PRETHODNO PRIOPĆENJE

DOI: 10.59245/ps.33.3.4
UDK: 343.98
Primljeno: listopad 2023.

TOMISLAV RODIN*, JAKOV KIŠ**, ROBERT MIKAC***

Komparativna analiza rezultata ispitivanja o znanju i iskustvima studentske populacije u korištenju kibernetičkog prostora

Sažetak

Kibernetički prostor predstavlja jedan od krvotoka suvremenog svijeta o kojem vrlo snažno ovise brojne države, međunarodne organizacije, razni poslovni subjekti, kritične infrastrukture, lokalne zajednice pa tako i pojedinci. Navedeni pruža brojne pogodnosti, kao i što otvara mnogo rizika, od kojih je jedan i kibernetički kriminal. Opći cilj ovog istraživanja jest ispitati i analizirati znanja i iskustva studentske populacije u korištenju kibernetičkog prostora. Dok se posebni ciljevi odnose na: usporedbu znanja i iskustva studentske populacije u korištenju kibernetičkog prostora iz dviju anketa provedenih s razmakom od dviju godina; uvid u ponašanje u online okruženju i obrasce korištenja interneta te izloženost kibernetičkom kriminalu. Odabrana je studentska populacija zato što, prema nekoliko parametara, predstavlja iznimno kvalitetnu publiku za provedbu istraživanja. Njihova znanja i iskustva u korištenju kibernetičkog prostora istražena su putem komparativne analize rezultata dvaju upitnika, čiji su rezultati poslužili kako bi se realizirali ciljevi istraživanja i odgovorilo na sljedeće istraživačko pitanje: Kako možemo procijeniti znanje i iskustva studentske populacije u sigurnom korištenju kibernetičkog prostora? Osim toga, rad donosi set preporuka što je moguće i potrebno činiti na pojedinačnoj razini i institucionalnoj razini kako bismo znali više o kibernetičkom prostoru i bili što je moguće manje izloženi kibernetičkom kriminalu.

***Ključne riječi**: kibernetički prostor, kibernetički kriminal, studentska populacija, znanja i iskustva.*

* mag. pol. Tomislav Rodin, Fakultet političkih znanosti Sveučilišta u Zagrebu, Zagreb, Hrvatska.

** mag. pol. Jakov Kiš, Hrvatska akademska i istraživačka mreža - CARNET, Sektor - Nacionalni CERT, Zagreb, Hrvatska.

*** izv. prof. dr. sc. Robert Mikac, Fakultet političkih znanosti Sveučilišta u Zagrebu, Zagreb, Hrvatska.

1. UVOD

U romanu *Neuromancer* iz 1984. William Gibson prvi je pokušao opisati kibernetički prostor i to na sljedeći način: „Konsensualna halucinacija koju svakodnevno doživljavaju milijarde legitimnih operatera, u svakoj naciji, djeca koja se uče matematičkim konceptima… Grafički prikaz podataka apstrahiran od strane svakog računala u ljudskom sustavu. Nezamisliva kompleksnost. Svjetlosne linije nanizane u ne-prostoru uma, nakupinama i konstelacijama podataka. Kao gradska svjetla, koja uzmiču…“ (Gibson, 1984: 67 prema Desforges, 2014: 69). Drugi autori kibernetički prostor vide kao „okruženje (Harknett et al., 2010), domenu (Carr, 2009), teatar operacija (Kempf, 2012), supstrat (Demchak, 2012), milije, sredstvo, ili medij (Libicki, 2012)” (Desforges, 2014: 67). Dok Alix Desforges izdvaja njegove bitne karakteristike i naglašava da je kibernetički prostor strateški koncept koji se koristi na najvišim razinama vlasti, u područjima kao što su vojne doktrine i u međunarodnim pregovorima (Desforges, 2014: 67.).

Thomas C. Folsom (2007: 80) smatra da je kibernetički prostor „utjelovljena komutirana mreža za kretanje informacijskog prometa, koju dalje karakteriziraju različiti stupnjevi pristupa, navigacije, informacijske aktivnosti, povećanja (i povjerenja)”. Rain Ottis i Peeter Lorents (2010: 267) mišljenja su da je „kibernetički prostor vremenski ovisan skup međusobno povezanih informacijskih sustava i ljudskih korisnika koji su u interakciji s tim sustavima”. *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga* Republike Hrvatske definira kibernetički prostor kao „virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na internet“ (Vlada Republike Hrvatske, 2018). Kibernetički prostor i internet usko su povezani i slični pojmovi. Budući da, prema definiciji, kibernetički prostor obuhvaća mreže i sustave neovisno o tome jesu li povezani na internet – svjetski sustav povezanih računalnih mreža koji podatke razmjenjuju internetskim protokolom – vidimo kako je kibernetički prostor širi i apstraktniji pojam pod koji spada i sam internet, a prema nekima i ljudi dok se njime koriste. Stoga ćemo u nastavku rada koristiti oba pojma uz naznaku da je internet dio kibernetičkog prostora, gdje spominjanje interneta svakako uključuje i raspravu o kibernetičkom prostoru.

Kibernetički prostor predstavlja jedan od krvotoka suvremenog svijeta o kojem vrlo snažno ovise brojne države, međunarodne organizacije, razni poslovni subjekti, kritične infrastrukture, lokalne zajednice pa tako i pojedinci. Suvremeni svijet, svakodnevni opći napredak i nebrojeni procesi jednostavno su nezamislivi bez kibernetičkog prostora, njegovih funkcionalnosti i mogućnosti koje pruža. Navedeni je postao jednako važan kao i „stvarni“, svakodnevni „fizički“ prostor (Mikac, 2023). Premda kibernetički prostor olakšava, ubrzava i pospješuje naš život, također otvara brojne rizike i opasnosti s kojima se svakodnevno susrećemo. Upravo to predstavlja širi interes ovog istraživanja. Unutar kibernetičkog prostora odvija se iznimno velik broj procesa presudnih za pitanja sigurnosti i medija, ekonomije i tržišta, politike i diplomacije, međunarodnih odnosa i društvenih aktivnosti, pa sve do pojedinačnih potreba građana za komunikacijom, informiranjem, kupnjom. Stoga je nužno stalno pratiti razvoj novih aktivnosti i prijetnji vezano uz korištenje kibernetičkog prostora kako bismo mogli što kvalitetnije i sa što manje rizika njime se kretati i služiti.

Korištenje kibernetičkog prostora otvara brojne izazove, rizike i opasnosti među kojima jest i kibernetički kriminal koji predstavlja kombinaciju informacijskih, financijskih i osobnih

sigurnosnih prijetnji svakom korisniku interneta. „Kibernetički kriminalitet prisutan je u društvu već dugo vremena u različitim pojavnim oblicima, ali na današnjem stupnju razvoja virtualne dimenzije društva predstavlja stalnu i rastuću prijetnju razvoju i gospodarskom prosperitetu svake suvremene države. Obuhvaća kaznena djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom komunikacijskih i informacijskih tehnologija“ (Vlada Republike Hrvatske, 2015). Kibernetički kriminal jedan je od najbrže rastućih oblika kriminala s izrazitim transnacionalnim karakterom. Brz razvoj interneta i računalne tehnologije omogućava gospodarski i društveni rast, međutim sve veće oslanjanje na internet stvara stalno rastući broj rizika i ranjivosti te otvora nove mogućnosti za kriminalne aktivnosti (Interpol, 2017). Kibernetički kriminal usmjeren je prema brojnim akterima, procesima i vrijednostima, odnosno prema svima onima koji se koriste kibernetičkim prostorom.

Na početku rasprave o istraživanju kibernetičkog kriminala prvi problem s kojim se suočavaju svi istraživači jest složenost definiranja pojma kibernetičkog kriminala (Rodin, 2022). Autori koji se bave tom tematikom općenito se slažu da ne postoji konkretna definicija, nego shvaćanje da je riječ o lepezi ilegalnih aktivnosti. Jonathan Clough sumirao je problem ustvrdivši da „postoji skoro jednak broj izraza koji opisuju kibernetički kriminal kao i njegovih oblika“ (Clough, 2015: 9). Jednu od radnih verzija definicije ponudili su Doug Thomas i Brian Loader, opisujući ga kao „računalno posredovane aktivnosti koje su ili ilegalne ili smatrane nedopuštenim po viđenju određenih strana i koje se mogu provesti kroz globalne elektroničke mreže“ (Thomas i Loader, 2000: 3, prema Yar, 2006: 9). Steven Furnell navodi razliku između kibernetičkog kriminala i računalnih zločina. Prvi pojam označava zločine „u kojima počinitelj koristi posebna znanja o kibernetičkom prostoru“ (Furnell, 2002: 21, prema Holt i Bossler, 2016: 6), dok se drugi događaju zato što „počinitelj koristi jedinstvena znanja o kompjuterskoj tehnologiji“ (Wall, 2001, prema Holt i Bossler, 2016: 6). Kibernetički kriminal je opasan jer je stalno u porastu, učestalo se mijenjaju načini prijevara, kriminalci su sve domišljatiji i vještiji te u konačnosti takav oblik kriminala može imati dalekosežne negativne posljedice za pojedince, organizacije i društvo u cjelini. Upravo zbog toga potrebno mu je posvetiti veliku pažnju i neprestano ga istraživati.

Ponašanje pojedinaca u kibernetičkom prostoru, pa tako i kibernetički kriminalitet može se objašnjavati različitim teorijskim okvirima, pristupima i perspektivama. Svaki kriminalitet, pa tako i kibernetički, događa se unutar „trokuta prijevare“ koji označava sistematizaciju triju važnih čimbenika koji mogu prouzročiti nastanak prijevare. Navedeni čimbenici koji su uključeni u trokut prijevare jesu: 1) prilika, 2) pritisak (motiv ili potreba) i 3) racionalizacija (stav) (Sever Mališ, Tušek i Žager, 2012: 446). Trokut prijevare osmislio je Donald Cressey 50-ih godina prošlog stoljeća (Kassem i Higson, 2012) u nastojanju da istraži zašto pojedinci zloupotrebljavaju povjerenje drugih i koje su okolnosti potrebne kako bi se prijevara realizirala. Istraživanje Donalda Cresseya bilo je ključno za razvoj teorije mogućnosti zločina (engl. *Crime opportunity theory*) koja objašnjava da počinitelji donose racionalne odluke i tako biraju mete (pojedince ili tvrtke) koje im omogućavaju veliku dobit uz malo truda i rizika. Michael Hindelang (1978) objašnjava da pojava kriminala ovisi o prisutnosti počinitelja koji ima priliku i motiv za počinjenje zločina te ga je spreman učiniti, kao što moraju postojati i uvjeti za realizaciju njegova čina. Predmetna teorija bila je ključna za razvoj teorije rutinskih aktivnosti (engl. *Routine activity theory*) koja se usredotočuje na situacije zločina, odnosno promatra zločin kao događaj i usko ga povezuje s okolinom u kojoj se događa. Teoriju rutinskih aktivnosti osmislili su Lawrence E. Cohen i Marcus Felson (1979) prilikom istraživanja

promjene učestalosti kriminalnih djela u SAD-u. Njihov središnji interes jest na zločinu kao događaju koji je usko povezan s okolinom u kojem se događa. Ta je teorija dobila široku primjenu u istraživanju i analizi brojnih oblika kriminalnih djela da bi u suvremenom dobu bila aplicirana i na područje kibernetičkog kriminaliteta (Leukfeldt i Yar, 2016). Teorija rutinskih aktivnosti iznimno je pogodna za istraživanje kibernetičkog kriminaliteta, i to kada je naglašen čimbenik prilike za počinjenje zločina (Al-Dosari, 2020: 37). Čimbenik prilike recipročno se povećava kako su znanja i iskustva u korištenju kibernetičkog prostora niska i ne pridaje im se dovoljno pažnje.

