Tipologija počinitelja kaznenih djela iz domene računalnog kriminaliteta

Horvat, Anja

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Education and Rehabilitation Sciences / Sveučilište u Zagrebu, Edukacijsko-rehabilitacijski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:158:066639

Sveučilište u Zagrebu

Edukacijsko-rehabilitacijski fakultet

Diplomski rad

Tipologija počinitelja kaznenih djela iz domene računalnog kriminaliteta

Anja Horvat

Zagreb, rujan, 2024.

Sveučilište u Zagrebu

Edukacijsko-rehabilitacijski fakultet

Diplomski rad

Tipologija počinitelja kaznenih djela iz domene računalnog kriminaliteta

Anja Horvat

Izv. prof. dr. sc. Dalibor Doležal

Zagreb, rujan, 2024.

Izjava o autorstvu rada

Potvrđujem da sam osobno napisao/napisala rad Tipologija počinitelja kaznenih djela iz domene računalnog kriminaliteta 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: Anja Horvat

Mjesto i datum: Zagreb, rujan, 2024.

Naslov rada: Tipologija počinitelja iz domene računalnog kriminaliteta

Studentica: Anja Horvat

Mentor: Izv. prof. dr. sc. Dalibor Doležal

Program/modul: Socijalna pedagogija/Odrasli

SAŽETAK RADA

Računalni kriminalitet postao je, s obzirom na brz razvoj tehnologije i sve veću ovisnost o digitalnim sustavima, jedan od najznačajnijih globalnih problema u suvremenom društvu. Složenost i dinamika ove vrste kriminaliteta predstavlja ozbiljnu prijetnju sigurnosti, ekonomiji i društvenom razvoju. Ovaj rad usredotočen je na počinitelje kaznenih djela protiv računalnih sustava, programa i podataka propisanih u Kaznenom zakonu Republike Hrvatske.

Cilj ovog rada je, na temelju znanstvene i stručne literature, pokušati objasniti fenomen računalnog kriminaliteta te prikazati tipologiju počinitelja kaznenih djela iz domene računalnog kriminaliteta, odnosno utvrditi njihove karakteristike i osobitosti. Predstavljene su individualne karakteristike i motivacija počinitelja računalnog kriminaliteta te razvoj tipologija od 1980-ih do 2022. godine. Analiza ovih tipologija pokazala je da su u početku bile jednostavne, fokusirane na osnovne tehničke vještine, ali su se s vremenom proširile kako bi obuhvatile širi spektar motiva i ciljeva počinitelja, uključujući pojavu novih kaznenih djela. Istraživanja su također otkrila da počinitelji čine vrlo raznoliku skupinu, s različitim razinama stručnosti i motivima, što dodatno komplicira borbu protiv računalnog kriminaliteta. Naglašena je važnost multidisciplinarnog pristupa u analizi ovog fenomena, koji uključuje suradnju stručnjaka iz različitih područja. Unatoč napretku, izazovi poput anonimnosti digitalnog okruženja i stalne evolucije tehnologije i dalje zahtijevaju daljnje istraživanje kako bi se bolje razumjele promjene i dinamika ovog rastućeg problema.

Ključne riječi: računalni kriminalitet, tipologija počinitelja, individualne karakteristike, motivacija

Title: Typology of offenders in the domain of computer crime

Student: Anja Horvat

Tutor: Izv. prof. dr. sc. Dalibor Doležal

The program/module: Social Pedagogy/Adults

SUMMARY

Cybercrime has emerged as one of the most significant global challenges in modern society, driven by the rapid advancement of technology and an increasing reliance on digital systems. The complexity and evolving nature of this crime present serious threats to security, the economy and societal development. This paper centers on the perpetrators of offenses against computer systems, programs, and data, as defined by the Penal Code of the Republic of Croatia.

The aim of this master's thesis is to, based on scientific and professional literature, explore the phenomenon of cybercrime and present a typology of the offenders in this domain, identifying their characteristics and distinct features. The study examines the individual traits and motivations of cybercrime offenders and traces the evolution of typologies from the 1980s to 2022. The analysis reveals that early typologies were straightforward, focusing on basic technical skills, but have since broadened to encompass a wider range of motives and goals, including the emergence of new forms of cybercrime. Research also indicates that offenders represent a highly diverse group, with varying levels of expertise and motivations, complicating efforts to combat cybercrime. The paper emphasizes the importance of a multidisciplinary approach to analyzing this phenomenon, requiring collaboration across various fields of expertise. Despite progress, challenges such as the anonymity of the digital environment and the ongoing evolution of technology continue to demand further research to better understand the changes and dynamics of this growing issue**.**

Keywords: cybercrime, offender typology, individual characteristics, motivation

Sadržaj

1. UVOD

Trendovi među znanstvenim istraživanjima u području računalnog kriminaliteta govore kako se istraživanje računalnog kriminaliteta često se nalazi u sjeni studija računalne sigurnosti, koje razmatraju *online* prijetnje iz različitih perspektiva, uključujući filozofiju, ekonomiju, humanističke znanosti i javno zdravstvo (Carley, 2020; prema Dupont, Fortin i Leukfeldt, 2024). Pravnici se bave definiranjem problematičnih *online* ponašanja i usklađivanjem pravnih okvira na globalnoj razini, dok psiholozi istražuju osobine ličnosti koje mogu predvidjeti sklonost ljudi da nasjednu na sumnjive *online* ponude. Znanstvenici u području političkih znanosti proučavaju povezanost između kriminalnih aktivnosti hakerskih grupa i njihove instrumentalizacije od strane država koje ih koriste kao digitalne plaćenike. Informatičari se fokusiraju na tehničke aspekte zlonamjernih softvera i sigurnosne propuste koje hakeri iskorištavaju, dok kriminolozi, s druge strane, analiziraju motive počinitelja i metode koje omogućuju iskorištavanje ranjivosti za nezakonitu dobit. Iako postoji mnogo različitih pristupa u istraživanju računalnog kriminala, svi su ograničeni unutar specifičnih teorijskih i metodoloških okvira, što posljedično uzrokuje nedostatak integriranog razumijevanja problema (Dupont i sur., 2024). Time se naglašava duboka kompleksnost i ozbiljnost problema jer ograničena suradnja između disciplina otežava cjelovito razumijevanje kibernetičkog kriminala.

Postoji sve više dokaza da računalni kriminalitet u svim svojim oblicima sada čini između 40 i 50% svih kaznenih djela u moderniziranim društvima (Aebi, Caneppele i Molnar, 2022; prema Dupont i sur., 2024), što ga čini najčešćim oblikom kriminala po broju slučajeva. Prema izvještaju Steve Morgan-a iz 2021., računalni kriminalitet predstavlja najkompleksniji oblik globalnog kriminala 21. stoljeća te „najveći problem s kojim se čovječanstvo ikada suočilo“ (Chinedu, Nwankwo, Masajuwa i Imoisi, 2021). Vlada Republike Hrvatske (2024) ističe računalni kriminalitet kao značajnu i rastuću prijetnju za gospodarski i društveni prosperitet zemlje. S napretkom elektroničkih komunikacija i digitalne tehnologije, računalni napadi postaju sve sofisticiraniji, ciljajući kritične infrastrukturne i financijske sustave, uključujući vladine institucije (Vlada Republike Hrvatske, 2024). Pravnici, analitičari i znanstvenici imaju različita mišljenja o tome kako najbolje definirati računalni kriminalitet. Definicije variraju od jednostavnih do složenih, u nastojanju da obuhvate sve aspekte ovog problema. Zakonodavci i međuvladina tijela, pri pokušaju rješavanja računalnog kriminala, moraju jasno odrediti koje

radnje namjeravaju kriminalizirati (Graham, 2023). Umjesto stroge definicije, primjerenije je koristiti široke opisne pojmove koji naglašavaju ulogu tehnologije u počinjenju kaznenog djela. Kako se priroda računalnog kriminaliteta mijenja s razvojem i upotrebom tehnologije, definicija bi trebala biti dovoljno fleksibilna da obuhvati te promjene i evoluira zajedno s kibernetičkom tehnologijom (Graham, 2023). Neki autori naglašavaju zlouporabu umreženih računalnih sustava ili podataka unutar tih mreža, dok se drugi fokusiraju na upotrebu računala kao sredstva za počinjenje kaznenih djela. Dio autora smatra da je računalni kriminalitet u suštini tradicionalni kriminalitet koji se izvršava pomoću računala i da ga treba procesuirati prema postojećim zakonima. S druge strane, neki vide računalni kriminalitet kao novu vrstu kriminala s posebnim izazovima, poput problema nadležnosti, međunarodne suradnje, namjere i identifikacije počinitelja (Graham, 2023). Definirati računalni kriminalitet na najjednostavniji način znači klasificirati ga kao bilo kakav kriminalni čin koji uključuje računala, digitalne uređaje i internet kao sredstvo izvršenja (Nwankwo i Ukaoha, 2019; prema Chinedu, 2021).

Računalni kriminalitet je izuzetno složen i stalno se mijenja, dok njegovi počinitelji postaju sve sofisticiraniji. U usporedbi s tradicionalnim kriminalom, računalni kriminalitet pruža veću razinu anonimnosti što omogućava napadaču da prikrije svoj pravi identitet *online*, a čak i da preuzme novi identitet (Nurse, 2019; prema Curtis i Oxburgh, 2022). Zbog osjećaja anonimnosti i udaljenosti od stvarnosti, korisnici Interneta često razvijaju lažan osjećaj sigurnosti. Počinitelji računalnog kriminaliteta su psihološki, socijalno i fizički distancirani od svojih postupaka i žrtava, što ih čini manje svjesnima i/ili zabrinutima za posljedice svojih djela (Curtis i Oxburgh, 2022). Većina se istraživanja u području *online* sigurnosti usmjerila na tehnološke aspekte, dok su ljudski čimbenici ostali u drugom planu. Iako se računalni zločini danas otkrivaju mnogo brže nego prije, i dalje postoji ograničena sposobnost utvrđivanja tko stoji iza tih zločina i koji su njihovi motivi (Chng, Yu Lu, Kumar i Yau, 2022). Mnogi su autori pokušali odgovoriti na ta pitanja sastavljajući tipologije počinitelja računalnog kriminaliteta. Razvijanjem takvih tipologija teži se grupiranju pojedinaca na temelju njihovih zajedničkih karakteristika u različite tipove (Stapley, O'Keeffe i Midgley, 2022). Nadovezujući se na to, cilj ovoga rada je pružiti sveobuhvatan pregled tipologija počinitelja kaznenih djela iz domene računalnog kriminaliteta, temeljen na znanstvenoj i stručnoj literaturi, kako bi se pokušao objasniti fenomen računalnog kriminaliteta s naglaskom na same počinitelje, njihove karakteristike i specifičnosti.

U prvome dijelu rada prikazana je problematika definiranja računalnog kriminaliteta, fenomenologija s naglaskom na kaznena djela Glave 25. Kaznenog zakona Republike

Hrvatske, pravni okvir i prevalencija u Republici Hrvatskoj. Nakon toga slijedi prikaz individualnih karakteristika *online* napadača, njihovih motivacija i tipologija počinitelja iz ove domene, od 1985. do 2022. godine, od strane raznih autora koji su se bavili ovom problematikom. Rad završava analizom prikazanih tipologija i njihovom značajnosti.

2. DEFINIRANJE RAČUNALNOG KRIMINALITETA

Internet, računala, mobiteli i ostale tehnologije revolucionirale su svaki aspekt ljudskog života tijekom posljednjih nekoliko desetljeća, uključujući način na koji komuniciramo, kupujemo, informiramo se i zabavljamo (Holt i Bossler, 2016). Oko 60% svjetske populacije služi se internetom, a globalno usvajanje digitalne tehnologije raste izrazito brzo (Phillips, Davidson, Farr, Burkhardt, Cneppele i Aiken, 2022). U relativno kratkom vremenu, odnos čovječanstva i tehnologije promijenio se iz povremenog i praktičnog u sveprisutnu nužnost u gotovo svim aspektima života (Holt i Bossler, 2016). Sve navedeno je, uz pojavu uređaja različitih oblika, veličina i namjena, utjecalo na evoluciju kriminalnog ponašanja, odnosno pojavom računalnog kriminaliteta (Phillips i sur., 2022).

Važno je jasno definirati računalni kriminalitet jer čak i male razlike u definicijama mogu utjecati na način mjerenja istog. Problemi u definiranju računalnog kriminaliteta započinju sa samom terminologijom. Koriste se raznovrsni termini, ponekad u kombinaciji s prefiksima *cyber*, računalno, e-, internetno, digitalno ili informacijsko. Termini se koriste nasumično, ističu preklapanje sadržaja ili ukazuju na važne praznine (Van der Hulst i Neve, 2008; prema Phillips i sur., 2022). Alternativna terminologija za računalni kriminalitet uključuje „kriminalitet u *cyber*-prostoru“, „kriminalitet povezan s računalima“, „elektronički kriminalitet“, „e-kriminalitet“, „tehnologijom potpomognuti kriminalitet“ i „kriminalitet visoke tehnologije“. Varijabilnost termina u računalnom kriminalitetu ističe nedostatak zajedničkog jezika među stručnjacima koji su specijalizirani u tom području (Phillips i sur., 2022).

Još od 1970-ih, pojedinci su koristili termin "računalni kriminalitet" (eng. *computer crime*) kako bi opisali zlouporabu računala i podataka (Parker, 1976; prema Holt i Bossler, 2016).

Parker (1976; prema Moitra, 2004) razlikuje četiri glavne vrste računalnog kriminaliteta: računalo kao objekt kriminalnog djela, stvaranje okruženja za kriminalno djelo pomoću računala, korištenje računala kao instrumenta za izvršenje kriminalnih radnji te simbolična upotreba računala. Izraz računalni kriminalitet najčešće se koristio za gotovo sve oblike kriminalnih aktivnosti povezanih s računalima sve do kasnih 1990-ih. Terminologija se počela mijenjati kada je korištenje tehnologije i pristup istoj dovelo do transformacije društva (Holt i Bossler, 2016). Mijenjanjem obrazaca korištenja tehnologije, istraživači poput Davida Walla počeli su koristiti izraz "*cyber* kriminalitet" za označavanje zločina počinjenih *online*. S druge strane, Peter Grabosky koristio je izraz „računalni kriminalitet“ (eng. *computer crime*) za zlouporabu računala. Ovi su se termini relativno jednako koristili među istraživačima i novinarima koji su se bavili računalnim kriminalitetom u tom razdoblju (Holt i Bossler, 2016).

***Cyber* kriminalitet** odnosi se na zločine "u kojima počinitelj koristi posebno znanje o *cyber* prostoru[1]", dok **računalni kriminalitet** (eng. *computer crime*) nastaje jer se "počinitelj služi posebnim znanjem o računalnoj tehnologiji" (Furnell, 2002; prema Holt i Bossler, 2016). Do sredine 2000-ih, kriminološki su istraživači usvojili izraz *cyber* kriminalitet za označavanje kriminalnih djela dostupnih putem tehnologije (Holt i Bossler, 2016). U ovom diplomskom radu koristit će se termin „računalni kriminalitet“ kao prijevod engleskog pojma *cybercrime*.

Phillips i suradnici (2022) su pregledom literature došli do konsenzusa da ne postoji jedna, precizna, sveobuhvatna i univerzalno prihvaćena definicija računalnog kriminaliteta. Međutim, definicije razvrstavaju tri skupine:

1. Jedan pojam koji obuhvaća raznovrsni skup kriminalnih i štetnih ponašanja

Računalni kriminalitet obuhvaća velik broj raznovrsnih ilegalnih djela ili onoga što se smatra nezakonitim postupanjem pojedinaca/grupa protiv računala, uređaja povezanih s računalom ili mreža informacijske tehnologije, kao i tradicionalnih zločina koji su počinjeni korištenjem interneta i/ili informacijske tehnologije (Donalds i Osei-Bryson, 2018). Stoga, iako ne postoji jedinstvena usuglašena i ujedinjena definicija računalnog kriminaliteta, široko se priznaje da se taj pojam koristi za obuhvaćanje raznih zločina i štetnih ponašanja. Wall (2001) govori kako računalni kriminalitet „ne čini puno više od označavanja pojave štetnog ponašanja koje je na

[1] U cyber prostoru, pojam prostora je apstraktan i matematički te nema konkretan volumen. Stoga, cyber prostor u klasičnom smislu predstavlja virtualni digitalni svijet izgrađen na temeljima različitih infrastruktura kao što su računala, mreže, podaci, informacije, hardver i softver (Ning, Ye, Bouras, Wei i Daneshmand, 2018). Obuhvaća kombinaciju internetskih i telekomunikacijskih tehnologija koje omogućuju snimanje, pohranu, dohvaćanje i prijenos informacija (Mbanaso i Dandaura, 2015).

neki način povezano s računalom“. Iako su takve definicije možda previše široke i nejasne, ipak su, u osnovi, točne (Phillips i sur., 2022).

2. *Najčešće citirane definicije računalnog kriminaliteta*

Phillips i suradnici ističu kako su dvije najčešće citirane akademske definicije računalnog kriminaliteta one koje su predložili Thomas i Loader te Gordon i Ford. Thomas i Loader (2000) definiraju računalni kriminalitet kao "računalno posredovane aktivnosti koje su ili ilegalne ili se smatraju nezakonitima od strane određenih stranaka i koje se mogu provoditi putem globalnih elektroničkih mreža", dok Gordon i Ford (2006; prema Phillips i sur., 2022) govore kako računalnim kriminalitetom podrazumijeva "bilo koji zločin koji je počinjen korištenjem računala, računalne mreže ili uređaja".

3. *Institucionalne i organizacijske definicije računalnog kriminaliteta*

Na organizacijskoj razini postoje globalne razlike u definicijama računalnog kriminaliteta. Konvencija o kibernetičkom kriminalu (2001) govori o nizu „ postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i računalnih podataka kao i zlouporaba istih utvrđujući kriminalizaciju takvog ponašanja“, dok su se na Desetom kongresu Ujedinjenih naroda o prevenciji kriminala i postupanju s počiniteljima spomenule sljedeće definicije (Akdemir, Sungur i Basaranel, 2020):

a. "svako nezakonito ponašanje počinjeno putem elektroničkih operacija koje cilja sigurnost računalnih sustava i podataka koje se njima obrađuju,"
b. "svako nezakonito ponašanje počinjeno putem računalnog sustava ili mreže, uključujući zločine poput ilegalnog posjedovanja te ponude ili distribucije informacija putem računalnog sustava ili mreže."

