KIBERNETSKO NASILJE V IZOBRAŽEVALNEM OKOLJU

ALEKSANDAR DONČEV,[1] EVA JEREB[2]

[1] Republika Slovenija, Ministrstvo za vzgojo in izobraževanje, Ljubljana, Slovenija
aleksandar.doncev@gov.si
[2] Univerza v Mariboru, Fakulteta za organizacije vede, Kranj, Slovenija
eva.jereb@um.si

Poglavje obravnava problematiko kibernetskega nasilja v izobraževalnem okolju. Poudarja potrebo po odgovorni rabi digitalnih medijev, ki je ključna za varno in odgovorno rabo digitalnih tehnologij pri učencih. Prikazan je sistematičen pristop k izobraževanju o digitalni vključenosti, ki vključuje širši družbeni in kritični pogled na uporabo digitalnih medijev. Povečana uporaba interneta v šolah prinaša priložnosti, a tudi izzive, kot so kibernetsko ustrahovanje, nadlegovanje in zalezovanje, širjenje lažnih novic, nevarnosti za zlorabe osebnih podatkov in kraja identitete ter odvisnost od digitalnih naprav. Pomembno je razumeti, kako anonimnost in dostopnost digitalnih platform omogočata zlorabe, ki lahko resno vplivajo na socialno in čustveno dobrobit učencev. Izpostavljena je potreba po ustrezni infrastrukturi, kibernetski vključenosti in enakih možnostih za vse učence.

DOI
https://doi.org/10.18690/um.fov.1.2026.7

ISBN
978-961-299-117-3

Ključne besede:
kibernetika,
kibernetsko nasilje,
kibernetsko ustrahovanje,
izobraževalno okolje,
digitalni mediji

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/10.18690/um.fov.1.2026.7

ISBN
978-961-299-117-3

Keywords:
cybernetics,
cyber violence,
cyberbullying,
educational environment,
digital media

University of Maribor Press

CYBER VIOLENCE IN THE EDUCATIONAL ENVIRONMENT

ALEKSANDAR DONČEV,[1] EVA JEREB[2]

[1] Republic of Slovenia, Ministry of Education, Ljubljana, Slovenia
aleksandar.doncev@gov.si
[2] University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
eva.jereb@um.si

The chapter deals with the issue of cyber violence in the educational environment. It emphasises the need for responsible use of digital media, which is key to safe and responsible use of digital technologies in schools. It demonstrates a systematic approach to digital inclusion education that encompasses a broader social and critical perspective on the use of digital media. The increased use of the Internet in schools brings opportunities but also challenges, such as cyberbullying, harassment, and stalking, the spread of fake news, the dangers of personal data misuse and identity theft, and addiction to digital devices. It is essential to understand how the anonymity and accessibility of digital platforms enable abuses that can have a profoundly negative impact on social and emotional well-being. The need for adequate infrastructure, cyber inclusion, and equal opportunities for all is highlighted.

1 Uvod

Nasilje v izobraževalnem okolju obstaja že dolgo in se kaže v različnih oblikah, kot so fizično nasilje (npr. pretepanje, izsiljevanje) in psihično nasilje (npr. nadlegovanje, zmerjanje). S pojavom tehnologije v sodobni dobi je svet postal močno odvisen od dostopa do interneta in izmenjave informacij. V zadnjih letih so se pojavile nove oblike komuniciranja, ki povezujejo prebivalstvo v globalnem kibernetskem prostoru. V tridesetih letih od začetka širjenja interneta se je ta razvil iz omrežja, ki je povezovalo le nekaj navdušencev, v ključni element sodobnega življenja za milijone ljudi S tem so se pojavile tudi nove grožnje, ki vplivajo na zasebnost in varnost uporabnikov v kibernetskem prostoru (UNODC, 2010; Bernik in Prislan, 2012).

