program koji se, bez pristanka, prenosi s računala počinitelja na računalo legitimnog korisnika.

e) **Miješani napadi** (izv. *Blended Attacks*) uključuju kombiniranje ranije navedenih napada usmjerenih na jedno računalo.

Zaključno, Yar (2006) naglašava da je shvaćanje „hakera“ kao male, visokoučinkovite i motivirane elitne skupine sve manje povezano s realnosti. Tehnike „hakiranja“ su se zbog pojave automatiziranih softverskih alata (eng. *automated software tools*) izuzetno promijenile. Isti autor (2006:32) smatra da je spomenuta tehnološka inovacija: „*demokratizirala „hakiranje“ jer ga je učinila dostupnim svim pojedincima s računalom, pristupom Internetu te željom da otkriju digitalno podzemlje*“.

4.2.1.3 Politički motivirano hakiranje

4.2.1.3.1 *Cyber*-terorizam

Shinder (2002: 116) definira *cyber*-terorizam kao: „*korištenje Interneta i računalnih vještina s ciljem ometanja i rušenja ključne infrastrukture i javnih usluga određene države*“. Dok Verton (2003; prema Yar, 2006:51) nudi sveobuhvatniju definiciju istog fenomena koja glasi: „*cyber-terorizam je izvršenje iznenadnog napada od strane inozemne terorističke skupine ili individualaca koji, zbog političke agende, koriste računalnu tehnologiju i Internet s ciljem oštećenja ili gašenja elektroničke i fizičke infrastrukture napadnute države*“.

Crozier (1974; prema Yar, 2006) klasični terorizam objašnjava kao posebni oblik kaznenog djela čije je ključno obilježje spajanje nasilja i politike. Ako dodamo Internet kao treći element, govorimo o *cyber*-terorizmu. Shinder (2002) osobe koje učestvuju u spomenutim aktivnostima naziva *cyber*-kriminalcima s političkom motivacijom u pozadini. Isti autor navodi da variraju od onih bezopasnih sa željom izražavanja vlastitih političkih stavova do organiziranih terorističkih skupina poput al Qa'ide i Hamasa (Shinder, 2002).

Mogući slučajevi *cyber*-terora su sljedeći (Denning, 2000; Gordon i Ford, 2003; Verton, 2003; prema Yar, 2006):

- Gubitak električne energije zbog napada na sustave koji kontroliraju energiju
- Prekidi u financijskim transakcijama koji blokiraju ekonomske sustave
- Oštećenje prijevoznih infrastruktura (poput zračnog i željezničkog prometa) putem upadanja u pripadajuće računalne sustave
- Krađa strogo čuvanih informacija vezanih za obranu i nacionalnu sigurnost (Yar, 2006)

4.2.1.3.2 *Cyber*-ratovanje/Informacijsko ratovanje

Termin „informacijsko ratovanje“ je prvi upotrijebio Dr. Thomas Runa. Od tada, definicije ovog termina često uključuju vojnu dimenziju (1976; prema Knapp i Boulton, 2008), pa je tako Libicki (1995; prema Knapp i Boulton, 2008:18) ponudio sedam kategorija informacijskog ratovanja koje su ispunjene vojnom terminologijom: „*ratovanje kontrolom i zapovijedanjem, ratovanje informacijama, elektronsko ratovanje, psihološko ratovanje, „hakersko“ ratovanje, ratovanje ekonomskim informacijama i cyber-ratovanje*“. Danas koristimo termine „informacijsko

ratovanje“ i *cyber*-ratovanje u imenovanju cijelog spektra konflikata koji uključuju političke, ekonomske, kriminalne, sigurnosne, građanske i vojne dimenzije (Knapp i Boulton, 2008).

4.2.1.3.3 Haktivizam

Jordan i Taylor (2004:1) definiraju „haktivizam“ kao : „*pojavu popularnog političkog djelovanja te samoaktivnosti skupine ljudi u cyber-prostoru*“. Isti autori navode da „haktivisti“ iskušavaju tehnološke mogućnosti *cyber*-prostora te ih koriste u pokušaju oblikovanja stvarnog svijeta. Radi se o specifičnom sociološkom i kulturološkom fenomenu nastalom krajem 20.st. prilikom kojeg se politika direktne akcije prenosi u *cyber*-prostor (Jordan i Taylor, 2004).

Maurushat (2015) navodi dva generalna principa „haktivizma“: a) poštovanje ljudskih prava i temeljnih sloboda (uključujući slobodu govora te pravo na privatnost) i b) obveza države da bude transparentna (odgovornost prema javnosti).

„Hakerska“ skupina „*Anonymous*“, na primjer, često poziva na političku važnost anonimnosti, što Coleman (2011) podsjeća na odluke Vrhovnog Suda SAD-a koji zaštitu anonimnog govora smatra ključem demokratskog diskursa. Štoviše, anonimni govor je opisan kao štit od tiranije većine (The Hacker Quarterly, 1998-99; prema Coleman, 2011). Nadalje, skupina „*WikiLeaks*“ djeluje prema principima liberalnog stava da transparentnost može biti korištena u ograničavanju državnih ovlasti (Coleman, 2011).

Coleman (2011) uočava ideološke sličnosti među „hakerima“, no primjećuje razlike u provođenju politike u stvarnom svijetu. Autorica smatra da ovakve razlike proizlaze iz činjenice da su „hakeri“ zaposleni na raznim područjima, započinju različite tipove projekata te su locirani u svim dijelovima svijeta. Dodatno, unutar same „hakerske“ zajednice se vode dugogodišnje debate o legitimnosti: pristupa, otvorenosti, transparentnosti, privatnosti i samog „hakiranja“. (Coleman, 2011).

Brenner (2001) opisuje „haktivizam“ kao korištenje *cyber*-prostora s ciljem uznemiravanja i sabotiranja određenih *web*-stranica koje sadrže aktivnosti ili podržavaju filozofiju koju „haktivisti“ smatraju neprihvatljivima. Autorica (2001) dodaje da „haktivisti“, iako oni sami ljutito odbijaju ovakav stav (Radcliff, 2000; prema Brenner, 2001), spadaju pod kategoriju *cyber*-terorista jer u suštini čine kaznena djela kako bi promovirali svoju političku agendu.

Yar (2006) uočava da su prednosti „haktivizma“ proizašle upravo iz korištenja „hakerskih“ tehnika. Osim što *cyber*-prostor omogućava okupljanje mnoštva sudionika prosvjeda koji su inače raspršeni među gradovima i državama, ovakve tehnike nude prosvjednicima značajan stupanj zaštite od policijskih službenika koji im, prilikom tradicionalnog prosvjeda, kontroliraju i ograničavaju okupljanje i kretanje (Yar, 2006).

Jedna od prvih skupina „haktivista“ su *Electrohippie Collective* (ili „*ehippies*“). „*Ehippies*“ su 1999. u Seattleu, prilikom sastanka Svjetske trgovinske organizacije (izv. *World Trade Organization* ili WTO), organizirali simultane *offline* i *online* prosvjede. Dok su prosvjednici blokirali ulice, „haktivisti“ su okupirali *web*-stranice. Spomenuta skupina je kreirala jednostavni program sa svrhom višestrukog učitavanja *web*-stranice WTO-a, te je cilj bio (ako se skupi dovoljno sudionika) srušiti *web*-stranicu. Bilo koja osoba, koja je odlučila sudjelovati u prosvjedu, je mogla preuzeti spomenuti program i koristiti ga na vlastitom računalu. Ova „virtualna“ akcija je bila usklađena s akcijom „na ulici“, kojoj je cilj bio zaustaviti sastanak Svjetske trgovinske organizacije. „*Ehippies*“ tvrde da je prosvjedu prisustvovalo 450 tisuća računala koja su, u periodu od pet dana, uspjela srušiti stranicu WTO-a dva puta te ju značajno usporiti tijekom trajanja konferencije (Electrohippies Collective, 2000; prema Jordan, 2002).

4.2.2 *Cyber*-kriminalitet povezan s prijevarom

4.2.2.1 Računalna prijevara i *scam*

Button i Cross (2017:6) definiraju prijevaru kao: „*široki spektar aktivnosti čije je zajedničko obilježje neistinito predstavljanje od strane počinitelja kako bi si osigurao korist ili prouzročio štetu drugima*“. Iako su trenutne konceptualizacije prijevare usko povezane s novom tehnologijom (poput Interneta), prijevara postoji od trenutka kada su ljudi naučili komunicirati te posjedovali imovinu (Button i Cross, 2017). Maurer (2000; prema Yar, 2006) dodaje da je povijest čovječanstva ispunjena ovakvim djelima, od onih drskih s velikim, do sitničavih s malim posljedicama.

