Cyber kriminalitet u pandemiji korona virusa

Popović, Lea

Sveučilište u Zagrebu
Edukacijsko-rehabilitacijski fakultet

Diplomski rad

Cyber kriminalitet u pandemiji koronavirusa

Lea Popović

Zagreb, rujan, 2022.

Sveučilište u Zagrebu
Edukacijsko-rehabilitacijski fakultet

Diplomski rad

Cyber kriminalitet u pandemiji koronavirusa

Lea Popović

Izv. prof. dr. sc. Dalibor Doležal

Zagreb, rujan, 2022.

Izjava o autorstvu rada

Potvrđujem da sam osobno napisala rad *Cyber* kriminalitet u pandemiji koronavirusa 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: Lea Popović
Mjesto i datum: Zagreb, rujan, 2022.

Naslov rada: *Cyber* kriminalitet u pandemiji koronavirusa

Studentica: Lea Popović

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

Program/modul: Socijalna pedagogija/Odrasli

SAŽETAK

Ljudska je svakodnevica postala gotovo neodvojiva od interneta i tehnologije što je olakšalo brojne aspekte života, ali ujedno i stvorilo rizike za počinjenje kaznenih djela iz područja *cyber* kriminaliteta. Čovječanstvo se 2020. godine našlo u novoj situaciji s prvim globalnim zatvaranjima čiji je cilj bio zaštititi ljudsko zdravlje od bolesti COVID-19 zbog čega je uloga tehnologije i interneta postala još izraženija. Ciljevi rada bili su: 1) opisati *cyber* kriminalitet (definirati pojam, razvoj i fenomenologiju *cyber* kriminaliteta, objasniti različitost u odnosu na tradicionalni kriminalitet, definirati međunarodni i nacionalni kaznenopravni okvir) te 2) istražiti pojavne oblike *cyber* kriminaliteta (i njihove promjene) u razdoblju pandemije koronavirusa uzevši u obzir situacijske čimbenike (poput prelaska na daljinski rad i *online* nastavu) i mogućnosti za prevenciju. Pokazalo se da su *cyber* kriminalci uključili COVID-19 u svoje napade i prijevare iskorištavajući ljudsku znatiželju i strah preko phishing poruka, neželjene pošte, mobilnih aplikacija, širenja dezinformacija i lažnih vijesti te malicioznih softvera i domena vezanih uz koronavirus. Pojavni oblici *cyber* kriminaliteta u doba pandemije postali su sofisticiraniji što se posebno odnosi na metode phishinga, ugrožavanje poslovne e-pošte i ransomware napade. *Cyber* kriminalitet je u svojoj srži uglavnom ostao isti, ali su se metodama društvenog inženjeringa mijenjale specifičnosti kriminalnog pristupa kako bi bile usklađenije s društvenim kontekstom što osigurava veću uspješnost napada. Prema inozemnim i nacionalnim podacima, broj kaznenih djela iz područja *cyber* kriminaliteta pokazuje uzlazan trend u razdoblju od 2017. do 2021. godine.

Ključne riječi: *cyber* kriminalitet, fenomenologija, kaznenopravni okvir, pandemija koronavirusa

Title: Cybercrime in coronavirus pandemic

Student: Lea Popović

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

The program/module: Social Pedagogy/Adults

SUMMARY

Human everyday life has become almost inseparable from the Internet and technology, which has facilitated numerous aspects of life but at the same time created risks for the commission of criminal offenses in the field of cybercrime. In 2020, humanity found itself in a new situation with the first global lockdowns whose goal was to protect human health from the COVID-19 disease which is why the role of technology and the Internet became even more pronounced. The objectives of the paper were: 1) to describe cybercrime (to define the term, development and phenomenology of cybercrime, to explain the difference in relation to traditional crime, to define the international and national criminal law framework) and 2) to investigate the emerging forms of cybercrime (and their changes) in the period of the coronavirus pandemic, taking into account situational factors (such as the transition to remote work and online classes) and opportunities for prevention. Cybercriminals have incorporated COVID-19 into their attacks and scams by exploiting people's curiosity and fear through phishing messages, spam, mobile apps, the spread of disinformation and fake news and coronavirus-related malware and domains. The emerging forms of cybercrime in the era of the pandemic have become more sophisticated, which especially refers to phishing methods, compromising business e-mails and ransomware attacks. Cybercrime in its core has mostly remained the same but the specifics of the criminal approach have changed with social engineering methods in order to be more aligned with the social context, which ensures a higher success rate of attacks. According to foreign and national data, the number of criminal offenses in the field of cybercrime shows an upward trend in the period from 2017 to 2021.

Keywords: cybercrime, pandemic, phenomenology, criminal law framework

SADRŽAJ

1.Uvod

Dosezi u razvoju tehnologije i informacijsko komunikacijske tehnologije čovječanstvu iz godine u godinu pružaju naprednije mogućnosti, od novih modela prijenosnih računala i mobilnih uređaja pa sve do modernih kućanskih uređaja s novim značajkama i namjenama. Razne baze podataka, datoteke i dokumenti u vlasništvu vlada, organizacija, tvrtki i pojedinaca digitalizirani su te se koriste i pohranjuju na računalima. Ljudska je svakodnevica postala gotovo neodvojiva od interneta i tehnologije čime su brojni aspekti života znatno olakšani, od uobičajenih aktivnosti poput traženja informacija jednostavnom Google pretragom pa sve do nešto zahtjevnijih postupaka kao što je *online* kupovina. S druge strane, ova je isprepletenost otvorila velika vrata novim oblicima kaznenih djela, *cyber* kriminalitetu. Okolnost koja problem *cyber* kriminaliteta čini relevantnim za područje socijalne pedagogije je činjenica da se djeca i mladi svakodnevno služe internetom i društvenim mrežama. S obzirom na već spomenutu veliku ulogu interneta u ljudskoj svakodnevici i funkcioniranju, na sve raniji kontakt djece s internetom koji potencijalno može pridonijeti njihovu postanku žrtvom, ali i budućim počiniteljima ovakvih kaznenih djela te rastuću raširenost *cyber* kriminaliteta, velika je vjerojatnost da će socijalni pedagozi u budućnosti sve češće u praksi nailaziti na *cyber* kriminalce i njihove žrtve.

Pojavom koronavirusa 2019. godine i njegove pandemije 2020. godine koja je uzrokovala globalna zatvaranja, tzv. *lockdown*-ove, čovječanstvo je dodatno ovisilo o informacijsko komunikacijskoj tehnologiji koja je na neki način postala oslonac za nastavak funkcioniranja uobičajenih ljudskih djelatnosti (tvrtke su prešle na rad od kuće, studenti i učenici na *online* nastavu, međuljudski odnosi održavali su se virtualno). Postavlja se logično pitanje: je li porast ljudskih aktivnosti na internetu uzrokovan pandemijom imao utjecaj na stope *cyber* kriminaliteta pružajući mu nove prilike?

Prvi će dio rada definirati pojam *cyber* kriminaliteta, opisati razvoj ove vrste kriminaliteta, objasniti različitost u odnosu na tradicionalni kriminalitet, njegovu specifičnost i fenomenologiju. U drugom dijelu rada bit će riječi o kaznenopravnom okviru, promotrit će se međuodnos cyber kriminaliteta i pandemije COVID-19 na svjetskoj i državnoj razini kao i potencijalno nastale promjene pojavnih oblika te prevencijske mogućnosti za nošenje s ovom vrstom kriminaliteta.

2. *Cyber* kriminalitet

2.1. Definiranje pojmova

Prema Oxford University Dictionary (2008), pojam *cyber* uključuje obilježja računalne kulture, informacijske tehnologije i virtualne stvarnosti. U prošlosti su se pojavili nazivi poput "*cyber* surfing" i "*cyber* shopping" koje su zamijenili nazivi "pretraživanje *weba"* i "*online* shopping" dok je prefiks *cyber* ostao u upotrebi kao oznaka za štetne i ilegalne aktivnosti kao što su npr. *cyber* uhođenje (eng. *cyber* stalking), *cyber* zlostavljanje (eng. *cyber* harassment) i *cyber* terorizam (Yar, 2006). Oxford Learner's Dictionaries (2022) *cyber* prostor (eng. *cyberspace*) opisuje kao zamišljeni prostor bez fizičke lokacije u kojem se odvija komunikacija preko računalnih mreža. U skladu s time, većina se *cyber* kriminaliteta odvija upravo u *cyber* prostoru. Ovaj je termin osmislio i popularizirao William Gibson 1984. godine u noveli Neuromancer gdje je predstavljao „*mentalno konstruirano virtualno okruženje u kojem se odvijaju aktivnosti umreženih računala*" te prema tome termin „*cyber* kriminalitet" u širem smislu opisuje kaznena djela koja se događaju unutar spomenutog prostora te simbolizira nesigurnost i rizik na internetu (Wall, 2007, str. 10). U hrvatskoj literaturi, *cyber* kriminalitet se najčešće nalazi pod pojmom "kibernetički kriminal" što potječe iz pogrešno prevedenog naziva konvencije Vijeća Europe iz 2001. godine, "Convention on *cybercrime*", čiji je cilj izjednačiti međunarodna kaznena zakonodavstva. Republika Hrvatska ratificirala je Konvenciju 2004. godine i uvela njene odredbe u svoj Kazneni zakon koristeći kibernetiku (eng. c*ybernetics*) kao istoznačnicu pojma *cybercrime* (Vojković i Štambuk-Sunjić, 2006) što terminološki ne može biti točno s obzirom da u hrvatskom jeziku ne postoji adekvatan prijevod riječi "*cyber*". Prema Hrvatskom jezičnom portalu *(2022),* kibernetika je *"znanost o istraživanju i automatskim sustavima kontrole u strojeva i živih bića"*. Izrazom "kibernetički kriminalitet" koriste se i godišnji statistički pregledi temeljnih sigurnosnih pokazatelja i rezultata rada (Ministarstvo unutarnjih poslova, 2020, 2021) dok se Glava Kaznenog zakona Republike Hrvatske posvećena *cyber* kriminalitetu naziva "*Kaznena djela protiv računalnih sustava, programa i podataka"* (Kazneni zakon, NN 125/11, 84/21). Zbog širine i općenitosti definicije kibernetike, izraz kibernetički kriminalitet ne može dostojno predstaviti ono što *cyber* kriminalitet podrazumijeva.

Drugi termin koji često nalazimo u hrvatskoj, ali i stranoj literaturi je računalni kriminalitet (eng. *computer crime*). Ovaj se naziv koristio za označavanje gotovo svih kriminalnih aktivnosti koje uključuju računala sve do kasnih devedesetih godina prošlog stoljeća. Terminologija se mijenjala usporedno s temeljitom transformacijom društva uzrokovanom korištenjem tehnologije i pristupačnošću iste. Istraživači poput Davida Walla (1998.; prema Holt i Bossler, 2016) koristili su izraz *"cyber* kriminalitet" za označavanje kaznenih djela izvršenih *online* dok je Grabosky (2001.; prema Holt i Bossler, 2016) rabio izraz računalni kriminalitet kako bi označio zlouporabu računala. Prema Britannica Dictionary (2022), izraz *online* odnosi se na "povezano s računalom, računalnom mrežom ili internetom ili učinjeno preko interneta". Među istraživačima i novinarima tog razdoblja, računalni kriminalitet i *cyber* kriminalitet koristili su se gotovo sinonimno (Furnell, 2002; Jordan i Taylor, 1998; Taylor, 1999; prema Holt i Bossler, 2016). Choi (2018; prema Choi, Lee i Louderback, 2020) navodi da je računalni kriminalitet potkategorija *cyber* kriminaliteta, ali ne nužno i njegov sinonim. Drugim riječima, *cyber* kriminalitet je krovni pojam računalnom kriminalitetu koji zahtijeva tek nešto više od osnovne razine vještina rada na računalu kako bi počinitelj viktimizirao druge korisnike računala. Razvojem tehnologije i povećanjem broja uređaja povezanih s internetom, zločini koji su nekoć bili ograničeni na računala, sada se mogu počiniti i upotrebom drugih tehnoloških uređaja čime termin računalni kriminalitet ponovno gubi na relevantnosti (Payne, 2020). Vojković i Štambuk-Sunjić (2006) smatraju da termin računalni kriminalitet ne obuhvaća sve oblike društveno neprihvatljivog ponašanja koje regulira Konvencija.

S obzirom da *cyber* kriminalitet kakav danas poznajemo ne bi postojao bez informacijsko komunikacijske tehnologije i računalnih sustava, bitno je naglasiti razliku između informacijske sigurnosti, sigurnosti informacijske i komunikacijske tehnologije (u daljnjem tekstu IKT sigurnosti) i *cyber* sigurnosti. Svima je zajednički cilj zaštita informacija pri čemu se *cyber* sigurnost izdvaja kao ključna u kontekstu *cyber* kriminaliteta s obzirom da se bavi zaštitom svih potencijalnih žrtava *cyber* napada: digitalnih informacija, informacijsko komunikacijske tehnologije i ljudi. Internacionalni standard ISO/IEC 27002, tj. standard Međunarodne udruge za standardizaciju/Međunarodnog elektrotehničkog povjerenstva (2005; prema Solms i Niekerk, 2013) definira informacijsku sigurnost kao očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija koje mogu biti u raznim oblicima (ispisane pisačem ili ručno na papiru, pohranjene elektronički, poslane poštom ili elektroničkim putem, prikazane filmom ili prenesene usmeno). Dok se informacijska

sigurnost bavi zaštitom informacija, IKT sigurnost orijentirana je na stvarne tehnološke sustave i infrastrukturu kojom se informacije procesiraju, pohranjuju i šalju zbog čega su informacijska sigurnost i IKT sigurnost iznimno usko povezane. Ovime zalazimo u područje *cyber* sigurnosti koja ih objedinjuje, ali i nadilazi s obzirom na ranjivosti i prijetnje s kojima se susreće (Solms i Niekerk, 2013). Međunarodna unija za telekomunikacije (ITU, 2008; prema Solms i Niekerk, 2013) *cyber* sigurnost definira kao: skup alata, politika, sigurnosnih koncepata, sigurnosnih zaštitnih mjera, smjernica, pristupa upravljanju rizikom, radnji, najboljih praksi, osiguranja i tehnologija koje se mogu koristiti za zaštitu *cyber* okruženja i organizacija te imovine korisnika. Imovina organizacije i korisnika podrazumijeva povezane računalne uređaje, osoblje, infrastrukturu, aplikacije, usluge, telekomunikacijske sustave te ukupnost prenesenih i/ili pohranjenih informacija. Rizici povezani s bilo kojim napadom ovise o tri čimbenika: prijetnjama (tko napada i s kojim ciljem), ranjivostima (slabosti koje su napadnute) i utjecajima (posljedicama napada). Upravljanje ovakvim rizicima smatra se osnovom učinkovite *cyber* sigurnosti (Fischer, 2016).

Povredom *cyber* sigurnosti može doći do kršenja povjerljivosti, cjelovitosti i dostupnosti informacija kao i u slučaju informacijske sigurnosti, međutim, ugroza ne prijeti samo informacijama i/ili tehnologiji kojom se informacije pohranjuju i prenose već svima onima koji djeluju u *cyber* prostoru: pojedincima, organizacijama i državama (Solms i Niekerk, 2013). Primjerice, u slučaju *cyber* zlostavljanja (eng. *cyber* bullying) nema spomenutog kršenja već je cilj napadača nauditi direktno pojedincu. Nadalje, svrha napada može biti ugrožavanje dobrobiti cijelog društva kao u slučaju *cyber* terorizma koji napada kritične infrastrukture države kojima ista stanovnicima pruža osnovne usluge (poput dostupnosti struje ili vode). Naposljetku, *cyber* sigurnost može se definirati kao zaštita samog *cyber* prostora, elektroničkih informacija, informacijsko komunikacijske tehnologije i korisnika *cyber* prostora uključujući sve njihove interese, bilo materijalne (npr. sigurnost kritične infrastrukture) ili apstraktne (npr. zaštita društvenih vrijednosti) koji su podložni napadima koji potječu iz *cyber* prostora (Solms i Niekerk, 2013).