2. DIZAJN ISTRAŽIVANJA

2.1. Problem, predmet i ciljevi istraživanja

Uvid u stanje kibernetičkog kriminaliteta u Hrvatskoj možemo analizirati uvidom u dvije različite baze, odnosno izvješća i statistike institucija nadležnih za predmetno područje. U prvom slučaju riječ je o godišnjim izvješćima Nacionalnog CERT-a. U posljednjem izvješću, onom za 2023., navedeno je da je CERT tijekom navedene godine zaprimio i obradio ukupno 1236 prijava klasificiranih kao računalno-sigurnosni incidenti. Vodeći tipovi incidenata su *phishing*, *phishing URL* i *scam* (Nacionalni CERT, 2023: 7)[1]. U drugom slučaju riječ je o statističkom pregledu temeljnih sigurnosnih pokazatelja i rezultata rada Ministarstva unutarnjih poslova. Iz posljednjeg izvješća vidljivo je da je u 2022. u MUP-u RH prijavljeno 1864 kaznenih dijela kibernetičkog kriminaliteta, gdje najveći udio predstavljaju računalne prijevare (1425) i iskorištavanje djece za pornografiju (311). Ostala prijavljena kaznena djela su s puno manjim udjelom u ukupnom broju (Ministarstvo unutarnjih poslova RH, 2023: 58). U oba slučaja riječ je o prijavama na razini cijele Hrvatske. Utemeljeno na usporedbi i analizi svih godišnjih izvješća Nacionalnog CERT-a i statistika MUP-a RH, kao i vlastitim radom u području kibernetičke sigurnosti, stručnjaci predmetnog područja ističu da su u porastu kaznena djela iz domene kibernetičke sigurnosti i da su znatno porasle štete prouzročene kibernetičkim kriminalom (HRT, 2024; Faktograf.hr, 2022; N1, 2023). Navedeno predstavlja problem ovog istraživanja.

Postoje brojna istraživanja zašto ljudi općenito, a studenti specifično koriste kibernetički prostor. Prema Thomasu Ruggieru (2000), pojedinci koriste kibernetički prostor, odnosno medije unutar njega kako bi zadovoljili svoje specifične potrebe koje prostor i mediji pružaju. Sukladno s istraživanjem Anite Whiting i Davida Williamsa (2013: 368), pojedinci koriste društvene medije zbog: društvene interakcije (88%), traženja informacija (80%), provođenja vremena (76%), zabave (64%), opuštanja (60%), pojedinačne komunikacije s drugim korisnicima (56%), izražavanja mišljenja (56%), traženja različitih pogodnosti (52%), dijeljenja informacija (40%), praćenja što rade drugi korisnici (20%). Saleem Alhabash i Mengyan Ma (2017: 6–8) istražili su motive studentske populacije

[1] U pojmovniku računalno-sigurnosnih incidenata *phishing* je definiran kao „pokušaj navođenja korisnika na odavanje povjerljivih podataka putem raznih komunikacijskih kanala“, *phishing URL* „poveznica do lažne Internet stranice na kompromitiranom web sjedištu ili sjedištu registriranom u svrhu krađe povjerljivih podataka“, *scam* „pokušaj navođenja potencijalne žrtve na djelovanje u korist prevaranta (najčešće putem elektroničke pošte)“ (Nacionalni CERT, 2023: 37–38).

za korištenje različitih društvenih mreža (Facebook, Twitter, Instagram i Snapchat). Došli su do spoznaja da se motivi korištenja tih platformi razlikuju ovisno o spolu i rasi/etničkoj pripadnosti. Studentice su najviše koristile Instagram za izražavanje stavova i traženje inspiracije, dok su studenti najviše koristili Twitter za izgradnju osobnog brenda. Istodobno, hispanoamerički i afroamerički studenti, za razliku od bijelih i azijskih studenata, češće koriste Snapchat za privatnu komunikaciju. Istraživanje Pavice Sheldon i Katherine Bryant (2016) o korištenju Instagrama studentske populacije pokazalo je da studenti primarno koriste tu mrežu kako bi pratili što njihovi kontakti rade, a potom da bi izrazili svoje misli, djela i putovanja.

U Hrvatskoj dosadašnja istraživanja vezana uz korištenje interneta studentske populacije uključuju različita područja interesa istraživača. Analize su obuhvatile korištenje internetskog bankarstva, učestalost, razloge korištenja i način korištenja internetskog bankarstva, kao i zadovoljstvo obavljenim uslugama (Milanović Glavan, 2015; Martić, 2018), internet kao novi kanal komunikacije, prodaje i distribucije za segment mladih potrošača (Škare, 2006), odrednice kupnje studentske populacije na internetu (Brstilo Lovrić, 2020), kao i korištenje portala e-Građani (Jurković, 2022). Međutim, nije pronađeno nijedno istraživanje koje bi se bavilo pitanjima ponašanja pojedinaca (studenata) u kibernetičkom prostoru i izazovima kibernetičkog kriminaliteta. Za potrebe ovog istraživanja, studentska populacija Sveučilišta u Zagrebu odabrana je kao predmet istraživanja, i to zbog nekoliko razloga.

Prvo, studentska je populacija raznolika u pogledu dobi, spola, socioekonomskog statusa, mjesta prebivališta i drugih čimbenika koji omogućuju raznolikost u uzorku ispitanika. Predmetna raznolikost može pomoći istraživačima da dobiju bolje razumijevanje različitih perspektiva i iskustava. Drugo, današnji studenti, sukladno sa Strauss-Howeovom generacijskom teorijom, pripadaju generaciji Z (rođeni između 1995. i 2012.) (Strauss i Howe, 1991; Strauss i Howe, 1997) kojoj je korištenje kibernetičkog prostora njihovo prirodno okruženje. Nadalje, studenti su često motivirani za sudjelovanje u istraživanju i spremni su uložiti vrijeme i trud. Razumiju proces istraživanja, prepoznaju važnost istraživanja, sami istražuju za vlastite potrebe tako da, sudjelovanjem u istraživanjima, kao ispitanici uvježbavaju i svoje vještine. Sljedeće, studentska populacija istraživačima je dostupnija od ostalih društvenih skupina, a pogotovo ako se istraživanje provodi *online* metodama. U tom slučaju velika je pretpostavka da će svi na odgovarajući način znati popuniti anketu, što vjerojatno ne bi u istoj mjeri bilo tako s drugim skupinama. Na kraju, studenti su trenutačna i buduća najsvjetlija perspektiva svake nacije pa su njihovi stavovi i mišljenja vrlo važni za svaku zemlju, njezine institucije i građane.

Na temelju problema i predmeta istraživanja za općenit cilj ovog istraživanja određeni su ispitivanje i analiza znanja i iskustva studentske populacije u korištenju kibernetičkog prostora. Iz navedenog cilja izvedeni su posebni ciljevi, i to: usporedba znanja i iskustva studentske populacije u korištenju kibernetičkog prostora iz dviju anketa provedenih s razmakom od dviju godina, uvid u ponašanje u *online* okruženju i obrasce korištenja interneta te izloženost kibernetičkom kriminalu.

Sukladno sa svim navedenim, postavlja se središnje istraživačko pitanje: Kako možemo procijeniti znanje i iskustva studentske populacije u sigurnom korištenju kibernetičkog prostora?

2.2. Teorijski okvir

Vezano uz teorijski okvir, u istraživanju će biti korištena dva teorijska pristupa: biheviorizam i racionalni izbor. Biheviorizam je usmjeren na istraživanje ponašanja pojedinaca i analizu zakonitosti njihova ponašanja u određenim situacijama. Općenita ideja biheviorizma jest da pojedinci uče kroz interakciju s okolinom u kojoj se nalaze i stečena iskustva primjenjuju u budućim interakcijama. Andrew Heywood (2013) objašnjava da je bihevioralni pristup omogućio istraživanja poput ponašanja pojedinaca pri glasanju, ponašanja zakonodavaca te ponašanja općinskih političara i lobista. Ellen Grigsby (2011) navodi da biheviorizam definiraju elementi fokusirani na političke aktere i njihovo ponašanje (ili stavove i mišljenja) te da mnogi bihevioristi koriste ankete kako bi usporedili stavove birača i onih koji ne glasaju, elita naspram neelita, stranački identifikatori u odnosu na neovisne ili druge podjedinice stanovništva. Za Roda Haguea, Martina Harropa i Johna McCormicka (2016), bihevioralni pristup ispituje politiku na razini pojedinca, oslanjajući se primarno na kvantitativnu analizu uzorkovanih istraživanja. U biheviorizmu je naglasak na pojedincima ispred institucija, proučavajući stavove i ponašanje pojedinaca u potrazi za znanstvenim generalizacijama.

Pristup racionalnog izbora nastao je u ekonomiji u drugoj polovici 20. stoljeća i proširio se i u druge znanstvene discipline. Bit pristupa vrlo je jednostavna, a tvrdi se da primarno objašnjenje za akciju jest da je akter izračunao koja mu je radnja najučinkovitiji način za postizanje željenog cilja (Robenson, 2004). Pristup racionalnog izbora snažno je oslonjen na bihevioralne stavove pojedinaca u odlučivanju o određenim akcijama. Za Andrewa Heywooda (2013), racionalni izbor temelji se na racionali osobnog interesa pojedinca i analizira njegovo ponašanje. S tim se slažu Stephen Tansey i Nigel Jackson (2008). Da bi pristup racionalnog izbora bio primjenjiv, Craig Parsons (2017) navodi kako moramo poći od pretpostavke da su svi pojedinci apsolutno racionalni u svojim odlukama te da raspolažu svim potrebnim informacijama na temelju kojih će razmotriti opcije koje im stoje na raspolaganju kako bi donijeli najbolju odluku.