Button i Cross (2017) naglašavaju da tehnologija nije utjecala na želju niti spremnost počinitelja da sudjeluju u prijevari, već na same metode počinjenja kaznenog djela. Pa je tako razvojem pošte došlo do prijevare putem pisama, a izumom telefona nastale su telekomunikacijske prijevare. Slijedom navedenog, pojavom Interneta nastaje računalna prijevara (eng. *cyber-fraud*) (Button i Cross, 2017).

Shinder (2002:25) definira računalnu prijevaru kao: *„promicanje neistina s ciljem prisvajanja određene vrijednosti ili koristi*“. Isti autor primjećuje da bi se ovaj oblik prijevare mogao svrstati među imovinska kaznena djela, no postoje određena obilježja koja ju odvajaju od takvog shvaćanja.

Za razliku od razbojništva ili krađe, koji iza sebe ostavljaju vidljive tragove (npr. tragovi provale ili nestanak bicikla), nakon prijevare ne postoje neosporni dokazi da je kazneno djelo počinjeno. Button i Cross (2017:7) razlikuju prijevaru (eng. *fraud*) i „*scam*“ (hrv. obmana; podvala) koju definiraju kao: „*obmanjujuće ponašanje kojem je cilj pridobiti materijalna sredstva ili informacije od prevarene osobe te se može shvatiti kao neetično postupanje, građansko ili upravno pitanje ili nezakonita prijevara*“. Prema tome, termin „*scam*“ obuhvaća ponašanja koja nisu nužno nezakonita (poput neetičnog postupanja), dok termin prijevara podrazumijeva samo nezakonitu stranu na kontinuumu (Button i Cross, 2017).

Kroz sljedeće primjere, isti autori obuhvaćaju spomenuti kontinuum:

a) „*Scam*“ s europskim zdravstvenim karticama

Za navedeni „*scam*“ koristile su se besplatne kartice, predviđene za građane Europske Unije, koje omogućavaju pristup raznim zdravstvenim uslugama. Nekoliko *web*-stranica je kreirano s ciljem prodavanja spomenutih kartica (za cijenu od približno 20 engleskih funti) te se pretpostavlja da je na ovaj način prevareno oko milijun korisnika. Budući da je na *web*-stranicama bilo naznačeno da postoji način da se zdravstvene kartice dobiju besplatno, kreatori nisu prekršili nijedan zakon (Massey, 2011; prema Button i Cross, 2017). Međutim, Button i Cross (2017) ovo ponašanje klasificiraju kao neetično, budući da postoji financijski gubitak za korisnika.

b) Osiguranje kredita

Financijske institucije su uzrokovale značajan problem u Ujedinjenom Kraljevstvu kada su prodavale kreditno osiguranje korisnicima koji ga, ili nisu trebali, ili ga uopće nisu mogli koristiti. Zbog skandala je odlučeno da su spomenute financijske institucije dužne nadoknaditi učinjenu štetu korisnicima od približno 25 milijardi engleskih funti (FCA, 2016; prema Button i Cross, 2017). Povrede od strane financijskih institucija su procijenjene neetičnim ponašanjem te upravnim propustima, no ne i nezakonitima (Button i Cross, 2017).

c) „Romantična prijevara“

Ovakav oblik prijevare obuhvaća širok spektar ponašanja koji uključuju povredu raznih prava. S jedne strane, situaciju kada se osoba prijavi na *web*-stranicu za pronalaženje partnera i neiskrena je o svom bračnom statusu možemo obilježiti kao neetično ponašanje, no ne i nezakonito (barem ne u većini država). S druge strane, kada počinitelj koristi lažni identitet da ostvari romantične odnose s više partnera kako bi pridobio materijalna sredstva, radi se o nezakonitom ponašanju. Međutim, postoji mnoštvo ponašanja između navedena dva ekstrema za koje se puno teže može dokazati da su nezakonita. Može se raditi o kaznenim djelima, ali i o građanskim razmiricama ili neetičnom postupanju (Button i Cross, 2017).

d) „Nigerijski princ“

Jedan od klasika računalne prijevare je „*Nigerian 419 scam*“. Tijekom ove vrste prijevare ciljanu osobu kontaktira „korumpirani službenik“, koji joj nudi naknadu ako mu dozvoli da joj na račun prenese ilegalno stečena sredstva. U slučaju da ostane na navedenom, radi se o kaznenom djelu pranja novca. Međutim, „korumpirani službenik“ često prvo traži uplatu od strane žrtve kako bi „pridobio povjerenje“ što rezultira financijskim gubitkom za žrtvu. Očito je da se u ovom slučaju radi o nezakonitoj prijevari jer, između ostalog, uključuje korištenje lažnog identiteta (Button i Cross, 2017).

S obzirom na ranije navedenu podjelu *cyber*-kriminaliteta na kaznena djela počinjena pomoću računala i kaznena djela koja ovise o računalu (Yar, 2005; McGuire i Dowling, 2013), Button i Cross (2017) dijele kaznena djela prijevare na: prijevaru počinjenu pomoću računala (izv. *Cyber-enabled fraud*) i prijevaru koja ovisi o računalu (izv. *Cyber-dependent fraud*). Prva skupina obuhvaća „hakiranje“ (ilegalno prisvajanje osobnih podataka zbog daljnjeg korištenja u prijevari) i „*monitoring*“ (hrv. nadgledanje; instaliranje programa na ciljano računalo s namjerom prisvajanja povjerljivih informacija poput korisničkog imena i lozinke). Prijevara počinjena pomoću računala obuhvaća sljedeće aktivnosti (Button i Cross, 2017):

a) Prijevara bez kartice (izv. *Card Not Present Fraud*; počinitelji prisvoje potrebne brojeve s kreditne kartice te ih koriste za *online* trgovinu)

b) Lažna prodaja (izv. *Fraudulent Sales*; prodaja pogrešno predstavljene ili nepostojeće robe)

c) Prijevara putem krađe identiteta (izv. *Phishing Scams*; predstavljanje, putem elektroničke pošte u ime legitimne organizacije s ciljem uvjeravanja korisnika te pribavljanja povjerljivih informacija)

d) Masovne marketinške prijevare (izv. *Mass Marketing Frauds*; uključuje raznolike oblike prijevare s ciljem osiguravanja plaćanja od strane žrtve; može se raditi o lažnim dobitcima na lutriji, informacijama o ostavštini, prilikama za poslovanje...)

e) Romantične prijevare (izv. *Romance Fraud*; opisano ranije u tekstu)

Naposljetku, Button i Cross (2017) navode da je razvoj tehnologije pripremio teren za stvaranje novih oblika prijevare koji, ili nisu postojali prije, ili ih je bilo puno teže uspješno izvršiti. Jedan od čimbenika koji olakšava uspjeh prijevare je prostorna udaljenost između žrtve i počinitelja (Duffield i Grabosky, 2001; prema Button i Cross, 2017). Prostorna udaljenost olakšava i uspješno prikrivanje identiteta, što postaje sve privlačnija metoda mnogim počiniteljima (Button i Cross, 2017).

4.2.2.2 Spam

Iako su ga mnogi smatrali više smetnjom nego kaznenim djelom, sve je izvjesnije da će „*spam*“ postati značajan socio-ekonomski problem (Industry Canada, 2005; prema Clough, 2010). Socia (2009:169) definira „*spam*“ kao: „*nepoželjnu komercijalnu poruku, poslanu elektroničkim putem na mnogo adresa odjednom*“. Ista autorica navodi da se ovakva poruka često pojavljuje u obliku ponude za prodaju farmaceutskih proizvoda; savjeta o dionicama; linkova *web*-stranica za upoznavanje, stranica s pornografskim sadržajem, ili pak ponude za razne poslovne prilike, često upitne legitimnosti.

Iako ga primarno povezujemo s elektroničkom poštom, „*spam*“ postaje sve češća pojava i u drugim medijima poput SMS i MMS poruka (Task Force of Spam, 2006; prema Clough, 2010).