Eden od novih pojavov je kibernetsko nasilje, ki predstavlja novo obliko nasilja na spletu. Naraščanje kibernetskega nasilja med mladimi v zadnjem desetletju je hkrati opazno in neopazno, saj žrtve redko govorijo o tej problematiki. To deloma izhaja iz prepričanja, da je internet varen prostor, kjer smo 'zaščiteni' pred nasiljem. Med mladimi je kibernetsko nasilje najbolj izraženo na spletnih socialnih omrežjih. (Bernik in Prislan, 2012).

Spletna socialna omrežja so izjemno priljubljena, saj nam pomagajo ohranjati stike v družinskem, osebnem in poslovnem okolju. Ni presenetljivo, da jih uporablja že skoraj 800 milijonov uporabnikov. Za mlade so ta omrežja pomembna za ustvarjanje ugleda in videza ter omogočajo sprejetje v širšo družbo, kar je v tej starosti izredno pomembno. Vendar pa neprevidnost pri varovanju in deljenju osebnih podatkov povečuje možnost zlorabe, kar lahko vodi do različnih oblik kriminalnih dejanj (Brečko, 2012).

Pogosto se pojavljajo kibernetske grožnje, povezane s priljubljenimi spletnimi socialnimi omrežji, saj se osebni podatki in informacije, ki jih mladi delijo na internetu, neprestano povečujejo, medtem ko se varnost podatkov in identiteta vzporedno zmanjšujeta. Ključno vprašanje postaja zasebnost, saj uporabniki nekritično delijo občutljive informacije, ki jih lahko zlorabi kdorkoli. Na primer deljenje občutljivih informacij, posnetkov ali slik na spletnih socialnih omrežjih lahko vodi do kraje identitete, ki potem omogoča izsiljevanje občutljivih informacij, posnetkov, slik ali celo denarja (Brečko, 2012).

2 Kibernetika

Preden lahko govorimo o kibernetskem prostoru in o vplivu na izobraževance, moramo razumeti izraz kibernetika. Kibernetika, izraz iz antične Grčije, označuje spretnost krmarjenja in znanstveno-raziskovalno področje, ki preučuje različne sisteme, kot so biološki, tehnološki in sociološki, ter njihovo sposobnost za krmiljenje in uravnavanje (Duden, 2002; Ivanuša, 2013).

V prvi polovici 19. stoletja je francoski fizik André-Marie Ampére v svoji klasifikaciji znanosti predlagal izraz kibernetika za še neobstoječo znanost nadzora, a je ta predlog kmalu zdrsnil v pozabo. Norbert Wiener je izraz ponovno vpeljal v svoji knjigi Cybernetics (1948), ki se šteje za začetek samostojne discipline kibernetike (Ivanuša, 2013).

Kibernetski prostor se lahko opiše kot virtualni prostor, v katerem posamezniki delujejo in komunicirajo; pravzaprav gre za prostor med prostori (Gibson, 1995; Dimc in Dobovšek, 2012). Ameriško ministrstvo za obrambo ga definira kot globalno domeno v informacijskem okolju, ki je sestavljena iz povezanih in soodvisnih omrežij informacijske tehnologije, kot so internet, telekomunikacijska omrežja in računalniški sistemi (Bernik in Prislan, 2012).

Skoraj vsak posameznik dnevno uporablja kibernetski prostor za dostop do informacij ali njihovo deljenje. Vse naše dejavnosti so načrtovane in izvedene ob upoštevanju digitalnega okolja, kar ustvarja potrebo po virtualnem svetu za izvajanje vsakodnevnih rutin. Ta vse večja prepletenost posameznikovega vsakdana s sodobno informacijsko-komunikacijsko tehnologijo postaja vse bolj opazna v zadnjih dvajsetih letih. Od nje smo postali popolnoma odvisni v zadnjih nekaj letih (Bernik in Prislan, 2012).

Na vsakem področju družbe so se pojavile teorije, ki obravnavajo kibernetski prostor kot pomembno družbeno spremembo, vsaka s svojim razumevanjem narave, pomena in vpliva te nove domene. Obstajata dve osnovni teoriji, ki poskušata opisati kibernetski prostor: ena poudarja prednosti in koristi, druga pa se osredotoča na razmerje med kibernetskim prostorom in državno močjo (Bernik in Prislan, 2012).