Važno je napomenuti da se većina organizacijskih definicija vjerojatno odnosi na kriminalitet u vezi s računalnom sigurnošću te se ne prihvaća široko tumačenje računalnog kriminaliteta koje je definirano u akademskoj literaturi (Phillips i sur., 2022).

3. FENOMENOLOGIJA

Budući da je ovaj diplomski rad fokusiran samo na počinitelje kaznenih djela navedenih u Glavi XXV. Kaznenog zakona Republike Hrvatske, u nastavku će samo ta kaznena djela biti razjašnjena.

3.1. Neovlašteni pristup

Članak 266. propisuje da zakon štiti samo računalne sustave s zaštitnim mjerama, stoga otvoreni i nezaštićeni sustavi nisu obuhvaćeni ovim kaznenim djelom. Strože kazne predviđene su za radnje prema sustavima državnih tijela, javnih ustanova ili trgovačkih društava od posebnog javnog interesa, te za prouzročenu značajnu štetu. Konvencija o kibernetičkom kriminalu zahtijeva kažnjavanje i pokušaja kaznenih djela iz ovog članka, a kazneni postupak se pokreće na prijedlog nadležnog tijela (Franjić, 2017). Ovo kazneno djelo opisuje tzv. *hakiranje* (eng. hacking) te se može usporediti s povredom nepovredivosti doma. Neovlašteni pristup informacijskim sustavima može uključivati više oblika aktivnosti, od krađe podataka do samog neovlaštenog pregledavanja podataka. Pravno dobro nije povrijeđeno samo kada netko bez ovlaštenja zamijeni ili „ukrade“ podatke, već i kada ih jednostavno razgledava. U osnovnom obliku, neovlašteni pristup ne zahtijeva da počinitelj stvarno pristupi datotekama ili pohranjenim podacima kao krajnjem cilju. Sam pojam pristupa nije strogo definiran, te obuhvaća pristup internetom, bežičnim komunikacijskim sredstvima, kao i pristup računalima koja nisu spojena na mrežu (Kokot, 2014).

3.2. Ometanje rada računalnog sustava

Članak 267. opisuje kazneno djelo ometanja računalnih sustava, gdje je ključna namjera počinitelja. Oslobađa se odgovornosti onaj tko nepažnjom prouzroči prekid komunikacije, poput isključivanja ključnih računala. Specifičnost računalnog kriminala je mogućnost napadača da koristi tuđu infrastrukturu, primjerice, širenjem crva koji inficira tisuće računala, bez znanja njihovih korisnika, čime se posredno oštećuju vlasnici tih računala. Konvencija o kibernetičkom kriminalu zahtijeva kažnjavanje i pokušaja ovih kaznenih djela (Franjić, 2017). Klasični oblici ometanja sustava, koje većina pravnih sustava prepoznaje, uključuju izmjenu, brisanje i prijenos podataka. Šira definicija može uključivati ne samo manipulaciju podacima,

već i prekid električnog napajanja, izazivanje elektromagnetskih smetnji ili kvarenje sustava na bilo koji način (Kokot, 2014).

3.3. Oštećenje računalnih podataka

Članak 268. ističe kako se u suvremenom poslovanju i javnoj upravi sve više koriste elektroničke baze podataka, koje često imaju veliku vrijednost. Njihova izmjena, uništavanje ili brisanje mogu uzrokovati značajne štete i predstavljaju veliku društvenu opasnost. Konvencija o kibernetičkom kriminalu zahtijeva kažnjavanje i za pokušaje ovih kaznenih djela (Franjić, 2017).

3.4. Neovlašteno presretanje računalnih podataka

Članak 269. propisuje sankcioniranje neovlaštenog presretanja nejavnih prijenosa računalnih podataka, bilo putem žičanih ili bežičnih prijenosa, uključujući elektromagnetske emisije. Zabranjuje se prisluškivanje podataka bez direktnog priključenja na telekomunikacijsku liniju. Konvencija o kibernetičkom kriminalu zahtijeva kazne i za pokušaj ovih djela, a podaci prikupljeni neovlaštenim presretanjem moraju biti uništeni (Franjić, 2017). Ovo kazneno djelo zapravo predstavlja tzv. računalnu špijunažu. Da bi se utvrdila postojanost kaznenog djela, presretanje mora biti neovlašteno te izvršeno s namjerom. Podatci moraju biti u prijenosu sve dok ne dođu do konačnog odredišta, bilo primatelja ili sustava. Tako je kriminalizirana radnja ograničena na pribavljanje podataka za vrijeme prijenosa koji obavezno mora biti povjerljiv odnosno ne javan (Matijević i Avramović, 2021).

3.5. Računalno krivotvorenje

Članak 270. navodi da se u modernom poslovanju i javnoj upravi sve više koriste elektroničke baze podataka, koje su često izuzetno vrijedne. Njihova izmjena, uništavanje ili brisanje mogu uzrokovati značajne štete i predstavljaju ozbiljnu društvenu opasnost. Konvencija o kibernetičkom kriminalu zahtijeva kažnjavanje i za pokušaj ovih kaznenih djela, a podaci dobiveni neovlaštenim presretanjem moraju biti uništeni (Franjić, 2017). Ovo kazneno djelo štiti vjerodostojnost isprave u digitalnom obliku te pokriva manipulaciju digitalnim podatcima i dokumentima (Kokot, 2014).

3.6. Računalna prijevara

Članak 271. naglašava da je ključan element ovog kaznenog djela pribavljanje protupravne imovinske koristi, što uzrokuje štetu drugima. Ovdje spadaju različiti oblici neovlaštenih upada u računalne sustave, poput promjene stanja na bankovnim računima, prijevara s kreditnim karticama i lažnih plaćanja. Također, uključuje blokade računalnih sustava kako bi se spriječila provjera valjanosti kartica ili brisanje loše kreditne povijesti. Kazna za ova djela ovisi o težini kaznenog djela, a podaci dobiveni neovlaštenim presretanjem moraju biti uništeni (Franjić, 2017). Neki pravni sustavi računalnu prijevaru ne propisuju kao zasebno kazneno djelo, već je tretiraju kao običnu prijevaru. Ključna je razlika u objektu napada. Kod tradicionalne prijevare prijevare, objekt napada je osoba koju počinitelj dovodi ili održava u zabludi, a u slučaju računalne prijevare objekt napada su računalni podatci ili računalni sustav. Najčešći oblik računalnog kriminaliteta u Republici Hrvatskoj jest podizanje gotovog novca iz bankomata, koristeći ukradenu, a često i krivotvorenu bankovnu karticu s pripadajućim PIN-om (Kokot, 2014).

3.7. Zlouporaba naprava

Članak 272. Kaznenog zakona ima za cilj sprječavanje stvaranja i širenja tržišta naprava i specijaliziranih programa koji se koriste za počinjenje kaznenih djela. Inkriminacija ovih djela često uključuje i legalne naprave i programe, što može stvoriti dodatne probleme. Prema članku, naprave i opisani programi će biti oduzeti, a podaci koji su nastali počinjenjem kaznenih djela bit će uništeni (Franjić, 2017). Pojam „naprava“ odnosi se na hardver i softverska rješenja namijenjena za počinjenje nekog kaznenog djela, odnosno programe ili viruse prilagođene za ostvarivanje neovlaštenog pristupa nekom računalnom sustavu (Kokot, 2014).

3.8. Teška kaznena djela protiv računalnih sustava, programa i podataka

Članak 273. usmjerava se na zaštitu računalnih sustava koji su u vlasništvu ili su od posebnog javnog interesa, kao što su tijela državne vlasti, javne ustanove ili trgovačka društva. Kazne se strogo određuju ovisno o težini djela, pri čemu se posebno sankcioniraju situacije u kojima se koristi tehnologija za napade na veći broj sustava ili uzrokuje znatna šteta (Franjić, 2017).

4. PRAVNI OKVIR

Složenost računalnog kriminaliteta raste kako u svijetu, tako i u Hrvatskoj, stoga je problematika regulirana kroz međunarodne konvencije koje su implementirane u nacionalno zakonodavstvo (Matijević i Avramović, 2021). Ključna među njima je Konvencija o kibernetičkom kriminalu iz 2001. godine[2], koju je donijelo Vijeće Europe s ciljem uspostavljanja zajedničke kaznene politike za zaštitu zajednice od računalnog kriminaliteta, ponajprije usvajanjem odgovarajućih zakona i jačanjem međunarodne suradnje. Hrvatski sabor je ovu Konvenciju potvrdio Zakonom o potvrđivanju Konvencije o kibernetičkom kriminalu 2002. godine. Ova konvencija, koja se sastoji od četiri glavna dijela, pokriva sva kaznena djela vezana uz računalni kriminalitet, uključujući povrede autorskih prava, računalne prijevare, dječju pornografiju te povrede sigurnosti računalnih mreža. Prvi dio propisuje kaznena djela, drugi dio obveze zemalja potpisnica za implementaciju konvencije, treći dio se bavi mehanizmima međusobne pomoći i međunarodne suradnje, dok četvrti dio sadrži završne odredbe. Vijeće Europe je kasnije donijelo Dodatni protokol uz Konvenciju o kibernetičkom kriminalu, kojim se inkriminiraju rasistička i ksenofobna djela počinjena putem računalnih sustava. Hrvatski sabor je ovaj protokol ratificirao 2008. godine. Nakon ratifikacije, Hrvatska je implementirala odredbe Konvencije u Kazneni zakon donošenjem Zakona o izmjenama i dopunama Kaznenog zakona, koji je stupio na snagu 1. listopada 2004. godine (Matijević i Avramović, 2021).

Osim Kaznenog zakona, usvojen je i niz drugih zakona i podzakonskih akata koji definiraju okvire, ciljeve i dosege sigurnosne politike u području informacijske i kibernetičke sigurnosti. Među njima su Zakon o sigurnosno-obavještajnom sustavu, Zakon o tajnosti podataka, Zakon o informacijskoj sigurnosti, Zakon o zaštiti osobnih podataka, Zakon o elektroničkoj trgovini, Zakon o elektroničkim komunikacijama te različiti pravilnici o sigurnosti podataka i poslovnoj suradnji (Matijević i Avramović, 2021).

Kako bi dodatno zaštitila kibernetički prostor, Republika Hrvatska donijela je Nacionalnu strategiju kibernetičke sigurnosti i akcijski plan za njezinu provedbu. Ova je strategija prva hrvatska sveobuhvatna inicijativa koja uključuje sve zakonske i podzakonske akte te sve

[2] Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, pristupljeno 03.06.2024. : https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html

društvene segmente potrebne za provedbu sigurnosnih mjera u kibernetičkom prostoru (Matijević i Avramović, 2021).

5. PREVALENCIJA U REPUBLICI HRVATSKOJ

Analizom podataka iz Statističkog pregleda temeljnih sigurnosnih pokazatelja i rezultata rada u 2023. godini Ministarstva unutarnjih poslova[3], mogu se pronaći sljedeće informacije o prevalenciji kaznenih djela protiv računalnih sustava, programa i podataka u Republici Hrvatskoj, prikazane u obliku tablice:

KAZNENA DJELA	**2019.**		**2020.**		**2021.**		**2022.**		**2023.**	
	P	**R**	**P**	**R**	**P**	**R**	**P**	**R**	**P**	**R**
Neovlašteni pristup	15	13	19	6	32	6	31	13	48	17
Ometanje rada računalnog sustava	8	4	7	3	10	4	5	2	5	1
Oštećenje računalnih podataka	5	1	12	3	21	1	25	7	39	5
Neovlašteno presretanje računalnih podataka	2	2	1	1	2	1	8	3	1	1
Računalno krivotvorenje	946	942	26	23	70	67	39	38	20	18
Računalna prijevara	1785	1639	951	579	1158	651	1425	771	1571	604
Zlouporaba naprava	51	49	17	14	4	4	7	7	4	3
UKUPNO	**2812**	**2650**	**1033**	**629**	**1297**	**734**	**1540**	**841**	**1688**	**649**

Tablica 1. Prikaz prijavljenih (u tablici oznaka P) i razriješenih (u tablici oznaka R) kaznenih djela u 2019., 2020., 2021., 2022. i 2023. godini (MUP, 2020; MUP, 2022; MUP, 2024).

U 2023. godini zabilježena su 2.032 kaznena djela računalnog kriminaliteta. U odnosu na 2022. godinu, u kojoj je zabilježeno 1.864 kaznena djela računalnog kriminaliteta, evidentiran je porast za 9%. Od 2.032 kaznena djela njih 1.688 pripada kaznenim djelima protiv računalnih sustava, programa i podataka. Kazneno djelo iskorištavanja djece za pornografiju prijavljeno je 342 puta, a kazneno djelo povrede žiga 2 puta (MUP, 2024).

[3] U daljnjem tekstu koristit će se skraćenica MUP.

Prema tablici, vidljiv je znatan pad u 2020. godini s obzirom na prijašnju 2019. godinu. Ta se razlika pripisuje usklađivanju statističkog prikaza kaznenih djela računalnog kriminaliteta s odredbom Kaznenog zakona o produženom kaznenom djelu (MUP, 2021). Tom se odredbom postupanje počinitelja, iako radi više odvojenih radnji, tretira kao jedno produženo djelo, a ne više djela, jer se zapravo radi o ostvarenju istih kaznenih djela. Također, 2020. godine, zbog COVID-19 pandemije, promijenio se način života cijelome svijetu. Pandemija je značajno proširila vrste i smjerove računalnih napada jer se povećalo korištenje digitalnih i internetskih rješenja. Tijekom 2020. godine zabilježen je porast materijala koji prikazuju seksualno iskorištavanje djece, uključujući i sadržaje koje djeca sama snimaju i dijele putem društvenih mreža. Povećala se i popularnost aplikacija za razmjenu poruka (Whatsapp, Viber i sl.) čime se povećao i rizik od seksualnog zlostavljanja djece (MUP, 2021).

Najbrojnije kazneno djelo zabilježeno svih pet navedenih godina je računalna prijevara, posebice napadi na računala korisnika internetskog bankarstva, neovlašteni prijenos novca na račune drugih osoba u inozemstvu te preuzimanje nadzora nad računalima oštećenika. Uzimajući u obzir navedeno usklađivanje statističkog prikaza s odredbom Kaznenog zakona o produženom kaznenom djelu 2020. godine, vidljiv je porast kaznenog djela računalne prijevare, oštećenja računalnih podataka i neovlaštenog pristupa, dok je kod kaznenog djela zlouporaba naprava primijećen pad (MUP, 2020; MUP, 2022; MUP, 2024).

KAZNENO DJELO	BROJ POČINITELJA KAZNENIH DJELA				
	2019.	2020.	2021.	2022.	2023.
Neovlašteni pristup	9	5	5	5	13
Ometanje rada računalnog sustava	2	1	1		
Oštećenje računalnih podataka	1	1	2	4	3
Neovlašteno presretanje računalnih podataka	3		1		
Računalno krivotvorenje	8	6	5	3	4
Računalna prijevara	94	122	139	175	200
Zlouporaba naprava	4	3		3	1
UKUPNO	121	138	153	190	221

Tablica 2. Prikaz broja počinitelja kaznenih djela računalnog kriminaliteta iz 2019., 2020., 2021., 2022. i 2023. godine (MUP, 2020; MUP, 2022; MUP, 2024).

Počinitelji kaznenih djela računalnog kriminaliteta najbrojniji su kod kaznenog djela računalne prijevare, a broj istih, kao što je vidljivo u tablici, povećavao se svake godine. Porast broja počinitelja očitovan je kod kaznenog djela neovlaštenog pristupa, dok je kod kaznenog djela računalnog krivotvorenja vidljiv pad s povećanjem broja počinitelja u 2023. godini, s obzirom na prijašnju 2022. godinu. Broj počinitelja kaznenog djela oštećenja računalnih podataka za godinu 2022. i 2023. veći je u odnosu na 2019., 2020. i 2021. godinu. Očitovan je pad broja počinitelja za kazneno djelo zlouporabe naprava, a kod kaznenih djela ometanja rada računalnog sustava i neovlaštenog presretanja računalnih podataka nije zabilježen niti jedan počinitelj u 2022. i 2023. godini (MUP, 2020; MUP, 2022; MUP, 2024).

6. ETIOLOGIJA

Važno je napomenuti kako ne postoji mnogo znanstvenih istraživanja koja testiraju postojeće kriminološke teorije u kontekstu računalnog kriminaliteta, ali postojeća literatura trenutno navodi sljedeće teorije kao najčešće: teoriju rutinskih aktivnosti, teoriju socijalnog učenja i opća teoriju kriminaliteta.

6.1. Teorija rutinskih aktivnosti

Teorija rutinskih aktivnosti, koju su zbog povećanja stope kriminaliteta u Sjedinjenim Američkim Država počeli razvijati Lawrence Cohen i Marcus Felson, primjenjuje se na makro i individualnoj razini kroz brojne studije kako bi objasnila različite obrasce kriminala i viktimizacije. Temelj ove teorije leži u ideji da se različite komponente kriminalnog događaja susreću u istom fizičkom prostoru u isto vrijeme, što ih čini pogodnim za objašnjavanje fizičke viktimizacije (Henson, 2020). Međutim, posljednjih deset godina, mnogi su istraživači počeli primjenjivati principe ove teorije na druge oblike kriminala, posebno računalni kriminalitet. Zbog ne-fizičke prirode interneta, bilo je potrebno napraviti određene prilagodbe. Unatoč tim prilagodbama, teorija rutinskih aktivnosti postala je uobičajena u proučavanju računalnog kriminaliteta (Henson, 2020). Teorija rutinskih aktivnosti sastoji od tri glavne kategorije:

- Motivirani počinitelji
- Prikladna meta
- Nedostatak učinkovite zaštite ili prigodnog čuvara osobe ili vlasništva

Teorija rutinskih aktivnosti (RAT) sugerira da će do kriminalnog djela doći kada se motivirani počinitelj nađe na istom mjestu u isto vrijeme s prikladnom metom, a pritom nedostaje učinkovita zaštita. Najčešće se ovakvi susreti događaju kada se rutinske aktivnosti potencijalne žrtve na neki način preklapaju s aktivnostima motiviranog počinitelja (Brantingham i Brantingham, 2004; prema Henson, 2020). U isto vrijeme kada su Cohen i Felson razvijali RAT, Michael Hindelang, Michael Gottfredson i James Garofalo radili su na sličnoj teoriji - teoriji životnog stila i izloženosti (LET). Prema LET-u, viktimizacija ovisi o tome koliko je osoba izložena potencijalno rizičnim situacijama. Drugim riječima, što je neko više izložen motiviranim počiniteljima, veća je vjerojatnost da će postati žrtva. Ubrzo su se te dvije teorije, poznate pod kraticom L-RAT, počele proučavati zajedno kroz četiri glavne komponente (Henson, 2020):

- Izloženost motiviranim počiniteljima – što je osoba više izložena, vjerojatnije je da će doći u kontakt s potencijalnim počiniteljima te da će posljedično postati žrtva;
- Blizina motiviranim počiniteljima – što je veći kontakt osobe s počiniteljima, veća je vjerojatnost da će postati žrtva (biti na istom mjestu u isto vrijeme kao potencijalni počinitelj povećava šanse za viktimizaciju);
- Privlačnost mete – počinitelj ovu komponentu određuje procjenom rizika i nagrada u određenoj situaciji;
- Zaštita – odnosi se na vrstu i razinu zaštite koju potencijalna žrtva može imati.