„*Spam*“ može imati mnogo negativnih utjecaja, prvenstveno na efikasnost elektroničke pošte legitimnog korisnika. Programi koji filtriraju poruke ponekad pogrešno svrstaju poštu, ili se pak željena pošta zagubi u velikoj količini „*spam*“ poruka (CAN-SPAM, 2003; prema Clough, 2010).

Iako uzrokuje mnogo negativnih posljedica, „*spam*“ nije teško stvoriti. „*Spammer*“ prvo mora osmisliti primamljivu poruku, dodati poveznice za ostale izvore na Internetu te distribuirati poruke

tako da dođu do što više primatelja. Danas, jedna od češćih metoda distribuiranja „*spam*“ poruka je upotrebom „*botneta*“ -mreže računala nad kojima su „hakeri“ tajno preuzeli kontrolu. Spomenuta „*zombie*“ računala šalju „*spam*“ poruke na elektroničke adrese pronađene na samom računalu ili na adrese s masovnih lista elektroničkih adresa (Socia, 2009).

„*Spam*“ je sam po sebi problematičan, no sadržaj koji prenosi može biti opasniji, poput uvredljivog, prijevarnog i zlonamjernog sadržaja (Clough, 2010). Iako neki „*spamovi*“ predstavljaju iskrene pokušaje za reklamiranjem određenog proizvoda, vrlo malo je takvih poruka, točnije oko 10% (Wall, 2005; prema Clough, 2010). Ostatak poruka su pokušaji prijevare, pa tako i prijevare putem krađe identiteta (izv. *Phishing*) koje postaju sve češće i sofisticiranije (*Federal Trade Commission*, 2007; prema Clough, 2010). Clough (2010) dodaje da se *„spam*“ poruke koriste i u distribuciji malicioznih programa poput virusa i Trojanskog konja.

Naposljetku, distribucija „*spam*“ poruka ponekad uključuje vezane aktivnosti koje same po sebi mogu biti nezakonite. Na primjer, osoba koja kreira „*spam*“ može koristiti tehniku „*spoofinga*“ što je ilegalna aktivnost jer se radi o krađi identiteta legitimnog vlasnika *web*-stranice (Socia, 2009).

4.2.3 Kršenje autorskih prava

Digitalno „piratstvo“ je oblik kršenja autorskih prava te ga Sampat (2009:143) definira kao: „*metodu ilegalnog dobavljanja i distribuiranja računalnih programa, igara, videa, glazbe i drugih medija, putem računala ili telekomunikacijskih uređaja*“. Ova metoda uključuje reprodukciju i distribuciju autorskog materijala bez pristanka samog autora (Sampat, 2009).

Iako „digitalno piratstvo“ nije prijevara samo po sebi, Clough (2010) ga smatra vezanim djelom jer uključuje neovlašteno miješanje u vlasnička prava druge osobe. Shinder (2002) „piratstvo“ svrstava među *cyber*-krađe, no Clough (2010) smatra da kod kršenja autorskih prava nije riječ ni o krađi, ni o „piratstvu“.

Clough (2010) navodi da rast pristupačnosti autorskih materijala u digitalnom obliku stvara dilemu. S jedne strane, ovakav razvoj otvara prostor za međunarodnu trgovinu, a s druge strane lakoća distribucije i dostupnost čine jednostavnijim i „digitalno piratstvo“. Iako je kršenje autorskih prava prepoznato kao nezakonito (Mass, 1994; prema Clough, 2010), provedba zakona o autorskim pravima je tradicionalno bila (i ostala) pitanje građanskog prava (Penney, 2004; prema Clough, 2010).

4.2.4 Dječja pornografija

Dječja pornografija nije uvijek smatrana značajnim elementom u nizu aktivnosti koje se povezuju sa seksualnim zlostavljanjem, već zanemarivim korelatom mnogo značajnijeg i šireg problema. Međutim, posljednja dva desetljeća, razumijevanje i identifikacija problema seksualnog zlostavljanja djece je u značajnom porastu, kako u laičkoj tako i u profesionalnoj zajednici (Taylor i Quayle, 2003). Pojedinci koji su htjeli doći do dječje pornografije u danima prije Interneta, morali su je osobno potraživati, čuvati u fizičkom obliku (npr. časopis, video-zapis, fotografija i sl.) i tako riskirati detekciju i razotkrivanje dokaza. Danas ovakvom materijalu mogu pristupiti koristeći osobno računalo s relativnom lakoćom (Home Office, 2005; prema Clough, 2010).

Prilikom definiranja dječje pornografije nailazimo na dileme, pa tako Taylor i Quayle (2003) navode da termin nije prikladan jer se može stvoriti paralela s „odraslom" pornografijom. Ovakva usporedba implicira povezanost dva termina, no isti autori naglašavaju da dječja pornografija ne predstavlja ništa drugo osim snimke zlostavljanja djeteta. Clough (2010) navodi da kazneni zakon SAD-a sadrži prikladnije termine poput „iskorištavanja" (izv. *child exploitation*) ili „dokaz zlostavljanja" djeteta (izv. „*child abuse" material*). Međutim, termin „dječja pornografija" se nastavlja koristiti u medijskoj prezentaciji i znanstvenoj literaturi.

Pa tako, Konvencija o kibernetičkom kriminalu definira dječju pornografiju kao „pornografski materijal" koji prikazuje (Konvencija o kibernetičkom kriminalu, 2001; prema Clough, 2010:255-256): „*maloljetnika/cu prilikom seksualne aktivnosti; osobu koja izgleda kao maloljetnik uključenu u seksualne aktivnosti; realistične prikaze koji predstavljaju maloljetnike/ce uključene u seksualne aktivnosti*."

Uzrok povećane svijesti i zabrinutosti o dječjoj pornografiji je sve veća izloženost posljedicama ovakvih ponašanja. Clough (2010) smatra da je jedan od tragičnijih aspekata računalne revolucije upravo olakšana proizvodnja i distribucija dječje pornografije. Prije popularizacije Interneta, spomenute materijale je bilo otežano prevoziti bez detekcije te su sama produkcija i korištenje opreme bili značajno kompliciraniji nego danas. Kako je digitalna tehnologija uzimala sve više maha tako je i broj kaznenih progona zbog dječje pornografije rastao (Clough, 2010).

Povezanost tehnologije i ovog tipa nedozvoljenog ponašanja je lako razumljiva. Nova tehnologija je relativno jeftina, pristupačna i prijenosna te dozvoljava pohranu ogromne količine materijala.

Mogućnosti za kreaciju dječje pornografije su povećane i zbog pojave isplativijih metoda proizvodnje digitalnih snimki koje prilikom prijenosa ne gube kvalitetu. Dodatno, snimke seksualnog zlostavljanja djece danas se mogu se odašiljati uživo pomoću *web*-kamera (ponekad na zahtjev klijenta) (Muir, 2008; prema Clough, 2010) te postoje načini za proizvodnju „virtualne" dječje pornografije koja uključuje snimke digitalno stvorene djece (Clough, 2010).

Međutim, Taylor i Quayle (2003) naglašavaju da Internet ne služi samo kao sredstvo distribucije već igra značajnu psihološku ulogu prilikom razvoja i širenja tržišta dječje pornografije. Isti autori navode kako postoji sve više dokaza da Internet olakšava razvoj seksualnog interesa za djecu kod odraslih, ne samo uz pomoć dječje pornografije već kroz stvaranje podržavajućeg konteksta za ovakva ponašanja te stvaranje prilika za anonimno komuniciranje s djecom.

Kozak (2009:24) navodi da su mnogi počinitelji kaznenih djela vezanih uz dječju pornografiju pedofili koje definira kao: *„seksualne prijestupnike koji traže neprikladne seksualne interakcije s djecom*".

Mahoney i Faulkner (1997; prema Taylor i Quayle, 2003:104-105) navode da Internet dozvoljava pedofilima sljedeće aktivnosti:

- *„trenutačni pristup pripadnicima vlastite skupine;*
- *otvorene rasprave o seksualnim potrebama;*
- *izmjenu ideja o načinima privlačenja potencijalne žrtve;*
- *zajedničku filozofiju o opravdanosti njihovih potreba i ponašanja;*
- *trenutačni pristup potencijalnim žrtvama diljem svijeta;*
- *prikrivanje identiteta prilikom upoznavanja s djecom te preuzimanje identiteta pripadnika njihove dobne skupine;*
- *pristup dječjim chat-roomovima;*
- *mogućnost pristupa osobnim podatcima poput adrese i kontakta;*
- *mogućnost za stvaranje dugotrajnog online odnosa prije pokušaja fizičkog kontakta s djetetom."*

Vjeruje se da velika količina dječje pornografije dolazi od strane organiziranih kriminalnih skupina Istočne Europe. Olakšavajući čimbenik za činjenje ovakvih kaznenih djela u nekim državama je nepostojanje „snažnih“ zakona koji se odnose na dječju pornografiju te ograničenost provedbe zakona zbog manjka resursa. Posljedično, spomenute skupine mogu nesmetano koristiti moć Interneta prilikom trgovine nedopuštenim materijalima (Kozak, 2009). Clough (2010) navodi da svjetsko tržište dječje pornografije postaje vrlo unosno te procjenjuje da je 2006. godine postojalo više od 100 tisuća *web*-stranica posvećenih distribuciji spomenutih materijala.