S obzirom na sve izneseno u poglavlju i činjenicu da pokušaji prijevoda engleskih naziva i termina na druge jezike često ne mogu biti doslovno prevedeni na način da budu leksički, gramatički i profesionalno prihvatljivi (Škrtić, 2011; prema Protrka, 2018), ovaj će se rad služiti engleskom riječju *cyber* kojom će označavati vrstu kriminaliteta, prostor u kojem se odvija te vrstu *online* sigurnosti kao i neke od pojavnih oblika *cyber* kriminaliteta.

2.2. Razvoj *cyber* kriminaliteta

Uvođenje računalnih sustava temeljenih na tranzistorima šezdesetih godina prošlog stoljeća dovelo je do porasta upotrebe računalne tehnologije s obzirom da su postali manji i jeftiniji u odnosu na računalne sustave s vakuumskom cijevi. U ovoj ranoj fazi, kaznena djela ograničena su na fizičko oštećivanje računalnih sustava i pohranjenih podataka (McLaughlin, 1978; prema ITU, 2012). Sedamdesetih godina fizička šteta i dalje ostaje učestali oblik kaznene zlouporabe računalnih sustava, ali se pojavljuju i novi oblici računalnog kriminaliteta koji se odnose na nezakonitu uporabu računalnih sustava i manipulacije elektroničkim podacima. Prijelaz s ručnih na računalno upravljane transakcije doveo je do još jednog novog oblika kriminala: računalne prijevare. S obzirom na financijske gubitke i širenje problema, u raznim se dijelovima svijeta počinje raspravljati o mogućim pravnim rješenjima. Izraz "računalni kriminalitet" počinje označavati zlouporabu računala i podataka (Parker, 1976; prema Holt i Bossler, 2016). Jedan od prvih zakona o računalnim kaznenim djelima u SAD-u donesen je 1978. godine čime je svaki neovlašteni pristup računalnim sustavima proglašen kaznenim djelom trećeg stupnja (Hollinger i Lanza-Kaduce, 1988; prema Holt i Bossler, 2016). Osamdesetih godina osobna računala postaju sve popularnija čime se povećava broj računalnih sustava, a time i potencijalnih meta. Povezivanjem računalnih sustava pojavile su se nove vrste kaznenih djela. Mreže su omogućile ulazak u računalni sustav bez prisutnosti na mjestu počinjenja kaznenog djela, a opcija distribucije softvera putem mreža omogućila je počiniteljima širenje zlonamjernih softvera što je rezultiralo porastom broja otkrivenih računalnih virusa (ITU, 2012). Uvođenje grafičkog sučelja (“WWW”) devedesetih godina prošlog stoljeća praćeno brzim rastom broja korisnika Interneta dovelo je do novih izazova. Informacije koje su legalno dostupne u jednoj državi postale su dostupne globalno (čak i u državama u kojima je objavljivanje neke vrste informacija kriminalizirano). Kriminalitet vezan uz računala dobio je transnacionalni karakter te mu je zbog brzine razmjene informacija bilo teško ući u trag. Osim toga, promijenili su se modaliteti činjenja nekih kaznenih djela, primjerice dječja pornografija počela se distribuirati *online*, putem *web* stranica i internetskih usluga čime je fizička razmjena knjiga i vrpci dobila svoj elektronički oblik. U 21. stoljeću javljaju se novi trendovi, a njegovim su prvim desetljećem dominirale nove, visoko sofisticirane metode počinjenja kaznenih djela kao što su *"phishing"*, *"botnet napadi"* te sve češća uporaba *"voice-over-IP”* komunikacijske tehnologije i *“cloud computinga”* čija je detekcija zahtjevnija. Nisu se promijenile samo metode, već i potencijalni opseg jednog napada.

Naime, počinitelji su postali sposobni automatizirati napade uz pomoć softvera i unaprijed instaliranih napada zbog čega jedan počinitelj može napasti tisuće računalnih sustava u jednom danu koristeći samo jedno računalo. Državne i međunarodne organizacije pokušavaju odgovoriti na rastuće izazove te su pokušajima pronalaska rješenja za nošenje sa *cyber* kriminalitetom posljednjih godina dale visok prioritet. Kaznena zlouporaba informacijske tehnologije i nužan pravni odgovor pitanja su o kojima se raspravlja posljednjih četrdesetak godina, a jedan od razloga zašto problem ostaje izazovan je stalni tehnički razvoj kao i promjene metoda i načina izvršenja kaznenih djela (ITU, 2012).

2.3. Definiranje *cyber* kriminaliteta

U područje *cyber* kriminaliteta ulazi svaka kriminalna aktivnost koja uključuje računalo kao instrument, metu ili sredstvo za počinjenje kaznenog djela iz čega se zaključuje da generalizirana definicija *cyber* kriminaliteta može glasiti "*nezakonita djela u kojima je računalo alat, meta ili oboje*" (Chawki, Darwish, Khan i Tyagi, 2015, str.3). Dragičević (2004; prema Protrka, 2018) definira *cyber* kriminalitet kao "*ukupnost kaznenih djela koja su kroz određeno vrijeme počinjena unutar kibernetičkog prostora ili uz njegovu pomoć korištenjem ili zlorabljenjem resursa ili servisa kibernetičkog prostora ili usluga uz pomoć informacijskih tehnologija koje čine njegovu infrastrukturu*. *Kako do danas ne postoji općeprihvaćena definicija pojma, tako je bitno naglasiti da termin cyber, kao prvi element riječi, u većini rječnika označava nešto vezano uz svijet prividne stvarnosti koji nastaje uporabom računala".*

Kako bi se izbjegle poteškoće u definiranju *cyber* kriminaliteta, neke institucije umanjuju važnost uspostave jedinstvene definicije (Donalds i Osei-Bryson, 2019; prema Phillips i sur., 2022). Ovo stajalište odražava filozofski pristup “instrumentalizma" koji definicije gleda kao alate koji ne trebaju biti podređeni konceptima. Uspostavljanje jasne definicije sekundarno je u odnosu na potrebu za pronalaskom odgovora na *cyber* kriminalitet (McGuire, 2020; prema Phillips i sur., 2022). Konsenzus unutar literature jest da ne postoji jedinstvena, jasna, precizna i općeprihvaćena definicija *cyber* kriminaliteta (Viano, 2017; Paoli, 2018; Sarre, 2018; Donalds i Osei-Bryson, 2019; prema Phillips i sur., 2022) s čime se slažu i akademici i organizacije (Viano, 2017; Paoli, 2018; Broadhead, 2018; Gillespie, 2015; prema Phillips i sur., 2022). Usprkos nepostojanju jedinstvene i sveobuhvatne definicije, one su i dalje potrebne kako bi se kaznena djela s područja *cyber* kriminaliteta mogla pravno sankcionirati.

Prema Payneu (2020), šest dinamika čini *cyber* kriminalitet izazovnim za definiranje u usporedbi s drugim vrstama kriminaliteta. To su: **povijest/evolucija koncepta, atipična, globalna i multidisciplinarna priroda *cyber* kriminaliteta, širina *cyber* prostora i nepostojanje empirijskih istraživanja.** Koncept *cyber* kriminaliteta iznimno je nov u usporedbi s raznim tradicionalnim vrstama kriminaliteta, a u svojoj je kratkoj povijesti označavan mnogim nazivima što je svakako zakompliciralo definiranje. Njegova se atipičnost ogleda u tome što za razliku od većine drugih zločina (npr. pljački ili podmetanja požara) ne može biti percipiran osjetilima, a žrtve iskustvo viktimizacije ne osjećaju nužno u samom trenutku počinjenja kaznenog djela. Širina *cyber* prostora spojila je pojedince koji se inače nikada ne bi sreli čime se drastično povećao broj mogućih počinitelja i žrtava. Tako veliko potencijalno „mjesto zločina" sa sobom donosi mnogo vrsta *cyber* kriminaliteta. Zbog njegove globalne prirode, jedan od očitih izazova je činjenica da se ne događa unutar jedne države već će različite definicije i pravni propisi različitih zemalja odrediti hoće li biti pravne reakcije. Payne (2020) smatra da u usporedbi s drugim temama, manje istraživača proučava *cyber* kriminalitet što djelomično proizlazi iz općeg otpora prema proučavanju novih stvari u kriminologiji i kaznenom pravosuđu. Istraživanja postoje, ali se mnoga uklapaju u kategoriju tradicionalnih kriminoloških studija koje testiraju konvencionalne teorije. Multidisciplinarna priroda *cyber* kriminaliteta vidljiva je u tome što proizlazi iz mnogo različitih disciplina uključujući: računalne znanosti, računalni inženjering, informacijsku tehnologiju, psihologiju, sociologiju, političke znanosti i pravo (što ga čini kompleksnijim za definiranje i sankcioniranje).

2.4. Specifičnosti *cyber* kriminaliteta

Širenje digitalne tehnologije, računalnih i komunikacijskih uređaja promijenili su ljudsko poslovanje, komuniciranje i život općenito. Zločin slijedi priliku zbog čega je gotovo svaki napredak popraćen i mogućnošću iskorištavanja u kriminalne svrhe (Chawki i sur., 2015). Neki istraživači smatraju da *cyber* kriminalitet sačinjavaju tradicionalne vrste kaznenih djela izvedene uz pomoć novih strategija, a jedan od njih je Grabosky (2001; prema Payne, 2020) koji postavlja pitanje: je li *cyber* kriminalitet "*staro vino u novim bocama*" ili "*novo vino*"? Rastuća ovisnost o računalima učinila je tehnologiju primamljivom metom: lakoća kojom se digitalni mediji dijele dovela je do eksplozije kršenja autorskih prava i širenja dječje pornografije, mogućnost elektroničkog bankarstva i internetske trgovine postala je plodno

tlo za prijevare dok je elektronička komunikacija poput e-pošte i SMS-a omogućila *cyber* uhođenje i uznemiravanje (Chawki i sur., 2015). 1980-ih godina pojedinci su mogli krasti glazbu izravno iz glazbene trgovine koja je prodavala kazete, dok se u 2000-ima glazba može krasti izravno s interneta. Prije nekoliko desetljeća, djeca bi postajala žrtvama zlostavljanja u školi, a danas često trpe zlostavljanje na internetu. Nekoć su se koristile različite strategije uništavanja tuđe imovine: nezadovoljni je radnik mogao vandalizirati uredski prostor dok danas može unijeti viruse u računalnu mrežu svoje tvrtke. Sve ove kriminalne aktivnosti nisu nužno nove vrste ponašanja već tradicionalni zločini koji se mogu počiniti korištenjem *cyber* tehnologija (Payne, 2020). Također, neke vrste *cyber* kriminaliteta ulaze u područje kriminaliteta bijelih ovratnika. Općenito govoreći, kriminalitet bijelih ovratnika odnosi se na kazneno djelo počinjeno na radnom mjestu, u domeni počiniteljeve profesije (Payne, 2018; prema Payne 2020). *Cyber* zločini bijelih ovratnika potklasificirani su u legitimne zločine bijelih ovratnika i poduzetničke zločine bijelih ovratnika, a razlikuju se u odnosu na to radi li počinitelj legitiman posao u trenutku počinjenja kaznenog djela. U poduzetničkim kaznenim djelima, počinitelj stvara lažni ili kriminalni posao koji iskorištava za počinjenje štete ili stjecanje dobiti (Friedrichs 2009; prema Payne, 2020).

Cyber kriminalitet jedno je od najbrže rastućih područja kriminaliteta zahvaljujući brzini, anonimnosti i pogodnostima modernih tehnologija koje počinitelji iskorištavaju kako bi počinili raznolike kriminalne aktivnosti (Chawki i sur., 2015). Iako je anonimnost iznimno važna za zaštitu ljudskih prava, vezana je uz *cyber* kriminalitet te se tvrdi da kriminalcima omogućuje korištenje interneta bez mogućnosti otkrivanja (Akdeniz, 2002; prema Chawki i sur., 2015). Počinitelji mogu s namjerom prikriti svoj identitet koristeći dvojnike računala poslužitelja (eng. *proxy servers*), lažne adrese elektroničke pošte ili IP adrese (Clough, 2010; prema Tomić, 2019). Jedna od pogodnosti koja je olakšala širenje *cyber* kriminaliteta je okolnost da je softverske alate koji počinitelju dopuštaju lociranje otvorenih portova ili nadvladavanje zaštite lozinkom postalo moguće kupiti *online*. Zahvaljujući tim alatima, izvršavanje kaznenih djela *cyber* kriminaliteta približeno je puno širem krugu ljudi, ne samo osobama koje posjeduju znanja iz područja računarstva (Chawki i sur., 2015).

Cyber prostor omogućuje ljudima razmjenu ideja na velikim udaljenostima i sudjelovanje u stvaranju potpuno nove, raznolike i kaotične demokracije, oslobođene geografskih i fizičkih ograničenja (N'oeil 2001; prema Chawki, 2015). Počinitelji koji bi inače bili izolirani u svom

kršenju zakona, pronalaze istomišljenike te mogu formirati virtualne zajednice u službi činjenja kaznenih djela (Clough, 2010; prema Tomić, 2019). U usporedbi s drugim kaznenim djelima, *cyber* kriminalitet općenito zahtijeva manja ulaganja te nije podložan državnim granicama. C*yber* kriminalci imaju sposobnost iskorištavanja praznina u kaznenom zakonu vlastite zemlje, ali i praznina u zakonodavstvima drugih zemalja (Chawki i sur., 2015). Prepoznavanje kriminalne aktivnosti može biti zastrašujuće težak zadatak kada počinitelj ima mogućnost usmjeriti svoju komunikaciju sa žrtvom preko računala u više država korištenjem tehnologije i tehnika šifriranja koje pružaju visoku razinu anonimnosti. Budući da se lokacija kriminalca može potpuno razlikovati od mjesta zločina, mnoga su *cyber* kaznena djela transnacionalna te kriminalci nastoje izbjegavati zakonodavno snažne države (ITU, 2012). Ako se počinitelji i mete nalaze u različitim zemljama, istrage kaznenih djela zahtijevaju suradnju agencija za provođenje zakona u svim pogođenim zemljama što je usporeno formalnim zahtjevima i vremenom koje je potrebno da se organizira uzajamna pravna pomoć. Načelo dvojne kažnjivosti može biti problematično ukoliko djelo nije inkriminirano u jednoj od zemalja uključenih u istragu, a počinitelji mogu namjerno uključiti treće zemlje u svoje napade kako bi je otežali (ITU, 2012).

3. Fenomenologija *cyber* kriminaliteta

3.1. Tipologija *cyber* kriminaliteta

Najčešće korišten sustav kategorizacije koji dosljedno prihvaćaju i istraživači i kreatori politika jest onaj koji razlikuje dvije vrste *cyber* kriminaliteta: "*cyber* omogućen" tj. potpomognut računalom i "*cyber* ovisan" tj. kriminalitet s računalom u fokusu (McGuire i Dowling, 2013; Paoli, 2018; Sarre, 2018; prema Phillips i sur., 2022). Ova se dvofaktorska kategorizacija temelji na definiciji koju je izvorno iznio Brenner (2007; prema Phillips i sur., 2022), a njome se razlikuju specifično *cyber* prijestupi od tzv. kriminaliteta iz stvarnog svijeta koji migrira u *cyber* prostor. "*Cyber* omogućena" kaznena djela su tradicionalni zločini koji su postojali i prije tehnologije, a sada su olakšani ili omogućeni informacijsko komunikacijskom tehnologijom. Alternativna terminologija za ovu kategoriju su kaznena djela potpomognuta računalom, kaznena djela povezana s računalima i kaznena djela povezana s ljudima (Furnell, 2002; Broadhead, 2018; Black, Lumdsen i Hadlington, 2019; prema Phillips i sur., 2022). "*Cyber* ovisni" kriminalitet odnosi se na kaznena djela koja se javljaju s tehnologijom, bez nje i van digitalnog svijeta ne mogu postojati. Različiti autori

koriste različitu terminologiju za opisivanje ovih dvaju kategorija pa se tako "*cyber* ovisna" kaznena djela nazivaju kaznenim djelima s računalom u fokusu, računalnim kriminalitetom i tehnološkim kriminalitetom (Furnell, 2002; Broadhead, 2018; Black, Lumdsen i Hadlington, 2019; prema Phillips i sur., 2022). Nadalje, McGuire i Dowling (2013) kaznena djela s računalom u fokusu dijele na dvije široke kategorije:

1) Neovlašteni pristup računalnim mrežama (npr. hakiranje)
2) Narušavanje ili smanjivanje funkcionalnosti računala i mreže (npr. virusi i DoS napadi)

Alternativni dvofaktorski sustav klasifikacije je spektralni pristup Gordona i Forda (2006.; prema Phillips i sur., 2022) koji *cyber* kriminalitet dijeli na dva tipa koja predstavljaju suprotne krajeve spektra. *Cyber* kriminalitet tipa I smatra se više tehničkim po prirodi i nalikuje "*cyber* ovisnoj" kategoriji kriminaliteta dok tip II uključuje više ljudskog kontakta te podsjeća na "*cyber* omogućena" kaznena djela. Na ovaj se pristup nadovezuje novija i modernija tipologija koju predlažu Sarre, Lau i Chang (2018; prema Phillips i sur, 2022), a zanimljiva je zbog širine kojom *cyber* kriminalitetu dodaje novu dimenziju:
1. *Cyber* kriminalitet tipa I: zločini tehničke prirode (npr. hakiranje),
2. *Cyber* kriminalitet tipa II: zločini koji uključuju ljudski kontakt (npr. *cyber bullying*),
3. *Cyber* kriminalitet tipa III: zločini počinjeni od strane umjetne inteligencije, robota/botova ili samoučeće tehnologije.