Kombinacija navedenih komponenata stvara priliku za počinjenje zločina. Kad bi se ispitivala primjenjivost L-RAT-a u objašnjenju računalnog kriminaliteta, potrebno je objasniti ove komponente u kontekstu *online* ponašanja (Henson, 2020). Prva komponenta predstavlja izloženost motiviranim počiniteljima, a u *online* kontekstu podrazumijeva vrijeme provedeno *online*, broj objavljenih videa/slika ili količinu osobnih informacija koja se dijeli. Što je veći digitalni trag osobe, to je veća izloženost potencijalnim počiniteljima. Nadalje, blizina motiviranim počiniteljima u *online* prostoru određuje se promatranjem broja i vrste virtualnih interakcija koje potencijalne žrtve mogu imati s počiniteljima. Mjere blizine motiviranim počiniteljima mogu uključiti faktore poput prihvaćanje zahtjeva za prijateljstvo ili učestalosti posjeta potencijalno opasnim web stranicama. Treća komponenta je privlačnost mete koja u virtualnom svijetu predstavlja percepciju ranjivosti i lako dostupnih informacija. Također, odsutnost mjera samozaštite, primjerice postavki privatnosti, može utjecati na razinu *online* privlačnosti mete (Henson, 2020). Posljednja je komponenta zaštita koja je centralna komponenta teorije rutinskih aktivnosti, a samim time i L-RAT-a. *Online* zaštita može se istraživati utvrđivanjem prate li roditelji ili skrbnici internet aktivnosti svoje djece. Također, *online* zaštita podrazumijeva i prisutnost sigurnosnih programa i/ili postavki privatnosti (Holt i Bossler, 2009; prema Henson, 2020).

Teorija rutinskih aktivnosti, osim što pruža jasan okvir za analizu računalnog kriminaliteta kroz navedene komponente, omogućava i praktičnu primjenjivost kroz omogućavanje identifikacije faktora rizika i preventivnih mjera. No, unatoč tome Henson (2020) ističu kako je potrebno razvijati preciznije mjere digitalnih aktivnosti, prikupljati longitudinalne podatke koji će pridonijeti boljem razumijevanju promjena u riziku kroz vrijeme te dodatno prilagoditi osnovna načela teorije omogućavajući bolju primjenu na izrazito dinamičan *online* svijet.

6.2. Teorija socijalnog učenja

Osnovna pretpostavka teorije socijalnog učenja je da isti proces u kontekstu društvene strukture, interakcije i situacije proizvodi i devijantno ponašanje. Vjerojatnost da će osobe sudjelovati u kriminalnom i devijantnom ponašanju se povećava, a da će se pridržavati normi se smanjuje kada se osoba druži s drugima koji čine kriminalno djela i podržavaju činjenje istih, kada su relativno više izloženi kriminalnim/devijantnim modelima, kada to definiraju kao poželjno ili opravdano u situaciji pogodnoj za to ponašanje i kada su u prošlosti primili i očekuju u sadašnjoj ili budućoj situaciji relativno veće nagrade nego kazne za to ponašanje (Akers, 1998; prema Navarro i Marcum, 2020).

S obzirom na prirodu mnogih kaznenih djela u području računalnog kriminaliteta, podrazumijeva se da se teorija socijalnog učenja može primijeniti na tu vrstu kriminalnih djela. Na primjer, kod vrlo sofisticiranih oblika računalnog kriminala (npr. hakiranje, distribucija zlonamjernog softvera/virusa), malo je vjerojatno da će počinitelji imati potrebna znanja za počinjenje djela bez povezivanja s iskusnijim kriminalcima. Čak i kod "niskotehnoloških" oblika računalnog kriminala (npr. elektroničko nasilje – eng. cyberbullying, virtualno uhođenje- eng. cyberstalking), počinitelji i dalje trebaju naučiti taktike i metode kako bi izbjegli otkrivanje prije nego što se upuste u kriminalnu radnju. Stoga je teorija socijalnog učenja snažna perspektiva za razumijevanje počinjenja računalnih kaznenih djela (Navarro i Marcum, 2020).

Prilikom temeljitog pregleda literature o hakiranju, Navarro i Marcum (2020) primijetile su da povezanost s devijantnim vršnjacima nije uobičajena pojava među hakerima. Takvo povezivanje hakerima pruža priliku da uče od drugih, racionaliziraju svoje postupke s istomišljenicima te da se hvale svojim „uspjesima“ stječući tako društveni kapital (Holt i Bossler, 2014). U ranijem istraživanju teorije socijalnog učenja i hakiranja, Skinner i Fream (1997; prema Navarro i Marcum, 2020) otkrili su da povezivanje s devijantnim vršnjacima i dijeljenje odobravajućih stavova prema devijantnosti predstavljaju čimbenike rizika za počinjenje hakiranja. Također su došli do zanimljivog otkrića da bi njima bliski odrasle osobe indirektno mogle ohrabriti potencijalne hakere ako prihvaćaju tako ponašanje. Kasnije studije o hakerskom ponašanju maloljetnika podržavaju ranije nalaze, specifično studija autora Marcum, Higgins i Ricketts (2014; prema Navarro i Marcum, 2020), koji su pronašli značajnu

vezu između povezanosti s devijantnim vršnjacima i počinjenja hakiranja. Točnije, mladi koji su se družili s devijantnim vršnjacima imali su veću vjerojatnost da će hakirati tuđi e-mail, račun na društvenim mrežama, a čak i web stranice.

Teorija socijalnog učenja definitivno se može smatrati jednom od korisnijih teorija za objašnjavanje računalnog kriminaliteta. Pružila je pouzdane prediktore za počinjenje računalnog kriminala protiv digitalne imovine, kao i za osobne zločine poput *cyberstalkinga* i *cyberbullyinga* (Navarro i Marcum, 2020). Nalazi spomenutih studija, kao i dosljedna medijska pokrivenost, osvijetlili su prave opasnosti računalnog kriminala i njegove izravne i neizravne učinke. Kontinuirana empirijska podrška teoriji socijalnog učenja kroz sve oblike kriminaliteta pokazuje njezinu korisnost za objašnjavanje novih metoda *online* prijestupa kako se pojavljuju. Međutim, definitivno postoji praznina u literaturi koja se odnosi na dinamiku *online* i *offline* odnosa s vršnjacima. Imaju li *offline* vršnjaci veći utjecaj na računalnu devijantnost u usporedbi s vršnjacima upoznatima *online*? Jesu li ponašanja vršnjaka koji su "prijatelji" *online* i *offline* utjecajnija u usporedbi s odnosom koji ima samo jednu dimenziju (Navarro i Marcum, 2020)?

6.3. Opća teorija kriminaliteta

1980-ih godina, Gottfredson i Hirschi radili su na razvoju jedinstvenog uzroka kriminalnog ponašanja. Njihov je rad bio odgovor na sve veći razvoj longitudinalnih i razvojnih istraživanja koji su rezultirali općom teorijom kriminaliteta. Ta je teorija sada poznatom kao teorija samokontrole koja je unaprijedila tradicionalnu literaturu o samokontroli u kriminologiji (Gottfredson i Hirschi, 1990; prema Higgins i Nicholson, 2020).

Smatra se da niska samokontrola i dostupne prilike igraju ključnu ulogu u predviđanju kriminalnog ponašanja. Teorija sugerira da osobe s niskom razinom samokontrole traže trenutno zadovoljstvo, često su neosjetljive prema drugima, imaju ograničene kognitivne i akademske vještine te su fizički aktivne (Moon, McCluskey i McCluskey, 2010). Zbog toga su takve osobe sklonije sudjelovati u delinkventnim ili kriminalnim radnjama koje pružaju brzo zadovoljstvo uz minimalan trud ili vještinu. Osim toga, teorija naglašava da samokontrola ne utječe samo na delinkventna ili kriminalna ponašanja, već također objašnjava slična ponašanja poput konzumacije alkohola, pušenja, kockanja, zlouporabe droga i kriminala bijelih ovratnika, jer sva ta ponašanja dijele slične karakteristike, uključujući brzo zadovoljstvo, minimalan trud i nebrigu za buduće posljedice (Gottfredson i Hirschi, 1990; prema Moon i sur., 2010). Gottfredson i Hirschi (1990; prema Moon i sur., 2010) također ističu da prilika igra ključnu ulogu u povezanosti između niske samokontrole i kriminalnog ponašanja, sugerirajući da su

osobe s niskom samokontrolom sklonije devijantnim ponašanjima kada im se pruži prilika. Autori teorije tvrde da su osobine kriminalnog ponašanja privlačne osobama s deficitom ili niskom razinom **samokontrole.** Privlačnost proizlazi iz činjenice da osobe s niskom samokontrolom dijele slične karakteristike kao i samo ponašanje. Na primjer, oni s niskom samokontrolom su skloni riziku i impulzivnosti, nedostaje im empatije, preferiraju jednostavne i brze zadatke te fizičke aktivnosti ((Gottfredson i Hirschi, 1990; prema Higgins i Nicholson, 2020). Zbog privlačnosti koju ove karakteristike stvaraju, pojedincima nije potrebna specifična motivacija za počinjenje zločina. Dovoljna im je procjena da će im kriminalno ponašanje donijeti više zadovoljstva nego boli (Gottfredson i Hirschi 1990; prema Higgins i Nicholson, 2020). Osim nedostatka informacija o određenom ponašanju, i razina samokontrole pojedinca može iskriviti percepciju zadovoljstva i boli vezanih uz kriminalno ponašanje, što im onemogućuje točno procjenjivanje dugoročnih posljedica svog ponašanja

Hirschi-jeva (2004) novija konceptualizacija dovela je do poimanja samokontrole ne kao osobinu ličnosti ili predispoziciju za kriminal, već kao sklonost razmatranju cijelog raspona potencijalnih posljedica (inhibicija) određenog čina. Pojedinci preispituju svoje inhibicije svjesno ili nesvjesno kada se suočavaju s bilo kojom situacijom. Hirschi (2004) je tvrdio da glavne inhibicije koje netko nosi sa sobom dolaze iz njihovih **socijalnih veza** prema teoriji socijalnog vezivanja (tj. predanost, uključenost, vjerovanje i privrženost). Drugim riječima, oni sa snažnijim vezama imaju više razine samokontrole te ti pojedinci ne žele prekršiti pravila jer razumiju posljedice koje bi nastale za te veze zbog prijestupa. Te posljedice služe kao inhibicije za kriminalno ponašanje.

Teorija samokontrole može pružiti dublje razumijevanje veze između niske samokontrole i različitih vrsta računalnog kriminaliteta. Komponente koje su opisali Gottfredson i Hirschi (1990; prema Higgins i Nicholson, 2020) lako se mogu prepoznati u djelu hakiranja. Oni pojedinci koji djeluju impulzivno i neosjetljivo prema drugima neće prepoznati da hakiranje podrazumijeva kršenje povjerenja i tuđe privatnosti. Također će zanemariti mjere poduzete za sprječavanje hakiranja i pravne posljedice povezane za potencijalnim otkrivanjem djela.

7. TIPOLOGIJA POČINITELJA

Za *normalna* i *abnormalna* ponašanja teško je pronaći jednu teorijsku perspektivu koja može objasniti svako ponašanje u određenoj situaciji. Stavovi i ponašanja rezultat su kombiniranog utjecaja osobnosti pojedinca i trenutne društvene situacije. Niti jedna teorija ili teorijska perspektiva ne može obuhvatiti sve vrste računalnih kriminalnih djela i kriminalaca koji se bave tim aktivnostima. Postoji mnogo tipova računalnih kriminalaca, od početnika koji *hakira* lozinke do *cyber-terorista*. Svaka teorija koja bi trebala objasniti ponašanje računalnih kriminalaca morala bi uzeti u obzir, prvo, vrstu ilegalne aktivnosti u kojoj je osoba uključena, i drugo, kategoriju računalnog kriminalca kojoj pripada. Tijekom posljednjih nekoliko desetljeća, nekoliko istraživača pokušalo je razviti sustav kategorizacije za pojedince koji se bave različitim oblicima računalnog kriminaliteta (Campbell i Kennedy, 2014) .

Tipologija je hijerarhijski sustav kategorija koji služi za organiziranje objekata prema njihovim sličnostima i razlikama (Mandara, 2003; prema Stapley i sur., 2022). Formira se grupiranjem više slučaja ili sudionika u različite tipove na temelju njihovih zajedničkih karakteristika, uzimajući u obzir kako svaki jedinstveni pojedinac predstavlja određeni obrazac značajki. Tipologizacijom se teži razumijevanju ljudskog ponašanja kroz detaljno promatranje pojedinačnih slučajeva (npr. koje su jedinstvene karakteristike ove osobe koje predstavljaju određeni tip osobnosti), uz kombinaciju pronalaženja sličnosti i razlika među slučajevima (npr. koliko je ova osoba slična/različita od ostalih slučajeva iste kategorije) (Stapley i sur., 2022).

Kategorizacija ima nekoliko koristi: omogućuje sustavna istraživanja, pomaže u izgradnji učinkovitih obrambenih sustava koji su manje ranjivi bez nepotrebnog trošenja resursa na manje vjerojatne prijetnje te olakšava prijavljivanje incidenata (Farahmand, Navathe, Sharp i Enslow, 2005). Posebno je važna u području računalne sigurnosti gdje osigurava nezanemarivanje različitih vrsta prijetnji, jasnije razjašnjava vrste prijetnji te omogućuje procjenu relativnih rizika istih i prioritizaciju njihovog rješavanja (Friedman i Hoffman, 2008; prema Seebruck, 2015). Ovo je posebno važno kod pojave računalnog kriminaliteta gdje se različite računalne kriminalce često grupira pod pojmom "haker" iako postoji velika varijacija u sposobnostima i motivacijama istih (Seigfried-Spellar i Treadway, 2014).

7.1. Pregled dosadašnjih tipologija

Haker je „osoba koja koristi ili piše računalne programe s entuzijazmom i vještinom te osoba koja koristi računala kako bi dobila pristup podacima na tuđem računalu ili telefonu bez dopuštenja“[4]. U kolokvijalnom smislu, termin "haker" proširio se kako bi obuhvatio različite oblike ponašanja jer se kroz vrijeme taj pojam koristio za označavanje bilo koje vrste računalnog kriminala (McBrayer, 2014).

Bill Landreth (1985; prema Campbell i Kennedy, 2014), bivši je haker i jedan od prvih teoretičara koji je razvio sustav klasifikacije za računalne kriminalce 1985. godine. Njegov sustav dijeli kriminalce u pet kategorija na temelju njihovog iskustva i vrste ilegalnih aktivnosti (Campbell i Kennedy, 2014):

1. **Početnici** (eng. Novice) imaju najmanje iskustva s računalima, smatraju se nestašnim osobama te uzrokuju najmanje elektroničke probleme;
2. **Studenti** su podosta znatiželjni, sve im dosta brzo dosadi, ne pronalaze dovoljno izazova u školi (Woo, 2003) te svoje vrijeme provode pregledavajući i istražujući neovlaštene računalne sustave;
3. **Turisti** neovlašteno pristupaju sustavima radi testiranja svojih mogućnosti te emocionalnog uzbuđenja koje proizlazi iz takvih aktivnosti;
4. **Rušitelj** (eng. Crashers) je zlonamjerni računalni kriminalac koji provaljuje u sustave te namjerno briše i uništava podatke i uzrokuje poremećaje u uslugama;
5. **Kradljivac** (eng. Thief) je kriminalac koji čini kriminalne radnje radi novčane dobiti.

Hollinger (1988; prema Woo, 2003) pak smatra da postoje tri kategorije računalnih kriminalaca: **pirati** (eng. Pirates) , **istraživači** (eng. Browsers) i **razbijači** (eng. Crackers). Pirati imaju nisku razinu hakerskih sposobnosti i uglavnom se bave internetskim piratstvom. Istraživači posjeduju srednju razinu tehničkih vještina te mogu pristupati osobnim datotekama pojedinaca, ali generalno ne uništavaju podatke. Posljednja grupa su razbijači koji imaju najnaprednije hakerske tehnike te ih se smatra najopasnijima.

S druge strane, Goodell (1996; prema Woo, 2003) računalne kriminalce dijeli u tri podgrupe sa sljedećim nazivima: **hakeri** (eng. Hackers), **razbijače** (eng. Crackers) te **telefonske hakere** (eng. Phreakers). Hakeri su uključeni u hakiranje radi stjecanja znanja i

[4] Oxford Learner’s Dictionaries, 2024. Preuzeto 20.05.2024. sa https://www.oxfordlearnersdictionaries.com/definition/english/hacker.

zadovoljenja intelektualne znatiželje, razbijači se često bave uništavanjem, vandalizmom i promjenom web stranica, a telefonski hakeri su usmjereni na manipulaciju i napade na telefonske sustave.