Ta dva teorijska pristupa bit će upotrijebljena u istraživanju znanja i iskustava studentske populacije u korištenju kibernetičkog prostora na više načina. S pomoću biheviorizma fokusirat ćemo se na analizu navika, kao i na istraživanje rizika i zaštite. Biheviorizam ima ograničenja, jer ne uzima u obzir sveukupne psihološke procese i socijalni kontekst, stoga ga kombiniramo s teorijskim pristupom racionalnog izbora. Navedeni pristup dvostruko je bitan. Prvo, služi za analizu motivacija i odlučivanja studenta u korištenju kibernetičkog prostora, gdje se pretpostavlja da pojedinci donose odluke zasnovane na maksimiranju koristi i minimiziranju rizika. Isto tako, može biti koristan u razumijevanju zašto studenti biraju određene platforme i aktivnosti na internetu te u identificiranju faktora koji utječu na njihovo *online* ponašanje. Drugo, na temelju rezultata istraživanja ovaj pristup može se koristiti kod formuliranja preporuka i programa dizajniranih za povećanje znanja o sigurnom korištenju kibernetičkog prostora.

2.3. Metoda istraživanja

„U svakodnevnom životu, ako želimo ispitati neki društveni fenomen, bio on individualan (kao što je odnos liječnika i pacijenta) ili kolektivan (kao što je ponašanje mase

na sportskom stadionu), u osnovi imamo dva načina prikupljanja podataka: promatranje i postavljanje pitanja“ (Corbetta, 2022: 95). Podatke možemo prikupljati putem postavljanja pitanja sudionicima uključenima u društveni fenomen metodom ankete (Corbetta, 2022: 95). „Anketa je najčešće korištena tehnika prikupljanja podataka u društvenim istraživanjima, osobito pogodna za opisna i uzročna istraživanja. Primjena ankete toliko je raširena da se čak smatra zasebnom metodom“ (Tkalac Verčić i drugi, 2010: 103). Anketa podrazumijeva tehniku prikupljanja podataka: postavljanjem pitanja, onim pojedincima koji su predmet istraživanja, koji pripadaju određenom uzorku, putem standardizirane procedure, s ciljem proučavanja odnosa među varijablama (Corbetta, 2022: 95). „Anketa je, dakle, prikupljanje podataka ispitivanjem uz primjenu posebnog formulara – anketnog upitnika“ (Tkalac Verčić i drugi, 2010: 103). Pitanja se postavljaju onim pojedincima koji predstavljaju predmet istraživanja (Corbetta, 2022: 95). Upitnik predstavlja unaprijed određenu listu pitanja koja postavljamo ispitanicima. Svi ispitanici odgovaraju na ista pitanja. Anketa se može provoditi strukturiranim intervjuom, samostalnim popunjavanjem upitnika od strane ispitanika, telefonski, poštom i putem interneta (Tkalac Verčić i drugi, 2010: 103). „Kako populaciju koju proučavamo obično čini velik broj pojedinaca, a u praksi je nemoguće ispitati ih sve, što zahtijeva da se za intervjuiranje odabere uzorak sudionika“ (Corbetta, 2022: 96). „Uzorak je skup jedinica populacije na kojima je provedeno istraživanje“ (Tkalac Verčić i drugi, 2010: 72). Prema vrsti, uzorke možemo podijeliti u tri skupine: slučajni, namjerni i mješoviti uzorci. Za potrebe ovog rada bit će kratko opisan namjerni uzorak i njegova podskupina – uzorak lančane reakcije. „Ovaj oblik uzorkovanja odnosi se na proces odabira uzorka korištenjem mreža. Za početak se odabire nekoliko pojedinaca u skupini ili organizaciji i od njih se prikupljaju tražene informacije. Njih se zatim moli da identificiraju druge u skupini ili organizaciji, pa tako ljudi koje oni odaberu postaju dio uzorka“ (Tkalac Verčić i drugi, 2010: 78).

Za predmetno istraživanje odabrana je studentska populacija Sveučilišta u Zagrebu. Jedinicu uzorka predstavlja svaki pojedinačni student u uzorku, dok je uzorak manja skupina studenata od kojih se prikupljaju podaci o znanju i iskustvima u korištenju kibernetičkog prostora. Za veličinu uzoraka (n) odlučili smo se da bude veća od stotinu ispitanika, za što smo procijenili da predstavlja točku zasićenja. Strategija određivanja uzorka bila je namjeran uzorak i njegov podskup – uzorak lančane reakcije. Do studenata koji su popunili anketu došli smo posredstvom njihovih nastavnika na različitim fakultetima Sveučilišta u Zagrebu.

3. REZULTATI ISTRAŽIVANJA

Za provedbu obaju istraživanja pitanja je odobrilo Etičko povjerenstvo Fakulteta političkih znanosti Sveučilišta u Zagrebu. Pitanja u anketi su podijeljena u nekoliko segmenata. Prvi dio čine općenita pitanja kako bi se determinirala struktura ispitanika kao što su visokoškolska ustanova, spol, dob, mjesto stanovanja, veličina mjesta iz kojeg potječu i razina srednjoškolskog obrazovanja. Drugi dio sastoji se od pitanja vezanih uz navike ispitanika kad je riječ o korištenju interneta, društvenih mreža i internetske trgovine. Treći dio ispituje stavove ispitanika o potencijalnim rizicima korištenja interneta, piratstvu, društvenim mrežama kao izvoru govora mržnje, individualnoj odgovornosti u prevenciji kibernetičkog kriminala i slično s pomoću seta izjava kojima je trebalo izraziti suglasnost, neutralnost ili protivljenje. Korištena je Likertova ljestvica, konkretno numerička ljestvica s pet stupnjeva. Posljednji segment predstavljaju pitanja o znanju i iskustvima ispitanika, specifičnije o kibernetičkom

kriminalu, dobrim navikama i lošim iskustvima. Upitnik je imao ukupno 40 pitanja, od kojih će u nastavku biti izdvojena ona za koja smo procijenili da će najbolje odgovarati potrebama istraživanja.

Prva anketa provedena je 2021., a druga 2023. godine. Obje su izrađene s pomoću softvera Google Forms za administraciju anketa. U obje ankete korištena su identična otvorena i zatvorena pitanja, s tim da je naglasak bio na onim zatvorenima. U istraživanju je prisutna greška pokrivenosti i uzorkovanja (neprobabilistički uzorak), no to je očekivano od *online* ankete. Anketa je po svojoj prirodi eksploratorna, pokušava uočiti pojave vezane uz kibernetički prostor i mlade, ali ne stvara kauzalne zaključke.

3.1. Prvo ispitivanje

Prvo ispitivanje provedeno je u svibnju 2021. na uzorku od 114 ispitanika, i to u značajnoj mjeri studenata Fakulteta političkih znanosti (93 ispitanika). Ostali ispitanici bili su studenti Pravnog fakulteta (14 ispitanika), Fakulteta elektrotehnike i računarstva (2) te po jedan student s Ekonomskog fakulteta i Fakulteta prometnih znanosti. Većinu ispitanika, njih dvije trećine, činile su studentice. Ispitanici su bile osobe isključivo u dvadesetim godinama, s naglašenom urbanom populacijom (više od 50% ispitanika bilo je ili iz velikoga grada ili grada srednje veličine). Najčešće srednjoškolsko obrazovanje ispitanika s više od 80% bilo je gimnazijsko, dok je informatika bila izborni predmet u samo jednom razredu kod najvećeg broja studenata (39). U sva četiri razreda srednje škole informatiku kao izborni predmet imalo je 29 ispitanika, u tri razreda 5 ispitanika (4,4%), a informatiku u srednjoj školi uopće nije pohađalo 8 studenata (Rodin, 2022).

Navike studentske populacije u korištenju kibernetičkog prostora ispitivane su s pretpostavkom da u ukupnoj populaciji najviše vremena provode na internetu i društvenim mrežama. Navedena teza testirana je s pomoću pitanja kojima je cilj bio provjeriti njihove *online* navike. Gotovo polovina ispitanika navela je da dnevno na internetu provede više od četiri sata, dok je najčešći uređaj za povezivanje pametni telefon (engl. *Smartphone*) (89,5% ispitanika). Navike su promatrane i u odnosu na pandemiju bolesti COVID-19, konkretno kako je nov način života, uvjetovan fizičkom distancom, nastavom od kuće i s vremenom u izolaciji od okoline promijenio njihove dnevne aktivnosti. Gotovo 60% ispitanika odgovorilo je da provodi značajno više ili više vremena *online* (Rodin, 2022: 22). Instagram je najpopularnija društvena mreža, s navikama čestog otvaranja aplikacija prisutnima kod velikog broja ispitanika (39,5%). Ispitanici su skloni *online* trgovini, i to najčešće pri kupnji odjeće i obuće.

Stavovi ispitanika o potencijalnim rizicima korištenja interneta, piratstvu, društvenim mrežama kao izvoru govora mržnje, individualnoj odgovornosti u prevenciji kibernetičkog kriminala i sl. ispitivani su serijom izjava o kojima su se ispitanici morali izjasniti u kojoj se mjeri slažu ili ne slažu s izjavom. Korištena je numerička, Likertova ljestvica s pet stupnjeva. Brojevi označavaju sljedeće: 1 – u potpunosti se ne slažem; 2 – djelomično se ne slažem; 3 – niti se slažem niti se ne slažem; 4 – djelomično se slažem; 5 – u potpunosti se slažem. Ispitanici su u velikoj većini (više od 90%) priznali da su svjesni potencijalnih opasnosti koje proizlaze korištenjem interneta. Izjašnjavanje o formalnom obrazovanju kao metode upoznavanja s potencijalnim izvorima prijetnji nije dalo izraženije stavove, čineći njegovu ulogu naizgled zanemarivom. Ispitanici imaju neutralan ili čak blago pozitivan pogled prema

ilegalnom skidanju sadržaja, što se može protumačiti nepostojanjem odgovarajućih edukacija i sankcija u slučaju njihova korištenja za vlastitu upotrebu. Ispitanici se načelno slažu da *online* kupnja nije jednako sigurna kao fizička, jer ih manje od 30% dijeli suprotno mišljenje. Ispitanici priznaju moguće negativne posljedice upotrebe društvenih mreža, specifično njihovo viđenje tog medija kao kanala za širenje govora mržnje, rasne netrpeljivosti i ksenofobije. Njih na taj način djelomično ili u potpunosti vidi četrdeset devetero ispitanika (Rodin, 2022: 22). Manjina vjeruje u vlastitu odgovornost pri zaštiti od kibernetičkog kriminala, dok ga je većina ispitanika spremna prijaviti nadležnim institucijama (Rodin, 2022: 23).