Kako bi djecu zaštitile od štete koju doticaj s dječjom pornografijom može uzrokovati, većina država strogo osuđuje njeno stvaranje, distribuciju i posjedovanje. Pa tako Sjedinjene Američke Države (i mnoge druge) izričito zabranjuju sve oblike ovakvog ponašanja te njihovi sudovi rutinski određuju dugotrajne kazne zatvora počiniteljima (Kozak, 2009).

4.2.5 *Cyber*-nasilje

4.2.5.1 Online-uznemiravanje i cyberbullying

Svake godine, tisuće adolescenata i odraslih osoba prijavljuje neki oblik *online* nasilja. Colt (2009) navodi da je ovakva pojava povezana s povećanim brojem korisnika računala i društvenih mreža koji dobrovoljno ili slučajno objavljuju svoje osobne podatke te osoba koje koriste istu tehnologiju i informacije s namjerom da povrijede druge.

Postoje razlike u terminologiji prilikom opisivanja spomenute pojave, poput „*cyber-bullyinga*“ (kada su djeca i mladi u pitanju) te *online*-uznemiravanja (izv. *online-harassment*). Trenutno, ne postoji univerzalna definicija *online*-uznemiravanja zbog neslaganja o tome što obilježavati kao kršenje zakona ili socijalnih normi (Colt, 2009). No, Colt (2009:41) navodi da *online*-uznemiravanje možemo smatrati: „*setom nasilničkih ponašanja koje uključuju korištenje Interneta za slanje štetnih poruka ciljanoj osobi te objavljivanje štetnog sadržaja o osobi*“. Isti autor dodaje da ovu pojavu možemo smatrati i aspektom *cyber-bullyinga*.

U većini slučaja se radi o *online* ponašanjima koja su namjerna, ponavljana i agresivna, te koja se često prenose u „stvarni“ svijet (i obrnuto), poput učionice, radnog mjesta ili društvenih funkcija (Colt, 2009).

Iako *online*-uznemiravanje neki smatraju manjim problemom, Colt (2009) naglašava da ga se treba shvatiti ozbiljno, čak i kada prijetnje i uhođenje nisu prisutni. Ignoriranjem *cyber-bullyinga* i

online-uznemiravanja, kako navodi Colt (2009), riskiramo povredu žrtve te sve komplikacije kojima ovakvo ponašanje može rezultirati.

4.2.5.2 *Cyber*-uhođenje

D'Ovidio i Doyle (2003; prema Yar, 2006:127) definiraju *cyber*-uhođenje (izv. *Cyberstalking*) kao: *„ponavljano korištenje Interneta, elektroničke pošte ili drugih uređaja za elektroničku komunikaciju kako bi smetali, uznemiravali ili prijetili ciljanoj osobi*".

Ogilvie (2000; prema Clough, 2010) navodi da se radi o kompleksnom fenomenu s raznim motivacijama u pozadini, poput ljubomore, ljutnje, opsesije ili želje za uspostavljanjem kontrole. Počinitelj može biti bivši partner, član obitelji, poznanik ili potpuni stranac. Iako se uhođenje popularno povezuje sa slavnim osobama, ovakva vrsta ponašanja se često javlja u slučajevima obiteljskog nasilja (Burgess, Douglas i Halloran, 1997; prema Clough, 2010). Slijedom navedenog, veća je vjerojatnost da će žrtva biti ženskog, a počinitelj muškog spola (Tjaden i Thoennes, 1998; prema Clough, 2010).

Uhođenje uključuje ponašanja poput praćenja i/ili nadziranja žrtve, ponavljane i uznemirujuće pozive te druge tipove komunikacije poput elektroničkih poruka, kao i uništavanje žrtvine imovine (Tjaden i Thoennes, 1998; prema Clough, 2010). Ovakve aktivnosti se mogu nastavljati kroz duže periode, često mjesecima te ponekad godinama (Clough, 2010).

Značajna razlika između *cyber*-uhođenja i uhođenja u tradicionalnom smislu je činjenica da *cyber*-uhođenje rijetko rezultira uznemiravanjem lice u lice. Analizom zabilježenih slučajeva *cyber*-uhođenja može se zaključiti da isto skoro uvijek započinje i završava u *cyber*-prostoru (Ogilvie, 2000; prema Yar, 2006).

Ogilvie (2000; prema Clough, 2010) navodi da *cyber*-uhođenje značajno utječe na mentalno zdravlje žrtve i uzrokuje stanja poput anksioznosti, nesanice, suicidalnosti te posttraumatske poremećaje. Yar (2006) naglašava da ne postoji opravdan razlog zbog kojeg bi se psihološka šteta tretirala manje ozbiljno nego tjelesna, budući da posljedice *cyber*-uhođenja mogu biti ekstremne i opasne. Bitno je naglasiti da, iako rijetko, *cyber*-uhođenje može rezultirati i fizičkim napadom na žrtvu ili njoj blisku osobu (Clough, 2010).

5 Kaznenopravni odgovor na *cyber*-kriminalitet

5.1 Međunarodni kaznenopravni okvir

Od izgradnje ARPANETA u 1960-tim godinama do eksplozije World Wide Weba-a u 1990-tima (Castells, 2001) svjedočili smo, osim dobicima i prednostima Interneta, i mračnijoj strani uporabe istog: *cyber*-kriminalu. Jaishankar (2018) navodi da je Internet postao područje slično „Divljem Zapadu“ što dodatno otežava činjenica da se radi o internacionalnom prostoru koji je upravljan samo od strane američkih zakona, a mnoštvo ostalih država nije znalo kako pravno reagirati na *cyber*-kriminal (Jaishankar, 2011).

Razlog za prvotnu nemogućnost država da pravilno odgovore na ovu društvenu pojavu leži u činjenici da se nedozvoljena ponašanja događaju u *cyber*-prostoru, što dovodi u pitanje legitimnost ranijih zakona koji se baziraju na geografskim granicama (Johnson i Post, 1996). Johnson i Post (1996) naglašavaju da Internet uništava povezanost geografske lokacije i:

a) Mogućnosti državnih vlasti u kontroliranju ponašanja na Internetu

b) Posljedica *online*-ponašanja za pojedince ili stvari

c) Legitimnosti državnih napora da provodi pravila primjenjiva na globalne pojave

d) Sposobnosti fizičke lokacije da objavi čija pravila se moraju poštovati

Mogućnost kontroliranja ponašanja u *cyber*-prostoru ima jako slabu povezanost s teritorijalnom lokacijom. Ipak, prvotni odgovor nekih država na prekograničnu komunikaciju i dijeljenje informacija je bio pokušaj kontrole i regulacije protoka tih informacija. Međutim, Johnson i Post (1996) smatraju da će se napori da se pravila i regulacije iz „fizičkog“ prostora prepišu u *cyber*-prostor vrlo vjerojatno pokazati uzaludnima, posebice u državama koje žele sudjelovati u globalnoj trgovini.

Jedan od prvih pokušaja stvaranja kaznenopravnog okvira u odnosu na *cyber*-kriminalitet je zabilježen u Sjedinjenim Američkim Državama kada je senator Abraham Ribicoff 1977. predložio savezni zakon o računalnom kriminalitetu. Iako zakon ni dvije godine kasnije nije izglasan (Goodman i Brenner, 2002; prema Chawki 2005), imao je velik utjecaj u promoviranju donošenja sličnih zakona u saveznim državama poput Floride i Arizone (Hogge, 2001: prema Chawki, 2005).