Ne glede na teoretične perspektive pa je praktična uporaba informacijsko-komunikacijske tehnologije razkrila, da globalno omrežje ustvarja novo, navidezno okolje, ki soobstaja s fizičnim svetom. Zaradi svoje virtualne narave ima ta 'novi' prostor lastnosti, ki se razlikujejo od resničnega vsakdanjega sveta (Bernik in Prislan, 2012).

Poleg že navedenih prednosti hiter razvoj informacijsko-komunikacijskih tehnologij prinaša tudi naraščajočo stopnjo kriminalnih aktivnosti in pojav novih oblik kriminalnih dejanj. Opredelitev tega pojava mora biti dovolj obsežna, da zajame vso raznolikost kriminalnih dejanj, povezanih z informacijsko-komunikacijskimi tehnologijami. Hkrati pa je treba obravnavati kazniva dejanja enako z vidika kazenskega procesnega prava, ne glede na to, ali so bila storjena v virtualnem ali resničnem svetu. Najpogosteje se pojavi definicija kibernetske kriminalitete kot nelegalnega dejanja, ki je bilo izvedeno z uporabo ali s pomočjo informacijsko-komunikacijskih tehnologij (Dimc in Dobovšek, 2012).

Izraz kibernetska kriminaliteta zajema različne oblike kaznivih dejanj, med katerimi je večina dejansko kaznivih. Vendar pa ta izraz vključuje tudi dejanja, ki so storjena v kibernetskem prostoru, ki v nekaterih primerih pa še niso kazniva po nacionalnem kazenskem pravu ali mednarodnih pravnih aktih. Kot je znano obstaja, veliko pomanjkljivosti pri določanju in razlagi obsega kibernetske kriminalitete, saj so kazniva dejanja opredeljena v kazenskem zakoniku glede na kraj izvršitve, na način, kako je bilo dejanje storjeno, in na kakšen način se je pojavilo (Bernik, 2014).

Ker je narava kibernetske kriminalitete specifična, se preganja le majhen del kaznivih dejanj, povezanih s kibernetskim prostorom (Bernik in Meško, 2011). Uporabniki kibernetskega prostora pogosto pričakujejo prilagojene predpise za obravnavo kibernetske kriminalitete, vendar je to brezpredmetno, saj so številni ukrepi že opredeljeni v kazenski zakonodaji posameznih držav (Bernik, 2014).

V zadnjih letih se je število kibernetskih napadov v Sloveniji občutno povečalo. Leta 2022 je bilo zabeleženih 4123 incidentov, kar predstavlja skoraj tretjinsko povečanje v primerjavi z letom prej. Med temi incidenti so izstopali phishing napadi, ki so se povečali z 950 na 1432 primerov. Najpogostejši vektorski napad je še vedno e-pošta, vendar so se napadi preko SMS sporočil in aplikacij za sporočanje močno povečali. To pomeni, da se grožnje selijo na pametne telefone, kjer ni tako učinkovitih filtrov

za zaščito pred phishingom kot na e-poštnih strežnikih (European Newsroom, 2023).

3 Kibernetska kriminaliteta

Kibernetski kriminal vključuje različne oblike, kot so izsiljevalska programska oprema, napadi na infrastrukturo in finančne goljufije. Evropski policijski urad Europol je v poročilu za leto 2023 opozoril na naraščajočo kompleksnost in prilagodljivost kibernetskih napadov, saj napadalci izkoriščajo nove tehnološke in geopolitične razmere. Število napadov na ključne infrastrukturne sisteme narašča, kar predstavlja resno grožnjo za nacionalno varnost in gospodarstvo (Europol, 2023).

Slovensko nacionalno odzivno središče za kibernetsko varnost (SI-CERT) je izpostavilo potrebo po večji ozaveščenosti in izobraževanju javnosti o kibernetski varnosti. Pomembno je, da uporabniki prepoznajo znake phishinga in drugih spletnih prevar ter uporabljajo večfaktorsko avtentikacijo in močna gesla za zaščito svojih podatkov (European Newsroom, 2023).