Wallov (2007) trokategorijski sustav klasifikacije bio je jedan od prvih objavljenih u akademskoj literaturi i stoga se često citira, a diferencira sljedeće:
1. "Zločini protiv stroja" poznati kao zločini protiv računalnog integriteta, npr. hakiranje, krekiranje, uskraćivanje usluge (DoS) i distribuirano uskraćivanje usluge (DDoS),
2. "Zločini korištenjem stroja" također poznati kao računalno potpomognuti zločini, npr. piratstvo, pljačke i prijevare,
3. "Zločini u stroju" istovjetni zločinima računalnog sadržaja, npr. *online* mržnja, uznemiravanje, dječja pornografija.

Gotovo jednaku distinkciju u tri kategorije usvojila je i Europska komisija (2013; prema Phillips i sur., 2022). Koristi se sljedeća terminologija:
1. Kaznena djela jedinstvena za računala i informacijske sustave (npr. napadi na informacijske sustave, uskraćivanje usluge i zlonamjerni softveri),

2. Tradicionalna kaznena djela (npr. prijevara, krivotvorenje i krađa identiteta),
3. Kaznena djela povezana sa sadržajem (npr. poticanje na rasnu mržnju i materijali seksualnog zlostavljanja djece (češće u literaturi navođeni kao dječja pornografija)).

Chandra i Snowe (2020) predlažu taksonomiju s fokusom na izravnu žrtvu kojom nastoje postići stabilnost, jasnoću, cjelovitost i uzajamnu isključivost kategorija koja zahtijeva pažljivo određivanje i usku definiciju tipa žrtve. Fokus usmjeren na žrtvu osigurava usporedivost s tradicionalnim kriminalitetom gdje se mjere poput otkrivanja, prevencije i kaznenog progona poduzimaju u skladu s prirodom i težinom pretrpljene štete. U identificiranju i definiranju direktne žrtve kao odlučujući kriterij koristi se prvi, izravni i neposredni utjecaj svakog *cyber* zločina. Neizravna tj. indirektna žrtva udaljena je u vremenu i prostoru od prvog, izravnog i neposrednog utjecaja te se odnosi na proširene i kasnije posljedice kaznenog djela. Chandra i Snowe (2020) *cyber* kriminalitet dijele na čistotehnološki i tehnologijom potpomognut. Čistotehnološki *cyber* kriminalitet kriminalno je djelo koje cilja ili viktimizira ekosustav računalne tehnologije te djelomično ili potpuno narušava njegovu povjerljivost, integritet ili dostupnost. Izravne žrtve čistog tehnološkog *cyber* kriminaliteta su: računalni sustavi (ugroženi radnjama protiv hardvera i softvera), povezane tehnologije (ugrožene radnjama usmjerenim na fizičke komponente ili operativne sustave računalnih tehnologija kao što su dronovi, umjetna inteligencija i roboti) i mrežne usluge. Ova kategorija uključuje radnje koje ometaju, prekidaju vezu, preusmjeravaju ili eliminiraju "sustav međusobno povezanih računala i komunikacijske opreme koja se koristi za povezivanje računala" (ISACA, 2019; prema Chandra i Snowe, 2020). Djela *cyber* potpomognutog kriminala koriste računalnu tehnologiju za ciljanje ili viktimizaciju fizičkih osoba, vlada, poslovnih subjekata ili imovine koja nije ekosustav računalne tehnologije pri čemu dolazi do uskraćivanja, ometanja ili oštećenja entiteta ili imovine. Izravne žrtve *cyber* potpomognutog kriminaliteta su: fizičke osobe, sva imovina koja nije računalni ekosustav ili mreža (sve vrste poslovnih subjekata, informacije) i državni entitet. Kod kaznenih djela gdje su izravna žrtva fizičke osobe, viktimizirana su pojedinačna zakonska i/ili ljudska prava, a uključene su radnje koje oštećuju tijelo, um i duh: napad i zlostavljanje, uznemiravanje, narušavanje privatnosti, uhođenje, prostitucija, dječji seksualni turizam, trgovina ljudima, otmica itd. Imovina koja nije računalni ekosustav ili mreža, kategorija je direktne žrtve koja uključuje lišavanje pravih vlasnika korištenja i/ili prava koristi imovine što podrazumijeva kaznena djela u kojima šteta nastaje kroz vandalizam, uništavanje i uklanjanje ili ograničenje kapaciteta/pristupa imovini. Kaznena djela protiv vlada djela su

čija je izravna žrtva državni entitet, a ciljaju naciju, državu ili suverenu zajednicu. Utječu na njihovu sposobnost da učinkovito funkcioniraju i izvršavaju svoje administrativne ili zakonske dužnosti te uključuju radnje koje ometaju, napadaju ili urušavaju njeno upravno tijelo ili institucije, mehanizme ili birokraciju, procese ili sustave putem kojih građani i skupine ostvaruju svoja prava i ispunjavaju obveze. Chandra i Snowe (2020) smatraju ovu taksonomiju doprinosom teoriji i proširenjem znanja, značajnom za praksu te polaznom osnovom za buduća kriminološka istraživanja.

3.2. Pojavni oblici *cyber* kriminaliteta

3.2.1. Hakiranje

Naziv haker (eng.*hacker*) potječe iz šezdesetih godina prošlog stoljeća, javlja se u svijetu računalnog programiranja uz pozitivnu konotaciju opisujući osobu vještu u kreiranju efektivnih rješenja za računalne probleme. "*Hack*" je podrazumijevao inovativno korištenje tehnologije koje rezultira benefitima, a osobe sposobne za ovakva nova i uzbudljiva tehnološka poboljšanja, hakeri, smatrale su se hrabrim novim pionirima računalne revolucije (Levy, 1984; prema Yar, 2006). Hakiranje je s vremenom postalo sinonim za činjenje kaznenih djela zbog čega su hakeri 1985. godine osmislili termin „*cracker*“ kojim se opisivala zlonamjerna osoba koja ruši (*“cracka”*) sigurnosne postavke računalnog sustava. Unatoč tome, termini haker i hakiranje uvriježili su se kao oznaka za ilegalne aktivnosti iz domene *cyber* kriminaliteta zbog čega je podjela na hakere i *crackere* više od kriminološkog nego ikakvog drugog značaja (Yar, 2006). Isti autor smatra hakiranje generičkom oznakom za niz različitih aktivnosti povezanih s upadom u računalo, manipulacijom i remećenjem. Najosnovniji oblik hakerske aktivnosti je ostvarivanje pristupa tuđim računalnim sustavima i kontroliranje istih. To je postalo moguće zahvaljujući umrežavanju računalnih sustava čija međusobna povezanost omogućuje pristup sustavu s drugih računala koja se na njega mogu povezati. Internet je s obzirom na “otvorenu arhitekturu” mreže mnogostruko olakšao izvedivost takvog upada.

Nakon što haker stekne pristup i kontrolu, moguć je niz zabranjenih aktivnosti (Yar, 2006):
1) Krađa računalnih resursa
Hakeri mogu koristiti resurse hakiranog sustava za vlastite svrhe kao što je pohranjivanje ilegalnih materijala. U jednom takvom incidentu, haker iz Švedske ilegalno je pristupio

sustavima američkog sveučilišta te ih iskoristio za pohranu i distribuciju piratskih glazbenih datoteka (Furnell, 2002; prema Yar, 2006).

2) Krađa vlasničkih ili povjerljivih informacija

Hakeri mogu iskoristiti neovlašteni pristup kako bi ukrali ili kopirali informacije uključujući softver, poslovne tajne, osobne podatke o zaposlenicima i klijentima organizacije kao što su informacije kreditnih kartica.

3) Sabotaža, izmjena i uništavanje sustava

Hakeri mogu nanijeti značajne količine štete računalnim sustavima uništavanjem i brisanjem sadržaja, ali najčešće selektivno izmjenjuju podatke čime ne dolazi do šteta tolikih razmjera. Selektivnom izmjenom podataka prikrivaju svoje tragove kako administrator sustava ne bi primjetio da je sustav kompromitiran čime ostvaruju stalni pristup istom i neometano upadanje. Podatke u sustavu mijenjaju s ciljem stjecanja osobne koristi, a zabilježeni su mnogostruki slučajevi upada studenata u sustave sveučilišta kako bi mijenjali ocjene.

4) Obezličenje *web* stranice i *spoofing*

Takvi hakerski napadi izravno ciljaju na same internetske stranice i mogu poprimiti različite oblike kojima je zajednička karakteristika izmijenjen sadržaj. Motiv za ovakva ponašanja hakera može biti želja da „zabavi“ posjetitelje stranice, treniranje vještina „hakiranja“ ili ideološki i politički oblik prosvjeda protiv država ili korporacija (Vegh, 2002.; Woo et al., 2004; prema Yar, 2006). Drugi oblik hakiranja usmjerenog na *web* stranice, *spoofing*, ne napada stvarne stranice organizacija već haker uspostavlja *spoof* tj. lažnu *web* stranicu na koju korisnik interneta biva preusmjeren. Radi se o prisvajanju identiteta legitimnog korisnika unutar *cyber* prostora od strane neovlaštene osobe (Schell i Martin, 2004; prema Tomić, 2019). Ove se metode koriste u počinjenju internetskih prijevara pri kojima krivotvorena *web* stranica izgleda gotovo identično legitimnoj koju nastoji oponašati. Korisnici ne budu svjesni da je stranica lažna pa je nastavljaju koristiti kao i obično pri čemu ponekad otkriju osjetljive privatne informacije poput korisničkih imena, lozinki i podataka kreditne kartice.

Yar (2006) spominje i hakerske aktivnosti koje ne zahtijevaju stjecanje pristupa i kontrole:

1) Napad uskraćivanjem resursa (*„flooding“*)

Uskraćivanje usluge (eng. Denial-of-Service, DoS) odnosi se na napad “koji korisniku ili vlasniku računala onemogućuje pristup uslugama dostupnim na vlastitom sustavu” (Esen, 2002; prema Yar, 2006). Internetski poslužitelji (eng. *servers*) preplavljuju se (eng. *flooding*)

s toliko zahtjeva da ne mogu odgovoriti dovoljno brzo što može uzrokovati njihovo zamrzavanje ili pad (McGuire i Dowling, 2013). U literaturi se u kontekstu ovakvih napada ponekad spominje i *botnet*. Nakon zaraze korisničkog računala, napadač ga može kontrolirati pomoću naredbi i pokretati različite scenarije napada s kontrolnog poslužitelja (eng. *command and control server*) koji šalje naredbe svim zaraženim računalima. Zaraženo računalo koje je dio bot mreže naziva se bot. Napadači koji upravljaju velikim *botnetovima* od njih mogu imati veliku financijsku dobit upravo zbog mogućnosti napada s velikog broja računala u različitim mrežama čime napad uskraćivanjem usluge prerasta u distribuirani napad uskraćivanjem usluge poznatiji kao DDoS (Vuković, 2018).

2) Distribucija malicioznog softvera

Maliciozni softver je program koji je tajno implementiran u drugi program ili računalni sustav s ciljem: „uništavanja podataka, pokretanja razornih programa, ugrožavanja povjerljivosti, integriteta ili dostupnosti podataka, aplikacija i operacijskog sustava legitimnom korisniku“ (Souppaya i Scarfone, 2013; prema Tomić, 2019).

McGuire i Dowling (2013) navode sljedeće kategorije zlonamjernih programa:

a) Virusi su jedna od najpoznatijih vrsta zlonamjernog softvera, uzrokuju blagu disfunkciju računala, ali mogu imati i ozbiljnije posljedice u smislu oštećenja ili brisanja hardvera, softvera ili datoteka. Oni su samoreplicirajući programi koji se šire unutar i između računala. Potreban im je domaćin (kao što je datoteka, disk ili proračunska tablica), ali ne mogu zaraziti računalo bez ljudske akcije pokretanja ili otvaranja zaražene datoteke (Moir, 2008; prema McGuire i Dowling, 2013).
b) Crvi su također programi koji se sami umnožavaju, ali se mogu širiti autonomno, unutar i između računala, bez potrebe za domaćinom ili bilo kakvom ljudskom radnjom. Utjecaj crva stoga može biti jači od virusa, uzrokujući uništavanje čitavih mreža (Beal, 2011.; prema McGuire i Dowling, 2013).
c) Trojanski konj je oblik zlonamjernog softvera za koji se čini da obavlja benignu ili korisnu funkciju, ali zapravo ima skrivene destruktivne sposobnosti koje postaju očite tek nakon što korisnik preuzme i instalira softver (Yar, 2006). Prema Gandhiju (2012), trojanski konj na računalnim sustavima otvara “stražnja vrata” (eng. *backdoor*) u obliku instaliranog programa ili modifikacije legitimnog programa. Ovom se metodom zaobilazi normalna provjera autentičnosti te se osigurava mogućnost pristupa računalu s udaljenosti.

d) Špijunski softver (eng. *spyware*) zadire u privatnost korisnika prikupljanjem osjetljivih ili osobnih podataka iz zaraženih sustava i nadziranjem posjećenih *web* stranica. Najjednostavniji oblik softvera za krađu podataka je softver za bilježenje pritisaka tipki, eng. *keystroke loggers* (Howard, Thomas, Burstein i Bradescu, 2008).

3.2.2. Računalne prijevare

Button i Cross (2017; prema Tomić, 2019) definiraju prijevaru kao: „širok spektar aktivnosti čije je zajedničko obilježje neistinito predstavljanje od strane počinitelja kako bi si osigurao korist ili prouzročio štetu drugima“. Prema Yaru (2006), prijevare odvajaju žrtve od njihovog novca ili imovine putem dezinformacija i obmana. Često je varanje žrtve pri *online* kupovini: a) naručeno i plaćeno nikada ne bude dostavljeno, b) prava vrijednost predmeta je mnogo manja od plaćene vrijednosti, c) predmet nije autentičan, d) nesvjesna kupovina nečeg ukradenog (preprodaja). Osim toga, žrtva može biti prevarena od strane pojedinca s kojim posluje dok se isti lažno predstavlja kao dio neke legitimne organizacije ili nositelj neke profesionalne uloge. Whitty (2020) spominje još primjera internetskih prijevara: a) lutrije i nagradne igre (žrtve putem e-pošte saznaju “da su dobitnici visoke novčane nagrade”), b) krađe identiteta (korisnici bivaju navedeni da kliknu na zlonamjernu poveznicu čime dolazi do krađe podataka), c) dobrotvorne prijevare (lažne dobrotvorne organizacije traže donacije) i d) investicijske prevare (obećanja visokih dobitaka). Investicijska prijevara najčešće uključuje trgovanje dionicama i traženje ulaganja u nepostojeće tvrtke (Yar, 2006). Zanimljiv je fenomen ljubavne ili romantične prijevare pri kojoj počinitelji koriste percepciju legitimne veze kako bi iskorištavali žrtvu što u većini slučajeva rezultira financijskim gubitkom. Počinitelj koristi povjerenje i razvijen odnos kako bi manipulirao žrtvom i iskorištavao je, kako financijski, tako i emocionalno. Ljubavna prijevara može uništiti živote kroz očite financijske gubitke u kombinaciji s teškim emocionalnim gubicima (npr. razvitak depresije ili suicidalnih misli), narušenim zdravljem i raspadom odnosa s obitelji i prijateljima (Button i sur. 2009, 2014; Cross i sur. 2016; prema Cross, 2020).