Bivši analitičar obavještajnih službi australske vojske, Nicholas Chantler, 1995. je godine proveo jedno od rijetkih empirijskih istraživanja o računalnim kriminalcima i njihovoj kulturi (Campbell i Kennedy, 2014). Ankete su poslane u razne grupe i *chat* sobe koje su posjećivali računalni kriminalci. Na temelju pet glavnih čimbenika koje je analiza podataka otkrila (vještine hakiranja, kriminalne aktivnosti, motivacije, opće znanje i dužina vremena provedenog hakirajući), Chantler je kreirao sljedeće kategorije računalnih kriminalaca (Campbell i Kennedy, 2014):

1. **Amateri** (eng. Lamers, losers) su se najkraće bavili ilegalnim aktivnostima u kontekstu računalnog kriminala te su najniže rangirani u smislu tehničkih vještina. Ova je grupa računalnih kriminalca najčešće motivirana krađom usluga i imovine ili osvetom;
2. **Neofiti** (eng. Neophytes) zreliji su od amatera, posjeduju više znanja i aktivno čine zločine računalnog kriminaliteta kako bi došli do novih i dodatnih informacija;
3. **Elitni članovi** (eng. Elite) imaju najvišu razinu općeg znanja o računalima i računalnom kriminalitetu. Njihova je motivacija intrinzična, vođeni su željom za znanjem i otkrivanjem novih informacija. Aktivni su u činjenju ilegalnih djela zbog intelektualnog izazova i uzbuđenja koje dožive kroz činjenje kaznenih djela.

Prema Chantleru (1995; prema Campbell i Kennedy, 2014), najmanji je postotak (10%) računalnih kriminalaca u to vrijeme pripadao skupini amatera, 30% pripadalo je skupini elitnih članova, a najviše je zabilježeno (60%) neofita.

Chandler (1996; prema Woo, 2003) je klasificirao hakere prema generacijama. **Prva generacija** obuhvaćala je pametne i tehnički orijentirane studente, programere i računalne znanstvenike, koji su hakirali iz akademskih i profesionalnih znatiželja. **Druga generacija** uključivala je tehnološke radikale koji su izrađivali "plave kutije" za besplatne međunarodne telefonske usluge. **Treću generaciju** činili su mladi „obožavatelji“ osobnih računala i računalnih igara koji su pokušavali dobiti zaštitne kodove za igre. **Četvrta generacija** uključuje osobe s kriminalnim motivima kao što su pohlepa, moć i/ili osveta.

Power (1998; prema Woo, 2003) je kategorizirao hakere kao **sportske uljeze** (eng. Sport intruders), **konkurentne obavještajce** (eng. Competitive intelligence) i **strane obavještajce** (eng. Foreign intelligence). Sportski uljezi provaljuju u servere, mijenjaju web stranice i

oštećuju datoteke. Konkurentni obavještajci izbjegavaju ilegalne i neetične aktivnosti, fokusirajući se na špijunažu, a strani se obavještajci bave hakiranjem u svrhu nacionalne sigurnosti ili ekonomskih interesa.

Analitičar za informacijsku sigurnost Donn Parker je 1998. godine razvio shemu kategorizacije računalnih kriminalaca u sedam razina. Ovu shemu formalizirao je kroz godine interakcije i strukturiranih intervjua s računalnim kriminalcima, a obuhvaća sljedeće kategorije (Campbell i Kennedy, 2014):

1. **Šaljivdžije** (eng. Pranksters) su karakterizirani svojom nestašnom prirodom, često podvaljuju drugima, ali rijetko nanose štetu (Woo, 2003);
2. **Hakerski entuzijasti** (eng. Hacksters) motivirani su znatiželjom i željom za znanjem. Šaljivdžije i hakerski entuzijasti su najmanje zlonamjerni od ostalih kategorija računalnih kriminalaca;
3. **Zlonamjerni hakeri** (eng. Malicious hackers) motivirani su potrebom za ometanjem i uništavanjem. Uživaju u nanošenju štete računalnim sustavima i financijskim gubicima pojedincima. Slični su već spomenutim razbijačima (Woo, 2003);
4. **Rješavatelji osobnih problema** (eng. Personal problem solvers) čine ilegalne aktivnosti za osobnu korist. Rješavatelji problema, koji su prema Parkeru najčešći tip računalnih kriminalaca, pribjegavaju kriminalu nakon neuspjelih pokušaja da riješe svoje poteškoće na legalan način;
5. **Karijerni** se **kriminalci** (eng. Career criminals) bave ilegalnim radnjama u *online* okruženju isključivo zbog novčane dobiti;
6. **Ekstremni zagovornici** (eng. Extreme advocates) imaju snažne veze s društvenim, vjerskim ili političkim pokretima. Ne tako davno su ti tipovi računalnih kriminalaca nazvani "haktivistima," kombinacijom hakera i aktivista, a spominje se i povezanost sa *cyber*-teroristima (Woo, 2003);
7. **Ovisnici, nezadovoljni i iracionalni pojedinci** (eng. Malcontents, addicts and irrational individuals) čine posljednju kategoriju u Parkerovoj shemi. Pojedinci u ovoj kategoriji obično pate od nekog oblika psihičkog poremećaja (npr. antisocijalni poremećaj ličnosti). Ova kategorija predstavlja onu najmanje predvidljivu (McBrayer, 2014).

Adamiski (1999; prema Woo, 2003) je spomenuo da hakerska zajednica ima labavu hijerarhiju koja se sastoji od **elite**, **običnih hakera** (eng. Ordinary) i **tipova s tamnom stranom** (eng. Darksiders). Elita posjeduje visoke tehničke vještine i može kreirati softver i alate za napad. Obični hakeri, slični *crackerima*, provaljuju u računalne sustave i napadaju telefonske sklopke. Tipovi s tamnom stranom bave se hakiranjem radi financijske dobiti.

Godine 1999. Marcus Rogers je istaknuo kako je nedostatak dogovorene definicije pojma "haker" predstavljao i predstavlja prepreku za istraživače koji proučavaju osobe uključene u hakerske aktivnosti (Rogers, 1999; prema McBrayer, 2014). Rogers (1999; prema McBrayer, 2014) je tvrdio da hakeri nisu homogena skupina te je predložio novu taksonomiju, pozivajući se na rad Donna Parkera i drugih istraživača u svojim studijama. U svojoj predloženoj taksonomiji, definirao je sljedeće kategorije hakera: **početnici/korisnici alata**(eng. Newbie/tool kit - NT), **računalni buntovnici** (eng. Cyber-punks - CP), **insajderi** (eng. Internals - IT), **programeri** (eng. Coders - CD), **hakeri stare garde** (eng. Old guard hackers - OG), **profesionalni kriminalci** (eng. Professional criminals - PC) i **računalni teroristi** (eng. Cyber-terrorists - CT). Početnici/korisnici alata (NT) bili su hakeri s ograničenim vještinama, često novi u svijetu hakiranja (Rogers, 1999; prema McBrayer, 2014). Računalni buntovnici (CP) imali su određeno tehničko znanje i namjeravali su nanijeti štetu svojim metama, slično Parkerovoj kategoriji zlonamjernih hakera (McBrayer, 2014). Insajderi (IT) bili su nezadovoljni zaposlenici koji su koristili svoj ovlašteni pristup računalnim sustavima kako bi nanijeli štetu tvrtkama za koje su smatrali da su ih nepravedno tretirale. Hakeri stare garde (OG) pripadali su prvoj generaciji hakera, bili su motivirani intelektualnim izazovima te s izrazito malo kriminalnih namjera. Rogers (1999; prema McBrayer, 2014) je tvrdio da su profesionalni kriminalci (PC) i računalni teroristi (CT) najopasniji jer su dobro obučeni i stručni u svojim napadima. Njegova je taksonomija stavljala kategorije hakera na kontinuum tehničke sposobnosti, od najniže, koju imaju početnici, do najviše koja pripada profesionalnim kriminalcima i računalnim teroristima (McBrayer, 2014).

Sljedeće je godine D. Kall Loper objavio svoju disertaciju o kriminologiji računalnih hakera. Loper (2000) je u svome radu naglasio da je iznimno veliki nedostatak u kreiranju tipologije računalnih kriminalaca to što ne postoji dogovorena definija hakera. Predložio je novu tipologiju hakera koristeći triangulacijsku proceduru u kojoj su nazivi za svaku kategoriju bili nazivi koje koriste hakerske zajednice. Loper je definirao sljedeće kategorije hakera: **hakeri stare škole** (eng. Old school hackers), **kućni hakeri** (eng. Bedroom hackers), **hakeri**

početnici (eng. Larval hackers), **WaRez D00dz**, **internetski hakeri** (eng. Internet hackers), **haktivisti** (eng. Hacktivists) i **skript-klinci** (eng. Script kiddies).

Hakeri stare škole bili su slični Rogersovoj kategoriji hakera stare garde, karakterizira ih znatiželja te nenamjerno kršenje zakona. Kućni hakeri bili su oni koji su hakirali iz svojih domova, često s ograničenim resursima i oslanjajući se na hakersku subkulturu za više resursa. Loper (2000) je hakere početnike smatrao novim hakerima koji su tek počeli učiti tehnike hakiranja. WaRez D00dz bili su pirati koji su svjesno kršili zakone o autorskim pravima softvera, tvrdeći da bi informacije trebale biti besplatne i dostupne na korištenje. Internetski hakeri obuhvaćali su široku skupinu hakera koji nisu spadali u druge kategorije, a od kućnih se hakera razlikuju po osjećaju zajedništva koju su dobivali iz hakerske subkulture. Loper (2000) je definirao haktiviste kao politički, socijalno ili religijski motivirane hakere, slično Rogersovim računalnim teroristima i Parkerovim ekstremnim zagovornicima (McBrayer, 2014). Script kiddies dijele sličnosti da hakerima početnicima, no ne pokazuju interes za unapređenje tehničkog znanja. Loper (2000) je u svojoj kategorizaciji razlikovao hakere prema njihovim resursima, vještinama i uklapanju u hakersku subkulturu. Ova tipologija bila je jedinstvena jer je koristila kategorijske oznake temeljene na hakerskom žargonu.

Kirsty Best (2003; prema McBrayer, 2014) istraživala je odnos između demokracije i hakiranja pri čemu je fokus bio na etici prisutnoj unutar hakerske subkulture. Napravila je razliku između dvije grupe hakera: malicioznih hakera, koje je nazvala "crackers" ili "blackhat" hakerima, te dobroćudnih hakera, koje je nazvala "whitehat" hakerima (Best, 2003; prema McBrayer, 2014). Razlikovala je staru školu hakera, koju je opisala kao "whitehat" hakere motivirane znatiželjom ili izazovom te novu školu hakera, koju je nazvala "blackhat" hakerima motiviranima pohlepom ili političkim stavom (Best, 2003; prema McBrayer, 2014).

Nakon opsežnog pregleda dosadašnjih teorija kategorizacije, Rogers (2005; prema Campbell i Kennedy, 2014) je razvio ažurirani kontinuum računalnih kriminalaca, temeljen na svom prethodnom radu. Ovaj kontinuum obuhvaća sljedeće kategorije koje su uglavnom temeljene na tehnološkoj stručnosti i motivaciji kriminalaca (Rogers, 2005; prema Campbell i Kennedy, 2014):

1. **Početnici (NV)** (eng. Novice) su kriminalci s najmanje tehničkog znanja i vještina. Članovi ove kategorije su relativno novi na sceni i koriste unaprijed napisane skripte/kodove i alate za počinjenje računalnih zločina. Njihova glavna motivacija je uzbuđenje zbog kršenja zakona, stjecanje ugleda te zadovoljavanju ega (Rogers, 2006).

Uglavnom se radi o mlađim pojedincima koji žele biti prihvaćeni u hakersku subkulturu i kako bi dokazali svoju vrijednost, nastoje "prikupiti trofeje". Ovo ponašanje slično je onome koje se nalazi u omladinskim bandama u kojima je cilj postati punopravnim članom, a za ostvarenje tog cilja nužno je počiniti neki zločin kako bi se dokazali (Rogers, 2006).

2. **Računalni buntovnici (CP)** (eng. Cyber punks) najviše odgovaraju tradicionalnom stereotipu hakera. Članovi ove kategorije su nešto napredniji od početnika. Ovi kriminalci imaju sposobnost stvaranja osnovnih skripti i programa za napade. Njihova tipična ponašanja uključuju „rušenje“ web stranica, DDoS napade[5], kartičnu prijevaru i telekomunikacijske prijevare. Njihova motivacija je potreba za pažnjom, slavom i financijskom dobiti, obično postignutom pretvaranjem svojih zločina u unosne poslove.

3. **Insjaderi (IN)** (eng. Internals) su bivši zaposlenici ili nezadovoljni radnici koji su na informatičkim pozicijama. Članovi ove kategorije imaju prednost u odnosu na vanjske napadače zbog svog posla i statusa unutar korporacije. Istraživanja pokazuju da su interni napadači odgovorni za većinu računalnih zločina i financijskih gubitaka. Njihova motivacija obično se temelji na osveti zbog percipirane nepravde (npr. otkaz, izostanak promocije). Shaw, Ruby i Post (1998; prema Rogers, 2006) identificirali su rizične čimbenike za ovu kategoriju te spominju da, kada su u kombinaciji s odgovarajućim čimbenicima okruženja (npr. stres), kreću u napad. Rizični čimbenici poput nedostatka empatije, osjećaja opravdanosti te loše interpersonalne vještine uobičajeni su među IT profesionalcima generalno (Shaw i sur., 1998; prema Rogers, 2006).

4. **Sitni lopovi (PT)** (eng. Petty thieves) su tradicionalni kriminalci koji su se okrenuli tehnologiji kako bi išli u korak s vremenom. Ove su osobe karijerni kriminalci čija je motivacija prvenstveno financijska dobit počinjena krađom od banaka, korporacija i pojedinaca.

5. **Hakeri stare garde (OG)** (eng. The old guard hackers) su računalni kriminalci s naprednim vještinama i tehničkim znanjem. Ove su osobe odgovorne za pisanje mnogih

[5] DDoS napadi ometaju mrežne usluge ciljanjem web-mjesta i poslužitelja s namjerom iscrpljivanja resursa aplikacija. Napadači preplavljuju web-mjesta velikom količinom nasumičnog prometa, što dovodi do smanjenja funkcionalnosti web-mjesta ili čak do potpunog prekida usluge. DDoS napadi imaju širok spektar djelovanja i mogu ciljati razne sektore te tvrtke različitih veličina diljem svijeta. Predstavljaju jednu od najčešćih prijetnji u svijetu računalne sigurnosti, s potencijalom da ugroze vaše poslovanje, internetsku sigurnost, prodaju i reputaciju (Microsoft, 2024).

programa koje koriste manje iskusni početnici i računalni buntovnici u svojim *cyber* napadima; međutim, oni nisu kriminalci u tradicionalnom smislu. Njihovo ilegalno ponašanje motivirano je željom za znanjem, znatiželjom te intelektualnom stimulacijom.

6. **Kreatori virusa (VW)** (eng. Virus writers) ne uklapaju se u Rogerovu taksonomiju uglavnom zbog nedostatka istraživanja o ovoj skupini pojedinaca. Rogers (2006) navodi kako ova kategorija predstavlja anomaliju iz razloga što je teško točno odrediti gdje spadaju unutar klasifikacije. Također napominje kako su izvrstan primjer kako svaka grupa zapravo može sadržavati svoje podgrupe. Gordon (2001; prema Rogers, 2006) navodi da unutar ove kategorije postoji kontinuum ponašanja te da pojedinci uglavnom prestaju s ovim devijantnim ponašanjem kada uđu u srednje ili kasne dvadesete godine.

7. **Profesionalni kriminalci (PC)** (eng. Professional criminals) su obično stariji i tehnološki opremljeniji od prethodnih kategorija. Članovi ovih kategorija mogu biti bivši vladini i obavještajni operativci motivirani financijskom dobiti. Često imaju pristup naprednoj tehnologiji i vješti su u industrijskoj špijunaži. Smatra ih se jednim od najopasnijih tipova računalnih kriminalaca. Često su dio organiziranih kriminalnih grupa koje su prepoznale potencijal korištenja tehnologije i interneta u kriminalnom svijetu (Keegan, 2002; prema Rogers, 2006).

8. **Informacijski ratnici (IW)** (eng. Information warriors) su visoko kvalificirani zaposlenici koji provode koordinirane napade na informacijske sustave u pokušaju da onesposobe ili destabiliziraju infrastrukturu. Ova skupina može biti motivirana odanošću i domoljubljem.

9. **Politički aktivisti (PA)** (eng. Political activists) obuhvaćaju hakere motivirane političkim, socijalnim ili vjerskim razlozima (Rogers, 2006).

Na temelju ovih osam kategorija, ne uključujući insajdere, Rogers (2005; prema Campbell i Kennedy, 2014) je stvorio osnovni kružni model tipologije računalnih kriminalaca koji je imao za cilj dodatno klasificirati računalne kriminalce. Rogersov model grupirao je računalne kriminalce u kružnom dijagramu koristeći dva kontinuuma: tehnološke vještine i motivaciju. Rogers (2006) je tvrdio da nova taksonomija prati kontinuum, slično kao prethodna, od najnižih tehničkih vještina do najviših, te da služi kao temelj za razvoj tipologije hakera temeljene na razinama vještina i motivacije (Rogers, 2006). Dodatno je unaprijedio ovu taksonomiju

uključivanjem komponente motivacije, pri čemu je identificirao četiri ključne motivacije (osvetu, financijsku dobit, slavu i znatiželju) i povezao ih s različitim kategorijama računalnih kriminalaca (Rogers, 2006). Ovo je istraživanje bilo jedno od prvih koje je izdvojilo motivaciju kao zasebni faktor u klasifikaciji računalnih kriminalaca i iskoristilo je kao dodatnu dimenziju za jačanje taksonomije (Rogers, 2006).

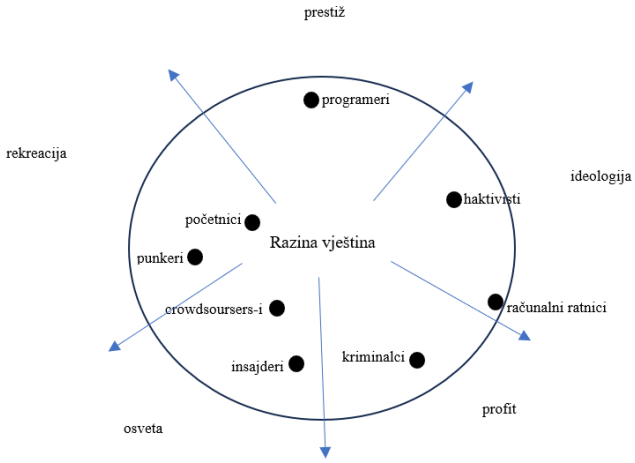
Do 2008. godine, hakeri i hakiranje su bili kategorizirani na različite načine, poput razine vještina, motivacije ili prema etikama (bijeli, crni ili sivi šeširi), kao i prema starim ili novim pristupima (McBrayer, 2014). Holt i Kilger (2008; prema McBrayer, 2014) predložili su novu klasifikaciju koja se fokusira na način korištenja tehnologije unutar hakerske zajednice. Predložili su podjelu hakera na dvije skupine: "**makecraftere**" i "**techcraftere**". "Makecrafteri" su oni koji stvaraju nove skripte, alate i proizvode, koji mogu biti zlonamjerni, benigni ili čak korisni. S druge strane, "techcrafteri" su hakeri koji koriste alate i proizvode koje su stvorili "makecrafteri". Holt i Kilger (2008; prema McBrayer, 2014) tvrdili su da ovakav sustav pruža bolji uvid u metode i taktike hakera jer uklanja etičke oznake poput crnih, bijelih ili sivih šešira.