U pogledu znanja i iskustva u zaštiti na internetu, četiri petine ispitanika koristi antivirusni program, ali samo polovica njih redovito ga ažurira. Ispitanici ne otvaraju mailove nepoznatih pošiljatelja, ali ih većina koristi istu lozinku za više elektroničkih usluga te je nikad ili jako rijetko mijenja. Ispitanici se načelno informiraju o pojavi novih računalnih prijevara putem medija i društvenih mreža (64%), 40,7% spaja se na otvorene bežične mreže, a 43,9% njih ne zna što je *phishing*. Zabilježeni su slučajevi narudžbe i plaćanja proizvoda koji nije došao (23), hakiranog profila na društvenim mrežama (20) te nekog oblika zlostavljanja putem interneta (25 ispitanika). Zabilježena su tri slučaja osvetničke pornografije. Od jedanaest ispitanika koji su priznali da su bili žrtva nekog oblika kibernetičkog kriminala, samo troje ih je taj zločin prijavilo nadležnim institucijama (Rodin, 2022: 23).

3.2. Drugo ispitivanje

Drugo ispitivanje provedeno je u svibnju 2023., točno dvije godine nakon prvog. Uzorak za to istraživanje čine 193 ispitanika, studenta Sveučilišta u Zagrebu, koji su pristupili ispunjavanju ankete i u potpunosti je ispunili. Prema sastavnicama to izgleda ovako: Fakultet političkih znanosti 128 studenata, Pravni fakultet 50 ispitanika, Fakultet prometnih znanosti 11, Ekonomski fakultet troje te Veterinarski fakultet s jednim studentom. Razvidno je da je najveći broj ispitanika (dvije trećine) s Fakulteta političkih znanosti, no to je bilo očekivano s obzirom na fakultetsku pripadnost istraživača i najveći doseg. Anketu je dominantno ispunila ženska populacija sa 136 ispitanice, dok su muškarci činili 29,2% ispitanika sa 56 kompletiranih anketa. Jedan se ispitanik nije izjasnio kad je o tome riječ. Dobna struktura ispitanika poprilično je raznovrsna, s obzirom na nominalno jednoličnu društvenu skupinu (studentska populacija). Najčešća dob ispitanika je 21 godina, najmanja 19, a najveća 45 godina. Geografska determinanta ispitanika postignuta je pitanjem o veličini mjesta iz kojeg potječu: gotovo polovina ispitanika (45,3%) potječe iz velikoga grada s više od 100.000 stanovnika, gotovo identičan broj ispitanika je iz malih gradova (manje od 50.000 stanovnika) i manjeg naselja/općine s manje od 10.000 stanovnika, dok je najmanje ispitanika, njih četrnaestero, iz grada srednje veličine (između 50.000 i 100.000 stanovnika). Četiri petine ispitanika ima gimnazijsko srednjoškolsko obrazovanje, zatim slijede četverogodišnja strukovna škola (33 ispitanika) te po jedan ispitanik s petogodišnjom i trogodišnjom strukovnom školom. Informatika kao izborni predmet u srednjim školama najčešće je bila u dva razreda (70 ispitanika) te u gotovo istom broju u jednom (68 ispitanika). U sva četiri razreda srednje škole informatiku kao izborni predmet imalo je 29 ispitanika, u tri razreda 11 ispitanika (5,8%), a informatiku u srednjoj školi uopće nije pohađalo 13 studenata (6,8%).

Sljedeći set pitanja bavio se navikama ispitanika kad je riječ o korištenju interneta, društvenih mreža i sl. Više od polovine ispitanika (53,6%) odgovorilo je da provodi više od četiri sata *online*, 75 njih navelo je da provodi dva do četiri sata *online*, dok je najmanji broj ispitanika (14) odgovorio kako na internetu provodi sat do dva na dan. Ponuđenu opciju manje od sat na dan nije izabrao nijedan ispitanik. Više od 90% ispitanika navelo je da je pametni telefon uređaj kojim najčešće pristupaju internetu, dok je ostatak ispitanika izabrao stolno ili prijenosno računalo. Pitanjem koje se odnosi na vrijeme provedeno u digitalnom svijetu prije i nakon pojave koronavirusa na početku 2020. trebalo je evaluirati stopu tranzicije koja je pogodila cjelokupno stanovništvo, uključujući i studentsku populaciju, ponajprije nastavom od kuće, *online* ispitima i sl. Anketa je pokazala da većina ispitanika (57%) provodi otprilike jednaku količinu vremena *online*, trideset dvoje odgovorilo je da provodi više vremena, gotovo identičan broj (33) manje vremena, dok se za ekstremnije vrijednosti opredijelilo najmanje ispitanika, njih 18. Trinaest ispitanika izjasnilo se da provodi znatno više vremena *online*, dok ih je petero značajnije smanjilo vrijeme provedeno na internetu.

Očekivano, društvene mreže iznimno su popularne među studentskom populacijom, i to ponajviše Instagram (171 ispitanik), zatim Facebook (123), TikTok (91), Twitter (43), Snapchat (30) te LinkedIn (19). Sedam ispitanika izjasnilo se da ne koristi društvene mreže. Zanimljiv je intenzitet otvaranja aplikacija tih društvenih mreža jer se pokazalo da najveći udio ispitanika (35,2%) omiljenu aplikaciju otvara više desetaka puta dnevno, 32,1% desetak puta dnevno, dok ih 50 otvara nekoliko puta, a samo devetero jednom ili dvaput. Ispitanici *online* trgovinu najčešće koriste za kupnju odjeće (137 ispitanika), zatim obuće (100), knjiga (59) te informatičke opreme (39). Averziju prema internetskoj trgovini iskazalo je 36 ispitanika. Učestalost korištenja *online* trgovine ispitana je pitanjem koje je ponudilo sljedeće odgovore: gotovo polovina ispitanika (47,2%) koristila je internetsku trgovinu nekoliko puta u posljednjih godinu dana, 21,8% više desetaka puta, 12,4% desetak puta, dok ih je 7,3% koristilo jednom. Nadalje, 22 ispitanika (11,4%) uopće nije koristilo internetsku trgovinu u posljednjih godinu dana.

Stavovi ispitanika o korištenju interneta te svim negativnim i potencijalno kriminalnim aspektima tih aktivnosti ispitani su nizom pitanja u kojima je korištena Likertova ljestvica, gdje su brojevi od 1 do 5 označavali razinu (ne)slaganja s izjavom. Stupanj/vrijednost 1 označava izrazito neslaganje s tvrdnjom, a vrijednost 5 potpuno slaganje. Više od 90% ispitanika u potpunosti se ili djelomično slaže s izjavom da je svjesno potencijalnih opasnosti koje proizlaze iz korištenja interneta. Na sljedeću izjavu: „Kroz formalno obrazovanje imao/la sam se priliku educirati o mogućim izvorima prijetnji na internetu“, dobiveni su sljedeći odgovori: 10 ispitanika u potpunosti se ne slaže, 42 djelomično se ne slaže, 63 se niti slaže niti ne slaže, 40 ih se djelomično slaže, dok ih se 38 u potpunosti slaže. Izjavom: „Ne vidim problem u skidanju sadržaja (video, audio, digitalni) za osobnu upotrebu“ ispitivao se stav ispitanika prema piratstvu. Dvanaest ispitanika u potpunosti se ne slaže s tom tvrdnjom, 26 se djelomično ne slaže, najveći udio ispitanika se niti slaže niti ne slaže (65), djelomično se slaže 49 ispitanika, dok se u potpunosti slaže 41 ispitanik. *Online* kupnju jednako sigurnom kao i fizičku smatra pet ispitanika, djelomično je smatra 29 ispitanika, dok njih 68 nije sigurno. Šezdeset pet ispitanika djelomično se ne slaže s tom izjavom, dok se njih 26 u potpunosti ne slaže s tom izjavom.

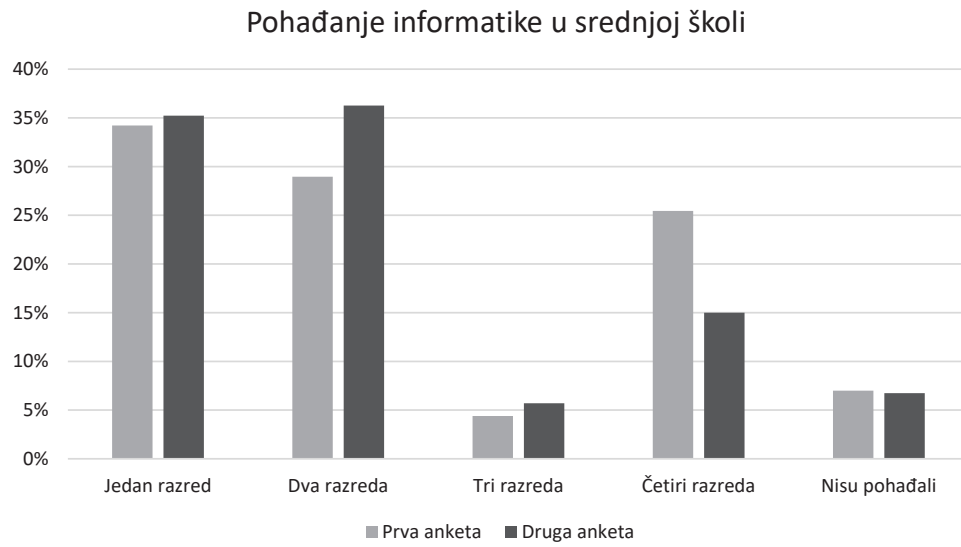
Društvene mreže kao medij za širenje govora mržnje, rasne netrpeljivosti i ksenofobije ne vidi manjina ispitanika (28), dok nije sigurno 29,5% ispitanika. Natpolovična veličina (55,9%) ispitanika društvene mreže detektira kao potencijalne načine širenja govora mržnje i

rasističkih stavova. Kada je riječ o povjerljivim podacima koji se prilažu stranicama, samo troje ispitanika u potpunosti je sigurno da se ti podaci neće zloupotrijebiti. Dvadeset devet ispitanika ima rezervirano povjerenje, dok 78 njih nije sigurno. Trideset dvoje ispitanika u potpunosti se ne slaže da stranice neće zloupotrijebiti podatke, dok ih se pedeset djelomično ne slaže. S tezom „Zaštita od kibernetičkog kriminala ovisi isključivo o pojedincu" u potpunosti se ne slaže 16,6% ispitanika, djelomično se ne slaže 28,5% ispitanika, dok ih nije sigurno 36,8%. Dvadeset sedam ispitanika djelomično se slaže s tom tezom, dok ih se osam u potpunosti slaže. Ispitanici su se podjednako raspodijelili kad je riječ o stavu oko promjene njihovih navika u korištenju interneta i digitalnih usluga u postpandemijskom razdoblju. Sedamdeset dva ispitanika (37,3%) u potpunosti se ili djelomično slaže da su njihove navike promijenjene, dok ih devedeset (46,7%) nije u značajnijoj mjeri mijenjalo navike. Natpolovična većina ispitanika (58,1%) spremna je prijaviti kibernetički kriminal nadležnim institucijama, dok ih je 14 izrazilo izrazito protivljenje tom činu.