3.2.2.1. Ransomware

Iako se radi o obliku zlonamjernog softvera, njegova je uloga iznuditi novac zbog čega ulazi u kategoriju računalne prijevare. Od žrtava se zahtijeva plaćanje naknade kako bi ponovno dobile pristup vlastitim sistemskim datotekama i podacima (Ferguson, 2013; prema Holt i Bossler, 2016). *CryptoLocker*, oblik ransomwarea, širi se putem privitaka u e-porukama ili

kao zlonamjerni softver koji se može preuzeti na internetu. Nakon pokretanja, šifrira podatke na svim tvrdim diskovima priključenim na zaraženi sustav. Žrtvi je potreban ključ za dešifriranje datoteka koji joj napadač obećava poslati nakon što uplati novac (Ferguson, 2013; prema Holt i Bossler, 2016). Ransomware prikazuje poruku o uvjetima otkupnine (eng. *ransom note*), a u ranim su danima ove pojave kriminalci pokušavali prestrašiti žrtvu tvrdeći da su pripadnici zakona. Odlazili bi toliko daleko da su poruke ponekad sadržavale razne optužbe protiv žrtve (npr. za dječju pornografiju) uz što bi naglašavali i razaranje njenog života ukoliko prijavi napad. Ove tehnike zastrašivanja osmišljene kako bi se izvukao novac povremeno su služile i za navođenje pojedinaca da si oduzmu život (O'Kane, Sezer i Carlin, 2018). Popularnost ove vrste zloćudnih programa porasla je krajem 2013. godine zbog pojave kriptovaluta koje su olakšale plaćanje otkupnine, odnosno otežale ulazak u trag napadačima (Vuković, 2018).

3.2.2.2. Phishing

Phishing većinom podrazumijeva slanje elektroničke pošte u kojoj se prevarant lažno predstavlja kao legitimna organizacija s ciljem da korisnik preda privatne podatke koji će se koristiti za krađu identiteta. U tim slučajevima, sadržaj poruke sadrži poveznicu koja korisnika usmjerava da posjeti *web* mjesto tj. lažnu stranicu (eng. *spoof*) radi promjene lozinke, ažuriranja svojih podataka koje legitimna organizacija već ima ili poduzimanja neke druge radnje koju je navodno potrebno hitno poduzeti (Gandhi, 2012). Nisu svi phishing napadi počinjeni putem neželjene pošte (eng.*spam*) već se smatra da postoje dvije vrste phishing tehnika: trojanske e-poruke i phishing poruke (Atkins i Huang 2013; prema Kigerl, 2020). Trojanski e-mailovi oslanjaju se na već spomenuto slanje poveznice na *web* mjesto koja usmjerava žrtvu na kompromitiranu *web* stranicu nakon čega se na računalo instalira zlonamjerni softver koji počinje skenirati zaraženi stroj u potrazi za povjerljivim podacima ili snimati pritiske na tipke (eng. *keystroke logger*). Phishing poruke se oslanjaju na društveni inženjering ili lažiranje pouzdanih usluga *web* mjesta koje meta koristi (npr. banka) kako bi natjerala korisnika da izravno otkrije svoje podatke poput lozinki i podataka kreditne kartice (Kigerl, 2020). Abraham i Chengalur-Smith (2010; prema Bullé i Junger, 2020) predložili su sljedeću definiciju društvenog inženjeringa: "Korištenje društvenih maski, kulturoloških smicalica i psiholoških trikova kako bi se korisnici računala (tj. mete) natjerali da pomognu hakerima (tj. počiniteljima) u njihovom nezakonitom upadu ili korištenju računalnih sustava i mreža."

3.2.2.3. Spam

Spam je postao sveprisutan u modernom dobu i uglavnom se smatra samo dosadnom smetnjom. Radi se o masovnom slanju neželjenih elektroničkih poruka obično u svrhu zarade koje od 2017. godine čini više od polovice svih e-poruka (Gudkova i sur., 2017; prema Kigerl, 2020) u što nije uračunata neželjena pošta poslana preko drugih elektroničkih komunikacijskih medija. Gotovo 90% neželjene pošte šalju bot mreže zato što spam ostvaruje zaradu kroz količinu, tj. zahtijeva da tisuće domaćina šalju neželjenu poštu u što je moguće većem opsegu. Prijevare utemeljene na spamu ciljaju na jednu od najslabijih karika koje štite računalne sustave od napadača: ljude. Napadači ne moraju imati sofisticiranu tehnologiju, resurse ili vještine hakiranja budući da je često lakše koristiti društveni inženjering (Kigerl, 2020). *Spamovi* iskorištavaju resurse sustava, utječu na propusnost, ispunjavaju kapacitete servera, koriste mrežnu infrastrukturu, predstavljaju ulaznu točku za širenje virusa i *phishing* napade na pristupne šifre i povjerljive informacije (Kokot, 2014). Nazvane prijevarama temeljenim na neželjenoj pošti, lažne poruke mogu imati mnogo različitih oblika: od manje štetne prijevare potrošača prodajom sumnjive robe do ozbiljnijih oblika prijevare kao što su nigerijska prijevara, krađe identiteta i novačenje novčanih mazgi koje su mete prevarene za pranje novca.

3.2.3. Kršenje autorskih prava

Digitalno piratstvo često se jednostavno definira kao "neovlaštena i nezakonita digitalna reprodukcija intelektualnog vlasništva" (Gunter 2008; prema Jennings i Bossler, 2020). U svojoj najosnovnijoj formi, intelektualno vlasništvo poprima oblik takozvanih "neopipljivih dobara" kao što su ideje, izumi, znakovi i informacije. Dok zakoni koji pokrivaju vlasništvo postavljaju prava nad opipljivim dobrima, zakoni o intelektualnom vlasništvu uspostavljaju vlasnička prava nad izvornim oblicima intelektualne proizvodnje (WIPO, 2001; prema Yar, 2006). Intelektualno vlasništvo može imati brojne priznate oblike: patente, trgovačke znakove, poslovne tajne, industrijski dizajn i autorska prava. Tipični objekti autorskog prava uključuju pisane materijale, glazbu, slike, crteže, audio-vizualne snimke i računalne softvere. Kao što izraz sugerira, autorsko pravo nositelju daje prava na kopiranje, reprodukciju, distribuciju, emitiranje i izvođenje djela ili sadržaja (Yar, 2006). Lee i suradnici (2018; prema Jennings i Bossler, 2020) definiraju digitalno piratstvo kao “reprodukciju, korištenje ili distribuciju informacijskih proizvoda, u digitalnim formatima i/ili korištenje digitalnih tehnologija bez ovlaštenja njihovih zakonskih vlasnika” iz čega se

zaključuje da je digitalno piratstvo više od pukog ilegalnog preuzimanja. Važno je uzeti u obzir da "digitalno piratstvo" predstavlja krovni pojam koji obuhvaća više vrsta neovlaštenih ponašanja i oblika (Jennings i Bossler, 2020).

4. Kaznenopravni okvir *cyber* kriminaliteta

Globalni karakter *cyber* kriminaliteta iziskuje pristup problemu na međunarodnom nivou o čemu svjedoče aktivnosti raznih organizacija poput Ujedinjenih naroda, Organizacije za ekonomsku suradnju i razvoj (OECD), Vijeća Europe (COE) te raznih međunarodnih udruženja za kazneno pravo. Aktivnost međunarodnih organizacija i udruženja uvelike je pomogla državama u uvođenju novih oblika kaznenih djela u svoja nacionalna zakonodavstva čime je postignut određeni stupanj harmonizacije (Dragičević, 2004; prema Carević, 2022). Najvažniji dokument u ovome pogledu je Konvencija o kibernetičkom kriminalu Vijeća Europe (u daljnjem tekstu Konvencija), usvojena na konferenciji održanoj u Budimpešti 23. studenog 2001. godine. S obzirom da se radi o takozvanoj okvirnoj konvenciji, njene odredbe nisu izravno primjenjive već ih svaka država mora implementirati u vlastito zakonodavstvo (Vojković i Štambuk-Sunjić, 2006). "Konvencija je prvi međunarodni ugovor o kaznenim djelima počinjenim putem interneta i drugih računalnih mreža, a posebno se bavi kršenjem autorskih prava, računalnim prijevarama, dječjom pornografijom i kršenjem mrežne sigurnosti. Glavni cilj, naveden u preambuli, provođenje je zajedničke kaznene politike usmjerene na zaštitu društva od *cyber* kriminala, posebno usvajanjem odgovarajućeg zakonodavstva i poticanjem međunarodne suradnje" (COE, 2022). Potpisivanjem Konvencije, države stranke preuzele su obvezu usvojiti zakonske i druge mjere kojima bi se omogućio kazneni progon počinitelja kaznenih djela protiv tajnosti, integriteta i dostupnosti računalnih sustava i podataka, kaznenih djela u svezi s računalom, kaznenih djela u svezi sa sadržajem, kaznenih djela u vezi s povredama autorskih i drugih srodnih prava uz obvezu kažnjavanja pokušaja, poticanja i pomaganja navedenih djela. Osim sankcioniranja, Konvencijom je predviđeno i rješavanje pojedinih procesnih pitanja (Kokot, 2014). U trenutku izrade ovog rada, Konvenciju je ratificiralo 66 zemalja, 16 potpisalo ili je pozvano da pristupi potpisivanju. Republika Hrvatska potpisala ju je istog dana kada je usvojena, ratificirala 17. listopada 2002. godine dok je na snagu stupila 1. srpnja 2004. godine (COE, 2022). Napori u izjednačavanju nacionalnih zakonodavstava ne staju na Konvenciji: 2003. godine donesen je Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akata rasizma i ksenofobije počinjenih putem računalnih sustava.

Od zemalja sudionica zahtijeva kriminalizaciju širenja rasističkih i ksenofobnih sadržaja putem računalnih sustava te negiranja holokausta i ostalih genocida. Republika Hrvatska postala je država potpisnica 26. ožujka 2003. godine, a ratificirala ga 4. srpnja 2008. godine.

Europski parlament i Vijeće Europske unije temeljem članka 83. stavka 1. Ugovora o funkcioniranju Europske unije donijeli su Direktivu 2013/40/EU o napadima na informacijske sustave s ciljem usuglašavanja kaznenih zakona država članica u području napada na informacijske sustave preko utvrđivanja minimalnih pravila o definiranju kaznenih djela i odgovarajućih sankcija. Razlog za donošenje Direktive 2013/40/EU bila je nedovoljna harmonizacija kaznenog prava u području *cyber* kriminala te manjkavost sadržaja što ne znači da je u suprotnosti s Konvencijom o kibernetičkom kriminalu već se na nju nadovezuje (Kokot, 2014).

Od svibnja 2022. godine, moguće je potpisati Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza. Usvojen je na sastanku Odbora ministara Vijeća Europe 17. studenog 2021. godine, a njime su predviđeni postupci za poboljšanje prekograničnog pristupa elektroničkim dokazima i visoka razina zaštitnih mjera u pogledu međunarodnih prijenosa osobnih podataka s ciljem olakšanja prijenosa podataka između država članica Europske Unije koje su stranke Drugog dodatnog protokola kao i trećih država koje su također stranke (Carević, 2022). U trenutku izrade ovog rada, 24 su države potpisale Drugi protokol (isključujući Hrvatsku), a ratifikacija nije bilo (COE, 2022).

4.1. Hrvatsko zakonodavstvo

Reformom hrvatskog kaznenog zakonodavstva 1997. godine uvedeno je prvo pravo kazneno djelo računalnog kriminaliteta člankom 223. Kaznenog zakona (u daljnjem tekstu KZ) pod nazivom „Oštećenje i uporaba tuđih podataka" u Glavi XVII.: Kaznena djela protiv imovine. Zakonom o izmjenama i dopunama KZ-a objavljenim 15. srpnja 2004. godine u NN 105/2004. unesena je u kazneno zakonodavstvo novela članka 223. koji je promijenio naziv u "Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava" te su dodani članci 223. a) "Računalno krivotvorenje" i 224. a) "Računalna prijevara" koji su stupili na snagu 1. listopada 2004. godine čime je kazneno zakonodavstvo usklađeno s odredbama Konvencije, iako ova kaznena djela i dalje ostaju u Glavi XVII

(Kokot, 2014). Hrvatski KZ je već u svom izvornom tekstu iz 1997. godine poznavao kaznena djela "iskorištavanje djece ili maloljetnih osoba za pornografiju" (čl. 196.) i "upoznavanje djece s pornografijom" (čl. 197.) Zbog širenja distribucije dječje i maloljetničke pornografije putem Interneta, kasnije se javlja potreba inkriminacije "dječje pornografije na računalnom sustavu ili mreži" člankom 197. a (Vojković i Štambuk-Sunjić, 2006). Aktualni KZ u Glavi XVII. Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta, člankom 163. inkriminira iskorištavanje djece za pornografiju dok članak 164. inkriminira iskorištavanje djece za pornografske predstave. Članak 165. inkriminira činjenje pristupačnim djeci mlađoj od 15 godina spise, slike, audiovizualne sadržaje ili druge predmete pornografskog sadržaja posredstvom računalnog sustava. Prema članku 163. KZ "dječja pornografija je materijal koji vizualno ili na drugi način prikazuje pravo dijete ili realno prikazano nepostojeće dijete ili osobu koja izgleda kao dijete, u pravom ili simuliranom spolno eksplicitnom ponašanju ili koji prikazuje spolne organe djece u spolne svrhe." Ovi su propisi usklađeni s Konvencijom, Konvencijom o zaštiti djece od seksualnog iskorištavanja i seksualnog nasilja te Direktivom 2011/93/EU o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije (Carević, 2022).

Kokot (2014) navodi da se velika kaznenopravna reforma dogodila 2011. godine kada je donesen novi Kazneni zakon (na snazi od 2013. godine) kojim je formirana zasebna Glava XXV. „Kaznena djela protiv računalnih sustava, programa i podataka" koja obuhvaća sljedeća kaznena djela:

• Čl. 266. Neovlašteni pristup

Kriminalizira se nezakoniti pristup tuđem računalnom sustavu čime se štiti integritet računalnog sustava, a neovlašteni se pristup uspoređuje s povredom nepovredivosti doma. Pravno dobro nije povrijeđeno samo kad osoba bez ovlaštenja zamijeni ili ukrade podatke koji se nalaze u informacijskom sustavu, nego i kad ga samo razgledava (Kokot, 2014).

• Čl. 267. Ometanje računalnog sustava

Rad sustava za obradu podataka mora biti ometan unosom, prijenosom, oštećenjem, brisanjem, mijenjanjem ili činjenjem neuporabljivim računalnih podataka ili programa s namjerom da se onemogući normalno funkcioniranje sustava za obradu podataka. Ometanje rada računala koje bi bilo obuhvaćeno oštećenjem fizičkih komponenti, infrastrukture i komunikacijske mreže objedinjeni su odredbama kojima se sankcionira oštećenje ili uništenje tuđe stvari (Škrtić, 2012; prema Carević, 2022).

• Čl. 268. Oštećenje računalnih podataka

U Konvenciji i Direktivi 2013/40/EU službeni prijevod glasi ometanje te se kazneno djelo oštećenja računalnih podataka dovodi u analogiju s kaznenim djelom ometanja rada računalnog sustava: oba kaznena djela mogu se počiniti oštećenjem, brisanjem, mijenjanjem ili činjenjem računalnih podataka neupotrebljivim (Kokot, 2014).

• Čl. 269. Neovlašteno presretanje računalnih podataka

Kriminalizacijom neovlaštenog presretanja zaštita se širi s podataka koji se nalaze u računalnom sustavu na podatke u prijenosu (Kokot, 2014).