Rege-Patwardhan (2009; prema McBrayer, 2014) istraživao je vrste hakiranja koje se koriste za napade na kritičnu infrastrukturu i pritom predložio tipologiju počinitelja temeljenu na slučajevima računalnog kriminala. Utvrdio je da hakeri često djeluju samostalno te da se razlikuju po tehničkim vještinama i motivacijama (Rege-Patwardhan, 2009; prema McBrayer, 2014). Autor je predložio da se hakeri kategoriziraju kao početnici, uključujući tu i "script kiddies", a zatim insajdere i profesionalce. Početnici, uključujući "script kiddies", su definirani kao novi hakeri koji se oslanjaju na unaprijed izrađene alate za provođenje svojih napada. Insajderi su definirani kao nezadovoljni zaposlenici koji koriste svoje ovlasti i znanje za osvetu. Profesionalci su hakeri s visokim stupnjem tehničkih vještina i nude svoje usluge uz naknadu. Osim toga, Rege-Patwardhan (2009; prema McBrayer, 2014) predlaže i kategoriju suradnika za hakere koji rade u grupama. Većina napada na kritičnu infrastrukturu uključivala je korištenje rootkita, alata koji omogućuje hakerima dobivanje administrativnog pristupa sustavima, što se razlikuje od korištenja unaprijed izrađenih malware alata koji ne zahtijevaju značajno tehničko znanje (Rege-Patwardhan, 2009; prema McBrayer, 2014).

Shaw, Ruby i Post (1998; 2006; 2011; prema Campbell i Kennedy, 2014) klasificiraju računalne kriminalce u dvije glavne kategorije: **vanjski uljezi** i **opasni insajderi**. Istraživanja se fokusiraju na ključne IT *insajdere* koji su uglavnom programeri, tehnička podrška, operateri

mreže, administratori, konzultanti i privremeni radnici unutar organizacija. Maliciozni insajderi (MI) predstavljaju potkategoriju takvih zaposlenika, a motivirani su pohlepom, osvetom, rješavanjem problema i zadovoljavanjem ega (Shaw i Stock, 2011; prema Campbell i Kennedy, 2014). Njihovo istraživanje, koje se temelji na korporativnim anketama i stotinama istraga koje su provele američka Tajna služba i Koordinacijski centar za odgovor na računalne prijetnje sveučilišta Carnegie Mellon (CERT-CC), nastojalo je sastaviti početni profil opasnih insajdera. Početni profil za maliciozne insajdere nalaže kako se radi o muškarcu u kasnim tridesetima koji radi u tehnološkom sektoru tvrtke. Maliciozni insajderi klasificiraju se u dvije kategorije: **privilegirani nezadovoljni lopov** (eng. the Entitled disgruntled thief) i **makijavelistički vođa** (eng. Machiavellian leader) (Shaw i sur., 1998; prema Campbell i Kennedy, 2014). Privilegirani nezadovoljni lopov se obično bavi krađom intelektualnog vlasništva. Oni kradu informacije na kojima su izravno radili ili koje su pomogli razviti. Osjećaju se kao da imaju pravo na određene informacije i obično će ih koristiti kao pomoć pri pronalaženju novog posla ili za poboljšanje svog učinka na već stečenom radnom mjestu. Makijavelistički vođa imaju unaprijed određene ciljeve, vođeni su osobnom ambicijom, a ne profesionalnim stresorima kao privilegirani nezadovoljni lopovi. Prema Shawu i suradnicima (1998; prema Campbell i Kennedy, 2014), opasni insajderi obično imaju introvertirane osobnosti. Pokazuju sklonost prema samostalnim intelektualnim aktivnostima te izbjegavaju međuljudske interakcije. Opasni insajderi racionaliziraju svoje zločine okrivljavajući svoju tvrtku ili nadređene za sve negativne posljedice koje su doživjeli. Smatraju da je bilo kakva elektronička šteta koju prouzrokuju krivnja organizacije koja ih je nepošteno tretirala. Istraživači također primjećuju da se mnogi insajderi više identificiraju s profesijom nego s tvrtkom u kojoj su zaposleni (Shaw i sur., 1998; prema Campbell i Kennedy, 2014).

Ryan Seebruck (2015) predlaže tipologiju u skladu s prethodnim istraživanjima, odnsono prema vještinama i motivaciji. Uz nedavno spomenute motivacije koje je spominjao Marcus Rogers, znatiželju, slavu, osvetu i novac, Seebruck (2015) dodaje i petu motivaciju – ideologiju – i preimenovao preostale četiri kao rekreaciju, prestiž, osvetu i profit. Ideologija obuhvaća političke aktiviste (one motivirane suvremenim društvenim problemima) i nacionaliste (napade koje pokreću patriotski građani ili računalni rat podržan od strane same države). Seebruck (2015) je prijašnjim tipologija dodao i ***crowdsourcers***-e – uz veći naglasak na kategoriji hacktivista. Ovo rezultira tipologijom koja se sastoji od osam tipova hakera, poredanih po razini tehničke stručnosti, započevši od najmanje: **početnici**, **crowdsourcers-i**, **punkeri**, **haktivisti**, **insajderi**, **kriminalci**, **programeri** i **računalni ratnici**.



Slika 1. Okvirni prikaz kružnog dijagrama tipologije hakera (Seebruck, 2015).

Na slici 1. nalazi se okvirni prikaz Seebruck-ovog kružnog dijagrama tipologije hakera. Crni manji krugovi predstavljaju tip hakera, a oni krugovi koji su bliži velikom krugu govore da taj tip posjeduje veću razinu vještina. Tekst izvan kruga predstavlja motivacije. U skladu s tim, haktivisti se smatraju napadačima srednje niže razine vještina koji su prvenstveno motivirani političkom ideologijom. Računalni ratinici označava visoko sofisticirane napadače motivirane ideologijom i profitom. Programeri su nemaliciozni hakeri srednje razine vještina koji traže prestiž. Kriminalci imaju srednje-jake vještine i prvenstveno su motivirani profitom, a sekundarno osvetom. Insajderi imaju srednje vještine i motivirani su osvetom ili profitom. Crowdsourcers posjeduju slabije tehničke metode i prvenstveno su motivirani osvetom, a sekundarno rekreacijom. Početnici koriste osnovne tehnike i motivirani su znatiželjom. Punkeri imaju niske do prosječne vještine i primarno su motivirani uzbuđenjem sudjelovanja u devijantnom ponašanju, a sekundarno osvetom (Seebruck, 2015).

Mark de Bruijne, Michel van Eeten, Carlos Hernández Gañán i Wolter Pieters (2017) razvili su tipologiju na temelju pet dimenzija – meta (ljudi, poduzeća, javni sektor i kritične infrastrukture), stručnost koju karakterizira razina znanja i vještina (visoka, srednja i niska), resursi (budžet i slobodno vrijeme), organizacija (razinu ili način na koji su akteri strukturirani kako bi obavili zadatak ili postigli ciljeve) i motivacija (osobna, ekonomska, ideološka i geopolitička). Vezano uz dimenziju organizacije, kako bi se povećala analitička relevantnost i konceptualna preciznost, koristi se poznata distinkcija iz institucionalne ekonomije: hijerarhija, koja se oslanja na kontrolu i centralizirani autoritet za koordinaciju zadataka, tržište, koje

uključuje kupnju sigurnosnih usluga i softvera, mreže, koje nemaju centralizirani autoritet nego se oslanjanju na dugoročne odnose i povjerenje, te kolektivi koji su najslabije organizirane skupine, a pripadaju im pojedinci sličnih interesa i očekivanih koristi (Bevir, 2012; prema de Bruijne i sur., 2017). Njihova se tipologija sastoji od sljedećih kategorija (de Bruijne i sur., 2017):

1. **Iznuđivači** (eng. extortionists) napadaju građane, poduzeća, bolnice, škole, vlade, a i kritične infrastrukture poput energetskog sektora i organizacija za upravljanje vodama. Stručnost među napadačima za izvođenje iznuđivačkih napada autori ocjenjuju kao nisku do srednju. Što se tiče resursa, procjena bi bila da je količina resursa potrebnih za izvođenje iznuđivačkog napada niska do srednja. Na organizacijskoj dimenziji, tip prijetnje bi bio hijerarhija, tržište ili mreža. I na kraju, motivacija bi se smatrala osobnom ili ekonomskom;
2. **Informacijski posrednici** (eng. information brokers) napadaju građane, poduzeća i javni sektor. Razina stručnosti u napadima može varirati od srednje do visoke. Količina resursa potrebnih za dobivanje informacija i podataka putem napada može se klasificirati kao niska do srednja. Alati za dobivanje tih izvora informacija lako su dostupni. Na organizacijskoj dimenziji, tip prijetnje mogao bi se klasificirati kao hijerarhija, tržište ili mreža. I na kraju, motivacija je ekonomska;
3. **Pomagači u počinjenju kaznenih djela** (eng. Crime facilitators) imaju iste mete i motivaciju kao prethodna kategorija. Stručnost za razvoj novih alata stalno raste i može se ocijeniti kao srednja do visoka. Količina resursa potrebna za razvoj tih alata i usluga klasificira se kao srednja, a organizacijska struktura koja ih karakterizira su tržišta i mreže;
4. **Digitalni pljačkaši** (eng. Digital robbers) najčešće napadaju pojedince, a nerijetko i financijska poduzeća, što podrazumijeva ekonomsku motivaciju. Posjeduju srednju do visoku stručnost i svojim napadima, količina dostupnih resursa također se klasificira kao srednja do visoka, a organizacijska je struktura mrežno utemeljena;
5. **Prevarantima** (eng. Scammers and fraudsters) su mete pojedinci, poduzeća i javni sektor. Razina stručnosti potrebna za ove vrste napada klasificira se kao niska do srednja, kao i razina resursa. Organizacijske strukture povezane s ovim napadima su individualne, tržišne ili mrežne, a motivacija je ekonomska;

6. **Haktivisti** (eng. Hacktivists) su motivirani ideološki, ali su slabo organizirani, bilo pojedinačno, kolektivima ili mrežama. Razina stručnosti u ovim napadima je niska do srednja;
7. **Razbijači** (eng. Crackers) mogu napadati od javnih do privatnih poduzeća, ali i kritične infrastrukture. Njih motivira zabava i mogućnost pokazivanja svojih sposobnosti što ukazuje na osobne motive, posebno za mlađe pojedince. Razine stručnosti smatraju se niskim do srednjim jer je dostupnost lako upotrebljivih i potencijalno destruktivnih alata sve veća. Količina resursa koju imaju na raspolaganju smatra se niskom. Crackeri su obično relativno stariji i djeluju individualno ili u slabo organiziranim kolektivima ili mrežama:
8. **Teroristi** (eng. Terrorists) čine napade na poduzeća, javni sektor ili kritičnu infrastrukturu. Ovakav napad zahtijeva razinu visoke stručnosti i srednju do visoku razinu resursa. Obično se služe organizacijskim strukturama tržišta ili hijerarhije za koordinaciju svojih napada, a motivacija je ideološka;
9. **Državni akteri** (eng. State actors) predstavljaju tradicionalne, tajne napade u kojima državni akteri ciljaju poduzeća, javni sektor ili kritične infrastrukture kako bi stekli pristup strateškim informacijama. Razina stručnosti i resursa uključenih u ove napade smatra se srednjom do visokom. Organizacijska struktura koja se koristi za provođenje ovih napada je hijerarhijska, a motivacija je geopolitička;
10. **Državno sponzorirana mreža** (eng. State sponsored network) imaju sumnjive veze s državnim akterima. Uglavnom ciljaju građane, poduzeća, javni sektor i kritične infrastrukture. Razina stručnosti koju pokazuju varira između srednje i visoke. Količina resursa je srednja ili visoka, s obzirom na činjenicu da se napadi koji su zabilježeni smatraju dugoročnim kampanjama. Organizacijska struktura pokazuje mrežne karakteristike, a motivacija se može klasificirati kao ideološka;
11. **Insajderi** (eng. Insiders) ciljaju organizacije u kojima rade, a to mogu biti javna ili privatna poduzeća. Razina stručnosti može varirati od srednje do visoke u slučaju iskusnih i dugogodišnjih zaposlenika. Količina resursa dostupnih za napade može se klasificirati kao niska, a motivacija kao osobna, ekonomska ili ideološka.

Caroline Moeckel (2019) predložila je izgradnju nove tipologije počinitelja utemeljene na stvarnim podatcima, služeći se analizom postojećeg teorijskog okvira i više od 200 javno dostupnih dokumenata koji sadrže detalje o računalnom kriminalitetu povezanom s digitalnim

bankarstvom. Predstavila je sljedeće profile počinitelja koji čine tipologiju specifičnu za slučaj digitalnog bankarstva (Moeckel, 2019):

	Istraživači sigurnosti sustava (eng. System challengers)	**Insajderi (eng. Insiders)**	**Ideolozi (eng. Ideologists)**	**Službenici (eng. Officials)**	**Profesionalci: Male grupe i pojedinci (eng. Proffesionals: Small groups and individuals)**	**Korisnici alata (eng. Toolkit users)**
Oznake	*White hat* , ljubitelji uzbuđenja ili lovci na slavu, mladi hakeri, hakeri početnici	Zaposlenici banaka, zaposlenici dobavljača trećih strana	Haktivisti, *online* aktivisti ili računalni teroristi	Države, vlada ili njezine agencije, vojne funkcije	Usamljeni hakeri i individualni napadači, male kriminalne grupe	"crime-in-a-box", "exploit" ili "crimeware"
Motivi	Zabava, izazov, otkrivanje ranjivosti sustava, hvaljenje pred drugima	Financijska dobit, osveta	Ideologija, u rijetkim slučajevima status i ego	Ideologija, računalno ratovanje	Financijska dobit	Financijska dobit
Kriminalna namjera	Niska do umjerena	Umjerena do visoka	Umjerena do visoka	Visoka	Visoka	Visoka
Resursi	Ograničeni raspon vještina i sredstava	Velik raspon vještina i sredstava	Umjerene do visoke razine	Veoma visoke razine vještina i financijska sredstva	Umjerene do visoke razine vještina i resursa	Ograničene vještine i sredstva
Aktivnosti	Neovlašteni pristup sustavima, testiranje sustava i javno	Korištenje unutarnjeg znanja za izravno izvlačenje	Napadi iz socijalnih i/ili političkih razloga	Špijunaža, protupropaganda, nadzor informacija i destruktivni	Phishing[6], malware napadi[7], ransomware[8], trojanski	Phishing, ransomware, trojanski programi i malware

[6] Phishing predstavlja ozbiljnu sigurnosnu prijetnju koja koristi napredne psihološke tehnike i društveni inženjering kako bi prevarila ljude da kliknu na poveznice zlonamjernih web stranica i unesu vrijedne osjetljive podatke, poput osobnih informacija ili podataka o korisničkim računima (Zieni, Massari i Calzarossa, 2023).
[7] Malware je zlonamjerni programski kod koji može preuzeti kontrolu nad uređajem ili sustavom, s namjerom krađe podataka, njihovog oštećenja ili jednostavno uznemiravanja korisnika. Ova prijetnja obuhvaća trojance, crve, botnete i viruse (Aurangzeb, Aleem, Azhar Iqbal i Arshad Islam, 2017).
[8] Kada se malware koristi za ucjenu, naziva se ransomware. Ransomware je zlonamjerni softver koji potajno inficira uređaj žrtve i zatim zahtijeva plaćanje otkupnine kako bi se omogućio pristup šifriranim podacima (Aurangzeb i sur., 2017).

	objavljivanje razine ranjivosti sustava	novca uništavanje sustava, industrijska špijunaža		napadi, cyber ratovanje	programi i upadi u sustav	napadi postojećim alatima
Razina opasnosti	Relativno niska, ali varira unutar grupe	Visoka, mogući značajni razmjeri štete	Visoka (uništavanje i počinjenje štete)	Visoka, iako je dosad potvrđeno malo dokaza i slučajeva	Srednja do visoka	Srednja do visoka

Samuel Chng, Han Yu Lu, Ayush Kumar i David Yau (2022) identificirali su jedanaest klasifikacija i tipologija računalnih kriminalaca, od kojih je većina spomenuta i u ovome radu, objavljenih tijekom tri desetljeća s namjerom sažimanja dotadašnjeg stanja. Predstavili su trinaest kategorija počinitelja i sedam jedinstvenih motiva, no jedna kategorija i jedan motiv izostavljeni su u ovome radu iz razloga što spadaju u seksualno motivirana kaznena djela. Njihov sažetak, a posljedično i predložena tipologija, izgleda ovako (Chng i sur., 2022):

1. **Početnici** (eng. novices): Ova se grupa odnosi na hakere s manje vještina koji se u velikoj mjeri oslanjaju na *online* alate drugih autora. Alternativni nazivi uključuju "script kiddies", "newbies" i "system challengers". Motivirani su znatiželjom, zabavom i slavom. Služe se gotovim kodovima i skriptama pronađenim na internetu i *Dark webu,* često s malo ili bez ikakvih modifikacija. Njihove niske razine vještina često rezultiraju nesposobnošću da prikriju svoje tragove. Njihovi tipični napadi uključuju instalaciju malware-a, phishing, ponovno korištenje lozinki i jednostavne DDoS napade.
2. **Studenti** (eng. students): Ovi pojedinci nemaju zle namjere, već hakiraju samo kako bi stekli znanje. Njihova je glavna motivacija znatiželja. Poput prethodne kategorije, studenti koriste postojeće kodove i skripte, ali uz neke modifikacije kako bi istražili ranjivosti u sustavima kao što su web poslužitelji, baze podataka i sl. Oni obično prijavljuju otkrivene ranjivosti odgovarajućim tvrtkama, istraživačima sigurnosti ili vlastima.
3. **Računalni buntovnici** (eng. cyberpunks): Radi se o počiniteljima niske do srednje razine vještina koji prouzrokuju štetu iz zabave. Poznati su i kao "crashers", "thugs", i "crackers". Njihove motivacije uključuju financijsku dobit, želju za slavom, osvetu i zabavu. Računalni buntovnici mogu koristiti postojeće kodove ili pisati vlastite kako bi

ostvarili svoje ciljeve. Njihove metode uključuju *bricking*[9] (trajno onesposobljavanje) računala, iskorištavanje bugova[10] u softveru, DDoS napade, phishing, spam pošta[11], SQL injekcije[12] i krađu osjetljivih informacija poput brojeva kreditnih kartica.