U pogledu znanja i iskustva o zaštiti na internetu, dvije trećine ispitanika koristi antivirusni program, no samo ih 41,1% redovito provjerava je li ažuriran. Gotovo 90% ispitanika ne otvara mailove nepoznatih pošiljatelja, dok 119 ispitanika (više od 60%) koristi istu lozinku za više digitalnih usluga. Nadalje, 57% ispitanika lozinku ne mijenja nikad, 30,1% jednom godišnje, a 11,9% svakih nekoliko mjeseci. Velika većina (160 ispitanika) ne koristi neki od programa za upravljanje lozinkama, dok 72% njih priznaje da se informira o pojavi novih računalnih prijevara putem medija i društvenih mreža. Nadalje, 65,3% ispitanika ne spaja se na nezaštićene (otvorene) bežične mreže, dok ih približno trećina ne poznaje pojam *phishing*. Trideset jedan ispitanik priznao je da mu *online* naručeni i plaćeni proizvod nikad nije došao, dok ih je 23 bilo žrtva hakiranog profila na društvenim mrežama. Jednom je ispitaniku ukraden i zloupotrijebljen identitet uz materijalnu štetu. Više od četvrtine ispitanika iskusilo je nekakav oblik zlostavljanja putem interneta (engl. *Cyberbullying*). Šest ispitanika bilo je žrtva osvetničke pornografije, dok ih je 10 priznalo da su bili žrtve nekog oblika kibernetičkog kriminala. Dvoje ispitanika prijavilo je kibernetički kriminal nadležnim institucijama. Na pitanje da se opiše konkretan kriminal s kojim se osoba susrela, najvažniji odgovori bili su sadržaj korišten za ucjenu te prijevara prilikom kupnje obuće sa sumnjive internetske stranice.

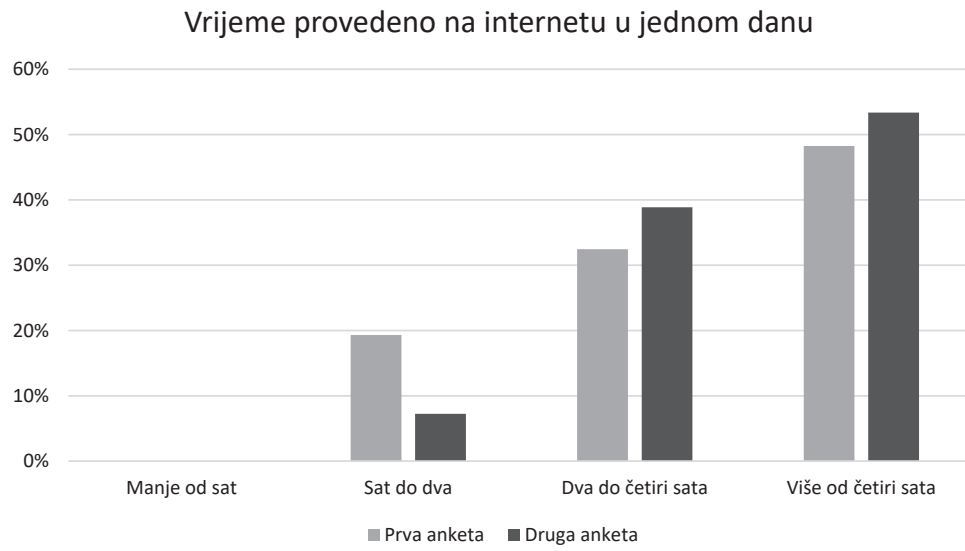
4. KOMPARATIVNA ANALIZA REZULTATA ISTRAŽIVANJA

Prvi dio komparativne analize rezultata istraživanja odnosi se na općenita pitanja vezana uz strukturu ispitanika (na kojem fakultetu studiraju; spol; dob; veličina mjesta u kojem stanuju; razina srednjoškolskog obrazovanja i koliko su razreda u srednjoj školi pohađali informatiku). Od svih odgovora izdvajamo one vezane uz pohađanje informatike u srednjoj školi. Studenti iz prve provedene ankete (n=114) pohađali su ukupno godina informatike prema sljedećim postocima: jedan razred 34,21% ispitanika, dva razreda 28,95%, tri razreda 4,4%, četiri razreda 25,44% te nisu pohađali 7%. U drugoj anketi (n=193) rezultati su sljedeći: jedan razred 35,23% ispitanika, dva razreda 36,26%, tri razreda 5,7%, četiri razreda 15% te nisu pohađali 6,74%. Primjećujemo da je nova generacija studenata pohađala manje godina informatike – u prvoj anketi četiri razreda informatike pohađalo je 25,44% ispitanika, u drugoj anketi tek 15%. Pojedinačno i općenito gledajući, možemo istaknuti da su studenti imali malo formalne izobrazbe vezano uz informatiku.



Grafikon 1: Pohađanje informatike u srednjoj školi

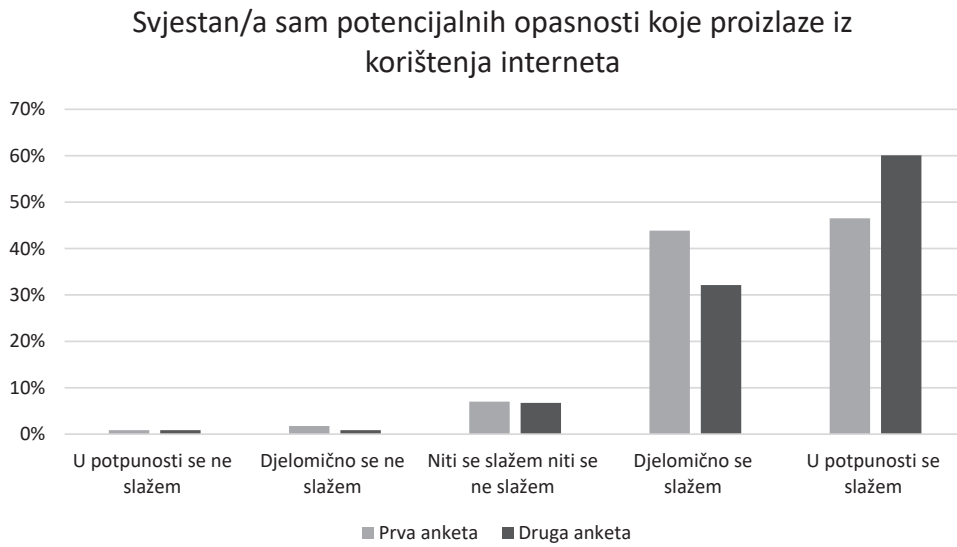
Iz drugog dijela komparativne analize rezultata istraživanja koji se odnosi na istraživanje navika u korištenju interneta, društvenih mreža i internetske trgovine izdvajamo odgovore na dva pitanja. Prvo, vezano uz vrijeme provedeno na internetu u jednom danu. Drugo, u odnosu na vrijeme prije pandemije bolesti COVID-19, koliko vremena provode na internetu. Vrijeme provedeno na internetu kod studenta u prvoj anketi (n=114) je sljedeće: manje od sat vremena 0%, sat do dva 19,3%, dva do četiri sata 32,45%, više od četiri sata 48,25%. Rezultati druge ankete (n=193) su sljedeći: manje od sat vremena 0%, sat do dva 7,25%, dva do četiri sata 38,86%, više od četiri sata 53,36%. Odgovori na pitanje vezano uz vrijeme provedeno na internetu tijekom pandemije bolesti COVID-19 u odnosu na vrijeme prije nje u prvoj anketi su sljedeći: značajno manje vremena 0,87%, manje vremena 4,38%, otprilike isto vremena 35%, više vremena 49,12%, značajno više vremena 10,52%. Dok su rezultati druge ankete sljedeći: značajno manje vremena 2,6%, manje vremena 17%, otprilike isto vremena 57%, više vremena 16,58%, značajno više vremena 6,73%. Vrlo je bitan podatak da studenti u obje ankete provode puno vremena na internetu, i to u prvoj anketi 48,25% ispitanih više od četiri sata na dan, u drugoj njih 53,36%. Navedeno je posebno važno u korelaciji s korištenjem društvenih mreža koje koriste prije svega za zabavu. U obje ankete najveći broj studenata otvara omiljene društvene mreže više desetaka puta na dan. Dok su kod drugog pitanja studenti koji su popunjavali anketu 2021. u tijeku pandemije bolesti COVID-19 kumulativno (više vremena i značajno više vremena) provodili više vremena na internetu, što je i logično s obzirom na brojne mjere i preporuke vezane uz fizičko distanciranje koje su tada bile na snazi. Dok kod ispitanika u drugoj anketi 2023. vidimo da se kumulativno (više vremena i značajno više vremena) vrijeme provedeno na internetu smanjuje i vraća u trendove prije pandemije. Pojedinačno i komparativno vidimo da studenti provode puno vremena na internetu.