Europske države su, zbog promjene paradigmi, 1970-tih prolazile kroz pravne reforme. Tada su kazneni zakoni ovih država bili fokusirani na zaštitu opipljivih stvari. Međutim, pojavom Interneta dolaze u fokus bestjelesne vrijednosti te informacije, na koje se informacijska tehnologija većinom oslanja. Posljedično, uviđena je potreba za novim kaznenopravnim okvirom koji uključuje spomenute bestjelesne vrijednosti. Razne države svijeta su, tijekom druge polovice 20. stoljeća, prošle četiri koraka u stvaranju kaznenopravnog okvira koji obuhvaća sve zabilježene oblike *cyber*-kriminala (Chawki, 2005):

1. **Zaštita privatnosti**- zbog povećanih mogućnosti za sakupljanjem, pohranjivanjem i prenošenjem podataka putem računala nastaju kaznenopravni okviri o zaštiti podataka (Švedska 1973., SAD 1974., Njemačka 1978., Austrija, Danska, Francuska 1979.) (Sieber, 1998; prema Chawki, 2005)

2. **Računalni imovinski kriminalitet**- zbog neadekvatnosti postojećih zakona, koji štite materijalne stvari, nastaju zakoni koji se fokusiraju na zaštitu nematerijalnih stvari poput zakona o neovlaštenom pristupu (SAD 1978., Italija 1979., Australija 1981., UK 1984., Hrvatska 1997.) (Sieber, 1998; prema Chawki, 2005.)

3. **Zaštita intelektualnog vlasništva**- zaštita autorskih prava za računalni softver, uključujući zakon o autorskim pravima te pravnu zaštitu topografija (Filipini 1972., SAD 1983., Mađarska 1984., Australija, Indija i Meksiko 1985.) (Sieber, 1998; prema Chawki, 2005.)

4. **Štetan i ilegalan sadržaj**- zabrane širenja pornografije, govora mržnje i klevete (UK 1994., Njemačka 1997.) (Goodman i Brenner, 2002; prema Chawki 2005)

Posljednja grupa pitanja se odnosi na minimalne sigurnosne mjere u interesu prava privatnosti te zabrane određenih mjera sigurnosti poput ograničenja kriptografije (Sieber, 1998; prema Chawki, 2005).

Kako suvremeni svijet povijesno pripada postmodernoj eri u kojoj svi ozbiljni problemi društva postaju globalni, tako je i pojava *cyber*-kriminala stavila naglasak na potrebu za izjednačavanjem kaznenih zakonodavstava pojedinih država (Vojković i sur., 2005). Upravo s tim ciljem je Vijeće Europe 1997. godine osnovalo Odbor stručnjaka za kriminalitet u *cyber*-prostoru. Zadaća Odbora bila je izrada međunarodnog dokumenta za suzbijanje *cyber*-kriminaliteta (Kokot, 2014).

Konvencija o kibernetičkom kriminalu (u daljnjem tekstu: Konvencija) je usvojena na konferenciji Vijeća Europe u Budimpešti 23.11.2001. godine (Kokot, 2014) te ju je potpisalo ukupno 38 država (među njima i nečlanice Vijeća Europe: Kanada, Japan, Južna Afrika i SAD), a ratificiralo 11 država : Hrvatska, Albanija, Bugarska, Cipar, Danska, Estonija, Luksemburg, Mađarska, Makedonija, Rumunjska i Slovenija. Iz navedenog je vidljivo da među državama koje su ratificirale Konvenciju nedostaju velike tehnološki razvijene države o kojima će ovisiti uspjeh Konvencije na globalnoj razini (Vojković i sur., 2005).

Ona predstavlja oblik međunarodnog ugovora te spada u krug takozvanih okvirnih konvencija što znači da njene odredbe nisu izravno primjenjive nego ih svaka država mora implementirati u vlastito zakonodavstvo (Vojković i sur., 2005).

Ranije, kazneno pravo je bilo usmjereno isključivo na računalni kriminalitet, a budući da je ovakva definicija postala preuska, kaznenopravna zaštita se Konvencijom proširila na cijeli *cyber*-prostor (Kokot, 2014).

Konvencija polazi od promjena koje su nastale globalizacijom, koje uključuju razne mogućnosti poput korištenja računalnih mreža i informacija za činjenje kaznenih djela te pohranjivanje i prenošenje dokaza vezanih uz ovakva kaznena djela. Osim toga, polazi i od potrebe za zaštitom legitimnih interesa prilikom korištenja i razvitka informacijskih tehnologija te spoznaje da učinkovita borba protiv *cyber*-kriminala zahtijeva bržu i uhodanu međunarodnu suradnju u kaznenopravnim predmetima (Škrtić, 2009).

Europski parlament i Vijeće Europske unije su, temeljem članka 83. stavka 1. Ugovora o funkcioniranju Europske unije, donijeli Direktivu 2013/40/EU (u daljnjem tekstu: Direktiva) o napadima na informacijske sustave. Ciljevi Direktive su bili usuglasiti kaznene zakone država članica u području napada na informacijske sustave utvrđivanjem minimalnih pravila o definiranju kaznenih djela i odgovarajućih sankcija. Bitno je napomenuti da Direktiva nije u suprotnosti s Konvencijom, već se na nju nadovezuje. Razlozi za donošenje Direktive, uz postojeću Konvenciju, su narav same Konvencije, nedovoljna harmonizacija kaznenog prava u području *cyber*-kriminala te manjkavosti glede sadržaja. Direktiva je donijela novitete u području materijalnog prava poput: proširenja kažnjivog ponašanja, uvođenja otežavajućih okolnosti te određivanja visina kazni (Kokot, 2014).

5.2 Kaznenopravni okvir Republike Hrvatske

Prvo pravo kazneno djelo *cyber*-kriminala je uvedeno u Kazneni Zakon Republike Hrvatske već 1997. u članku 223. KZ-a pod nazivom „Oštećenje i uporaba tuđih podataka“ u Glavi XVII. Kaznena djela protiv imovine. Potpisivanjem Konvencije, RH se obvezala da će usvojiti takve zakonske i druge mjere kojima bi se omogućio kazneni progon počinitelja kaznenih djela protiv tajnosti, integriteta i dostupnosti računalnih sustava i podataka, kaznenih djela u svezi s računalom, kaznenih djela u svezi sa sadržajem, kako i kaznenih djela u vezi s povredama autorskih i drugih srodnih prava te kažnjavanje pokušaja, poticanja i pomaganja tih djela (Kokot, 2014).

Zakon o izmjenama i dopunama Kaznenog zakona objavljen je 15.7.2004. godine u NN 105/2004. te su njime implementirane odredbe Konvencije (Kokot, 2014). Tada su u KZ Republike Hrvatske uvedena nova kaznena djela, no i ona su (poput „Oštećenja i uporabe tuđih podataka“ kojih nema u novijoj verziji zakona) većinom pripala Glavi XVII. Kaznena djela protiv imovine. Radi se o sljedećim djelima i pripadajućim člancima iz KZ-a (1997):

- **Čl.223.** Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava
- **Čl.223.a** Računalno krivotvorenje
- **Čl.224.a** Računalna prijevara

Kazneno djelo opisano u članku 9. Konvencije (Kaznena djela vezana uz dječju pornografiju) obuhvaćeno je u Glavi XIV. Kaznena djela protiv spolne slobode i spolnog ćudoređa (Škrtić, 2009):

- **Čl.197.a** Dječja pornografija na računalnom sustavu ili mreži

Kokot (2014) navodi da se sljedeća velika kaznenopravna reforma dogodila 2011.godine kada je donesen novi Kazneni zakon koji je stupio na snagu 2013. godine. Novim Zakonom je formirana Glava XXV. „Kaznena djela protiv računalnih sustava, programa i podataka“ koja obuhvaća sljedeća kaznena djela (KZ, 2019:68-71):

- **Čl. 266. Neovlašteni pristup**
- **Čl. 267. Ometanje računalnog sustava**
- **Čl. 268**. **Oštećenje računalnih podataka**
- **Čl. 269. Neovlašteno presretanje računalnih podataka**

- **Čl. 270**. **Računalno krivotvorenje**
- **Čl. 271**. **Računalna prijevara**
- **Čl. 272**. **Zlouporaba naprava**
- **Čl. 273**. **Teška kaznena djela protiv računalnih sustava, programa i podataka**

Kokot (2014) navodi da su u kazneno zakonodavstvo Republike Hrvatske implementirane odredbe koje proizlaze iz Konvencije i Direktive. Međutim, autor smatra da način na koji su preuzete pravno-tehnički slabi njihovu uporabnost. Problem prvenstveno uočava u definiranju ključnih pojmova, kao što su računalni podatci, programi i mreža koji su različito prevedeni i nisu dovoljno jasno postavljeni. Većina kaznenih djela postavljena su šire od minimalnih okvira Konvencije i Direktive, dok su pojedina djela ostala nedorađena. Dodaje i da su uočljive pravne praznine, što se odnosi na djela neovlaštenog ostajanja u računalnom sustavu i neovlaštenog pribavljanja računalnih podataka (Kokot, 2014).