4. **Hakeri stare garde** (eng. Old guard hackers): Kao i studenti, ovi ne-zlonamjerni hakeri ne poštuju privatnost drugih, a uključuju one pojedince koji spadaju u prijašnje navedene kategorije "white hats", "sneakers", "grey hats", i "tourists". Motivirani su znatiželjom, notornošću, zabavom i ideologijom. Koriste prilagođene kodove, skripte i alate za testiranje mogućnosti upada u sustav kako bi otkrili ranjivosti u postojećim sustavima. Oni mogu prijaviti te ranjivosti vlasnicima sustava, istraživačima sigurnosti ili javnosti te često surađuju s tvrtkama za sigurnost i vlastima.
5. **Insajderi** (eng. Insiders): Nezadovoljni su sadašnji ili bivši zaposlenici koji zlorabe svoj pristup kako bi dobili što žele. U ovu skupinu spadaju "internals", "user malcontents" i "corporate raiders" kao kategorije drugih autora. Njihove motivacije su financijska dobit, osveta i ideologija. Ovi pojedinci koriste svoje privilegirane pristupe za krađu osjetljivih podataka unutar organizacije, kao što su podaci o klijentima ili zaposlenicima. Također, zbog nepažnje mogu nenamjerno ugroziti sigurnost mreže.
6. **Sitni lopovi** (eng. Petty thieves): Radi se o kriminalcima koji su, motivirani financijskom dobiti i osvetom, svoje aktivnosti preselili *online*. Uključuju iznuđivače, prevarante, lopove i digitalne pljačkaše. Koriste jednostavne metode kao što su trojanski virusi, keylogging[13], phishing i ransomware za stjecanje financijskih podataka ili iznuđivanje novca.

[9] Radi se o svjesnom narušavanju ili uništavanju softvera s ciljem da se smanji ili ugrozi funkcionalnost proizvoda (Tusikov, 2019).

[10] Bug je zlonamjerni kod, nevidljiv korisniku, postavljen na web stranice na način koji omogućava trećim stranama da prate korištenje web poslužitelja i prikupljaju informacije o korisniku, uključujući IP adresu, naziv hosta, vrstu i verziju preglednika, naziv i verziju operativnog sustava te kolačiće web preglednika (National Institute of Standards and Technology, n.d.).

[11] Spam je svaka nebitna i neželjena poruka ili email koju napadač šalje velikom broju primatelja koristeći email ili bilo koji drugi medij za dijeljenje informacija. Spam emailovi mogu sadržavati viruse, trojance i daljinske alate za upravljanje. Napadači često koriste ovu tehniku kako bi namamili korisnike na *online* usluge. Oni mogu slati spam mailove s privicima koji imaju višestruke ekstenzije datoteka ili s URL-ovima koji vode korisnike na zlonamjerne i spam web stranice, što može rezultirati krađom podataka ili financijskom prevarom, kao i krađom identiteta (Ahmed, Amin, Aldabbas, Koundal, Alouffi i Shah, 2022).

[12] SQL injekcija je vrsta napada koja se obično događa kada napadači mijenjaju, brišu, čitaju i kopiraju podatke s poslužitelja baze podataka, a smatra se jednom od najopasnijih vrsta napada na web aplikacije. Uspješna SQL injekcija može ugroziti sve aspekte sigurnosti, uključujući povjerljivost, integritet i dostupnost podataka. SQL (*structured query language*) koristi se za pisanje upita za sustave upravljanja bazama podataka (Alghawazi, Alghazzawi i Alarifi, 2022).

[13] Keyloggeri su vrsta zlonamjernog softvera (rootkita) koji prati unose s tipkovnice i pohranjuje ih u datoteke, omogućujući time krađu osjetljivih podataka poput lozinki, korisničkih imena i PIN-ova. Ovi podaci se zatim prenose napadaču bez privlačenja pažnje korisnika. Keyloggeri predstavljaju ozbiljnu prijetnju za aktivnosti

7. **Digitalni pirati** (eng. Digital pirates): Poznati kao kršitelji autorskih prava, ovi pojedinci nezakonito dupliciraju, distribuiraju, preuzimaju ili prodaju zaštićene materijale. Motivirani su financijskom dobiti, a od strategija im se pripisuje krađa i distribucija zaštićenog sadržaj poput muzike, filmova, igara i softvera putem web stranica, torrenta[14] i društvenih medija.
8. **Pomagači u počinjenju kaznenih djela** (eng. Crime facilitators): Pružaju potrebne alate i tehničko znanje cyber kriminalcima, omogućujući im da pokrenu sofisticirane napade koji inače ne bi bili mogući. Obično su motivirani financijskom dobiti. Nude usluge poput phishing kampanja, iznajmljivanja malware-a i botneta, hosting usluga[15], i skrivanje ilegalnih transakcija. Djeluju na forumima i web stranicama na Dark webu, povezujući kupce i prodavače.
9. **Profesionalci** (eng. Professionals): Radi se o visoko vještim pojedincima koji djeluju kao "najamni hakeri" ili u svrhu daljnjeg razvoja svog kriminalnog carstva. Motivirani su financijskom dobiti i osvetom. Poznati su i kao "black hats", "elites", "criminals", "organized criminals", "information brokers" i lopovi. Izvode sofisticirane napade koristeći širok spektar metoda i prilagođenih kodova. Njihove operacije su dobro prikrivene kako bi izbjegli detekciju od strane vlasti. Djeluju samostalno, u malim grupama ili u suradnji s kriminalnim organizacijama.
10. **Državni hakeri** (eng. Nation state hackers): Oni su visoko obučeni i izuzetno vješti kriminalci koji rade direktno ili indirektno za jednu vladu kako bi destabilizirali, ometali i uništavali sustave i mreže druge države ili vlade. Motivirani su financijskom dobiti, osvetom i ideologijom. Ova kategorija uključuje "information warriors", "cyber terrorists", "cyber warriors", "state actors", "state-sponsored networks" i špijune. Izvode složene napade u više faza, uključujući socijalni inženjering, instalaciju malware-a, dobivanje administrativnih prava i prikupljanje podataka. Njihove operacije su visoko koordinirane i ciljane na državne i kritične infrastrukture.
11. **Crowdsourceri** (eng. Crowdsourcers): Radi se o pojedincima koji se okupljaju kako bi riješili neki problem, često koristeći upitne metode ili slijedeći sumnjive ciljeve.

poput internetskog bankarstva, e-trgovine, slanja e-mailova i upravljanja bazama podataka (Singh, Choudhary, Singh i Tyagi, 2021).

[14] Torrent datoteke dostupne na *online* platformi za dijeljenje (poput The Pirate Bay stranice) uglavnom sadrže materijale zaštićene autorskim pravima, pri čemu nositelji prava nisu dali dozvolu operaterima ili korisnicima te platforme za dijeljenje tih sadržaja (Groom, 2017).

[15] Pružatelji web hosting usluga osiguravaju sistemske resurse poput prostora na disku, procesora, memorije i internetske propusnosti kako bi omogućili pohranu i pristup sadržajima na webu za pojedince, organizacije i tvrtke koje nemaju potrebne resurse ili stručnost za samostalno održavanje web stranice (Tseng i Yang, 2007).

Motivirani su željom za notornošću, osvetom, zabavom i ideologijom. Djeluju kolektivno na forumima za hakiranje, surađujući na razvoju novog malware-a, upravljanju botnetima i dijeljenju tehnika infiltracije.

12. **Hacktivisti** (eng. Hacktivists): Poznati su kao politički aktivisti i ideolozi, koriste svoje tehničke vještine kako bi promicali svoje političke agende ili koristili internet kao alat za političke promjene. Motivirani su notornošću, osvetom, zabavom i ideologijom. Rade u grupama koristeći metode kao što su SQL injekcije, DDoS napadi i kompromitiranje društvenih medija kako bi skrenuli pažnju na svoje ciljeve. Također, koriste platforme za distribuciju lažnih vijesti ili phishing linkova.

Svaki od ovih tipova hakera koristi specifične strategije koje odgovaraju njihovim ciljevima i razinama vještine te operiraju u različitim kontekstima potaknuti različitim motivacijama. Iako postoji mnogo tipologija hakera, mnoge od njih često nisu dovoljno sveobuhvatne (Chng i sur., 2022). Iz tog su razloga Chng i suradnici (2022) razvili ažurirani okvir tipologije računalnih kriminalaca i njihovih motivacija koji obuhvaća trinaest različitih grupa počinitelja i sedam jedinstvenih motivacija.

Ono što je posebno važno u ovoj tipologiji jest da ona prikazuje tipične strategije napada koje koristi svaki od predloženih trinaest tipova hakera. To omogućava prepoznavanje specifičnih tipova kriminalaca, ili barem širokih grupa kojima pripadaju, kroz promatranje njihovih aktivnosti tijekom pripreme ili provođenja napada. Na primjer, ako je meta napada poduzeće ili državna infrastruktura i ako su korišteni sofisticirani malware ili skripte, a tragovi su teško uočljivi, može se zaključiti da su hakeri visoko kvalificirani. Ovisno o složenosti napada i razini potrebne stručnosti, može se zaključiti je li u napadu sudjelovalo više hakera (državni hakeri, hacktivisti) ili jedan (profesionalac) (Chng i sur., 2022).

Autori naglašavaju da bi ovaj okvir trebalo periodički ažurirati kako bi pratio razvoj novih strategija i pojavu novih tipova s obzirom na promjene u društvu i tehnologiji. Njihov cilj je da ovaj okvir posluži kao koristan alat analitičarima računalne sigurnosti u detekciji i obrani od budućih računalnih napada te u post-incidentnim forenzičkim analizama (Chng i sur., 2022).

7.2. Individualne karakteristike počinitelja

Internet pruža gotovo optimalno okruženje za počinjenje kriminala, ali pažnju treba usmjeriti na same računalne kriminalce. Prema literaturi, počinitelji računalnog kriminaliteta, posebno hakeri, nisu homogena skupina kako se ranije mislilo (Furnell, 2010; prema Curtis i Oxburg, 2023). Sve veći broj tipologija počinitelja, koje se razvijaju istodobno s razvojem računalnog kriminaliteta, prikazuju različite motive, osobine ličnosti, metode i sposobnosti (Moeckel, 2019). Iako situacijski čimbenici mogu objasniti dio ponašanja nekih računalnih kriminalaca, ne smije se zanemariti utjecaj osobina pojedinaca na njihove nezakonite aktivnosti. Stavovi i ponašanja često su rezultat kombinacije situacijskih utjecaja i individualnih osobina (Campbell i Kennedy, 2014). Zbog utjecaja Hollywooda i netipične prirode današnjih zločina, postoji mnogo stereotipa o tome kako izgledaju i tko su zapravo počinitelji računalnog kriminaliteta. Neki od tih stereotipa uključuju da: (1) su društveno nesposobni, ali inteligentni; (2) posjeduju velike tehničke vještine i znanje te imaju vrlo visok IQ; (3) su muškarci, generalno mladići; (4) su tinejdžeri s računalima i opasni kriminalci; te (5) da nikada nisu nasilni (Zuhri, 2016).

Istraživanja o karakteristikama računalnim kriminalaca ispitivala su demografske karakteristike počinitelja (dob i spol), njihovu pripadnost političkoj zajednici (državljanstvo) i njihove obrasce ponašanja (suradnja s drugim kriminalcima). Prema studijama, "stereotipni" počinitelj računalnog kriminaliteta je "muškarac, star između 12 i 28 godina, socijalno disfunkcionalan samac, vjerojatno iz disfunkcionalne obitelji" (Rogers, 2011, str. 223; prema Hadzhidimova i Payne, 2019). Međutim, Rogers (2011; prema Hadzhidimova i Payne, 2019) naglašava da navedeni specifični čimbenici nisu najbitniji za izradu profila računalnih kriminalaca; važnije je razumjeti kontekst koji vodi do počinjenja ilegalnih radnji. Drugi istraživači ističu da je, za individualiziraniji profil, bitno prikupiti informacije o razini tehničkog znanja počinitelja, njihovim osobinama, socijalnim karakteristikama i motivacijama (Saroha, 2014; prema Hadzhidimova i Payne, 2019). Nadalje, zemlja podrijetla računalnog kriminalca, sposobnosti države za provođenja zakona i zakonodavni okvir za borbu protiv računalnog kriminala također mogu utjecati na odlučnost počinitelja da počini računalni zločin (Chang, 2013; prema Hadzhidimova i Payne, 2019).

Poznate demografske karakteristike računalnih kriminalaca razlikuju se od tradicionalnih prijestupnika na određene načine. Na primjer, obrazovanje i zaposlenje su obično značajno povezani sa smanjenim rizikom od počinjenja tradicionalnih kaznenih djela, ali takva veza ne postoji kod računalnog kriminala (Weulen Kranenbarg, Ruiter, van Gelder i Bernasco, 2018).

Međutim, zaposlenje i obrazovanje specifično povezano s informacijskom tehnologijom može biti povezano s povećanim rizikom od računalnog kriminala (Weulen Kranenbarg i sur., 2018). Prema već spomenutom HPP-u saznajemo da računalni kriminalci, specifično hakeri, često počinju dok su mladi, njih čak 61% započinju između 10 i 15 godina, a dodatnih 32% između 16 i 20 godina. Samo 5% ih je počelo između 21. i 25. godine, što pokazuje da hakiranje obično započinje u ranoj dobi, a nakon 20. godine vrlo je malo slučajeva "prvih" hakera. Samo 2% ispitanika izjavilo je da su počeli između 26. i 30. godine, dok je 1% počelo nakon 40. godine (niti jedan ispitanik nije izjavio da je počeo između 31. i 40. godine) (Chiesa, Ducci i Ciappi, 2008). Zapravo, prosječna dob osumnjičenika u istragama Nacionalne jedinice za računalni kriminalitet u Velikoj Britaniji 2015. bila je 17 godina (NCA, 2017; prema Curtis i Oxburg, 2023). Međutim, hakeri variraju u dobi i često odstupaju od ovog stereotipa (Steinmetz, 2016). Osim toga, istraživanja pokazuju da je tipični haker "rasno bijel, muškog roda i srednje klase" (Steinmetz, 2016: str. 36). Ovo se odnosi na većinu računalnih kriminalaca jer su Harbinson i Selzer (2019) otkrili da su osuđeni počinitelji računalnih zločina obično bijele rase i muškoga spola, s prosječnom dobi od 38,2 godine, što je daleko od tinejdžerskog stereotipa hakera. Međutim, predloženo je da se ozbiljnost računalnih zločina (a samim time i vjerojatnost osude i uključivanja u takva istraživanja) povećava s dobi počinitelja (Hutchings, 2014; prema Curtis i Oxburg, 2023).

Zbog percepcije anonimnosti i udaljenosti od stvarnog svijeta, korisnici interneta osjećaju lažni osjećaj sigurnosti. *Online* počinitelji su psihološki, socijalno i fizički udaljeniji od svojih kaznenih djela i žrtava te se suočavaju s manje i/ili manje ozbiljnim posljedicama svojih ponašanja, što ih dodatno ohrabruje da recidiviraju (Curtis i Oxburg, 2023).

Prema Kabay-u, neki računalni kriminalci pokazuju neiskrenost i nepoštenje u kombinaciji s površnim šarmom i pojačanom intelektualnom sposobnošću, osobinama koje su u skladu s kriterijima za antisocijalni poremećaj ličnosti prema Dijagnostičkom i statističkom priručniku za mentalne poremećaje IV (American Psychiatric Association, 1994; prema Campbell i Kennedy, 2014). Također napominje da neki računalni kriminalci čine nezakonite radnje za izrazito malo ili nimalo nagrada unatoč prijetnji ozbiljnim kaznama. Još jedna ključna karakteristika antisocijalnog poremećaja ličnosti je nedostatak jasnog uvida počinitelja u njihovo ponašanje. Istraživači su primijetili da računalni kriminalci ne doživljavaju svoje kriminalne radnje kao štetne ili nezakonite (Kabay, 1996; Campbell i Kennedy, 2014). Ovakvi počinitelji ponekad opravdavaju ili eksternaliziraju svoje ponašanje tako što okrivljuju razne

mrežne administratore i programere za nepravilno osiguravanje svojih računala i programa (Campbell i Kennedy, 2014).

Istraživanjem Seigfried-Spellar, Villacís-Vukadinović i Lynam (2017), prilikom kojeg se koristio Elemental Psychopathy Assessment test temeljen na Velikih pet osobina ličnosti, ispitivali su povezanost između psihopatije i računalnog kriminala. Rezultati su pokazali da, slično kao i kod pojedinaca koji se bave drugim oblicima antisocijalnog ponašanja, počinitelji računalnog kriminaliteta pokazuju visoke razine psihopatskih osobina, posebno antagonizma, dezinhibicije i narcizma. Kranenbarg, van Gelder, Barends i de Vries (2023) ispitivali su razlike između *online* i *offline* počinitelja. Primijetili su da računalni kriminalci pokazuju značajnu razliku u marljivosti (koja je aspekt savjesnosti) u usporedbi s tradicionalnim kriminalcima i ne-kriminaliziranim članovima zajednice, postignuvši mnogo više rezultate u toj kategoriji. Također, računalni kriminalci su manje ekstremni u socijalnoj odvažnosti u usporedbi s tradicionalnim kriminalcima. Međutim, u četiri druge osobine—strpljenje, perfekcionizam, oprez i znatiželja—*online* kriminalci su sličniji ne-kriminaliziranim članovima zajednice nego *offline* kriminalcima (Kranenbarg i sur., 2023).