V Sloveniji se krepi sodelovanje med javnim in zasebnim sektorjem v boju proti kibernetski kriminaliteti. Evropski policijski urad in druge mednarodne organizacije poudarjajo pomen mednarodnega sodelovanja pri izmenjavi informacij in najboljših praks za učinkovito preprečevanje in odzivanje na kibernetske grožnje. Za nadaljnje zmanjšanje kibernetske kriminalitete v Sloveniji bo pomembna tudi krepitev zakonodaje in uvajanje novih tehnologij za zaznavanje in preprečevanje kibernetskih napadov. Z vedno večjo digitalizacijo družbe in gospodarstva postaja kibernetska varnost vse bolj ključna, zato je nujno, da se temu področju nameni več pozornosti in virov (Europol, 2023).

Kibernetska kriminaliteta v izobraževalnem okolju je zaskrbljujoča težava, saj zahteva večjo pozornost v sodobni digitalni dobi. Z razširjeno dostopnostjo internetnih naprav in spletnih platform se mladi vse pogosteje vključujejo v različne oblike neprimernega vedenja na spletu. Ta vedenja segajo od kibernetskega ustrahovanja in nadlegovanja do kraje identitete in nezakonitega prenašanja datotek. Eden od glavnih izzivov je pomanjkanje ozaveščenosti in razumevanja med mladimi učenci glede pravnih in etičnih posledic njihovih spletnih dejanj. Kibernetski

kriminal v izobraževalnih sistemih v Sloveniji postaja vse bolj pereč problem, ki zahteva celovite preventivne ukrepe in izobraževalne programe. Med pandemijo COVID-19 se je število kibernetskih napadov na šole močno povečalo, saj so se učenci in učitelji preselili na spletne platforme za izobraževanje na daljavo (Europol, 2023).

Napadi z zavrnitvijo storitve (DDoS), kraje podatkov in phishing napadi so med najpogostejšimi oblikami kibernetskega kriminala v izobraževalnih institucijah. Po podatkih Slovenskega odzivnega centra za kibernetsko varnost (SI-CERT) se v zadnjih letih povečuje število prijavljenih incidentov, ki vključujejo šole. Učenci so pogosto tarče phishing napadov, kjer prevaranti poskušajo pridobiti njihove osebne podatke preko lažnih e-poštnih sporočil ali spletnih strani. Težava je še posebej izrazita, ker mlajši učenci nimajo zadostnega znanja o kibernetski varnosti in so bolj dovzetni za prevaro (SI-CERT, 2023).

Slovenske šole se soočajo s temi izzivi, pri čemer so učenci, nekateri celo mlajši od deset let, pogosto vpleteni v kibernetske napade bodisi zaradi neznanja bodisi zaradi namernih poskusov sabotaže. Da bi se spoprijele s temi težavami, šole izvajajo različne preventivne ukrepe, vključno z izobraževalnimi programi, ki učence poučujejo o nevarnostih kibernetskega kriminala in o pravnih posledicah takšnih dejanj (European Newsroom, 2023).

Slovenska vlada in lokalne oblasti sodelujejo z mednarodnimi organizacijami in zasebnim sektorjem pri oblikovanju strategij za zaščito šolskih sistemov. Vključujejo izboljšanje kibernetske varnosti z uvajanjem novih tehnologij in varnostnih protokolov ter s spodbujanjem mednarodnega sodelovanja pri izmenjavi informacij o grožnjah in najboljših praksah. Kibernetski kriminal v šolah v Sloveniji zahteva celovit pristop, ki vključuje izobraževanje, tehnološke izboljšave in mednarodno sodelovanje. S povečano ozaveščenostjo in ustreznimi varnostnimi ukrepi lahko zmanjšamo tveganje za kibernetske napade in zaščitimo naše izobraževalne ustanove (Europol, 2023).