• Čl. 270. Računalno krivotvorenje

Pravno dobro koje se štiti jest vjerodostojnost isprave u digitalnom obliku. Ono pokriva manipulaciju digitalnim dokumentima, odnosno podacima (Kokot, 2014).

• Čl. 271. Računalna prijevara

Kriminalizira se protupravno stjecanje imovinske koristi napadom na računalni sustav ili računalne podatke, a ovo se kazneno djelo može počiniti samo s namjerom (Kokot, 2014).

• Čl. 272. Zlouporaba naprava

Kriminalizira se izrada, nabava, prodaja, posjedovanje ili činjenje drugom dostupnim uređaja ili računalnih programa ili računalnih podataka koji su stvoreni ili prilagođeni za počinjenje kaznenih djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava (KZ, NN 125/11, 84/21).

• Čl. 273. Teška kaznena djela protiv računalnih sustava, programa i podataka

Jedan od prigovora Konvenciji bio je da ne propisuje kazne za najteže i najštetnije oblike napada na računalne sustave zbog čega je za njih hrvatski zakonodavac predvidio ovaj članak (Kokot, 2014).

Isti autor smatra da način na koji su odredbe preuzete ne definira i ne prevodi jasno računalne podatke, programe i mreže što pravno-tehnički slabi njihovu uporabnost. Većina kaznenih djela postavljena je šire od okvira spomenutih međunarodnih dokumenata dok su pojedina djela ostala nedorađena. Uočava i pravne praznine u odnosu na djela neovlaštenog ostajanja u računalnom sustavu i neovlaštenog pribavljanja računalnih podataka.

5. C*yber* kriminalitet u pandemiji koronavirusa

U prosincu 2019. godine, u kineskom gradu Wuhanu prijavljeno je izbijanje bolesti uzrokovane novim koronavirusom, a Svjetska je zdravstvena organizacija (u daljnjem tekstu

WHO) uskoro službeno potvrdila da je riječ o virusu SARS-CoV-2 dok se bolest koju uzrokuje naziva COVID-19. Krajem veljače, zabilježen je znatan porast broja slučajeva ove bolesti u Europi (Vijeće Europske unije, 2022). Nakon što je WHO sredinom ožujka proglasio pandemiju, zemlje diljem svijeta pokrenule su globalna zatvaranja, tzv. *lockdown*-ove kojima su vlade država ograničile kretanje ljudi, naredile ostajanje u vlastitim domovima te zatvorile nacionalne granice s ciljem zaštite ljudskog zdravlja (Onyeaka, Anumudu, Al-Sharify, Egele-Godswill i Mbaegbu, 2021). Čovječanstvo je počelo ovisiti o informacijsko komunikacijskoj tehnologiji koja je na neki način postala oslonac za nastavak funkcioniranja društva. Tvrtke su prešle na rad od kuće, studenti i učenici na *online* nastavu, a međuljudski odnosi održavali su se virtualno. Postavlja se logično pitanje: je li porast ljudskih aktivnosti u *cyber* prostoru uzrokovan pandemijom koronavirusa imao utjecaj na stope *cyber* kriminaliteta pružajući mu nove prilike? Prema izvještaju Svjetskog ekonomskog foruma (WEF, 2022), ispitanici Globalne ankete o percepciji rizika (GRPS) uvrstili su "neuspjehe *cyber* sigurnosti" u 10 najvećih rizika od početka korona krize. U Kini, Izraelu, Singapuru, UAE, Japanu i Danskoj smjestili su se u prvih pet najvećih rizika dok su Australija, Velika Britanija, Irska i Novi Zeland "neuspjehe *cyber* sigurnosti" rangirale kao rizik broj jedan.

Na temelju opsežne analize podataka primljenih od zemalja članica i privatnih partnera, Interpol (2020a) je kao glavne prijetnje u vezi s pandemijom COVID-19 naveo ransomware, maliciozne domene, phishing, prijevare, zlonamjerne softvere i lažne vijesti.

National Cyber Security Centre (u daljnjem tekstu NCSC) je 2020. godine obradio trostruko više ransomware incidenata u Ujedinjenom Kraljevstvu u odnosu na 2019. godinu (NCSC, 2021). Da ransomware postaje opasno rastuća prijetnja i problem za javnu sigurnost, smatra i 85% članova Zajednice voditelja *cyber* sigurnosti (eng. *Cybersecurity Leadership Community*) Svjetskog ekonomskog foruma (WEF, 2022). Afrički kontinent zabilježio je kontinuirani porast *cyber* napada pri čemu su napadi na platforme internetskog bankarstva u 2020. godini porasli za 238% (Interpol, 2021) dok je upravo ransomwareom navodno bilo pogođeno više od 61% afričkih tvrtki (neki od napada bili su usmjereni na kritičnu infrastrukturu zdravstvenog i pomorskog sektora). Tijekom pandemije se većina prijava Europolu (2020c) odnosila na ranije poznate obitelji ransomwarea što sugerira umiješanost poznatih kriminalaca koji nastavljaju s napadima. U ožujku 2020. godine, prijavljeno je da se phishing povećao za 600% (Shi, 2020; prema Ventrella, 2020). Prema informacijama koje

su Interpolu (2020a) dostavile zemlje članice i privatni partneri, glavni oblici phishing napada u vezi s COVID-19 su: e-poruke nacionalnih ili globalnih zdravstvenih tijela, vladine naredbe i inicijative za financijsku potporu, lažni zahtjevi za plaćanje i povrat novca, ponude cjepiva i medicinskih potrepština, mobilne aplikacije za praćenje COVID-19 te zahtjevi za donacije u dobrotvorne svrhe. Phishing e-poruke čiji su navodni pošiljatelji bili nacionalna ministarstva zdravstva ili WHO sadržavale su privitke sa zlonamjernim softverima kao što su Emotet, Trickbot i Cerberus (dizajniran posebno za krađu informacija) te su od strane zemalja članica i privatnih partnera Interpola registrirani kao široko korišteni u phishing e-pošti (Interpol, 2020a). Phishing napadi imaju stopu uspješnosti od 30% ili više te je iznimno zabrinjavajuća činjenica da je napadaču potreban mali postotak klikova kako bi ostvario financijsku dobit ili druge interese (Pranggono i Arabo, 2021). U ranim fazama pandemije, pojavile su se već spomenute aplikacije za mobilne uređaje. Naime, organizacije kao što su Google, WHO i američko sveučilište Johns Hopkins izradile su aplikacije s online kartama koje su sadržavale podatke i statistike o stopama zaraze i smrtnosti te vizualne demonstracije širenja virusa koje su ljudima omogućavale da prate njegovo kretanje. *Cyber* napadači su iskoristili priliku i izradili realistične karte slične onima legitimnih organizacija kako bi širili zlonamjerni softver ili pratili korisnike (Saleous i sur., 2022). Nakon što se aplikacija preuzme, zlonamjerni softver dobiva pristup korisnikovu sustavu, fotografijama i videozapisima uređaja te podacima o lokaciji (Ventrella, 2020). Slična se aplikacija pojavila pod nazivom CovidLock, a radilo se o ransomware napadu koji zaključa žrtvin mobilni uređaj ostavivši joj 48 sati da uplati 100 dolara u kriptovalutama ako ga želi oporaviti (Khan, Brohi i Zaman, 2020). Početkom pandemije došlo je i do porasta registriranih domena s ključnim riječima "COVID" i "korona" te se za mnoge smatra da su razvijene sa zlonamjernim ciljem *cyber* kriminalaca koji pokušavaju iskoristiti sve veći broj ljudi koji traže informacije o virusu. Od veljače do ožujka 2020. godine, Palo Alto Networks je kao jedan od Interpolovih privatnih partnera otkrio rast od 569% u registracijama zlonamjernih domena koje uključuju malware i phishing (Interpol, 2020a), a do kraja ožujka 2020. godine, otkrivene su 2.022 zlonamjerne i 40.261 visokorizična novoregistrirana domena (Interpol, 2020b). Poznati zlonamjerni softveri koji su bili relativno neaktivni, ponovno su otkriveni početkom izbijanja korona krize poprimajući nove oblike ili koristeći COVID-19 za jačanje taktika društvenog inženjeringa (Interpol, 2020c).

Cyber kriminalci vrebaju emocionalnu ranjivost ljudi do koje je došlo zbog neizvjesnosti i poteškoća tijekom pandemije, a procjenjuje se da je više od 80% eksploatacija uspješno

zahvaljujući upravo tehnikama društvenog inženjeringa (Naidoo, 2020). Naidoo (2020) u svojoj analizi *cyber* kaznenih djela za vrijeme pandemije zaključuje da kriminalci imaju tendenciju slijediti dinamički proces koji se sastoji od četiri razine: prikupljanje informacija o situacijskim čimbenicima, identificiranje ciljeva, odabir metoda napada i korištenje tehnika socijalnog inženjeringa. Isti autor smatra da počinitelji pribjegavaju sve lukavijim tehnikama integrirajući više elemenata situacijskih čimbenika u dizajne svojih prijevara. Mouton i sur. (2014; prema Ventrella, 2020) društveni inženjering definiraju kao "znanost o korištenju društvene interakcije kao sredstva za uvjeravanje pojedinca ili organizacije da udovolji specifičnom zahtjevu napadača gdje ili društvena interakcija, uvjeravanje ili zahtjev uključuju entitet povezan s računalom". Kriminalci često pribjegavaju metodama formuliranja lažnih poruka na način koji ostavlja dojam nagrađivanja žrtve za brzu akciju ili kažnjavanja za odgođenu akciju, npr. počinitelj koji se lažno predstavlja kao banka može koristiti kazne kao taktiku zastrašivanja kojom će vjerojatno potaknuti žrtvu na brzu akciju (Naidoo, 2020).

U ožujku 2020. godine dogodili su se razni *cyber* napadi diljem svijeta, a česta meta bile su bolnice i sveučilišta. Sveučilišna bolnica u Brnu koja posjeduje najveći laboratorij za testiranje na koronavirus u Češkoj, pogođena je ransomware napadom (Pranggono i Arabo, 2020). Incident je natjerao bolnicu da odgodi hitne operacije, preusmjeri nove akutne pacijente u obližnju alternativnu bolnicu i ugasi cijelu svoju informatičku mrežu. Ove vrste napada tijekom krize javnog zdravlja kao što je pandemija COVID-19 posebno su prijeteće i nose vrlo stvarne rizike za ljudske živote (Europol, 2020b). Ransomware je doživjela i medicinsko istraživačka tvrtka sa sjedištem u Londonu pri čemu su objavljeni osobni i medicinski podaci tisuća njihovih bivših pacijenata. Sustavi skupine bolnica u Parizu bili su meta DDoS napada koji su poremetili pristup poslužitelju i e-pošti, a sličan se napad dogodio i Američkom Ministarstvu zdravstva (Pranggono i Arabo, 2020). Početkom svibnja, NCSC je u UK-u izvijestio o nekoliko pokušaja *cyber* napada na sveučilišne institucije koje se bave istraživanjem koronavirusa i cjepiva s ciljem krađe informacija i ometanja usluga. Pokušani su krađa lozinki, ransomware i špijunaža, a sumnja se da su napadi došli od zlonamjernih strana iz stranih država (Saleous i sur., 2022). U lipnju 2020. godine meta je bilo Sveučilište Kalifornija San Francisco koje je radilo na cjepivu te je ransomware napadom prisiljeno platiti 1,14 milijuna dolara skupini *cyber* kriminalaca pod nazivom Netwalker (Pranggono i Arabo, 2020). U Africi je najozbiljniji napad pretrpio južnoafrički Life Healthcare Group odgovoran za 66 zdravstvenih ustanova (Interpol, 2021). Pokušaji hakiranja zdravstvenih

organizacija ukazali su na probleme povezane sa *cyber* sigurnošću u zdravstvenom sektoru, a jedan od glavnih razloga nezadovoljavajuće *cyber* sigurnosti ovakvih ustanova je ograničen proračun koji je obično pod strogom kontrolom s obzirom da se radi o gradskom ili državnom financiranju (Pranggono i Arabo, 2020). Unatoč brojnim ransomware napadima usmjerenim na zdravstvene ustanove, Europol (2020b) navodi da su se događali i prije nego što je kriza imala znatan učinak u Europi i SAD-u što sugerira da pandemija nije bila okidač za ove vrste napada. Budući da organizacije generalno trpe poremećaje u poslovanju kada ne mogu pristupiti svojim datotekama, kriminalci imaju relativno veliku šansu primiti isplatu zbog čega svoje ransomware napade usmjeravaju na podatke visoke vrijednosti ili imovinu unutar organizacija koja je posebno osjetljiva na zastoje tako da motivacija za plaćanje otkupnine bude visoka. Najbolji su primjer bolnice budući da prekid rada bolničkog informacijsko tehnološkog sustava potencijalno može dovesti do gubitka života dok su ostale napadačima atraktivne mete vladine agencije, sveučilišta i organizacije unutar proizvodnog sektora (Europol, 2020c). Ono što bolnice također čini privlačnima *cyber* kriminalcima je mogućnost brzog prikupljanja velike količine osobnih informacija koje poslije mogu prodati kao što su puna imena, osobni podaci i podaci kreditnih kartica (PwC, 2020; prema Chigada i Madzinga, 2021).

Prisutnost dezinformacija postala je ključna značajka korona krize te su mnoge države članice Europola prijavile probleme vezane uz širenje dezinformacija. Ovakve prijetnje nazivaju se hibridnima, a unatoč njihovu potencijalu za poticanje kriminalnih aktivnosti, agencije za provođenje zakona i državna zakonodavstva obično ne sankcioniraju širenje dezinformacija i lažnih vijesti (Europol, 2020b). Jedna od strategija ostvarivanja financijske dobiti bilo je širenje lažnih vijesti o mogućim lijekovima za COVID-19 i učinkovitim mjerama prevencije koje su kriminalcima omogućile prodaju artikala za koje tvrde da će spriječiti ili izliječiti virus (Europol, 2020b). Poznat je slučaj stranice „coronavirusmedicalkit.com" koju je izradio američki državljanin tvrdeći da WHO dijeli komplete cjepiva za čiju je dostavu potrebno uplatiti 4.95 dolara. Stranica je sadržavala poveznicu koja preusmjerava kupce na FedEx stranicu s logotipom gdje osoba treba unijeti podatke o kreditnoj kartici i potvrditi plaćanje. Počinitelj je na stranicu postavio i fotografiju dr. Anthonyja Faucija, direktora američkog Nacionalnog instituta za alergije i zarazne bolesti kako bi stvorio dojam pouzdanosti, a nekoliko je osoba pretrpjelo krađu identiteta i financijske gubitke uzrokovane radnjama okrivljenika (Eboibi, 2020).

Procvat u gospodarstvu pandemije doživljava i prodaja krivotvorene ili nekvalitetne robe, a osobito je velika potražnja za određenim vrstama zdravstvenih i higijenskih proizvoda (maske, rukavice, dezinfekcijski gelovi, farmaceutski proizvodi) što je stvorilo značajno tržište za krivotvoritelje proizvoda i prevarante (Europol, 2020c). Taktike vlasnika lažnih *web* stranica uključuju: kopiranje legitimne stranice, prodaju nelicenciranih artikala ili krivotvorene robe i primanje uplata za artikle koji nikad neće biti isporučeni (Interpol, 2020a). Meta su postala poduzeća koja kupuju spomenute potrepštine, a u jednoj državi članici Europola zabilježen je slučaj kupovine gelova i maski u vrijednosti od 6,6 milijuna eura koje oštećenoj tvrtki nikad nisu dostavljene. U drugom slučaju koji je prijavila država članica, tvrtka je pokušala kupiti 3,85 milijuna maski pri čemu je izgubila 300.000 eura (Europol, 2020c).

Cyber kriminalci iskorištavaju i situacijske čimbenike poput prelaska na rad od kuće i *online* nastavu kao i kritičnu ovisnost organizacija i pojedinaca o virtualnim okruženjima (Naidoo, 2020).