Istraživači su ukazali i na potencijalnu povezanost između hakiranja i Aspergerovog sindroma (u daljnjem tekstu AS), razvojnog poremećaja koji se nalazi na blažem kraju spektra pervazivnih razvojnih poremećaja. AS karakteriziraju poteškoće u socijalnoj komunikaciji, ponavljajuće interese i ponašanja, te normalne do superiorne kognitivne sposobnosti. Iako osobe s AS-om često imaju normalan jezični razvoj, njihov socijalni kontakt je ograničen (Campbell i Kennedy, 2014). Jedna od karakteristika AS-a koja se anegdotalno povezuje s računalnim kriminalom je intenzivna preokupacija intelektualnim interesima, poput tehnologije, što može voditi prema odabiru karijere u tim područjima. Istraživači su primijetili sličnosti između osobina osoba s AS-om i računalnih hakera, uključujući socijalnu nespretnost, egocentričnu komunikaciju i opsesivan interes za tehnologiju (Campbell i Kennedy, 2014). Ipak, nije pronađen jasan empirijski dokaz koji bi potvrdio uzročno-posljedičnu vezu između AS-a i računalnog kriminala. Većina osoba s AS-om opisana je kao poštena i zakonita te je pogrešno pretpostaviti da su svi hakeri osobe s AS-om ili obrnuto. Dok se osobine AS-a mogu češće pojavljivati kod hakera, ne postoji jedinstven profil koji bi opisivao sve računalne kriminalce (Campbell i Kennedy, 2014).

7.3. Motivacija počinitelja

Jedan od najjednostavnijih pristupa razumijevanju mentalnog sklopa računalnih kriminalaca je da sami počinitelji opišu svoje motive vlastitim riječima. Korištenjem različitih metoda samoprijavljivanja, uključujući ankete, upitnike s otvorenim pitanjima i intervjue licem u lice, istraživači su dosljedno pronalazili niz uobičajenih objašnjenja koja računalni kriminalci koriste kako bi opravdali svoje nezakonito ponašanje (Chiesa i sur., 2008).

Prema sociologu Paulu Tayloru (1999; prema Campbell i Kennedy, 2014), računalni kriminalci navode da motivaciju pronalaze u međusobnom djelovanju šest glavnih kategorija: ovisnost, znatiželja, dosada, moć, priznanje i politika. Korištenjem fenomenološko-interpretativnog pristupa intervjuiranju koji naglašava percepciju stvarnosti od strane intervjuirane osobe, sociologinja Orly Turgeman-Goldschmidt (2005) također je otkrila da računalni kriminalci navode znatiželju, traženje uzbuđenja i potrebu za moći kao motive za svoje ponašanje. Taylor (1999; prema Campbell i Kennedy, 2014) sugerira da opsežna upotreba računala od strane tih kriminalaca može biti rezultat kombinacije kompulzivnog ponašanja i intelektualne znatiželje. Iz perspektive vanjskog promatrača, potreba naprednog korisnika računala da zadovolji brzo mijenjajuće zahtjeve računalne industrije može se činiti kao pokazatelj računalne zloupotrebe, dok je zapravo stalna upotreba tehnologije posljedica prirode tog područja. Neprestana znatiželja i želja za tehnološkim napretkom također se često koriste kao motivacija računalnih kriminalaca (Taylor, 1999; prema Campbell i Kennedy, 2014) .

U jednom od najambicioznijih pokušaja razumijevanja mentalnog sklopa računalnih kriminalaca, konzultant za računalnu sigurnost i bivši računalni kriminalac Raoul Chiesa i njegovi kolege pokrenuli su Projekt profiliranja hakera (eng. Hackers Profiling Project - HPP). Cilj HPP-a bio je, korištenjem tehnika profiliranja, razviti sveobuhvatan profil hakera. Raoul Chiesa razvio je upitnik koji je distribuiran poznatim hakerima, a pitanja su se odnosila na osobne demografske podatke, tehnološke vještine, povijest kriminala i društvene odnose. Istraživanje je pokazalo da su neki od glavnih motiva hakera znatiželja, osjećaj avanture te dokazivanje vlastite vrijednosti sebi i drugima. Navedeni su motivi također povezani s osjećajima bijesa, frustracije i pobune protiv autoriteta (Chiesa i sur., 2008).

Suprotno njihovim stereotipnim prikazima u medijima i fikciji, čini se da računalni kriminalci imaju podosta široke društvene mreže kako u *online*, tako i u *offline* svijetu. Potreba za moći i

priznanjem od strane njihovih vršnjaka može biti motivirajući faktor za neke računalne kriminalce (Campbell i Kennedy, 2014).

Motive za počinjenje računalnog kriminaliteta moguće je podijeliti i ovako (The Institute of Company Secretaries of India, 2016):

1. **Ekonomski motivirani računalni kriminalitet:**

Kao i kod mnogih tradicionalnih zločina, novac je glavni motiv za mnoga računalna kaznena djela. Budući da su opasnosti kriminala manje očite kada se počinitelj krije iza mreže, percepcija niskog rizika i potencijalno visokih financijskih nagrada poticaj je mnogima za ulazak u računalni kriminalitet. Na primjer, procjene pokazuju da kriminalci koji ciljaju na *online* bankovne račune godišnje zarađuju oko 700 milijuna dolara na globalnoj razini.

2. **Ideološki motivirani računalni kriminalitet:**

Nakon što su financijske tvrtke poput Visa, MasterCard i PayPal odbile omogućiti korisnicima da doniraju kontroverznoj neprofitnoj organizaciji WikiLeaks, hakerska grupa *Anonymous* organizirala je niz napada botovima[16] na servere tih tvrtki, čineći ih nedostupnim za korisnike interneta. Ovakvi napadi provode se iz etičkih, ideoloških ili moralnih razloga, kako bi se izrazilo nezadovoljstvo prema pojedincima, korporacijama, organizacijama, a čak i vladama.

3. **Situacijski motivirani računalni kriminalitet:**

Osim motiva samih kriminalaca, okruženje u kojem se odvija računalni kriminalitet također doprinosi njegovoj rasprostranjenosti. Sve više osobnih i osjetljivih informacija pohranjuje se *online*, što povećava potencijalne nagrade za počinitelje. Primjerice, antivirusna tvrtka Norton navodi da je čak 41% računala u 2012. godini bilo bez ažurirane sigurnosne zaštite.

4. **Osobno motivirani računalni kriminalitet:**

Računalni kriminalitet često je rezultat osobnih emocija i osvete. Od nezadovoljnog zaposlenika koji instalira virus na uredska računala do tinejdžera koji hakira web stranicu škole samo da dokaže da može, mnogi su zločini zapravo zločini iz strasti počinjeni putem interneta.

[16] Bot je program dizajniran za potpuno automatizirano obavljanje ponavljajućih zadataka na web stranicama. Zlonamjerni botovi su napravljeni za izvođenje raznih štetnih aktivnosti i predstavljaju glavni izvor sigurnosnih prijetnji na web stranicama. Ti napadi mogu varirati od manjih, poput kopiranja cijena i lažnog klikanja na oglase, do ozbiljnijih, poput krađe podataka o kreditnim karticama (Ur Rahman i Tomar, 2020).

7.4. Analiza i značajnost tipologija

Analiza navedenih tipologija računalnih kriminalaca kroz nekoliko desetljeća ukazuje na značajan napredak u klasifikaciji ove specifične vrste kriminala, kao i na napredak u razumijevanju samih počinitelja. Od početnih pokušaja kategorizacije u 1980-ima do suvremenih i sveobuhvatnijih modela, primjećuje se razvoj pristupa, pri čemu su autori nadograđivali prethodna znanja i prilagođavali ih promjenama u tehnologiji i društvu.

Kontinuirano prepoznavanje i naglašavanje različitih razina stručnosti pristupnih kod računalnih kriminalaca ono je što se smatra jednim od pozitivnih aspekata ovih tipologija. Počevši od „script-kiddiesa“, termina koji se često spominjao u više tipologija, s niskim tehničkim znanjem, pa sve do sofisticiranih državnih hakera, većina ja autora prikazalo širok spektar znanja i vještina koje ovakvi kriminalci posjeduju. Ove spoznaje mogu pomoći u prilagođavanju strategija borbe protiv računalnih prijetnji jer omogućuju raznolik pristup koji uzima u obzir specifičnosti svake kategorije. Također, tipologije su s vremenom postajale sveobuhvatnije, uključujući različite aspekte računalnog kriminaliteta koje prethodne klasifikacije nisu u potpunosti obuhvatile. Na primjer, kasnije tipologije prepoznaju ne samo kriminalne aktivnosti usmjerene na neposrednu financijsku dobit, već i one s dugoročnim ciljevima poput špijunaže, političkih ili ideoloških motiva. Upravo to i potvrđuje da su autori prilagođavali svoje tipologije razvoju tehnologije, pojavi novih vrsta kaznenih djela u domeni računalnog kriminaliteta, ali i promjenama u društvu koje su se istovremeno pojavljivale. Širina spoznaje o razinama stručnosti može stručnjacima za sigurnost omogućiti bolje razumijevanje konteksta u kojem se *online* napadi događaju i primjenu odgovarajućih mjera zaštita, ne samo protiv trenutno poznatih prijetnji, već i protiv potencijalnih budućih rizika. Također, uzimajući u obzir motivaciju počinitelja, može se pridonijeti dubljem razumijevanju različitih vrsta kriminalaca i njihovih ponašanja. Na taj način tipologije postaju ne samo preciznije, već i korisnije za razvijanje učinkovitih strategija prevencije i suzbijanja kriminala. Campbell i Kennedy (2014) predlažu proaktivni pristup koji se sastoji od uspostavljanja legalnih mreža za hakiranje za početnike što korisnicima omogućuje eksperimentiranje na legalan način. Omogućavanje sigurnih prostora za hakiranje gdje početnici, a čak i *cyberpunks*-i, imaju neograničen pristup mrežama i programima, moglo bi smanjiti psihološki otpor koji dolazi od strogih ograničenja pristupa računalima i resursima. Takve legalne mreže za hakiranje također bi usmjerile korisnike na tehničke aspekte računarstva i tradicionalne hakerske aktivnosti, umjesto na pokušaje probijanja sustava. Usmjeravanjem znatiželje adolescenata prema

legalnim hakerskim i tehničkim aktivnostima unutar otvorene mreže, korisnici bi mogli biti manje skloni upuštanju u kriminalne aktivnosti (Campbell i Kennedy, 2014). Slično primjećuju Shaw i Stock (2011; prema Campbell i Kennedy, 2014) koji su htjeli suzbiti prijetnju zlonamjernih *insajdera.* Autori smatraju da se uvođenjem sveobuhvatnijih metoda provjere zaposlenika, koje uključuju analizu društvenih medija, provjere prošlosti, testiranje na zlouporabu supstanci te psihološke procjene, može smanjiti rizik od krađe intelektualnog vlasništva. Dodatno, jedan od učinkovitijih i isplativijih načina smanjenja krađe IP-a mogao bi biti putem povećanja svijesti zaposlenika o sporazumima o povjerljivosti podataka i osvještavanje posljedica kršenja tih sporazuma (Shaw i Stock, 2011; prema Campbell i Kennedy, 2014).

Jedan od glavnih nedostataka navedenih tipologija, kojeg su čak i mnogi autori naglašavali, jest nedovoljna preciznost u korištenju termina „haker“. U početku je opisivao jako vještog programera i tehničara, s vremenom je dobio negativnu konotaciju, a čak se koristio i za imenovanje počinitelja raznih vrsta kaznenih djela u *online* prostoru. Iako je i Rogers (2006), jedan od najznačajnijih autora u ovom području, primijetio kako se termin „haker“ koristio za grupiranje svih računalnih kriminalaca u jednu opću kategoriju, naziv se nastavljao koristiti. Navedeno je moguće primijetiti u posljednjoj tipologiji koja je navedena, ona od strane autora Chng-a i suradnika (2022) koji su u svojoj tipologiji također koristili navedeni termin, dok „tipovi“ u toj klasifikaciji koriste različite strategije, odnosno čine različita kaznena djela. To stvara problem u primjeni tipologija na međunarodnoj razini, što je vidljivo na primjeru Hrvatske u kojoj se *hakiranje* definira isključivo kao neovlašteni pristup računalnim sustavima. Kako bi se razvili odgovarajući kriminološki pristupi računalnom kriminalu, važno je empirijski analizirati međunarodne podatke o počiniteljima računalnih zločina. Posebnu pažnju treba posvetiti ispitivanju uvjeta u zemlji iz koje počinitelji potječu, kao i uvjeta u zemlji u kojoj nanose štetu i gdje su suočeni s kaznenim progonom. Također, potrebno je usporediti ova okruženja u njihovoj složenosti, uzimajući u obzir različite čimbenike koji mogu poticati ili sprječavati računalni kriminal (Hadzhidimova i Payne, 2019). Vidljiv je još jedan nedostatak koji ističe kako ipak neke tipologije nisu prilagodljive brzim promjenama u tehnologiji i metodama kojima se služe računalni kriminalci. Neki modeli ne uzimaju u obzir najnovije

oblike prijetnji poput *deepfake*[17] tehnologije ili naprednih oblika socijalnog inženjeringa[18], što može dovesti do zastare postojećih tipologija. Pojavom umjetne inteligencije pojavili su se ne samo nove vrste kriminalnih djela, već i drugačiji profili počinitelja računalnog kriminaliteta. Prisustvo problema i izazova kao rezultat pojave umjetne inteligencije vjerojatno je koliko za samu sigurnost pojedinaca, sustava i kritičnih infrastruktura, toliko i za samo zakonodavstvo i kazneni progon.

Sve veći broj tipologija počinitelja računalnog kriminaliteta, koji postaju sve složeniji kako se zločini i počinitelji razvijaju, obuhvaća različite motive, osobine ličnosti, metode i sposobnosti. Nije sporno da poznavanje tipologije počinitelja pruža sveobuhvatniji okvir za bolje razumijevanje i otkrivanje zločina, no zbog anonimne prirode računalnih kriminalaca i oslanjanje na podatke počinitelja koji su uhvaćeni, što predstavlja manjinu, teško je potvrditi značajnost ovih tipologija (Curtis i Oxburgh, 2022).

[17] Deepfake označava prividno realistične, ali lažne slike, audiozapise, videozapise i druge digitalne medije proizvedene metodama umjetne inteligencije. Realistične deepfake slike i videozapisi mogu se koristiti za zaobilaženje prepoznavanja lica, stvaranje političkih nemira i lažnih vijesti, ucjenjivanje, i sl. (Zhang, 2022)
[18] Socijalni inženjering je vještina manipuliranja korisnika da kompromitiraju informacijske sustave. Umjesto tehničkih napada na sustave, socijalni inženjeri ciljaju ljude s pristupom informacijama, manipulirajući ih da otkriju povjerljive podatke ili čak da izvrše njihove zlonamjerne napade. Tehničke mjere zaštite obično su neučinkovite protiv ove vrste napada (Krombholz, Hobel, Huber i Weippl, 2014).

8. ZAKLJUČAK

Internet povezuje ljude širom svijeta, stvarajući neviđene mogućnosti za komunikaciju, trgovinu i obrazovanje. Međutim, ta globalna povezanost također otvara vrata kibernetičkim zločinima, koji su postali ozbiljan problem na globalnoj razini. Ovi zločini utječu na različite aspekte ljudskog života, uključujući privatnost, sigurnost podataka, financijske transakcije i osobnu sigurnost (Varshney, Munjal, Jash, Bhattacharya i Saboo, 2020).

Motivacija igra ključnu ulogu u razumijevanju ponašanja računalnih kriminalaca i njihove sklonosti prema određenim vrstama kaznenih djela. Prema brojnim istraživanjima i tipologijama, motivi kriminalaca variraju od osobnih do situacijskih, a najčešće se svode na četiri glavne kategorije: ekonomske, ideološke, situacijske i osobne motive. Ekonomska motivacija, poput želje za brzom i lakom zaradom, jedan je od najčešćih motiva. Kao i kod tradicionalnih zločina, novac često predstavlja glavni poticaj, a percepcija niskog rizika uz visoku potencijalnu nagradu dodatno pojačava ovu vrstu kriminaliteta. Ideološki motivirani kriminalci, s druge strane, često koriste svoje vještine kako bi promovirali ili branili određene političke ili moralne stavove, primjerice napadima na korporacije ili vladine institucije. Situacijski motivi uključuju okolnosti u kojima su osjetljive informacije lako dostupne, dok osobni motivi često proizlaze iz želje za osvetom ili dokazivanjem svojih sposobnosti. Različiti autori, poput Taylora (1999; prema Campbell i Kennedy, 2014) i Turgeman-Goldschmidt (2005), ukazuju na to da motivi poput znatiželje, potrebe za moći, priznanja i avanture također imaju značajnu ulogu. Chiesa i suradnici (2008), kroz svoj Hackers Profiling Project, naglašavaju da su ovi motivi često povezani s osjećajima bijesa i frustracije, što dodatno ukazuje i na složenost motivacija te potrebu za daljnjim istraživanjima istih. Motivacija računalnih kriminalaca nije niti jednostavna niti jednoznačna. Razumijevanje ovih složenih poticaja ključno je za razvoj učinkovitijih preventivnih mjera te boljih strategija za otkrivanje, praćenje i rehabilitaciju počinitelja.

Individualne karakteristike računalnih kriminalaca odražavaju složenost njihove ličnosti i motivacija. Istraživanja ukazuju na to da računalni kriminalci nisu homogena skupina, već da postoji širok raspon osobina koje mogu utjecati na njihovo ponašanje i pristup kaznenim djelima. Jedna od ključnih osobina koja se često spominje je visoka inteligencija i visoka razina tehničkih vještina, što im omogućava savladavanje kompleksnih sustava i tehnoloških izazova. Međutim, istovremeno, neki računalni kriminalci pokazuju antisocijalne osobine, poput

nedostatka empatije, površnog šarma i neiskrenosti, što su karakteristike koje se često povezuju s antisocijalnim poremećajem ličnosti. Istraživanja također sugeriraju da su mnogi računalni kriminalci skloni psihopatskim osobinama, uključujući antagonizam, dezinhibiciju i narcizam. Demografski, stereotipni profil računalnog kriminalca često uključuje mladog muškarca, bijele rase, socijalno izoliranog i s disfunkcionalnim obiteljskim pozadinama, no ovaj profil nije uvijek točan. Na primjer, hakeri su često opisani kao tinejdžeri ili mladi odrasli, ali neka istraživanja pokazuju da su osuđeni računalni kriminalci obično stariji, prosječne dobi od oko 38 godina. Osim toga, računalni su kriminalci povezani i s Aspergerovim sindromom, osobito hakeri. Osobe s Aspergerovim sindromom često imaju intenzivne preokupacije intelektualnim interesima, poput tehnologije, što ih može navesti na računalni kriminal. Međutim, važno je napomenuti da ne postoji empirijski dokaz koji bi potvrdio uzročnu vezu između Aspergerovog sindroma i računalnog kriminala, iako određene karakteristike mogu povećati sklonost ka takvom ponašanju. U konačnici, individualne karakteristike računalnih kriminalaca su raznolike i često odstupaju od popularnih stereotipa, što upućuje na potrebu za detaljnijim i prilagođenijim pristupom u razvijanju profila počinitelja.