Poleg tega anonimnost in dojemljivost oddaljenosti digitalnega sveta pogosto spodbujata mlade k tveganim vedenjem, ki jih v interakcijah zunaj spleta morda ne bi upoštevali. Izobraževalne institucije morajo odigrati ključno vlogo pri reševanju te težave z uvedbo celovitih programov digitalne pismenosti, ki učencem

omogočajo, da se seznanijo z odgovorno uporabo interneta, spletno varnostjo in posledicami kibernetske kriminalitete. Poleg tega je treba spodbujati odprto komunikacijo med učitelji, starši in učenci, ki lahko ustvari podporno okolje, v katerem se mladi počutijo udobno pri pogovoru o svojih spletnih izkušnjah in iskanju nasveta ob morebitnih spletnih grožnjah. Z zagotavljanjem znanja mladim učencem in spretnosti za odgovorno krmarjenje po digitalnem svetu lahko zmanjšamo pojavnost kibernetske kriminalitete v šolah ter spodbujamo varnejšo spletno skupnost za vse (Europol, 2023).

4 Kibernetsko nasilje

Nasilje v digitalnem prostoru se razume kot nova oblika nasilja (Turan et al., 2011, v Žakelj, 2013), kjer pogosto strani storilca minimalizirajo ali racionalizirajo njegovo pomembnost kot zgolj šalo ali zabavo, medtem ko odziv žrtve ostaja neznan. Anonimnost, ki zagotavlja storilcu občutek varnosti, saj ne bo odkrit, je ključen dejavnik, ki definira nasilje v digitalnem prostoru kot edinstven pojav (Erdur-Baker, 2010; v Žakelj, 2013). Ta anonimnost zahteva drugačen pristop kot klasično nasilje, ki se dogaja v osebnih interakcijah v živo (Kowalski et al., 2008, v Žakelj, 2013).

Potencial za nasilje v digitalnem prostoru med mladimi narašča skupaj z večanjem uporabe informacijsko-komunikacijske tehnologije. Nasilje v digitalnem prostoru omogočajo splošne značilnosti komunikacije prek računalnika ali mobilne telefonije. Anonimnost (»saj ne veš, kdo sem«), nevidnost (»saj me ne vidiš«), asinhronost (»se 'vidimo' pozneje«), razdružena imaginacija (»saj je samo igra«) so le nekatere značilnosti, ki spodbujajo negativne posledice kršenja družbenih norm v digitalnem prostoru (Suler, 2004; v Žakelj, 2013).

Te značilnosti komunikacije prek informacijsko-komunikacijske tehnologije povzročijo, da mladi v digitalnem prostoru brez večjih zadržkov pošiljajo ali objavljajo vsebino ali sporočila, ki lahko prizadenejo, nadlegujejo, žalijo ali ustrahujejo prejemnike (Žakelj, 2013).

Kadar prejemamo žaljiva in ustrahovalna sporočila, komentarje ali SMS-e, govorimo o spletnem trpinčenju in nadlegovanju. Na družbenih omrežjih, forumih ali blogih nas obrekujejo, objavljajo naše zasebne fotografije in jih tudi zlorabljajo na žaljiv način. Pogosto se ustvarjajo lažni profili in sovražne skupine na družbenih omrežjih,

ki se pretvarjajo, da smo mi. Prav tako je pogosta uporaba spletne kamere za namene nadlegovanja in izsiljevanja. Vse to predstavlja spletno ustrahovanje, trpinčenje, nadlegovanje, imenovano tudi cyberbullying (Safe.si).

Spletno nadlegovanje se lahko pojavi iz različnih razlogov, med drugim zaradi jeze, želje po maščevanju, zavisti, potrebe po pozornosti, želje po moči in prevladi. Poleg tega se lahko spletno nadlegovanje zgodi iz dolgočasja ali preprosto iz zabave. Izvajanje spletnega nadlegovanja lahko vključuje neposredne ali posredne napade. Neposredno nadlegovanje pomeni, da napadalci neposredno pošiljajo sporočila žrtvi. Pri posrednih napadih pa sodelujejo drugi posredniki, ki se lahko zavedajo svoje vloge ali pa tudi ne (Brečko, 2012).