Organizacije su morale brzo prilagoditi sustave, mreže i aplikacije radu na daljinu dok su kriminalci povećane sigurnosne ranjivosti koje iz toga proizlaze iskoristili za krađu podataka, stvaranje profita i izazivanje poremećaja (Interpol, 2020a). Rad od kuće povećava izloženost *cyber* rizicima iz razloga što zaposlenici pristupaju korporativnim mrežama putem osobnih uređaja pri čemu se ponekad povezuju pomoću manje pouzdanih i nezaštićenih internetskih veza (Simonovich 2020; prema Chigada i Madzinga, 2021). Pandemija i posljedičan prelazak na daljinski rad (eng. *remote working*) mogu se smatrati katalizatorima porasta učestalosti napada na poslovnu e-poštu (eng. *Business Email Compromise*) i phishing napada s ciljem krađe podataka za prijavu u poslovne sustave (Venkatesha, Reddy i Chandavarkar, 2021). Ugrožavanje poslovne e-pošte (u daljnjem tekstu BEC) vrsta je prijevare usmjerena na organizacije radi stjecanja financijske dobiti ili krađe podataka. *Cyber* kriminalci u ovom kontekstu obično koriste *key logging* i *phishing* metode ili lažiraju legitiman račun e-pošte kako bi slali lažne e-poruke tražeći prijenos sredstava ili osjetljivih podataka predstavljajući se kao legitimni vlasnici računa pri čemu obično oponašaju rukovoditelje na visokoj razini koji rade u financijama (Interpol, 2021). Moguće je i oponašanje djelatnika tehnoloških tvrtki koji kontaktiraju poduzeće kako bi ponudili usluge videotelefonije ili neke druge (Naidoo, 2020). Učestalost BEC napada značajno je porasla i tvrtkama prouzročila vrlo visoke financijske gubitke u razdoblju rada

na daljinu (Al-Musib, Al-Serhani, Humayun i Jhanjhi, 2021). Osim toga, BEC napadi postali su sofisticiraniji, a njihovi su počinitelji počeli bolje odabirati mete (Europol, 2020b). Prema Trend Micro-u (Interpol, 2021), najviše pokušaja BEC-a bilo je u zemljama engleskog govornog područja kao što su SAD, Australija i UK. Izvješće o internetskom kriminalu za 2020. godinu FBI-jevog Centra za žalbe na internetski kriminal pokazuje da je BEC rezultirao s 19.369 prijavljenih pritužbi/kaznenih djela što je ukupno iznosilo 1,8 milijardi dolara gubitaka (FBI, 2020).

Online oblik školskog i fakultetskog obrazovanja postao je glavni način izvođenja nastave što je rezultiralo povećanom upotrebom telekonferencijskih *online* platformi. Kreator Zooma, Eric Yuan, izvijestio je o porastu broja korisnika s 10 milijuna diljem svijeta na otprilike 200 milijuna u ožujku 2020. godine (Saleous i sur., 2022). Analizom politike privatnosti aplikacija kao što su Google Meet, Microsoft Teams i Zoom, stručnjaci su zaključili da prikupljaju više podataka nego što njihovi korisnici misle dok je Zoom koji je ujedno i najrašireniji alat za internetske konferencije bio na meti kritika stručnjaka za *cyber* sigurnost koji su upozorili da nije dovoljno siguran (Khan, Brohi i Zaman, 2020). Pojavio se i novi fenomen nazvan *Zoom bombing*, a odnosi se na neželjene upade u videopozive (neovisno o imenu telekonferencijske platforme na kojoj se odvijaju). Sigurnosne ranjivosti u softveru ovakvih platformi dopuštaju hakerima da presretnu vjerodajnice za autentifikaciju i ubace nepoželjan sadržaj kao što su pornografski materijali i nasilne slike u naizgled sigurne *online* sastanke (Weil i Murugesan, 2020). Jedan se ovakav slučaj dogodio na indijskom Nirma Sveučilištu gdje je u Zoom *online* predavanje upao haker i počeo masturbirati (Upadhyay i Rathee, 2022). Postoji niz medijskih izvješća da su dječja pornografija i seksualno iskorištavanje još jedan potencijalni rizik povezan s pandemijom. Odjel FBI-ja u Bostonu izvijestio je da se diljem države Massachusetts pojavljuju otmice video telekonferencija s ciljem seksualnog iskorištavanja djece te da se videopozivi prekidaju pornografskim fotografijama (Olofinbiyi i Singh, 2020).

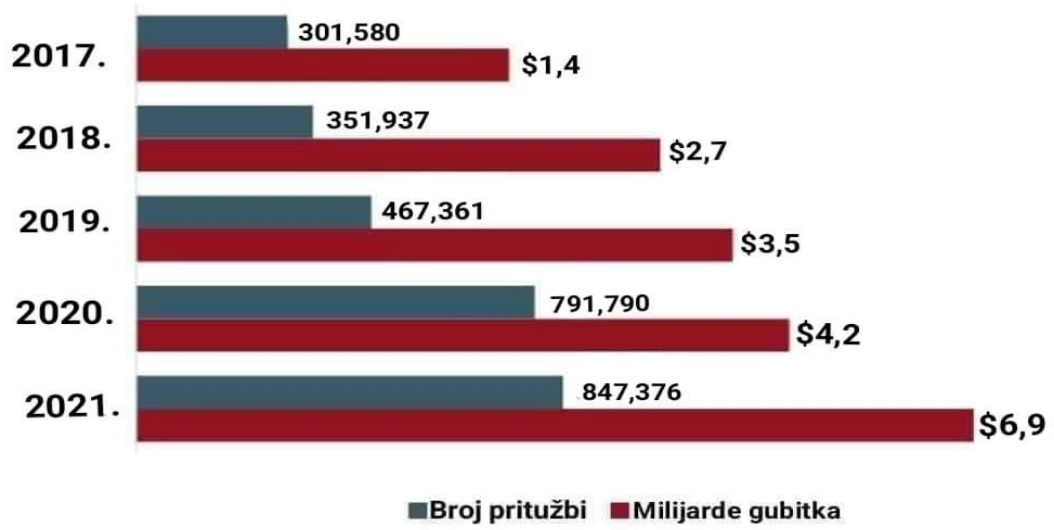
Prema Europolu (2020a), zemlje članice izvijestile su o porastu broja pokušaja pristupa ilegalnim *web* stranicama koje sadrže materijale seksualnog iskorištavanja djece (eng. *child sexual exploatation material*, u daljnjem tekstu CSEM) blokirane njihovim filtrima. U Španjolskoj je primijećen značajan porast broja pritužbi na CSEM od početka ožujka 2020. godine dok je Danska izvijestila o trostrukom porastu pokušaja pristupanja ovakvim ilegalnim *web* stranicama. CSEM se također nastavlja distribuirati putem platformi Dark

weba na kojem postoje znakovi povećanja aktivnosti oko ove kriminalne domene za vrijeme trajanja pandemije (Europol, 2020a). Jedan od pokretača stalnog rasta CSEM-a na internetu je materijal koji djeca produciraju sama čemu je značajno doprinijela karantena povezana s koronavirusom zbog koje su djeca više vremena provela na internetu dijeleći slike i videozapise koji su kasnije završili kod počinitelja (Europol, 2020b). Također, raširenији su postali prijenosi uživo (eng. *livestreams*) seksualnog zlostavljanja djece te se njihov broj nastavlja povećavati (Europol, 2020b).

Jedan od Interpolovih partnera iz privatnog sektora navodi da je u razdoblju od siječnja do kraja travnja 2020. godine otkriveno 907.000 neželjenih poruka, 737 incidenata povezanih sa zlonamjernim softverom i 48.000 zlonamjernih URL-ova, a sve navedeno bilo je povezano s bolešću COVID-19 (Interpol, 2020a). U travnju je FBI-jev Centar za žalbe na internetski kriminal dnevno primao između 3 i 4 tisuće pritužbi u vezi sa *cyber* sigurnošću u usporedbi s prosječnih tisuću dnevnih pritužbi prije pandemije (Cimpanu, 2020; prema Naidoo, 2020). Američka savezna komisija za trgovinu procijenila je da je 12 milijuna dolara izgubljeno zbog prijevarnih aktivnosti povezanih s koronavirusom između siječnja i 14. travnja 2020. godine s ukupno 18.235 prijava (ZDNet, 2020; prema Hakak, Khan, Imran, Choo i Shoaib, 2020). Tijelo za prepoznavanje i izbjegavanje prijevara Australske komisije za tržišno natjecanje i zaštitu potrošača pod nazivom Scamwatch od pojave koronavirusa primilo je više od 6.415 prijava prijevara u kojima se spominje COVID-19 (najčešće phishing krađe osobnih podataka te prijevare vezane uz *online* shopping i mirovinsko osiguranje) s više od 9.800.000 američkih dolara gubitaka (Scamwatch, 2021).

Centar za žalbe na internetski kriminal FBI-ja (u daljnjem tekstu IC3) središte je za upozoravanje javnosti i domaćin portala na kojem žrtve mogu prijaviti internetske kriminalne aktivnosti. Osim toga, IC3 izvršava analize, bavi se povratom imovine te je u partnerstvu s privatnim sektorom kao i s lokalnim, državnim, federalnim i međunarodnim agencijama. Svaku podnesenu pritužbu pregledava IC3 analitičar, kategorizira je prema vrsti kaznenog djela i prilagođava visinu gubitka ukoliko podaci o pritužbi ne podržavaju prijavljeni iznos (FBI, 2021). Uvidom u podatke IC3 može se saznati da je u posljednjih 5 godina zaprimljeno prosječno 552.000 pritužbi godišnje na širok spektar internetskih prijevara koje su utjecale na žrtve diljem svijeta. Ne računajući SAD, najviše je pritužbi 2020. godine došlo iz UK, Indije, Kanade, Grčke i Australije (FBI, 2020). Zanimljiv je

podatak da su najviše pritužbi 2020. i 2021. godine podnijele osobe starije od 60 godina, a pretrpjele su i najveće financijske gubitke (FBI, 2020, 2021). Ukupan broj pritužbi u razdoblju od 2017. do 2021. godine iznosi 2,76 milijuna dok se gubici penju na ukupno 18,7 milijardi dolara. Primjetan je trend rasta u broju pritužbi, a najveći je skok zabilježen upravo s 2019. na 2020. godinu. S brojem pritužbi rastu i financijski gubici pri čemu je najveći skok vidljiv s 2020. na 2021. godinu koja bilježi najdrastičnije gubitke u posljednjih 5 godina.



Slika 1: Broj pritužbi i visina gubitaka u razdoblju od 2017. do 2021. godine (FBI, 2021).

Podaci IC3 kontinuirano pokazuju da su u razdoblju od 2017. do 2021. godine najzastupljenije bile pritužbe koje su analitičari prema vrsti kategorizirali u:

1) phishing,
2) prijevara neisplaćeno/neisporučeno,
3) iznuda,
4) neovlašten pristup i korištenje osobnih podataka i
5) krađa identiteta.

IC3 definira phishing kao upotrebu neželjene e-pošte, tekstualnih poruka (eng. *smishing*) i telefonskih poziva (eng. *vishing*) od strane navodno legitimne tvrtke koja zahtijeva osobne podatke i/ili vjerodajnice za prijavu. Neplaćanje/neisporuka (eng. *non-payment/non delivery*) odnosi se na 2 slučaja: 1) roba ili usluge se isporuče, a plaćanje se ne izvrši, 2) uplata je napravljena, ali se roba/usluge nikad ne isporuče ili budu slabije kvalitete. Kategorija iznude (eng. *extortion*) podrazumijeva nezakonito izvlačenje novca ili imovine

putem zastrašivanja ili neopravdanog korištenja vlasti te može uključivati prijetnje fizičkom ozljedom ili kaznenim progonom. *Personal data breach* tj. neovlašten pristup i korištenje osobnih podataka opisan je kao sigurnosni incident u kojem se osjetljivi, zaštićeni ili povjerljivi podaci pojedinca kopiraju, prenose, pregledavaju, kradu ili ih koriste neovlaštene osobe. IC3 navodi da se krađa identiteta (eng. *Identity theft*) odnosi na slučajeve krađe i korištenja osobnih podataka za identifikaciju (npr. imena ili broja socijalnog osiguranja) bez dopuštenja za počinjenje prijevare ili drugih zločina (FBI, 2021).

Tablica 1: Broj pritužbi na najučestalijih 5 vrsta *cyber* kriminaliteta u posljednjih 5 godina

	2017.	**2018.**	**2019.**	**2020.**	**2021.**
Phishing/Smishing/Vishing	25344	26379	114702	241342	323972
Prijevara neplaćeno/neisporučeno *(Non-payment/non-delivery)*	84079	65116	61832	108869	82478
Iznuda *(Extortion)*	14938	51146	43101	76741	39360
Neovlašten pristup i korištenje osobnih podataka *(Personal Data Breach)*	30904	50642	38218	45330	51829
Krađa identiteta *(Identity Theft)*	17636	16128	16053	43330	51629

Izvor: 2021 Internet Crime Report (FBI, 2021).

Uvidom u podatke IC3 može se zaključiti da 3 od 5 kategorija najučestalijih pritužbi u posljednjih 5 godina pokazuju rastući trend s 2020. na 2021. godinu (phishing, neovlašten pristup i korištenje osobnih podataka te krađa identiteta), a isto je vidljivo s 2019. na 2020. godinu u svih 5 kategorija. Najveći porast pritužbi zabilježen je u kategoriji phishinga koji neumorno dostiže sve veće brojke održavajući rastući trend još od 2018. godine što nije slučaj s ostalim kategorijama koje su barem jednom u petogodišnjem razdoblju zabilježile pad. Iako broj pritužbi na prijevare neplaćenog/neisporučenog generalno ne pokazuje rastući

trend u spomenutom razdoblju, zanimljiv je skok s 2019. na 2020. godinu s obzirom da se radi o povećanju od čak 47.037 pritužbi. Ista je situacija s krađom identiteta kod koje je prisutan stabilan trend sve do 2020. godine koja je donijela povećanje od čak 27.277 pritužbi u odnosu na 2019. godinu, a rastući trend se nastavlja i u 2021. godini. Pri tumačenju ovih podataka treba imati na umu da broj pritužbi ne predstavlja broj pojedinaca koji su podnijeli pritužbu. Također, postoji mogućnost da su neki od podnositelja pritužbi učinili to više puta za isto kazneno djelo.

5.1. Promjene u pojavnim oblicima *cyber* kriminaliteta

Cyber kriminalci su se uspjeli brzo prilagoditi, iskoristiti tjeskobe i strahove čovječanstva te raznim kriminalnim metodama iskoristiti krizu za vlastite interese. Tipovi kriminalaca koji iskorištavaju pandemiju bili su aktivni i prije nje, ali se vjeruje da su za vrijeme pandemije intenzivirali svoje aktivnosti i aktivno vrbovali suradnike kako bi maksimalno povećali njihov učinak (Europol, 2020b). Pandemija koronavirusa pokazala je kako *cyber* kriminal u svojoj srži uglavnom ostaje isti, ali se metodama društvenog inženjeringa mijenjaju specifičnosti kriminalnog pristupa kako bi bile usklađenije s društvenim kontekstom čime se povećavaju stope uspješnosti napada. *Cyber* kriminalci pokazuju poboljšanu razinu operativne sigurnosti i visoku svijest o načinima sakrivanja identiteta i kriminalne aktivnosti od tijela za provođenje zakona i kompanija iz privatnog sektora (Europol, 2020b). Ključni trend 2020. godine odnosi se na rastuću sofisticiranost phishinga koji je postalo teže otkriti, a *web* stranice za krađu identiteta postale su gotovo identične onima koje nastoje imitirati. Phishing kampanje postale su automatiziranije prisiljavajući ispitanike da brže djeluju jer u nekim slučajevima između krađe podataka i napada prođe tek 24 sata. Nadalje, počele su se primjenjivati cjelovitije strategije phishinga pokazujući visoke razine kompetencija kriminalaca vezane uz korištenje alata, sustava i njihovih ranjivosti koje iskorištavaju preuzimajući lažne identitete. U nekim slučajevima, u trenutku istrage krađe identiteta, cijela kriminalna infrastruktura već je nestala (Europol, 2020b). Nadalje, napadi su postali mnogo ciljaniji. Počinitelji se specijaliziraju za aktivnosti prikupljanja informacija i profiliranja žrtava pri čemu se više fokusiraju na pomno odabrane osobe nego na nasumične skupine s ciljem optimizacije financijske dobiti (Europol, 2020b). U doba pandemije izričito se ciljalo na stariju populaciju (često manje senzibiliziranu za *online* rizike) kako bi preuzeli i proslijedili zaražene poveznice neželjene e-pošte vezane uz virus i proširili dezinformacije među prijateljima i obitelji (UNODC, 2020). Cybercrime kao usluga (eng. *Cybercrime-as-*

a-Service) olakšava phishing i ransomware te preko ponuda na Dark webu pomaže kriminalcima da značajno poboljšaju tehničku složenost svojih napada ukoliko to ne znaju izvesti samostalno. Sofisticiranije su postale i metode napada ransomwareom te je razdoblje između početne infekcije i aktivacije postalo kraće. Također, sposobnost organa za provođenje zakona da prate plaćanja povezana s kriminalnim aktivnostima postala je znatno niža zahvaljujući korištenju kriptovaluta (Europol, 2020b). Dok ukupni troškovi ulaganja u ransomware rastu kao i štete uzrokovane zastojima u radu ustanova koje pogađa, ujedno raste i potencijalna zarada napadača. U 2020. godini, u većini država članica EU zabilježen je veći broj ugrožavanja poslovne e-pošte (BEC) što je u skladu s rastućom sofisticiranošću metoda i ciljanijim pristupom kriminalaca. Sofisticiranost BEC-a odražava se u uspostavi složenih kriminalnih mreža koje služe za pranje prihoda stečenih prijevarom, a napredne metode sežu čak do korištenja umjetne inteligencije za oponašanje glasa utjecajnih čelnika kompanija (Europol, 2020b).