6 Prevalencija *cyber*-kriminaliteta u Republici Hrvatskoj

Proučavanjem baza podataka Državnog zavoda za statistiku (DZS, 2016;2017) može se doći do sljedećih informacija (uobličenih u tablicu) o prevalenciji kaznenih djela protiv računalnih sustava, programa i podataka u RH:

Tablica 1: Broj prijavljenih, osuđenih i optuženih osoba u 2017. godini

	Prijavljene osobe (N)	**Optužene osobe (N)**	**Osuđene osobe (N)**
Ukupno	661	88	78
Neovlašteni pristup	41	/	/
Ometanje računalnog sustava	5	/	/
Oštećenje računalnih podataka	13	1	1
Neovlašteno presretanje podataka	3	/	/
Računalno krivotvorenje	20	/	/
Računalna prijevara	569	87	77
Zlouporaba naprava	10	/	/

Izvor: DZS (2017)

Prilikom analize gore navedenih podataka, uočljiva je značajna razlika između broja prijavljenih osoba te osoba koje su u konačnici optužene. Razlog za spomenuti nesrazmjer je činjenica da za mnoga djela ne postoji poznati počinitelj. Od ukupno 661 prijavljenih kaznenih djela, 2017. godine, za njih svega 175 postoji poznati počinitelj (što čini 26%) (DZS, 2017).

Iako su muški počinitelji češće prijavljivani i osuđivani za kaznena djela *cyber*-kriminaliteta, može se zaključiti da više žena sudjeluje u kaznenim djelima protiv računalnih sustava, programa i podataka nego općenito u kaznenim djelima. Udio osuđenih ženskih počinitelja, u 2016. i 2017., je približno 12%, dok njihov udio u kaznenim djelima *cyber*-kriminaliteta iznosi čak 31% od svih osuđenih osoba (DZS, 2016;2017).

Najučestalije kazneno djelo, ako uzmemo u obzir podatke iz 2016. i 2017., je računalna prijevara. Ona čini oko 80% svih prijavljenih djela *cyber*-kriminaliteta u spomenutom periodu. Iza prijevare, po učestalosti, slijedi neovlašteni pristup te računalno krivotvorenje (DZS, 2016;2017).

Postoje zabilježeni slučajevi maloljetnika koji su prijavljeni, optuženi i osuđeni za spomenuta kaznena djela. Iako je 2017. samo 6 maloljetnika prijavljeno, no ne i optuženo zbog računalne prijevare, 2016. su maloljetnici prijavljivani (osim zbog računalne prijevare) i za neovlašteni pristup i oštećenje računalnih podataka (DZS, 2016;2017).

Što se tiče posljedica za osuđene odrasle počinitelje *cyber*-kaznenih djela, njih 13% je osuđeno na kaznu zatvora, a oko 86% na uvjetnu kaznu zatvora (od ukupno 177 osuđenih osoba). Maloljetnicima, koji su 2016. optuženi za računalnu prijevaru, je dodijeljena odgojna mjera pojačanog nadzora, dok je ostalim prijavljenim maloljetnicima, ili odbačena prijava, ili je državno odvjetništvo postupalo po principu uvjetovanog oportuniteta (DZS,2016;2017).

Naposljetku, bitno je naglasiti da su svi zaključci doneseni na temelju informacija DZS-a, što ih čini površnima, jer velik udio prijavljenih počinitelja nije poznat. Dodatno, prilikom donošenja zaključaka o obilježjima počinitelja *cyber*-kaznenih djela, u obzir se mora uzeti (gotovo neizmjerljiva) tamna brojka kriminaliteta.

7 Prevencija *cyber*-kriminaliteta

Stručna literatura o *cyber*-kriminalitetu pruža neke dosljedne dokaze o njegovoj prirodi, poput ponašajnih, vrijednosnih i demografskih korelata činjenja kaznenih djela i viktimizacije. Spomenuta saznanja se mogu koristiti u kreiranju učinkovitih tehnika za prevenciju *cyber*-kriminaliteta (Clarke, 1983; prema Holt i Bossler, 2016), poput tehnika nastalih u sklopu situacijske prevencije kriminaliteta (Collins, Sainato i Khey, 2011; prema Holt i Bossler, 2016).

Situacijska prevencija kriminaliteta vidi počinitelje kao aktivne sudionike koji odabiru sudjelovati u kriminalnim aktivnostima s obzirom na percipirani rizik, potencijalnu nagradu i situacijske faktore. Slijedom navedenog, postoji pet kategorija aktivnosti koje direktno utječu na mogućnosti činjenja kaznenih djela: a) otežavanje činjenja kaznenih djela; b) povećanje rizika detekcije; c) smanjivanje potencijalne nagrade; d) smanjivanje provokacija za činjenje kaznenih djela; e) uklanjanje opravdanja za spomenute aktivnosti (Cornish i Clarke, 2003; prema Holt i Bossler, 2016). U daljnjem tekstu će biti navedeno nekoliko primjera tehnika situacijske prevencije korištenih prilikom prevencije *cyber*-kriminaliteta.

Strategije situacijske prevencije kriminaliteta, koje se mogu neposredno primijeniti na *cyber*-kriminalitet, su prvenstveno povezane s **pokušajima otežavanja činjenja kaznenog djela**, poput jačanja sigurnosti korisnikovog računala, sustava i osobnih podataka (Newman i Clarke, 2003; prema Holt i Bossler, 2016). Jedan od najučestalijih mehanizama za zaštitu računalnog sustava od napada je instaliranje programa koji uključuju aktivnosti poput skeniranja sustava (*anti*-virusni programi) i *anti-spywarea* (Bossler i Holt, 2009; Choi, 2008; prema Holt i Bossler, 2016).

Druga strategija otežavanja činjenja kaznenog djela se odnosi na korisnikovo razvijanje vještina korištenja računala (Bossler i Holt, 2009; Bossler, Holt i May, 2012; Holt i Bossler, 2009; prema Holt i Bossler, 2016). Vjeruje se da će pojedinci s osnovnim shvaćanjem tehnologije lakše uočiti da je računalni sustav napadnut te identificirati elektroničku poštu povezanu s prijevarom kao i privitke koji mogu trajno oštetiti uređaje i podatke (Mitnick i Simon, 2002; Symantec Corporation, 2014; prema Holt i Bossler, 2016).

Iako gotovo svi sustavi (uključujući *web*-stranice, elektroničku poštu te pristupe internim bazama podataka), zahtijevaju upotrebu korisničkog imena i lozinke zbog autorizacije pristupa, jedan od

najutjecajnijih ograničenja računalne sigurnosti je problem sigurnosti lozinke. Spomenuti problem proizlazi iz korištenja lozinki koje nemaju odgovarajuću razinu sigurnosti ili lozinki koje korisnik već koristi prilikom pristupa drugim sustavima (Condliffe, 2015; prema Holt i Bossler, 2016). Nedavnim razvojem ekrana na dodir omogućeno je korištenje lozinki koje nisu alfanumeričke već uključuju različite uzorke. Ovakve lozinke otežavaju pristup „hakerima", no mogu se otkriti ako ekran nije čist (Diepe, 2012; prema Holt i Bossler, 2016). Dodatno, neki proizvođači počinju ugrađivati biometrijske mjere sigurnosti u uređaje, poput Apple mobilnih uređaja koji se otključavaju pomoću otiska prsta (Holt i Bossler, 2016).