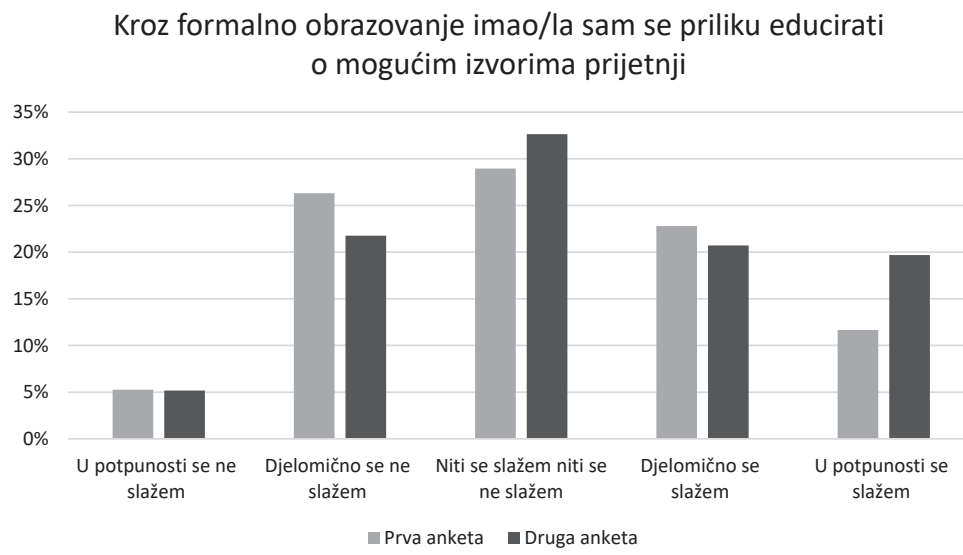
Grafikon 2: Vrijeme provedeno na internetu u jednom danu

Treći dio komparativne analize uspoređuje stavove ispitanika o potencijalnim rizicima korištenja interneta, piratstvu, društvenim mrežama kao izvoru govora mržnje, individualnoj odgovornosti u prevenciji kibernetičkog kriminala. Svi su rezultati znakoviti, no za potrebe analize izdvajamo odgovore na tri pitanja (teze), i to: „Svjestan/a sam potencijalnih opasnosti koje proizlaze iz korištenja interneta"; „Kroz formalno obrazovanje imao/la sam se priliku educirati o mogućim izvorima prijetnji"; i „U slučaju svjedočenja bilo kojem obliku kibernetičkog kriminala spreman/a sam ga prijaviti nadležnim institucijama". Rezultati svjesnosti potencijalnih opasnosti koje proizlaze iz korištenja interneta u prvoj anketi (n=114) su sljedeći: u potpunosti se ne slažem 0,87%, djelomično se ne slažem 1,75%, niti se slažem niti se ne slažem 7%, djelomično se slažem 43,86%, u potpunosti se slažem 46,5%. A u drugoj anketi (n=193) su sljedeći: u potpunosti se ne slažem 0,87%, djelomično se ne slažem 0,87%, niti se slažem niti se ne slažem 6,73%, djelomično se slažem 32,12%, u potpunosti se slažem 60,1%. Vrijedna spoznaja jest da je u obje ankete velika većina ispitanika djelomično ili u potpunosti svjesna potencijalnih opasnosti koje proizlaze iz korištenja interneta. Dok na prvi pogled ta spoznaja ohrabruje, rezultati na sljedeće pitanje poprilično su zabrinjavajući. U prvoj anketi kumulativno više od 31,5% ispitanika ima ozbiljne dvojbe oko toga da su se formalnim obrazovanjem imali priliku educirati o mogućim izvorima prijetnji (ukupni rezultati: u potpunosti se ne slažem 5,26%, djelomično se ne slažem 26,31%, niti se slažem niti se ne slažem 28,95%, djelomično se slažem 22,8%, u potpunosti se slažem 11,66%), dok je u drugoj anketi riječ o njih gotovo 27% koji imaju isti stav (ukupni rezultati: u potpunosti se ne slažem 5,18%, djelomično se ne slažem 21,76%, niti se slažem niti se ne slažem 32,64%, djelomično se slažem 20,72%, u potpunosti se slažem 19,69%). Međutim, vrlo su zabrinjavajući rezultati na posljednje izdvojeno pitanje (tezu) o spremnosti prijave nadležnim institucijama svjedočenja o bilo kojem obliku kibernetičkog kriminala. U prvoj anketi s time se u potpunosti ne slaže 4,38% ispitanika, djelomično se ne slaže njih 14,91%, dok čak 22,8% niti se slaže niti se ne slaže. Rezultati u drugoj anketi poprilično su slični, i to: u potpunosti ne slaže 7,25% ispitanika, djelomično se ne slaže njih 11,91%, dok čak 22,8%

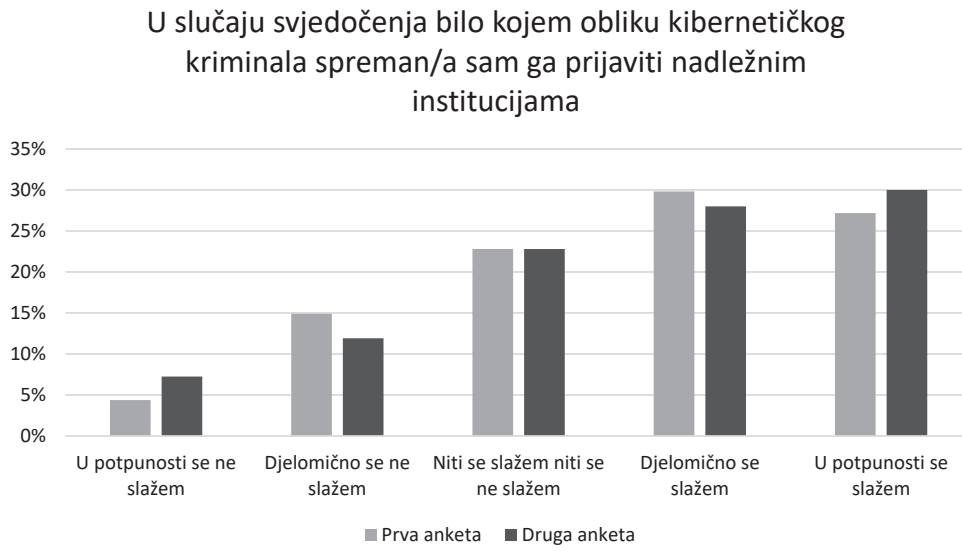
niti se slaže niti se ne slaže. Ti su rezultati vrlo zabrinjavajući. Pojedinačno i komparativno gledajući, golem postotak ispitanika ne bi prijavio kibernetički kriminal, dok u obje ankete čak 22,8% ispitanika nema definiran stav o potrebi prijave kibernetičkog kriminala. Iz tog dijela vidimo da velika većina ispitanika smatra kako su svjesni opasnosti u kibernetičkom prostoru, međutim analiza nam pokazuje (ovdje i u prethodnom poglavlju) da nisu dovoljno educirani o opasnostima niti čine dovoljno na samozaštiti te u značajnom dijelu nisu spremni prijaviti kriminal nadležnim institucijama.



Grafikon 3: Svjesnost studenata o potencijalnim opasnostima koje proizlaze iz korištenja interneta



Grafikon 4: Stavovi studenata o mogućnosti educiranja o izvorima prijetnji putem formalnog obrazovanja



Grafikon 5: Spremnost studenata za prijavu kibernetičkog kriminala nadležnim institucijama

Četvrti dio uspoređuje znanja i iskustva ispitanika o kibernetičkom kriminalu, dobrim navikama i lošim iskustvima korištenja kibernetičkog prostora. Dio rezultata prikazan je u prethodnom poglavlju, stoga ćemo se ovdje fokusirati na šest pitanja i odgovora prema sljedećem rasporedu: Znate li što je *phishing*?; Jeste li ikad bili žrtva hakiranog profila na društvenim mrežama?; Jeste li iskusili zlostavljanje putem interneta (engl. *Cyberbullying*)?; Jeste li ikad bili žrtva osvetničke pornografije (engl. *Revenge porn*)?; Jeste li ikad bili žrtva nekog oblika kibernetičkog kriminala?; Ako ste bili žrtva nekog oblika kibernetičkog kriminala, jeste li ga prijavili nadležnim institucijama? U prvoj anketi (n=114) 43,9% ispitanika nije znalo što je *phishing*, a u drugoj anketi (N=193) njih 30,57%. Usporedno gledajući, u odnosu na prvu anketu, stanje se u drugoj popravilo, međutim ti su pokazatelji dvostruko zabrinjavajući. Ponajprije, riječ je o visokim postocima ispitanika koji ne znaju što je *phishing*, a on je vodeći tip sigurnosnog incidenta u kibernetičkom prostoru. Drugo, rezultat je potrebno staviti u kontekst s rezultatom o svjesnosti spram potencijalnih opasnosti koje proizlaze iz korištenja interneta iz prethodnog dijela. Ondje smo vidjeli da je u obje ankete velika većina ispitanika djelomično ili u potpunosti svjesna potencijalnih opasnosti koje proizlaze iz korištenja interneta. Ondje smo naveli da, na prvi pogled, takva spoznaja ohrabruje, međutim nakon rezultata o znanju što je to *phishing*, rezultati o svjesnosti potencijalnih opasnosti tijekom korištenja interneta pokazuju da ta svjesnost nije utemeljena na znanju, nego na osjećaju. Dalje, znatan udio ispitanika bio je žrtva hakiranog profila na društvenim mrežama – u prvoj anketi 17,54%, drugoj 11,91%. U drugoj anketi manji postotak ispitanika bio je žrtva hakiranog profila, no opet je riječ o velikim udjelima. Posebno zabrinjava koliko je ispitanika bilo zlostavljano putem interneta. U prvoj anketi njih 21,93%, a u drugoj 26,94%. U prvom slučaju riječ je o svakoj petoj osobi, dok se u razdoblju od samo dviju godina stanje pogoršalo i svaka četvrta osoba iskusila je zlostavljanje putem interneta. Vezano uz osvetničku pornografiju, u prvoj anketi 2,63% ispitanika bili su žrtve, a u drugoj anketi njih 3,1%. Premda je riječ o naizgled malim postocima, oni su svakako znakoviti jer takva vrsta

zločina potencijalno ostavlja duboke i dugoročne posljedice na žrtve. Ukupno gledajući, udio ispitanika izloženih bilo kojoj vrsti kibernetičkog kriminala u prvoj je anketi iznosio 9,64% te 5,18% u drugoj anketi. Vidljiv je pad trenda izloženosti kibernetičkom kriminalu, što svakako ohrabruje. Međutim, spoznaja da 27,27% izloženih kibernetičkom kriminalu iz prve ankete i 20% iz druge ankete nisu to prijavili nadležnim institucijama, jako zabrinjava. Iz tog dijela posebno ističemo da je značajan udio ispitanika koji imaju nedostatno znanje o opasnostima, znatan ih je dio bio žrtva kibernetičkog kriminala, a oni koji su bili žrtve, u golemom postotku to nisu prijavili nadležnim institucijama.

5. ZAKLJUČAK I PREPORUKE

Kibernetički prostor koji, prema različitim definicijama, uključuje i internet i sve njegove korisnike neizbježnost je suvremenog svijeta, medij koji, zbog različitih razloga, koristi velika većina ljudi diljem svijeta, a koji donosi i određene izazove. Jedan od njih koji je ovim istraživanjem stavljen u fokus odnosi se na kibernetički kriminal. Navedeni se odvija diljem svijeta i znatno utječe na pojedince, zajednice i društvo u cjelini. Može dovesti do fizičke i emocionalne štete, ekonomskih gubitaka i gubitka povjerenja u institucije. Da bi došlo do tog kriminala, mora postojati „trokut prijevare“ koji uključuje: 1) priliku, 2) pritisak (motiv ili potreba) i 3) racionalizaciju (stav). Dodatno, prema teoriji mogućnosti zločina, počinjenju kibernetičkog kriminala pogoduje dulja prisutnost potencijalnih žrtava na internetu, dok se prema teoriji rutinske aktivnosti zločin događa kada za njega postoji prilika. Čimbenik prilike recipročno se povećava kako su znanja i iskustva o korištenju kibernetičkog prostora niska i ne pridaje im se dovoljno pažnje.