5.2. C*yber* kriminalitet u Hrvatskoj

Nacionalni CERT odjel je Hrvatske akademske i istraživačke mreže (CARNET) osnovan 2007. godine prema Zakonu o informacijskoj sigurnosti Republike Hrvatske kako bi obnašao ulogu nacionalnog tijela za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava. Osnovna zadaća CERT-a je obrada računalno-sigurnosnih incidenata s ciljem očuvanja *cyber* sigurnosti u državi (CERT, 2020). Tijekom 2020. godine zaprimio je i obradio ukupno 1710 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u njihovoj nadležnosti, a vodeći tipovi incidenata bili su phishing URL, phishing i pogađanje zaporki. Uvidom u podatke CERT-a moguće je zaključiti da je cyber kriminalitet u Hrvatskoj donekle pratio svjetske trendove: zabilježene su phishing kampanje sa zlonamjernim privicima poput Emoteta vezane uz COVID-19 i phishing napadi koji uključuju lažna predstavljanja (WHO, Ministarstvo zdravstva Republike Hrvatske). Primjetna su dva skoka u broju incidenata, a prvi je zabilježen u travnju radi povećanog broja incidenata uslijed velikog broja phishing kampanja vezanih uz COVID-19. U tom su razdoblju mnoge države bile u *lockdownu* zbog čega se poslovanje brojnih tvrtki prebacilo na model rada od kuće što je napadačima dalo dodatnu motivaciju za kreiranje phishing kampanja (CERT, 2020).

Temeljem podataka Državnog zavoda za statistiku (DZS, 2017, 2018, 2019) te statističkih pregleda temeljnih sigurnosnih pokazatelja i rezultata rada (Ministarstvo unutarnjih poslova, 2020, 2021) može se doći do sljedećih statističkih podataka o kaznenim djelima protiv računalnih sustava, programa i podataka:

Tablica 2: Broj osuđenih osoba prema spolu i dobi za razdoblje od 2017. do 2021. godine

	UKUPAN BROJ OSUĐENIH	M	Ž	MALOLJETNE OSOBE	MLAĐI PUNOLJETNICI	PUNOLJETNE OSOBE
2017.	78	53	25	0	10	68
2018.	111	82	29	3	18	90
2019.	111	93	18	1	15	95
2020.	138	110	28	10	10	118
2021.	153	105	48	12	15	126

Izvor: DZS (2017, 2018, 2019) i Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2020. i 2021. godini (Ministarstvo unutarnjih poslova, 2020, 2021)

Uzevši u obzir podatke o broju osoba osuđenih za kaznena djela iz Glave XXV. unazad zadnjih 5 godina, uočljiv je trend rasta. Osobito je primjetan u skupini maloljetnih osoba gdje se broj osuđenih u 2020. godini, u odnosu na prethodnu godinu, udeseterostručio. Broj punoljetnih počinitelja dosljedno, iz godine u godinu, pokazuje rastući trend: 2017. je osuđeno 68 osoba, 2018. 90, 2019. 95, 2020. godine 118 osoba dok je 2021. godine broj punoljetnih osuđenika iznosio 126. Zanimljiva je činjenica da u 2020. godini postotak žena među osuđenima za kaznena djela protiv računalnih sustava, programa i podataka iznosi 20.29% dok je njihov udio u ukupnom kriminalitetu iste godine bio tek 13%. U 2021. godini, počiniteljice su činile 14.38% ukupnog kriminaliteta dok su žene osuđene za kaznena djela protiv računalnih sustava, programa i podataka bile odgovorne za čak 31.73% počinjenih kaznenih djela iz te skupine (Ministarstvo unutarnjih poslova, 2020; 2021).

Tablica 3: Broj prijavljenih i osuđenih osoba prema godini i vrsti kaznenog djela

P=prijavljeni, O=optuženi, Os=osuđeni

	2019.			2020.		2021.	
	P	O	Os	P	Os	P	Os
UKUPNO	656	119	111	1033	138	1297	153
Neovlašteni pristup	40	2	2	19	5	32	5
Oštećenje računalnih podataka	17	1	1	12	1	21	2
Ometanje računalnog sustava	12	2	2	7	1	10	1
Neovlašteno presretanje podataka	6	0	0	1	0	2	1
Računalno krivotvorenje	16	2	2	26	6	70	5
Računalna prijevara	552	108	100	951	122	1159	139
Zlouporaba naprava	13	4	2	17	3	4	0

Izvor: DZS (2019) i Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2020. i 2021. godini (Ministarstvo unutarnjih poslova, 2020, 2021)

Ono što pri prvom pogledu na tablicu s podacima o kaznenim djelima *cyber* kriminaliteta postaje očito je veliki nesrazmjer između broja prijavljenih i osuđenih osoba. U 2019. godini prijavljeno je 656 kaznenih djela od kojih za njih 457 nije poznat počinitelj, a optuženo je samo 119 osoba. Sljedeće su godine prijavljena 1033 kaznena djela od čega je poznatih počinitelja bilo samo 26. Možemo zaključiti da je broj osoba koje prođu nekažnjeno iznimno visok. Najučestalije kazneno djelo koje ujedno pokazuje popriličan uzlazni trend je računalna prijevara. Broj prijava je 2020. godine u odnosu na prethodnu godinu porastao za 42% dok je 2021. godine prijava bilo 18% više nego u 2020. godini. Računalna prijevara tvorila je 84% prijavljenih kaznenih djela protiv računalnih sustava, programa i podataka

2019. godine, čak 92% 2020. godine dok se 2021. godine 89.36% prijavljenih kaznenih djela *cyber* kriminaliteta odnosilo na računalne prijevare. Drugo najučestalije prijavljivano kazneno djelo je neovlašteni pristup, a slijede ga računalno krivotvorenje i oštećenje računalnih podataka. Interesantan je trend porasta broja prijava za računalno krivotvorenje što je moguće dovesti u vezu s krivotvorenjem potvrda o cijepljenju protiv koronavirusa pri čemu je osobito indikativan broj prijava u 2021. godini koji je iznosio čak 70. Svi su zaključci doneseni na temelju statističkih podataka DZS-a što s obzirom na tamnu brojku kriminaliteta i mali broj poznatih počinitelja u velikom broju prijava ne pruža sveobuhvatne informacije.

6. Zaključak

Razdoblje pandemije bilo je izazovno i zahtjevno te je sa sobom donijelo brojne promjene kojima se društvo moralo prilagoditi. Iznimne sposobnosti prilagodbe iskazali su *cyber* kriminalci koji su se dokazali kao pravi oportunisti nemilosrdno koristeći najljudskiji strah, onaj za vlastito zdravlje i život. Sudeći prema svemu iznesenom u ovom radu, možemo zaključiti da je doba pandemije bilo pogodno za *cyber* kriminalce koji su vješto profitirali iskoristivši velik interes čovječanstva za informacije o koronavirusu, pomoć bolešću ugroženim državama/osobama i nabavu higijenskih potrepština bez kojih je život postao nezamisliv. S obzirom na prikupljene i u radu prikazane inozemne i državne podatke, primjetan je uzlazan trend broja kaznenih djela iz područja *cyber* kriminaliteta. Prema stranim podacima, globalni porast vidljiv je u razdoblju od 2019. do 2021. godine dok nacionalni podaci pokazuju uzlazni trend već od 2017. godine. Prema podacima FBI-jeva Centra za žalbe na internetski kriminal, najviše je pritužbi u razdoblju od 2017. godine do 2021. godine pristiglo upravo za phishing i prijevare s neisporukom ili neplaćanjem dobara i usluga. Kod prijevara s neisporukom ili neplaćanjem, interesantan je skok s 2019. na 2020. godinu s obzirom da se radilo o povećanju od čak 47.037 pritužbi iz čega možemo zaključiti da je pandemija kriminalcima pružila dodatne prilike. Kao trenutačno najveći i najrašireniji problem, osobito na globalnoj razini, nemoguće je ne istaknuti phishing koji već malim brojem klikova kriminalcima može osigurati dobru zaradu. Tijekom pandemije, zabilježeni su brojni ransomware napadi na razne ustanove diljem svijeta koje su kriminalcima općenito privlačne neovisno o nastaloj situaciji s obzirom na veliku vjerojatnost uspješnog i materijalno unosnog napada. Možemo zaključiti da *cyber* kriminalci čine sve kako bi se domogli što više novca pritom se često služeći metodama socijalnog inženjeringa čija

sofisticiranost postaje pomalo zastrašujuća. Na nacionalnoj razini, u trogodišnjem razdoblju od 2019. do 2021. godine prednjači kazneno djelo računalne prijevare koja bilježi rastući trend pri čemu je u 2020. godini bilo 399 prijava više u odnosu na 2019. godinu dok je u 2021. godini bilo 108 prijava više nego prethodne godine. Indikativno je da je u 2021. godini zabilježen velik porast prijava računalnog krivotvorenja što možemo pripisati krivotvorenju potvrda o cijepljenju protiv COVID-19. Također, zanimljiva je činjenica da u Republici Hrvatskoj više žena sudjeluje u kaznenim djelima *cyber* kriminaliteta nego u ukupnom kriminalitetu.

Pojava pandemije i mjera održavanja koronavirusa pod kontrolom prisilili su ljude na brojne prilagodbe i promjene s naglaskom na novonastalu pojačanu ovisnost o informacijsko komunikacijskoj tehnologiji: rad od kuće, *online* nastavu i virtualno održavanje međuljudskih odnosa. Zajednička karakteristika udaljenih načina poslovanja i obrazovanja je činjenica da su se tvrtke, fakulteti i škole zajedno sa svojim zaposlenicima, studentima i učenicima našli u novoj situaciji za koju vjerojatno nisu dovoljno informatički educirani kao ni svjesni *cyber* opasnosti. Moguće je da su zaposlenici tvrtki, škola i fakulteta imali poteškoća sa snalaženjem u novim uvjetima rada što su *cyber* kriminalci pokušavali iskoristiti. Također, djeca su zahvaljujući globalnim zatvaranjima (eng. *lockdown*) provela više vremena kod kuće i na internetu nego što bi to bio slučaj u normalnim uvjetima čime su potencijalno postala ugroženija i nedvojbeno dostupnija. Ova je okolnost doprinijela porastu materijala dječjeg seksualnog iskorištavanja koji djeca proizvode samostalno, a sama je pandemija donijela porast potražnje za ovakvim materijalima kao i porast aktivnosti oko ove domene na Dark webu. Sudeći prema inozemnim podacima, starija je populacija još jedna od skupina koje su se našle na meti *cyber* kriminalaca koji računaju na njihovu naivnost i manju senzibiliziranost za *cyber* rizike. Prema Bači i Ćosiću (2013), najčešći uzroci zbog kojih građani i poduzeća postaju žrtve *cyber* kriminaliteta su upravo sigurnosni propusti i needuciranost u domeni informacijsko komunikacijske tehnologije.

Strategije situacijske prevencije kriminaliteta koje se mogu neposredno primijeniti na *cyber* kriminalitet su prvenstveno povezane s pokušajima otežavanja počinjenja kaznenih djela tj. jačanjem sigurnosti korisnikova računala, sustava i osobnih podataka (Newman i Clarke, 2003; prema Holt i Bossler, 2016). Ovaj se prevencijski pristup doima najzastupljenijim te se očituje u borbi sa zlćudnim programima koji često potpomažu i tvore razne oblike hakiranja, phishinga i zlonamjernih domena (što je bio slučaj i u razdoblju pandemije koje

bilježi porast malicioznih domena, phishinga i malicioznih softvera). Zloćudni programi reguliraju se antivirusnim programima, a njihov su izvor: 1) e-pošta (dolaze u privitku koji korisnika usmjerava na *web* stranicu), 2) komunikacijske mreže (npr. poruke na Whatsappu i Viberu), 3) društvene mreže (npr. komentari na Facebooku), 4) prijenosni mediji (npr. USB stick), 5) ranjive mrežne usluge na računalu te 6) preuzimanje i instalacija neprovjerenih programa s interneta (Vuković, 2018). Antivirusni programi su alati koji nadziru poruke koje korisnik dobiva te ga upozoravaju pri preuzimanju datoteka i programa s interneta, a mogu raditi na dva načina: 1) skenirati računalo kako bi otkrili postojanje „otisaka" zloćudnih programa (preduvjet je da je antivirusna tvrtka identificirala „otisak" kao maliciozan zbog čega je bitno ažurirati bazu zloćudnih programa u antivirusnom alatu jer neidentificirani programi ne mogu biti otkriveni), 2) nadzirati sustav i programe koji se izvode kako bi detektirali rizične i atipične obrasce poput programa koji pristupa resursima koji mu zapravo ne trebaju, podacima drugih programa ili otvara mrežne konekcije iz nejasnih razloga (Vuković, 2018). Sustavi iz druge skupine posjeduju veću funkcionalnost nadzora računala i ubrajaju se u domenu sustava za otkrivanje uljeza (eng. Intrusion Detection System, u daljnjem tekstu IDS) čija je mana što ne mogu uvijek prepoznati je li neki program doista prijetnja pri čemu kao takve ponekad označavaju legitimne programe. O prijetnji se često obavještava korisnik koji sam odlučuje kako će postupiti, a problem se javlja kad isti nema dovoljno tehničkih znanja da bi razumio što podaci koje mu sustav nudi znače (Vuković, 2018). Postoje oblici IDS-a koji rade proaktivno pri čemu sustav automatski odgovara na prijetnje (na taj se način zaobilazi problem neinformiranih korisnika). Usprkos nedostacima, IDS je iznimno vrijedan jer funkcionira drugačije i naprednije od antivirusnih alata i vatrozida (Scarfone i Mell, 2010.; prema Holt i Bossler, 2016). Antivirusni alati utemeljeni na otiscima ne daju informacije o cjelokupnim obrascima prometa određene mreže te samo zaustavljaju napade na pojedinačni sustav dok vatrozidi ograničavaju pristup različitim mrežnim resursima koji dolaze izvan granica mreže, ali ne daju informacije o unutarnjim prijetnjama kao ni upozorenje na otkrivene prijetnje (Scarfone i Mell, 2010.; prema Holt i Bossler, 2016). Poduzeća mogu koristiti različite alate za otkrivanje napada kao što je IDS te na taj način osigurati resurse za ograničavanje vjerojatnosti infekcija i phishing kampanja, ali ako zaposlenici nemarno koriste strategije *cyber* sigurnosti, od njih neće biti prevelike koristi (Holt i Bossler, 2016). Jednom kada počinitelj uspješno pristupi sustavu određene organizacije, vrlo je vjerojatno da će tražiti povjerljive podatke koji mu mogu osigurati materijalnu dobit zbog čega su tvrtke razvile mehanizme skrivanja ili maskiranja podataka što također pripada strategijama situacijske prevencije te pomaže kod kaznenih djela

povezanih s obmanom i krađom (Fujinkoki, 2015; Newman i Clarke, 2003; Oracle, 2013; prema Holt i Bossler, 2016). Prema Fischeru (2016), upravljanje rizicima od *cyber* napada obično uključuje: 1) uklanjanje izvora prijetnje (npr. zatvaranjem botneta ili smanjenjem prilika za kriminalce), (2) rješavanje ranjivosti putem jačanja IKT imovine (npr. krpanjem softvera i obukom zaposlenika) i (3) smanjenje utjecaja ublažavanjem štete i obnavljanjem funkcija (npr. raspolaganjem rezervnim resursima koji osiguravaju kontinuitet operacija kao odgovor na napad). Vezano uz jačanje IKT imovine i mrežne sigurnosti, potrebno je redovito ažurirati nove zakrpe, tj. nadogradnje operacijskog sustava i aplikacija koje dorađuju pronađene sigurnosne propuste (Vuković, 2018).