Stručnjaci koji se bave situacijskom prevencijom često koriste raznolike metode nadzora s ciljem **povećanja rizika od detekcije** neovlaštenog pristupa (Clarke, 1997; Newman i Clarke, 2003; prema Holt i Bossler, 2016). Ključan resurs u povećanju rizika detekcije je sustav detekcije upada ili *Intrusion Detection System* (IDS) koji se koristi za identifikaciju dvije vrste prometa: a) zlouporaba resursa baziranih na općenitim obilježjima poznatih malicioznih programa (Debar, Dacier i Wespi, 1999; Lee i Stolfo, 2000; prema Holt i Bossler, 2016) i b) anomalija u standardnim obrascima korištenja mreže koje nagovještavaju zlouporabu računalnog sustava (Debar i sur., 1999; Patcha i Park, 2007; prema Holt i Bossler, 2016). Posljedično, IDS ograničava mogućnosti napada „iz vana", kao i aktivnosti internih aktera čiji je cilj iskorištavanje resursa pripadajuće organizacije (Holt i Bossler, 2016).

Bitno je spomenuti i formalne mehanizme koji su razvijeni sa svrhom ometanja ilegalnih *online* zajednica koje sudjeluju u raznim vrstama *cyber*-kriminaliteta (Poulsen, 2012; prema Holt i Bossler, 2016). Određene policijske agencije su prepoznale važnost Interneta, *chat*-soba i drugih oblika komunikacije u aktivnostima seksualnih prijestupnika, te su zbog toga formirane tajne operacije s ciljem identificiranja osoba koje, iz pogrešnih razloga, kontaktiraju djecu ili sudjeluju u trgovini dječje pornografije (Hinduja, 2007; Jenkins, 2001; Wolak, Finkelhor i Mitchell, 2012; prema Holt i Bossler, 2016).

Mehanizmi koji se koriste prilikom **smanjivanja potencijalne nagrade** počinitelja su raznoliki te se prvenstveno odnose na kaznena djela povezana s obmanom i krađom (Newman i Clarke, 2003; prema Holt i Bossler, 2016). Jednom kada počinitelj uspješno pristupi sustavu određene organizacije, vrlo je vjerojatno da će tražiti povjerljive podatke koji mu mogu osigurati materijalnu dobit. Zbog toga su korporacije razvile mehanizme skrivanja ili maskiranja podataka (Fujinkoki,

2015; Oracle, 2013; prema Holt i Bossler, 2016). Dodatno, osmišljena je tehnika smanjivanja potencijalne nagrade koja utječe na mehanizme plaćanja ilegalnih usluga, podataka ili materijala. Kroz eliminiranje usluga *online* plaćanja, koje koriste počinitelji, agencije za provedbu zakona mogu ograničiti ilegalne aktivnosti koje uključuju razmjenu materijalnih sredstava (Newman i Clarke, 2003; prema Holt i Bossler, 2016).

Ključna metoda **uklanjanja opravdanja za sudjelovanje u *cyber*-kriminalitetu** je javna i jasna objava dopuštenih ponašanja u *online* okruženjima (Newman i Clarke, 2003, prema Holt i Bossler, 2016). Stoga, mnoštvo firmi, sveučilišta i javnih knjižnica pružaju informacije o ponašanjima koja nisu dopuštena prilikom korištenja *cyber*-prostora kroz Propise za korištenje Interneta (izv. Internet Use Policies) i Propise pravednog korištenja (izv. Fair Use Policies) (Sommestad, Hallberg, Lundholm i Bengtsson, 2014; prema Holt i Bossler, 2016). Dodatno, pravne inovacije utječu na rast prijavljivanja neovlaštenih pristupa od strane velikih organizacija (Holt i Schell, 2013; National Conference of State Legislatures, 2012; prema Holt i Bossler, 2016).

Naposljetku, bitno je naglasiti da postoje pokušaji uklanjanja opravdanja za sudjelovanje u *cyber*-kriminalitetu kroz utjecaj na proces neutralizacije te na počiniteljevo prihvaćanje devijantnih i kriminalnih aktivnosti. Većinom se radi o kampanjama čiji je cilj osvijestiti članove zajednice o nedopuštenosti određenih ponašanja, posebno kršenja autorskih prava kroz „piratstvo“ (Newman i Clarke, 2003; prema Holt i Bossler, 2016).

8 Zaključak

Najznačajnije specifičnosti *cyber*-kriminaliteta su prostor u kojem se odvija (*cyber*-prostor) te digitalna tehnologija čije značajke olakšavaju činjenje kaznenih djela. No, postoje nedoumice o smjeru izučavanja *cyber*-kriminaliteta. Neki autori, poput Graboskyja (2001; prema Yar, 2006) te Kirwana i Powera (2012) smatraju da *cyber*-kriminalitet nije nova i specifična pojava te da se postojeće teorije kriminaliteta (poput socijalne konstrukcije kriminaliteta, bioloških teorija, teorija učenja, teorija ličnosti, psihoanalitičke teorije, teorije ovisnosti i uzbuđenja, neutralizacije i rutinske aktivnosti) mogu koristiti prilikom objašnjavanja spomenutih ponašanja. Međutim, postoje i pokušaji kreiranja zasebne teorije koja će objašnjavati uzročnost *cyber*-kriminaliteta. Dodatno, formirana je i nova disciplina, *cyber*-kriminologija, koja izučava upravo etiologiju *cyber*-kriminaliteta iz ponašajne perspektive. Nedostatak opravdanih etioloških objašnjenja *cyber*-kriminaliteta leže u činjenici da ne postoji dovoljno empirijskih dokaza koji bi opravdali korištenje većine spomenutih teorija te se javlja potreba za sveobuhvatnijom teorijom.

Najšira kategorizacija *cyber*-kriminaliteta dijeli nezakonita i neprihvatljiva djela na: kaznena djela počinjena pomoću računala i „čista“ kaznena djela *cyber*-kriminaliteta (kaznena djela s računalom u fokusu). Razlika između ove dvije kategorije je činjenica da su sva kaznena djela počinjena pomoću računala postojala i bez elementa korištenja računala, dok su „čista“ *cyber*-kaznena djela nastala tek razvojem informacijske tehnologije. Nadalje, ako se u obzir uzmu posljedice *cyber*-kriminaliteta, kaznena djela se mogu podijeliti na ona s imovinskim posljedicama, posljedicama po osobu i tehničke „ne-prijestupe“.

Prilikom proučavanja pojavnih oblika *cyber*-kriminaliteta, mogu se uočiti sljedeći oblici kršenja zakona i ponašanja upitne prihvatljivosti: „hakiranje“, *cyber*-kriminalitet povezan s prijevarom, kršenje autorskih prava, dječja pornografija i *cyber*-nasilje.

Pojam „haker“ je raznoliko shvaćen i opisivan kroz posljednjih nekoliko desetljeća. Prema tome, određene skupine vide „hakere“ kao asocijalne pojedince, dok ih druge skupine smatraju izuzetno talentiranim osobama. „Hakeri“ mogu sudjelovati u sljedećim aktivnostima: krađi računalnih resursa/osobnih i povjerljivih informacija; izmjeni, sabotaži i uništavanju računalnog sustava; „obezličenju“ *web*-stranica i „*spoofingu*“; napadu uskraćivanjem resursa; distribuciji malicioznog

softvera. Osim „hakiranja“ s motivacijom materijalne koristi u pozadini, postoji i politički motivirano „hakiranje“ koje uključuje: *cyber*-terorizam, *cyber*-ratovanje i „haktivizam“.

Računalna prijevara, *scam* i *spam* pripadaju *cyber*-kriminalitetu povezanim s prijevarom. Može se zaključiti da su računalna prijevara i *scam* nezakonite ili neetične aktivnosti koje mogu koristiti *spam* kao tehniku izvršenja. Spomenute aktivnosti su olakšane postojanjem *online*-bankarstva koji omogućava pristup materijalnim dobrima određene osobe, putem Interneta.

S jedne strane, stručnjaci se najrjeđe slažu oko nezakonitosti i štetnosti *online* „piratstva“ ili kršenja autorskih prava te se dovodi u pitanje koliko određeni materijali mogu i trebaju biti zaštićeni od masovne upotrebe. S druge strane, distribucija i posjedovanje dječje pornografije, koje je olakšano zbog napretka digitalne tehnologije, se gotovo jednoglasno smatraju ilegalnima i djelima s neizmjernim negativnim posljedicama, prvenstveno po djecu.

Cyber-nasilje obuhvaća ponašanja poput *online*-uznemiravanja i *cyberbullyinga* koje mnogi smatraju usko povezanima i sličnima. Radi se o nasilničkim ponašanjima koja su olakšana zbog korištenja Interneta i koja se, najčešće, manifestiraju isključivo u *cyber*-prostoru.