Kroz analizu različitih tipologija računalnih kriminalaca, očita je složenost ovog fenomena. U početku su tipologije bile jednostavne, temeljene na osnovnim tehničkim vještinama, no s vremenom su se razvijale kako bi obuhvatile širi spektar motiva i ciljeva počinitelja. Jedan od ključnih doprinosa razvoju tipologija računalnih kriminalaca bio je rad autora Rogersa, čiji je model iz 2006. godine značajno unaprijedio razumijevanje različitih razina stručnosti među hakerima. Rogers (2006) je jasno razlikovao „script kiddiesa“ s osnovnim znanjem od sofisticiranih profesionalaca te državnih hakera, pružajući korisnu klasifikaciju koja i danas služi kao referentni model. Ovaj pristup omogućio je bolju analizu metoda napada i bolje razumijevanje strategija koje računalni kriminalci koriste. Suvremene tipologije nadograđuju ovu osnovu, uključujući analize motivacije, socijalnih i psiholoških čimbenika koji utječu na ponašanje računalnih kriminalaca, što dovodi do dubljeg razumijevanja raznih vrsta kriminalaca i njihovih ciljeva, od financijskih do političkih i ideoloških. Međutim, istraživanja o računalnom kriminalitetu suočavaju se s izazovima poput nedostatka integracije ljudskih čimbenika i dugoročnih studija o motivacijama počinitelja. Pristupi su često razdvojeni i ne povezuju različite discipline, što otežava sveobuhvatno razumijevanje problema. Da bi se unaprijedila istraživanja i razvile učinkovite strategije, potrebno je primijeniti multidisciplinarni pristup koji uključuje stručnjake iz područja kriminologije, psihologije, informatike i prava te osigurati longitudinalne studije koje će pratiti promjene u ponašanju

počinitelja. Analizom različitih tipova počinitelja moguće je razviti ciljane strategije prevencije, kao što su edukacijski programi i promicanje legalnih hakerskih aktivnosti, što može smanjiti privlačnost kriminalnih aktivnosti među mladima. Proučavanje specifičnih metoda napada može poboljšati sposobnost otkrivanja prijetnji, dok razumijevanje motiva i razina stručnosti počinitelja može doprinijeti razvoju strategija za rehabilitaciju i tretman. Iako su tipologije postale složenije i sveobuhvatnije, još uvijek postoje izazovi. Na primjer, preciznost u terminologiji, kao što je upotreba pojma „haker“, može dovesti do nejasnoća, a mnoge tipologije još uvijek ne obuhvaćaju najnovije prijetnje poput deepfake tehnologije ili naprednih metoda socijalnog inženjeringa. Mnoge tipologije oslanjaju se na male uzorke uhvaćenih počinitelja, što ograničava njihovu primjenjivost i može zanemariti sofisticiranije kriminalce koji nisu uhvaćeni. Ovi nedostaci naglašavaju potrebu za daljnjim istraživanjima i razvojem ažuriranih, sveobuhvatnih tipologija koje bolje odražavaju stvarnost računalnog kriminala i omogućuju učinkovitiju prevenciju i kazneni progon. Kontinuirani rad na unapređenju tipologija može pomoći u prilagodbi novim prijetnjama i promjenama u tehnologiji, čime doprinosi boljem razumijevanju i pristupu ovom području.

Kako elektroničke komunikacije i digitalne tehnologije napreduju, računalni napadi i njegovi počinitelji postaju sve sofisticiraniji, usmjeravajući se na ključnu infrastrukturu i financijske sustave, uključujući i vladine agencije. Prema izvještaju Vlade Republike Hrvatske iz 2024. godine, računalni kriminalitet se prepoznaje kao ozbiljna i rastuća prijetnja koja može značajno ugroziti gospodarski i društveni razvoj zemlje. Da bi se efikasno borila protiv tih prijetnji, Vlada ulaže značajna sredstva u tehnologiju i obuku. Ministarstvo unutarnjih poslova, kroz Nacionalni program oporavka i otpornosti, investira milijune eura u jačanje kibernetičke otpornosti, uključujući nabavku naprednih alata i tehnoloških rješenja za identifikaciju počinitelja i prikupljanje elektroničkih dokaza. Uz to, provode se kampanje za podizanje svijesti među građanima i tvrtkama, poput "Web heroj: Ulovimo lika s weba, koji tvoje eure vreba", koje educiraju o prijetnjama i zaštitnim mjerama. Nacionalni CERT[19] (eng. Computer Emergency Response Team) osnovan je 2007. godine, a nadležan je za upravljanje računalno-sigurnosnim incidentima koji uključuju entitete unutar Hrvatske ili su povezani s .hr domenom i hrvatskim IP adresnim prostorom. Nacionalni CERT ima ključnu ulogu u prevenciji i zaštiti od prijetnji u području računalne sigurnosti, a njegov glavni zadatak je obrada sigurnosnih incidenata kako bi se osigurala kibernetička sigurnost na nacionalnoj razini. Kao odgovor na

[19] Pristupljeno 23.08.2024.: https://gov.hr/hr/nacionalni-cert/1230?lang=hr.

rastuće prijetnje u *cyber* prostoru, Sigurnosno-obavještajna agencija[20] Republike Hrvatske (SOA) uspostavila je 2019. godine Centar za kibernetičku sigurnost s ciljem zaštite nacionalnog kibernetičkog okruženja. Zajedno sa Zavodom za sigurnost informacijskih sustava, razvila je program pod imenom SK@UT. SK@UT je ključni nacionalni sustav za otkrivanje, rano upozorenje i zaštitu od *cyber* prijetnji. Ovaj sustav se temelji na mreži senzora raspoređenih u važnim državnim institucijama i pravnim osobama, a omogućuje identifikaciju sofisticiranih napada u njihovim ranim fazama i u svim segmentima *cyber* prostora koje pokriva navedena mreža senzora. Ovi napori pokazuju ozbiljnost kojom se Hrvatska suočava s izazovima računalnog kriminaliteta, gradeći temelje za učinkovitiju zaštitu nacionalnog *cyber* prostora.

Računalni kriminalitet predstavlja složen i stalno rastući problem, posebno s pojavom novih oblika kaznenih djela. Mnoge prijetnje ostaju skrivene zbog anonimnosti digitalnog okruženja, što otežava njihovo otkrivanje i razumijevanje. Unatoč naporima da se razviju strategije za suzbijanje ovog problema, značajan dio računalnog kriminaliteta i dalje ostaje neotkriven i neistražen. S obzirom na kontinuirane promjene u digitalnom svijetu, ključno je razumjeti prirodu računalnog kriminala i njegovih počinitelja kako bi se stvorila sigurnija budućnost u kojoj će tehnologija služiti kao alat za stvaranje napretka, a ne kao izvor prijetnje.

[20]Sigurno-obavještajna agencija (n.d.). Pristupljeno 23.08.2024.:https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/.

9. LITERATURA

1. Ahmed, N., Amin, R., Aldabbas, H., Koundal, D., Alouffi, B., i Shah, T. (2022). Machine learning techniques for spam detection in email and IoT platforms: analysis and research challenges. *Security and Communication Networks*, *2022*(1). https://doi.org/10.1155/2022/1862888.

2. Akdemir, N., Sungur, B., i Başaranel, B. (2020). Examining the challenges of policing economic cybercrime in the UK. *Güvenlik Bilimleri Dergisi*, (International Security Congress Special Issue), 113-134. https://doi.org/10.28956/gbd.695956.

3. Alghawazi, M., Alghazzawi, D. i Alarifi, S. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal of Cybersecurity and Privacy, 2*, 764–777. https://doi.org/10.3390/jcp2040039.

4. Aurangzeb, S., Aleem, M., Iqbal, M. A. i Islam, M. A. (2017). Ransomware: A Survey and Trends. *Journal of Information Assurance and Security, 12*. Preuzeto 27.7.2024. sa https://www.researchgate.net/profile/Muhammad-Aleem-7/publication/317380115_Ransomware_A_Survey_and_Trends/links/5e19a33ea6fdcc283769077c/Ransomware-A-Survey-and-Trends.pdf.

5. Campbell, Q. i Kennedy, D. M. (2014). The Psychology of Computer Criminals. U Bosworth, S., Kabay, M. E. i Whyne, E. (Ur.), Computer Security Handbook. John Wiley & Sons, Inc.

6. Chiesa, R., Ducci, S., i Ciappi, S. (2008). *Profiling hackers*. Auerbach Publications.

7. Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., i Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education Online*, *11*(7).

8. Chng, S., Lu, H. Y., Kumar, A., i Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*. https://doi.org/10.1016/j.chbr.2022.100167.

9. Curtis, J., i Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573-592. https://doi.org/10.1177/0032258X221107584.

10. de Bruijne, M., Eeten, M. V., Gañán, C. H., i Pieters, W. (2017). Towards a new cyber threat actor typology. Preuzeto 27.7.2024. sa https://repository.wodc.nl/bitstream/handle/20.500.12832/2299/2740_Volledige_Tekst_tcm28-273243.pdf?sequence=1&isAllowed=y.

11. Donalds, C. i Osei-Bryson, K. M. (2018). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior, 92*, 403-418. doi:10.1016/j.chb.2018.11.039.

12. Dupont, B., Fortin, F., i Leukfeldt, R. (2024). Broadening our understanding of cybercrime and its evolution. *Journal of Crime and Justice*, 1-5.

13. Farahmand, F., Navathe, S. B., Sharp, G. P., i Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*, 203-225.

14. Franjić, Š. (2017). Kaznena djela računalnog kriminaliteta iz glave XXV. Kaznenog zakona u Republici Hrvatskoj. *Pravne teme, 10*, 105-114.

15. Graham, A. (2023). *Cybercrime: Traditional Problems and Modern Solutions*. [Diplomski rad]. Te Herenga Waka-Victoria University of Wellington. Preuzeto 3.8. 2024. sa https://openaccess.wgtn.ac.nz/articles/thesis/Cybercrime_Traditional_Problems_and_Modern_Solutions/22300909?file=39669757.

16. Groom, J. (2017). The Pirate Bay: CJEU rules that operating a torrent file indexing site is a communication to the public. *Journal of Intellectual Property Law & Practice, 12* (12), 965–968. https://doi.org/10.1093/jiplp/jpx176.

17. Hadzhidimova, L. I., i Payne, B. K. (2019). The profile of the international cyber offender in the US. *International journal of cybersecurity intelligence & cybercrime*, *2*(1), 40-55.

18. Harbinson, E., i Selzer, N. (2019). The risk and needs of cyber-dependent offenders sentenced in the United States. *Journal of Crime and Justice*, *42*(5), 582-598. https://doi.org/10.1080/0735648X.2019.1692422.

19. Henson, B. (2020). Routine Activities. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 469-489). Springer International Publishing.

20. Higgins, G.E. i Nicholson, J. (2020). The General Theory of Crime. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 567-581). Springer International Publishing.

21. Hirschi, T. (2004). Self-control and crime. *Handbook of self-regulation*, 537-552.

22. Holt, T. i Bossler, A. (2016). Cybercrime in Progress. New York: Routledge.

23. Holt, T. J., i Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant behavior*, *35*(1), 20-40.

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

25. Kranenbarg, M. W., Van Gelder, J. L., Barends, A. J., i de Vries, R. E. (2023). Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in human behavior*, *140*. https://doi.org/10.1016/j.chb.2022.107576.

26. Krombholz, K., Hobel, H., Huber, M., i Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

27. Loper, D. K. (2000). *The criminology of computer hackers: A qualitative and quantitative analysis*. [Doktorski rad]. Michigan State University. Preuzeto 3.8.2024. sa https://d.lib.msu.edu/etd/28359.

28. Matijević, G. i Avramović, Ž, Z. (2021). Kibernetički kriminalitet u Republici Hrvatskoj, kazneno-pravni okvir i stanje sigurnosti. U Avramović, Ž. Z. i Marinković D. (Ur.), ITeO Zbornik radova, (str. 114-126). Panevropski univerzitet Apeiron.

29. Mbanaso, U. M., i Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *17*(3), 17-24.

30. McBrayer, J. (2014). *Exploiting the digital frontier: hacker typology and motivation*. [Doktorski rad]. The University of Alabama.

31. Microsoft (2024). What is a DDoS attack? Preuzeto 2.8.2024. sa https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack.

32. Ministarstvo unutarnjih poslova (2020). Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2019. godini. Preuzeto 20.6.2024. sa https://mup.gov.hr/UserDocsImages/statistika/Statisticki_pregled_2019_WEB.pdf.

33. Ministarstvo unutarnjih poslova (2021). COVID i kriminalitet u 2020. - Komentar pokazatelja sigurnosti u Republici Hrvatskoj. Preuzeto 20.6.2024. sa https://mup.gov.hr/UserDocsImages/2021/04/Covid%20i%20kriminalitet%20u%202020%20-%20Komentar%20pokazatelja%20sigurnosti%20u%20Republici%20Hrvatskoj.pdf.

34. Ministarstvo unutarnjih poslova (2022). Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2021. godini. Preuzeto 20.6.2024 sa

https://mup.gov.hr/UserDocsImages/statistika/2022/Statisticki_pregled_2021_Web.pdf.

35. Ministarstvo unutarnjih poslova (2024). Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2023. godini. Preuzeto 20.6.2024 sa https://mup.gov.hr/UserDocsImages/statistika/2024/3/Statisticki_pregled_2023_.pdf.

36. Moeckel, C. (2019). Examining and constructing attacker categorisations: An experimental typology for digital banking. *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*. ACM. https://doi.org/10.1145/3339252.334034.

37. Moitra, S. D. (2004). Cybercrime: Towards an Assessment of its Nature and Impact. *International Journal of Comparative and Applied Criminal Justice, 28*(2), 105–123. doi:10.1080/01924036.2004.967871.

38. Moon, B., McCluskey, J. D., i McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, *38*(4), 767-772.

39. National Institute of Standards and Technology. (n.d.). Web bug. *NIST Computer Security Resource Center*. Preuzeto 2.8.2024. sa https://csrc.nist.gov/glossary/term/web_bug.

40. Navarro, J. N. i Marcum, C.D. (2020). Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime .U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 527-545). Springer International Publishing.

41. Ning, H., Ye, X., Bouras, M. A., Wei, D., i Daneshmand, M. (2018). General cyberspace: Cyberspace and cyber-enabled spaces. *IEEE Internet of Things Journal*, *5*(3), 1843-1856.

42. Oxford Learner's Dictionaries, 2024. Preuzeto 20.05.2024. sa https://www.oxfordlearnersdictionaries.com/definition/english/hacker.

43. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., i Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

44. Rahman, R. U., i Tomar, D. S. (2020). A new web forensic framework for bot crime investigation. *Forensic Science International: Digital Investigation*, *33*. https://doi.org/10.1016/j.fsidi.2020.300943.

45. Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, *3*(2), 97-102.

46. Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital investigation*, *14*, 36-45.

47. Seigfried-Spellar, K. C., Villacís-Vukadinović, N., i Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, *51*, 67-73.

48. Seigfried-Spellar, K.C. i Treadway, K.N. (2014) Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences, *Deviant Behavior, 35*(10), 782-803. doi: 10.1080/01639625.2014.884333.

49. Sigurno-obavještajna agencija (n.d.). Preuzeto 23.08.2024 sa https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/.

50. Singh, A., Choudhary, P., Singh, A. K. i Tyagi, D. K. (2021). Keylogger detection and prevention. *Journal of Physics: Conference Series*, *2007* (1). Preuzeto 3.8.2024. sa https://iopscience.iop.org/article/10.1088/1742-6596/2007/1/012005/pdf.

51. Stapley, E., O'Keeffe, S., & Midgley, N. (2022). Developing typologies in qualitative research: The use of ideal-type analysis. *International Journal of Qualitative Methods*, *21*. https://doi.org/10.1177/16094069221100633.

52. Steinmetz, K. F. (2016). Hacked: A radical approach to hacker culture and crime. New York: NYU Press. Preuzeto 3.8.2024. sa https://books.google.hr/books?hl=hr&lr=&id=xdQ3DQAAQBAJ&oi=fnd&pg=PR11&dq=Steinmetz+KF+(2016)+Hacked:+A+Radical+Approach+to+Hacker+Culture+and+Crime.+New+York:+NYU+Press,+Vol.+2.&ots=Mhn7mY9c5J&sig=sZXEiECUxWciCZB4FTEUhVgv5UE&redir_esc=y#v=onepage&q&f=false.

53. The Institute of Company Secretaries of India. (2016). *Cyber crime: Law and practice*. The Institute of Company Secretaries of India. Preuzeto 26.7.2024. sa https://www.icsi.edu/media/webmodules/publications/Cyber_Crime_Law_and_Practice.pdf.

54. Thomas, D., i Loader, B. (Ur.). (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. Psychology Press.

55. Tseng, C. W., i Yang, C. S. (2007). System support for web hosting services on server clusters. *Computers & Electrical Engineering*, *33*(3), 208-220.

56. Turgeman-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review, 23*(1), 8-23. https://doi.org/10.1177/0894439304271529.

57. Tusikov, N. (2019). Regulation through "bricking": private ordering in the "Internet of Things". *Internet Policy Review, 8*(2). https://doi.org/10.14763/2019.2.1405.

58. Vlada Republike Hrvatske (2024). Izvješće o radu policije u 2023. godini.

59. Wall, D. (Ed.). (2001). Crime and the Internet. New York: Routledge.

60. Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J. L., i Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of developmental and life-course criminology, 4*, 343-364.

61. Woo, H. J. (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities.* [Doktorski rad]. University of Georgia.
62. Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu – NN 9/2002. Preuzeto 03.06.2024. sa https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html.

63. Zhang, T. (2022). Deepfake generation and detection, a survey. *Multimedia Tools and Applications*, *81*(5), 6259-6276.

64. Zieni, R., Massari, L. i Calzarossa, M. C. (2023). Phishing or Not Phishing? A Survey on the Detection of Phishing Websites. *IEEE Access, 11,* 18499 - 18519. doi: 10.1109/ACCESS.2023.3247135.

65. Zuhri, F.A. (2016). The Profile of a Cybercriminal. *Digital Forensic Magazine.*