Provedeno istraživanje dalo je zanimljive i, u nekim dijelovima, zabrinjavajuće rezultate te pokazalo određenu diskrepanciju između onoga što studenti znaju i onoga što u praksi čine. Rezultati obiju anketa imali su, očekivano, jako slične pokazatelje. Analiza je pokazala da postoje veliki nedostaci u znanju i iskustvu studenata vezano uz sigurno korištenje kibernetičkog prostora i samozaštite od kibernetičkog kriminala. U ukupnom broju anketiranih u obje ankete golem broj studenata ne koristi antivirusni program niti redovito provjerava je li ažuriran. U pogledu lozinke, mnogi koriste istu lozinku za više digitalnih usluga te je nikad ne mijenjaju, dok velika većina ne koristi neki od programa za upravljanje lozinkama. Također, značajan broj ne poznaje pojam *phishing*, iz čega izvlačimo zaključak da će, ako ne poznaju najčešću opasnost na internetu, imati umanjene izglede od nje se zaštititi. Mnogi su bili žrtve hakiranog profila na društvenim mrežama, iskusili određeni oblik zlostavljanja putem interneta, bili žrtve osvetničke pornografije te žrtve nekog oblika kibernetičkog kriminala, dok značajan udio oštećenih nije prijavio slučaj nadležnim institucijama, što je također problem.

Istraživanje je potvrdilo relevantnost njegove provedbe i korištenja odabranog pristupa. Teorija biheviorizma omogućila nam je analizu i spoznaju navika studentske populacije u korištenju kibernetičkog prostora, svjesnosti rizika i zaštite. Iz svega istraženog zaključujemo da studenti provode puno vremena na internetu i smatraju da su svjesni opasnosti, za što smo utvrdili da je više utemeljeno na osjećaju, a ne na znanju. Isto tako smo spoznali da ispitanici nedovoljno pažnje pridaju zaštiti na internetu. Putem teorije racionalnog izbora možemo zaključiti da se studenti, premda svjesni opasnosti tijekom korištenja kibernetičkog prostora, većinom nedovoljno odgovorno ponašaju te su u značajnom udjelu bili žrtvama

različitih oblika kriminala, no zabrinjavajući dio njih nije se odlučio to prijaviti nadležnim institucijama. Anketa kao metoda istraživanja bila je izvrstan alat za prikupljanje podataka za potrebe istraživanja. Vezano za ciljeve istraživanja, možemo istaknuti da su postignuti i općenit cilj i posebni ciljevi istraživanja. Odrađeni su ispitivanje i analiza znanja i iskustva studentske populacije u korištenju kibernetičkog prostora (općenit cilj) kao i usporedba znanja i iskustva studentske populacije u korištenju kibernetičkog prostora iz dviju anketa provedenih s razmakom od dviju godina, uvid u ponašanje u *online* okruženju i obrasce korištenja interneta te izloženost kibernetičkom kriminalu (posebni ciljevi). Kada je riječ o središnjem pitanju ovog istraživanja (kako možemo procijeniti znanje i iskustva studentske populacije u sigurnom korištenju kibernetičkog prostora), smatramo da je znanje studenata vrlo upitno te nedostatno za sigurno (koliko je god to moguće) korištenje kibernetičkog prostora. Dodatno, smatramo da su iskustva studentske populacije poprilično zabrinjavajuća, kako za njih tako i društvo u cjelini.

Od kibernetičkog kriminala ne postoji apsolutna zaštita, međutim najbolja i najučinkovitija zaštita predstavlja znanje pojedinaca i institucija o preventivnoj zaštititi od raznovrsnih kriminalnih akata unutar kibernetičkog prostora. Rizično ponašanje u kibernetičkom prostoru opasno je za pojedince, ali i za ustanove čijim mrežama pristupaju. Obrazovne ustanove često su meta kibernetičkih napada zbog podataka koje posjeduju, a koji mogu biti iskorišteni za krađu identiteta i druge ilegalne radnje. Rizik povećava i praksa korištenja privatnih računala na fakultetima, jer osoblje ne može kontrolirati osobna računala studenata.

S obzirom na intenzitet digitalnih interakcija i korištenja digitalnih usluga, nužno je podignuti razinu educiranosti među mladima. Formalno obrazovanje, konkretno srednjoškolsko, u ovom se trenutku nedovoljno bavi upozoravanjem mladih i prevencijom kibernetičkog kriminala. Informatika kao izborni predmet više se bavi tehničkim aspektom i učenjem vještina, ali nedovoljno ljudskim aspektom digitalne sfere. Potencijalno je rješenje uvesti kibernetičku higijenu i dobre prakse u *online* ponašanju u osnovnoškolski kurikulum, i to građanskim odgojem ili nekim sličnim predmetom koji će učenike učiti o odgovornom internetskom ponašanju. Visokoškolske ustanove, sudeći prema odnosu prema tom problemu, studente tretiraju kao osobe potpuno svjesne svih opasnosti i otporne na kibernetičke prijetnje. Rezultati ankete pokazali su da takvo stajalište nije realno. Je li najbolji način za podizanje svijesti o *online* prijetnjama osnovnoškolsko i srednjoškolsko obrazovanje, kao što je spomenuto u prijašnjem istraživanju (Rodin, 2022), ili su velike medijske kampanje bolja metoda, ostaje tema otvorena za raspravu. Ono što je na temelju ovih dvaju istraživanja jasno jest da studentska populacija kao društvena skupina s najupečatljivijim kibernetičkim otiskom pristupa digitalnim interakcijama s nedovoljnom razinom opreza koja može potencijalno rezultirati ozbiljnim materijalnim, ali i psihofizičkim posljedicama. Stoga u nastavku iznosimo određene preporuke za unapređenje znanja o sigurnijem korištenju kibernetičkog prostora koje se odnose na pojedince, ali i na druge aktere.

Radi kvalitetnijeg upoznavanja s kibernetičkim prostorom i prevencijom od kibernetičkog kriminala, potrebno je činiti stalne i usklađene aktivnosti između pojedinaca i institucija. Pojedinci trebaju što je moguće više se samoeducirati, prije svega o onom što ih najviše zanima unutar kibernetičkog prostora. Institucije, u ovom slučaju posebno visokoškolske ustanove, trebale bi stalno osmišljavati i provoditi formalnu i neformalnu edukaciju o sigurnom korištenju kibernetičkog prostora te o zaštiti od kibernetičkog kriminala. Samo udruženim

nastojanjima moguće je graditi otpornije i sigurnije pojedince i društvo. Ovo istraživanje i analiza predstavljaju doprinos u tom smjeru.

Kampanje podizanja svijesti o kibernetičkoj sigurnosti pokazale su se kao jedan od najboljih alata za sprječavanje kibernetičkih incidenata i promjenu ponašanja (Bada i dr., 2015 prema Taha i Dahabiyeh, 2020). Budući da je glavni cilj kampanje podizanja svijesti – promjena ponašanja, uporišne teorije za njihovo kreiranje pronalaze se u psihologiji (Taha i Dahabiyeh, 2020). Najčešće se koriste: teorija odvraćanja (engl. *General deterrence theory*), teorija motivacije zaštite (engl. *Protection motivation theory*) i teorija planiranog ponašanja (engl. *Theory of planned behavior*) (Taha i Dahabiyeh, 2020). Teorija odvraćanja polazi od pretpostavke da su pojedinci racionalni te da donose odluke na temelju procjene troškova i koristi. Zato ih je potrebno motivirati na ponašanje koje je u skladu sa sigurnosnim politikama (Bada i dr., 2015; D'Arcy i dr., 2009 prema Taha i Dahabiyeh, 2020). Prema teoriji motivacije zaštite, smatra se da pojedinci proračunato djeluju kako bi zaštitili svoje interese (Bulgurcu i dr., 2010; Johnston i dr., 2015 prema Taha i Dahabiyeh, 2020), dok teorija planiranog ponašanja predviđa namjere ponašanja na temelju triju čimbenika: stava, subjektivne norme i percipirane kontrole ponašanja (Ajzen, 1991 prema Taha i Dahabiyeh, 2020).

Prema uputi Agencije Europske unije za kibernetičku sigurnost (ENISA) i njihova vodiča „AR-in-a-Box" za kreiranje programa za podizanje svijesti, svaka kampanja treba: definirati ciljeve i ciljanu publiku, osigurati financije i ljudske resurse te odabrati primjerene alate i vremenski plan provedbe (ENISA, 2023). Nakon provedbe kampanje potrebno ju je evaluirati kako bi se procijenila njezina uspješnost, a buduće kampanje dodatno prilagodile. Ciljana skupina bili bi studenti, a ciljevi kampanje proizlaze iz procjene rizika organizacije te moraju biti: specifični, mjerljivi, ostvarivi, relevantni i vremenski ograničeni. Neki mogući ciljevi kampanje su: podizanje svijesti o kibernetičkoj sigurnosti, promoviranje najbolje politike i procedure, promoviranje kulture kibernetičke sigurnosti i higijene i sl.

Za provedbu takve kampanje nije potrebno mnogo resursa. Fakulteti se mogu uključiti u obilježavanje Europskog mjeseca kibernetičke sigurnosti (engl. *EU Cyber Security Month – ECSM*), koji se obilježava svake godine tijekom listopada. ECSM je kampanja posvećena podizanju svijesti o kibernetičkoj sigurnosti svih građana i organizacija Europske unije, a provodi se od 2012. godine. ENISA, Europska komisija, zemlje članice te brojni partneri cijele godine surađuju na odabiru relevantnih tema i kreiranju konačne kampanje, a svi su edukativni materijali kampanje besplatni i slobodni za korištenje. Koordinator kampanje na nacionalnoj razini u Republici Hrvatskoj jest Nacionalni CERT, na čijem se internetskom portalu i društvenim mrežama mogu pronaći materijali ECSM kampanje, ali i mnogi drugi.