Društveni odgovor na *cyber*-kriminalitet kroz formiranje kaznenopravnog okvira je, u međunarodnom smislu, prošao kroz nekoliko faza razvoja. Ovakvo postepeno uvođenje novih zakona je rezultat postepenog pojavljivanja različitih kaznenih djela u *cyber*-prostoru. Prema tome, razvoj međunarodnog kaznenopravnog okvira uključuje sljedeće faze: zaštitu privatnosti, zaštitu nematerijalnih dobara (računalni imovinski kriminalitet), zaštitu intelektualnog vlasništva te zabranu širenja štetnog i ilegalnog sadržaja. Budući da je izuzetno bitno uskladiti zakone određenih država (s obzirom na *cyber*-kriminalitet), nastala je Konvencija o kibernetičkom kriminalu koju je potpisala i ratificirala Republika Hrvatska. Nakon ratifikacije Konvencije, RH je u Kazneni zakon uvela novu glavu kaznenih djela s nazivom „Kaznena djela protiv računalnih sustava, programa i podataka“. Proučavanjem prevalencije *cyber*-kriminaliteta može se zaključiti da su kaznena djela računalne prijevare i neovlaštenog pristupa najučestaliji oblici *cyber*-kaznenih djela u RH.

Naposljetku, bitno je naglasiti da postoje pokušaju preveniranja *cyber*-kriminaliteta kroz tehnike situacijske prevencije kriminaliteta. Navedeni pokušaji uključuju: otežavanje činjenja kaznenih djela, povećanje rizika od detekcije, smanjivanja potencijalne nagrade i uklanjanje opravdanja za činjenje kaznenih djela.

9 Literatura

1) Brenner, S. (2001). Is There Such a Thing as 'Virtual Crime'?. *California Criminal Law Review, 4(1).* Preuzeto s: „https://poseidon01.ssrn.com/delivery.php?ID=113078126115089090127088111001107027003089005085064035004103096071017009074072001069098036057038114126109088023000002006099121010075001029042123095119110102105001020013063024020074082127123023071079025115125116010022030117116090121124126098119076084&EXT=pdf (pristupljeno dana 25.4.2019.)“

2) Button, M., i Cross, C. (2017). *Cyber Frauds, Scams and their Victims*. New York: Routledge.

3) *Cambridge Dictionary*, https://dictionary.cambridge.org/ (pristupljeno dana 26.2.2019.)

4) Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford: Oxford University Press. „Preuzeto s https://books.google.hr/books?id=Q1Mo3ObWWgC&pg=PA275&lpg=PA275&dq=the+internet+galaxy&source=bl&ots=w0PH30M9aj&sig=ACfU3U0v4Qa9Nm5kEidh3KEU1GhleHEdNw&hl=hr&sa=X&ved=2ahUKEwjf_dyp_4vhAhWtsaQKHUqaDUkQ6AEwCHoECAEQAQ#v=onepage&q=the%20internet%20galaxy&f=false (pristupljeno dana 14.1.2019.)”

5) Chawki, M. (2005). *A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy*, http://www.droit-tic.com/pdf/chawki4.pdf (pristupljeno dana 8.2.2019.).

6) Clough, J. (2010). *Principles of Cybercrime*. New York: Cambridge University Press.

7) Coleman, G. (2011). Hacker Politics and Publics. *Public Culture, 23(3),* 511-516. doi: 10.1215/08992363-1336390

8) Colt, J.P. (2009). Cyber Bullying, Threats, Harassment, and Stalking. U McQuade, S. (ur.), *Encyclopedia of Cybercrime* (str. 41-43). Westport: Greenwood Press.

9) *Državni zavod za statistiku*, https://www.dzs.hr/ (pristupljeno dana 27.4.2019.)

10) Holt, T. and Bossler, A. (2016). *Cybercrime in Progress*. New York: Routledge.

11) *Hrvatski jezični portal*, http://hjp.znanje.hr/ (pristupljeno dana 26.2.2019.)

12) Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology With an Avant-Garde Anthology. U K. Jaishankar (ur.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. (str. 27-35). Boca Raton: Taylor and Francis Group.

13) Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. *International Journal of Cyber Criminology*, 12 (1), 1-8.

14) Johnson, D.R. i Post, D.G. (1996). Law and Borders- the Rise of Law in Cyberspace. *Stanford Law Review*, 48 (5), 1367-1402.

15) Jordan, T. (2001). *Activism!: direct action, hactivism and the future of society*. London: Reaktion Books Ltd.

16) Jordan, T., i Taylor, P. (2004). *Hacktivism and cyberwars*. London: Routledge.

17) Kazneni zakon. *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, 143/12, 125/11, 144/12, 56/15, 61/15, 101/17, 118/18.*

18) Kirwan, G., i Power, A. (2012). Can Theories of Crime be Applied to Cybercriminal Acts?. U G. Kirwan i A. Power, *The Psychology of Cyber Crime: Concepts and Principles* (str. 37-51). Information Science Reference.

19) Knapp, K., i Boulton, W. (2008). Ten Information Warfare Trends. U L. Janczewski i A. Colarik (ur.), *Cyber Warfare and Cyber Terrorism* (str. 17-25). Hershey: Information Science Reference.

20) Kokot, I. (2014). Kaznenopravna zaštita računalnih sustava, programa i podataka. *Zagrebačka pravna revija,* 3 (3), 303-330.

21) Kozak, M.J. (2009). Child Pornography. U McQuade, S. (ur.), *Encyclopedia of Cybercrime* (str. 23-25). Westport: Greenwood Press.

22) Maurushat, A. (2015). Hacktivism and Whistleblowing in the Era of Forced Transparency?. U R. Smith, R. Cheung i L. Lau (ur.), *Cybercrime Risks and Responses: Eastern and Western Perspectives* (str. 253-266). London: Palgrave Macmillan.

23) McGuire, M. i Dowling, S. (2013*). Cybercrime: A review of the evidence*. Home Office. Preuzeto s

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

24) Moise, A.C. (2014). Some considerations on the phenomenon of cybercrime. *Journal od Advanced Research in Law and Economics*, 5(1), 38-43.

25) Sampat, N. (2009). Piracy. U McQuade, S. (ur.), *Encyclopedia of Cybercrime* (str. 143-144). Westport: Greenwood Press.

26) Schell, B., i Martin, C. (2004). *Cybercrime: A Reference Handbook*. Santa Barbara: ABC-CLIO, Inc.

27) Shinder, D.L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Burlington: Syngress.

28) Socia, K. (2009). Spam. U McQuade, S. (ur.), *Encyclopedia of Cybercrime* (str. 169-171). Westport: Greenwood Press.

29) Souppaya, M., i Scarfone, K. (2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. U M. Borelli (ur.), *Malware and Computer Security Incidents: Handling Guides* (str. 1-57). New York: Nova Science Publishers, Inc.

30) Stalans, L.J. i Finn, M.A. (2016). Understanding How the Internet Facilitates Crime and Deviance. *Victims & Offenders, 11(4)*, 501-508, DOI: 10.1080/15564886.2016.1211404

31) Škrtić, D. (2009). Implementacija odredbi Konvencije o kibernetičkom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo. U T. Pavšič Mrevlje (ur.), *Zbornik povzetkov. X. Slovenski dnevi varstvoslovja* (str. 61-62). Ljubljana, Fakulteta za varnostne vede.

32) Taylor, M. i Quayle, E. (2003). Child Pornography: An Internet Crime

33) Thomas, D. (2002). *Hacker culture*. Minneapolis: University of Minnesota Press.

34) Tintor, A. (2016). Moć umreženog društva- Manuel Castells i važnost umreženog društva današnjice (Završni rad). Sveučilište u Rijeci, Filozofski fakultet, Rijeka.

35) Vojković, G. i Štambuk-Sunjić, M. (2006). Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske. *Zbornik radova Pravnog fakulteta u Splitu*, 43 (1), 123-136.

36) Yar, M. (2005). The Novelty of ´Cybercrime´An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407-427 „doi: (10.1177/147737080556056)“

37) Yar, M. (2006). *Cybercrime and Society*, https://epdf.tips/cybercrime-and-society.html (pristupljeno dana 17.2.2019.).

38) Yu, S. (2014). *Distributed Denial of Service Attack and Defense*. New York, NY: Springer.

39) Zimmermann, K.A. i Emspak, J. (2017). *Internet History Timeline: ARPANET to the World Wide Web*, https://www.livescience.com/20727-internet-history.html (pristupljeno 5.3.2019.)