Možemo zaključiti da je većina metoda prevencije usmjerena na jačanje računalnih sustava i podataka s ciljem otežavanja raznih *cyber* napada i neovlaštenog ulaska u računalni sustav. Prevencija *cyber* kriminaliteta neophodna je i korisna za njegovo suzbijanje, ali kao i kod svake druge vrste kriminaliteta, ima svoja ograničenja i poteškoće. Stječe se dojam da su spomenute preventivne metode orijentirane na kaznena djela s računalom u fokusu (*cyber* ovisna kaznena djela) dok su *cyber* omogućena kaznena djela tj. ona potpomognuta računalima prevencijski zahtjevnija i kompleksnija. Problem prevencije je činjenica da kaznena djela poput prijevara, krađa identiteta, ugrožavanja poslovne e-pošte i phishinga računaju na ljudsku pogrešku koju nije jednostavno prevenirati s obzirom da ljudi kao korisnici interneta, kućnih i korporativnih sustava ponekad namjerno zanemaruju smjernice za očuvanje *cyber* sigurnosti, čine nehotične pogreške ili nisu svjesni opasnosti. Neophodan je multidisciplinarni pristup koji bi spojio znanja i vještine informacijsko tehnoloških stručnjaka i kriminologa te je vjerojatno da će se kao takav pokušati nametnuti pristup situacijske prevencije.

Ono što spaja tvrtke, njihove zaposlenike, obrazovne ustanove, njihove polaznike i stariju populaciju je zajednička potreba za edukacijom i osvješćivanjem opasnosti koje skriva internet. Potrebna je edukacija mlađih naraštaja popraćena razvijanjem informatičke pismenosti već od osnovne škole s obzirom da djeca rano počinju koristiti internet i društvene mreže pritom ne razmišljajući o phishingu i ostalim oblicima *cyber* kriminaliteta za koje možemo pretpostaviti da će u budućnosti biti još napredniji i opasniji. S obzirom na zabilježen porast ugrožavanja poslovne e-pošte (eng. *Business Email Compromise*) i općenitu podložnost ransomware napadima, tvrtke i javne ustanove trebale bi posvetiti više pažnje *cyber* sigurnosti i edukaciji netehničkog osoblja u što je potrebno uložiti dodatna

sredstva i resurse. Sudeći prema inozemnim i nacionalnim podacima (prikazanima u ovom radu) koji sugeriraju značajan trend porasta phishinga, prevencija istog nije jednostavan zadatak. Budući da se radi o najčešćem vektoru napada s nekom vrstom društvenog inženjeringa, korisnici bi trebali biti izrazito sumnjičavi prema porukama upitnog sadržaja te uvijek provjeriti istinitost poruke prije nego li postupe prema dobivenim uputama, odaju vlastitu lozinku, podlegnu prijevari ili instaliraju potencijalno zloćudni program. Osim toga, ne bi smjeli nasjedati na ponude besplatnih sadržaja, programa i medija (Vuković, 2018). Isto vrijedi za prijevare s neplaćanjem i neisporukom usluga ili dobara koje su prema inozemnim podacima u korona krizi zabilježile velik porast. Potreban je oprez i pažljiva inspekcija stranice što može biti zahtjevno s obzirom da su lažne stranice postale iznimno uspješne u imitiranju legitimnih. Prevencija mora polaziti od edukacije i senzibilizacije za problem, a prvi bi korak trebalo biti približavanje informatičkog rječnika široj javnosti s obzirom da većina osoba koje koriste internet vjerojatno ne bi znala odgovoriti na pitanje što je to phishing ili lažna stranica (eng. *spoof*).

Svijet današnjice ima tendenciju digitalizacije gotovo svega zbog čega nije izgledno da će *cyber* kriminalitet u budućnosti biti manje zastupljen. Relativno mali rizik detekcije i mala ulaganja vjerojatno će nastaviti biti privlačni čimbenici za upuštanje u počinjenje ovakvih kaznenih djela. Sudeći prema podacima prikazanim u radu, može se očekivati daljnji uzlazni trend kaznenih djela iz ovog područja. S obzirom na konstantne tehnološke pomake i nova dostignuća, sigurno je pretpostaviti da će *cyber* kriminalci uvijek tražiti način da upotrijebe korisne izume u antisocijalne svrhe. Tehnološki napredci i nove društvene situacije u budućnosti neupitno će sa sobom donositi neke nove izazove iz područja *cyber* kriminaliteta s kojima će se čovječanstvo morati nositi, a najslabija karika u čuvanju digitalnih informacija vjerojatno će zauvijek biti ljudi. Iz tog razloga, važno je prevencijske napore uložiti u edukaciju te osvijestiti cjelokupnu populaciju o rizicima koji vrebaju iz *cyber* prostora. Održavanje sigurnosti osoba u *cyber* prostoru golem je i transnacionalan zadatak koji iziskuje jačanje međunarodne suradnje i dijaloga između vlada, UN-a, Europola, Interpola i brojnih drugih organizacija.

7. Literatura

1. Al-Musib, N.S., Al-Serhani, F.M., Humayun, M. i Jhanjhi, N.Z. (2021). Business email compromise (BEC) attacks. Materials Today: Proceedings. doi: 10.1016/j.matpr.2021.03.647

2. Bača, M. i Ćosić, J. (2013). Prevencija računalnog kriminaliteta. Policija i sigurnost, 22 (1), 146-158. Preuzeto 31.8.2022. s https://hrcak.srce.hr/105623

3. Britannica Dictionary (2022). https://www.britannica.com/dictionary/online (pristupljeno 23.8.2022).

4. Carević, N. (2022). Kaznena djela počinjena uporabom računala, računalnih sustava i programa (Diplomski rad). Sveučilište u Zagrebu, Pravni fakultet, Zagreb. Preuzeto 3.8.2022. s https://urn.nsk.hr/urn:nbn:hr:199:529680

5. Chandra, A. i Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. International Journal of Accounting Information Systems, Vol. 38/2020 (100467), 1-20.

6. Chawki, M., Darwish, A., Khan, M. A., i Tyagi, S. (2015). Cybercrime, Digital Forensics and Jurisdiction. Springer International Publishing.

7. Chigada, J. i Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review, South African Journal of Information Management 23(1), a1277. doi: https://doi.org/10.4102/sajim.v23i1.1277

8. Choi, K., Lee, C. S. i Louderback, E. R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 27-43). Springer International Publishing

9. Council of Europe (2022). https://www.coe.int/en/web/cybercrime/the-budapest-convention (pristupljeno dana 12.8.2022.)

10. Cross, C. (2020). Romance Fraud. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 917-937). Springer International Publishing

11. Državni zavod za statistiku, https://dzs.gov.hr/ (pristupljeno dana 18.8.2022.)

12. Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and

institutional accountability. Commonwealth Law Bulletin, 46:1, 78-109, doi: 10.1080/03050718.2020.1748075

13. Europol (2020). Catching the virus – Cybercrime, disinformation and the Covid-19 pandemic. Preuzeto 15.8.2022. s https://www.europol.europa.eu/cms/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

14. Europol (2020). Internet Organised Crime Threat Assessment (IOCTA). Luxembourg: Publications Office of the European Union. Preuzeto 13.8.2022. s https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020#downloads

15. Europol (2020). Pandemic profiteering: how criminals exploit the COVID-19 crisis. Preuzeto 13.8.2022. s https://www.europol.europa.eu/cms/sites/default/files/documents/pandemic_profiteering-how_criminals_exploit_the_covid-19_crisis.pdf

16. FBI (2020). 2020 Internet Crime Report. Preuzeto 29.8.2022. s https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

17. FBI (2021). 2021 Internet Crime Report. Preuzeto 29.8.2022. s https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

18. Fischer, E. A. (2016). Cybersecurity Issues and Challenges: In Brief. Congressional Research Service, Unclassified.

19. Gandhi, V.K. (2012). An Overview Study on Cyber crimes in Internet. Journal of Information Engineering and Applications, 2, 1-5.

20. Hakak, S., Khan W. Z., Imran, M., Choo K. R., Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. IEEE Access. 2020 Jun 30;8:124134-124144. doi: 10.1109/ACCESS.2020.3006172.

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

22. Howard, R., Thomas, T., Burstein, J. i Bradescu R. (2008). Cyber Fraud Trends and Mitigation. The International Journal of Forensic Computer Science (IJoFCS), 2008, Vol. 3, 1, str. 9-24.

23. Hrvatski jezični portal (2022). https://hjp.znanje.hr/ (pristupljeno dana 2.8.2022.)

24. International Telecommunication Union (2012). Understanding cybercrime - phenomena, challenges and legal response. Preuzeto 2.8.2022. s https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

25. Interpol (2021). African cyberthreat assessment report: Interpol's key insight into cybercrime in Africa preuzeto 13.8.2022. s https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

26. Interpol (2020). Cybercrime: COVID-19 Impact. Lyon: INTERPOL General Secretariat. Preuzeto 13.8.2022. s https://www.interpol.int/en/News-andEvents/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-duringCOVID-19

27. Interpol (2020). Global landscape on covid-19 cyberthreat. Preuzeto 13.8.2022. s https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

28. Jennings, K. i Bossler, A. M. (2020). Digital Piracy. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 1025-1045). Springer International Publishing

29. Kazneni zakon, NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21

30. Khan, N. A., Brohi, S. N., Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID- 19 Pandemic. TechRxiv. doi: https://doi.org/10.36227/techrxiv.12278792.v1

31. Kigerl, A. (2020). Spam-Based Scams. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 877-897). Springer International Publishing

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

33. McGuire, M. i Dowling, S. (2013). Cybercrime: A review of the evidence. Home Office. Preuzeto 5.8.2022. s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

34. Ministarstvo unutarnjih poslova, Glavno tajništvo, Sektor za pravne poslove i strateško planiranje, Služba za strateško planiranje, statistiku i unaprjeđenje rada (2021). Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2020. godini. Preuzeto 2.8.2022. s

https://mup.gov.hr/UserDocsImages/statistika/2021/Statisticki_pregled_2020_web.pdf

35. Ministarstvo unutarnjih poslova, Glavno tajništvo, Sektor za pravne poslove i strateško planiranje, Služba za strateško planiranje, statistiku i unaprjeđenje rada (2022). Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2021. godini. Preuzeto 2.8.2022. s https://mup.gov.hr/UserDocsImages/statistika/2022/Statisticki_pregled_2021_web.pdf

36. Nacionalni CERT (2021). Godišnji izvještaj Nacionalnog CERT-a za 2020. godinu. Preuzeto 13.8.2022. s https://www.cert.hr/GINC2020

37. Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29:3, 306-321, DOI: 10.1080/0960085X.2020.1771222

38. National Cyber Security Centre (2021). Annual Review 2021. Preuzeto 15.8.2022. s https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf

39. O'Kane, P., Sezer, S., i Carlin, D. (2018). Evolution of ransomware. IET Networks, 7, 321-327. Preuzeto 7.8.2022. s https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-net.2017.0207

40. Olofinbiyi, S. A. i Singh, S. B. (2020). The Role and Place of Covid-19: An Opportunistic Avenue for Exponential World's Upsurge in Cyber Crime. International Journal of Criminology and Sociology, 2020, 9, 221-230.

41. Onyeaka, H., Anumudu, C. K., Al-Sharify, Z. T., Egele-Godswill, E. i Mbaegbu, P. (2021). COVID-19 pandemic: A review of the global lockdown and its far-reaching effects. Sci Prog. 104(2):368504211019854. doi: 10.1177/00368504211019854

42. Oxford Learner's Dictionaries (2022). https://www.oxfordlearnersdictionaries.com/ (pristupljeno dana 2.8.2022.)

43. Oxford University Dictionary. (2008). A Dictionary of Computing. Oxford University Press.

44. Payne, B. K. (2020). Defining Cybercrime. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 3-25). Springer International Publishing

45. 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. MDPI AG. Preuzeto 2.8.2022. s http://dx.doi.org/10.3390/forensicsci2020028

46. Pranggono, B. i Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. Internet Technology Letters. 2020;1–6. doi: https://doi.org/10.1002/itl2.247

47. Protrka, N. (2018). Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru (Disertacija). Sveučilište u Zadru, Zadar. Preuzeto 2.8.2022. s https://urn.nsk.hr/urn:nbn:hr:162:8344

48. Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K.R., Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digital Communications and Networks (2022), doi: https://doi.org/10.1016/ j.dcan.2022.06.005.

49. Scamwatch (2021). https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams (pristupljeno 28.8.2022)

50. Solms, R. i Niekerk, J. (2013). From Information Security to Cyber Security. Computers & Security, 38, 97-102. doi: https://doi.org/10.1016/j.cose.2013.04.004

51. Tomić, M. (2019). Cyber kriminalitet - novo područje za socijalnopedagoške intervencije (Diplomski rad). Sveučilište u Zagrebu, Edukacijsko rehabilitacijski fakultet, Zagreb. Preuzeto 2.8.2022. s https://urn.nsk.hr/urn:nbn:hr:158:286999

52. UNODC (2020). Cybercrime and Covid19: Risks and Responses. Preuzeto 15.8.2022. s https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf

53. Upadhyay, N. K., Rathee, M. (2022). Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Medicine, law & society, Vol. 15, No. 1, pp. 89–106, doi: 10.18690/mls.15.1.89-106.2022

54. Vijeće Europe (2022). https://www.consilium.europa.eu/hr/policies/coronavirus/timeline/ (pristupljeno 20.8.2022.)

55. Venkatesha, S., Reddy, K. R., Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. SN Comput Sci. 2021;2(2):78. doi: 10.1007/s42979-020-00443-1.

56. Ventrella, E. (2020). Privacy in emergency circumstances: data protection and the COVID-19 pandemic. ERA Forum 21, 379–393 (2020). doi: https://doi.org/10.1007/s12027-020-00629-3

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

58. Vuković, M. (2018). Osobna sigurnost i zlođudni programi na Internetu. U T. Velki i K. Šolić (Ur.), Priručnik za informacijsku sigurnost i zaštitu privatnosti (str. 71-90) .Osijek: Fakultet za odgojne i obrazovne znanosti, Sveučilište Josipa Jurja Strossmayera u Osijeku. Preuzeto 4.8.2022. s https://csi.hr/2020/05/03/prirucnik-za-informacijsku-sigurnost-i-zastitu-privatnosti

59. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge, UK: Polity Press.

60. WEF (2022). The global risks report 2022 17th edition. Preuzeto 17.8.2022. s https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

61. Weil, T., Murugesan, S. (2020). IT Risk and Resilience-Cybersecurity Response to COVID-19. IT Professional 22(3):4-10, DOI: 10.1109/MITP.2020.2988330

62. Whitty, M.T. (2020). Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. European Journal on Criminal Policy and Research, 26, 399-409.

63. Willem Bullée, J. i Junger, M. (2020). Social Engineering. U T. J. Holt i A. M. Bossler (Ur.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (str. 849-875). Springer International Publishing

64. Yar, M. (2006). Cybercrime and Society. Preuzeto 2.8.2022. s https://epdf.tips/cybercrime-and-society.html