Alati kao što su infografike, savjeti, posteri, videomaterijali, prezentacije, vježbe, kvizovi i dr. već su dostupni za besplatno korištenje, a na ustanovama je da ih iskoriste i promoviraju putem svojih kanala komunikacije kao što su internetske stranice, mailing liste i društvene mreže. Budući da su se društvene mreže pokazale izrazito popularne među studentima, preporuka je iskoristiti ih i putem njih educirati studente o kibernetičkoj sigurnosti. Fakulteti također imaju mogućnost organizirati predavanja na tu temu i na oglasnim pločama izvjesiti plakate sa savjetima, ali i osnovati kolegije koji se bave tom temom. Informacijska i kibernetička sigurnost dio su naše svakodnevice i danas je teško pronaći zanimanje koje se barem djelomično ne obavlja s pomoću informacijsko-komunikacijske tehnologije. Zato bi svakom studentu kao budućem radniku takav kolegij bio iznimno koristan. Nakon provedene kampanje evaluacija se može provesti s pomoću ankete poput ovih. Praćenjem rezultata uvidjet

će se trendovi i uspješnost kampanje, što će biti osnova za daljnje djelovanje i prilagodbu novim situacijama, jer je kibernetička sigurnost kontinuirani proces koji se zbog razvoja tehnologije i novih oblika prijetnji, mijenja iz dana u dan. U konačnici, kako bi prisilili studente na pridržavanje sigurnosnih praksi, fakulteti mogu donijeti odluku o sankcijama za neprimjereno ili maliciozno korištenje fakultetske infrastrukture, kao i za ponašanje koje dovodi u opasnost njihovu infrastrukturu (npr. ilegalno preuzimanje sadržaja ili korištenje zaraženog računala na fakultetu).

LITERATURA

1. Alhabash, S. & Ma, M. (2017). A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat Among College Students?. *Social Media + Society*, 3(1): 1-13. DOI: 10.1177/2056305117691544.
2. Al-Dosari, K. N. K. A. (2020). Cybercrime: Theoretical Determinants, Criminal Policies, Prevention & Control Mechanisms. *International Journal of Technology and Systems*, Vol.5, Issue 1, No.3. pp 34–63, https://www.iprjb.org/journals/index.php/IJTS/article/download/1133/1247/3565.
3. Brstilo Lovrić, I. (2020). Sociološki osvrt na odrednice studentskoga internetskog kupovanja u Hrvatskoj. *Revija za sociologiju*, 50(1):31–59, DOI: 10.5613/rzs.50.1.2.
4. Clough, J. (2015). *Principles of Cybercrime.* Cambridge: Cambridge University Press.
5. Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*. 44 (4): 588-608. DOI:10.2307/2094589.
6. Corbetta, P. (2022). *Istraživanje u društvenim znanostima: Teorija, metode i tehnike*. Zagreb: Fakultet političkih znanosti Sveučilišta u Zagrebu.
7. Desforges, A. (2014). Representations of Cyberspace: A Geopolitical Tool. *Hérodote*, 152–153(1–2) 67–81. https://doi.org/10.3917/her.152.0067.
8. ENISA (2023). 2023 AR in a box material. https://www.enisa.europa.eu/topics/cybersecurity-education/2023-ar-in-a-box-material.
9. Faktograf.hr (2022). Tijekom pandemije značajno porasle štete prouzročene kibernetičkim kriminalom. https://faktograf.hr/2022/02/23/tijekom-pandemije-znacajno-porasle-stete-prouzrocene-kibernetickim-kriminalom.
10. Folsom, T. C. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). *The Tulane Journal of Technology & Intellectual Property*, 9 (Spring 2007), 75–121.
11. Grigsby, E. (2011). History of the Discipline. U: Ishiyama; J. T. & Breuning, M. (ur.) *21st century Political Science* (str. 3-8), Thousand Oaks: SAGE Publications, Inc.
12. Holt, T. J. & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses*. New York: Routledge.
13. HRT (2024). U porastu kaznena djela iz domene kibernetičke sigurnosti. https://vijesti.hrt.hr/hrvatska/u-porastu-kaznena-djela-iz-domene-kiberneticke-sigurnosti-11339877.
14. Interpol (2017). Global Cybercrime Strategy Summary, https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf.
15. Jurković, A. (2022). Korištenje portala e-Građani u studentskoj populaciji. *Sveučilište u Zagrebu Ekonomski fakultet*, https://urn.nsk.hr/urn:nbn:hr:148:177936.

16. Leukfeldt, R. E. & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, *Deviant Behavior*, 37:3, 263–280, DOI: 10.1080/01639625.2015.1012409.
17. Kassem, R. & Higson, A. (2012). The New Fraud Triangle Model. *Journal of Emerging Trends in Economics and Management Studies*. 3(3): 191–195, https://www.researchgate.net/publication/256029158_The_New_Fraud_Triangle_Model.
18. Hague, R.; Harrop, M. & McCormick, J. (2016). *Political Science: A Comparative Introduction.* Palgrave Macmillan, 8th edition.
19. Heywood A. (2013). *Politics*. Palgrave Macmillan, 4th edition, Printed and bound in China.
20. Hindelang, M. (1978). *Victims of personal crime: an empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger Publishing Co.
21. Martić, K. (2018). Korištenje internet i mobilnog bankarstva među studentskom populacijom. *Sveučilište u Rijeci Ekonomski fakultet*. https://urn.nsk.hr/urn:nbn:hr:192:640278.
22. Milanović Glavan, Lj. (2015). Analiza korištenja internet bankarstva među studentskom populacijom u Republici Hrvatskoj, *Zbornik radova Veleučilišta u Šibeniku*, Vol. 9 No. 3–4. https://hrcak.srce.hr/file/220748.
23. Ministarstvo unutarnjih poslova RH (2023). Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2022. godini. https://mup.gov.hr/UserDocsImages/statistika/2023/Statisticki_pregled_2022_za_webfinal.pdf.
24. Mikac, R. (2023). EU's Cyber-Security Policy Results and Challenges, *Applied Cybersecurity & Internet Governance journal*, Vol. 2 No.1. https://acigjournal.com/resources/html/article/details?id=617215.
25. Nacionalni CERT.hr (2023). Godišnji izvještaj. https://www.cert.hr/wp-content/uploads/2024/02/Godisnji-izvjestaj-Nacionalnog-CERT-a-za-2023.-godinu.pdf.
26. N1 (2023). Kibernetički kriminal u porastu! Evo kako prepoznati prijevaru i zaštititi se. https://n1info.hr/vijesti/online-prijevare-kako-ih-prepoznati-i-kako-se-zastititi.
27. Ottis, R. & Lorents, P. (2010). Cyberspace: Definition and Implications. in Proceedings of the 5th International Conference on Information Warfare and Security, 267-270. Academic Publishing Limited. https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.
28. Parsons, C. (2017). *Introduction to political science: How to think for yourself about politics*, Pearson Education.
29. Robenson, D. (2004). *The Routledge Dictionary of Politics*, London: Routledge, 4th edition.
30. Rodin, T. (2022). Rastuća prijetnja kibernetičkog kriminala: Studija slučaja znanja studentske populacije. *Sveučilište u Zagrebu Fakultet političkih znanosti*. https://urn.nsk.hr/urn:nbn:hr:114:136442.
31. Ruggiero, T. E. (2000). Uses and Gratifications Theory in the 21st Century. *Mass Communication and Society*. 3(1): 3–37. https://www.tandfonline.com/doi/abs/10.1207/S15327825MCS0301_02.
32. Sheldon, P. & Bryant, K. (2016). Instagram: Motives for its use and relationship to narcissism and contextual age. *Computers in Human Behavior*, 58, 89–97. https://doi.org/10.1016/j.chb.2015.12.059.
33. Sever Mališ, S.; Tušek, B. & Žager, L. (2012), Revizija - načela, standardi, postupci / Žager, Lajoš (ur.), *Hrvatska zajednica računovođa i financijskih djelatnika*.
34. Strauss, W. & Howe, N. (1991). *Generations: The History of America's Future, 1584 to 2069* (1 ed.). New York: Quill.
35. Strauss, W. & Howe, N. (1997). *The Fourth Turning: An American Prophecy* (1 ed.). New York: Crown.

36. Škare, V. (2006). Internet kao novi kanal komunikacije, prodaje i distribucije za segment mladih potrošača, *Market-Tržište*, Vol. 18 No. 1–2, https://hrcak.srce.hr/file/34568.
37. Taha, N. & Dahabiyeh, L. (2020). College Students Information Security Awareness: A comparison between smartphones and computers, *Education and Information Technologies*, 26(2): 1721–1736.
38. Tansey, S. & Jackson, N. (2008). *Politics: The basics*, London: Routledge, 4th edition.
39. Vlada Republike Hrvatske (2018). Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine, broj 64/2018., https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html.
40. Vlada Republike Hrvatske (2015). Nacionalna strategija kibernetičke sigurnosti, Narodne novine, broj 108/2015., https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html.
41. Tkalac Verčić, A.; Sinčić Čorić, D. & Pološki Vokić, N. (2010). *Priručnik za metodologiju istraživačkog rada: Kako osmisliti, provesti i opisati znanstveno i stručno istraživanje*. Zagreb: M.E.P. d.o.o.
42. Whiting, A. & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research: An International Journal*, 16(4), 362–369. https://doi.org/10.1108/QMR-06-2013-0041.
43. Yar, M. (2006). *Cybercrime and Society*. London: SAGE Publications.

Abstract

Tomislav Rodin[*], Jakov Kiš[**], Robert Mikac[***]

Comparative Analysis of Results of the Student Population's Knowledge of and Experiences in the Use of Cyberspace

Cyberspace is one of the life lines of the modern world. Many states, international organizations, various business entities, critical infrastructures, local communities, as well as individuals, rely very strongly on it. Cyberspace provides numerous benefits, but it also involves great risks, one of which is cybercrime. The general aim of this research is to investigate and analyze the knowledge and experiences of the student population in using cyberspace. The specific objectives are: to compare the results of two surveys conducted two years apart on the knowledge and experiences of the student population in using cyberspace; to gain insight into online behavior and internet usage patterns; and to assess the level of exposure to cybercrime. The student population was chosen because, based on several relevant parameters, they are exceptionally suitable subjects for such research. Their knowledge and experiences in using cyberspace were investigated through a comparative analysis of the responses in two questionnaires. The results were used to achieve the research objectives and to obtain an answer to the following research question: how can we assess the knowledge and experiences of the student population in the safe use of cyberspace? In addition, the paper provides a set of recommendations on what is possible and necessary to do at both individual and institutional level in order to learn more about cyberspace and avoid exposure to cybercrime as much as possible.

Keywords: Cyberspace, cybercrime, student population, knowledge and experience.

[*] MA in political science Tomislav Rodin, Faculty of Political Science, University of Zagreb, Zagreb, Croatia.

[**]MA in political science Jakov Kiš, Croatian Academic and Research Network – CARNET, Sector - National CERT, Zagreb, Croatia.

[***] Assoc. Prof. Robert Mikac, Faculty of Political Sciences, University of Zagreb, Zagreb, Croatia.