Med spletno nadlegovanje sodi tudi snemanje in deljenje nasilnih ali družbeno neprimernih posnetkov, na primer posnetki šolskih pretepov. Objavljanje in deljenje takšnih posnetkov med prijatelji ali v skupnosti prav tako spadata v to kategorijo (Safe.si).

Doksanje

Ena najhujših oblik kibernetskega nasilja je t. i. doksanje (angl. *doxing*). Doksanje pomeni namerno javno objavljanje osebnih podatkov posameznika brez njegove privolitve, z namenom povzročanja škode, ponižanja ali ogrožanja varnosti. Ta oblika nasilja je posebej zaskrbljujoča zaradi svojih resnih posledic, ki lahko segajo od psihološkega stresa do fizične ogroženosti žrtve. Raziskave kažejo, da doksanje lahko vodi do hudih psiholoških posledic, kot so anksioznost, depresija, posttravmatska stresna motnja (PTSD) in celo samomorilne misli (Douglas, 2016).

Ko so osebni podatki, kot so domači naslov, telefonska številka, delovno mesto ali celo finančni podatki, javno objavljeni, je žrtev izpostavljena stalnemu nadlegovanju in grožnjam, kar lahko močno vpliva na njeno duševno zdravje. Ena izmed študij, ki je obravnavala psihološke učinke doksanja, je pokazala, da se žrtve pogosto soočajo z občutkom nemoči in strahu za svojo osebno varnost Poleg tega je socialna izključenost, ki pogosto spremlja javno razkritje osebnih podatkov, dodatno breme za žrtve, saj se lahko soočijo z izgubo socialnih vezi in podpore, kar še povečuje občutke izolacije in osamljenosti (Kowalski, 2014).

Doksanje ni le osebni napad na žrtev, temveč ima lahko tudi širše družbene posledice. Z razkrivanjem osebnih podatkov se lahko sproži verižno ustrahovanje, kjer več posameznikov ali skupin začne nadlegovati žrtev, kar še povečuje intenzivnost in obseg trpljenja. To lahko vodi do resnih varnostnih vprašanj, saj so žrtve lahko izpostavljene fizičnemu nasilju ali celo napadom na dom. Doksanje kot oblika kibernetskega nasilja zahteva resno pozornost in ukrepanje, saj njegove posledice lahko trajno poškodujejo duševno in fizično zdravje žrtev. Potrebno je ozaveščanje in izobraževanje javnosti o resnosti tega problema ter razvoj učinkovitih mehanizmov za zaščito in podporo žrtvam (Whittaker in Kowalski, 2015).

Analiza raziskav o definiciji in bistvenih elementih kibernetskega ustrahovanja razkriva raznolikost pojmov. Izraz ustrahovanje (angl. *bullying*) se v kontinentalni Evropi pogosto uporablja za opis nasilja v šolskem okolju in med mladostniki. Nasprotno pa se v Veliki Britaniji in drugih anglosaških državah ta izraz ne uporablja le za opis nasilja med vrstniki (mladoletniki), temveč tudi za opis nasilnih dejanj v družinskih, partnerskih odnosih, na delovnem mestu ter med otroki, mladostniki in odraslimi (Završnik, 2013). Psihologi kot glavni razlog za tako široko pojmovanje nadlegovanja (in posledično tudi za njegovo obravnavanje) navajajo, da so ločene obravnave (in opredelitve, kot so zloraba starejših, vrstniško nasilje, mobbing na delovnem mestu) podobnih pojavov vodile v neenakomerno poznavanje posameznih oblik ustrahovanja in ločenost strokovnjakov, kar bi združeno lahko pripeljalo do celovitejšega razumevanja in s tem bolj kakovostnega preprečevanja in ukrepanja (Završnik, 2013).

5 Kibernetsko nadlegovanje, zalezovanje in ustrahovanje v osnovnošolskem izobraževalnem sistemu

Kibernetsko ustrahovanje, še posebej med učenci, je postalo resna skrb v dobi digitalizacije, ki predstavlja kompleksen niz izzivov za učitelje, starše in odločevalce. Razmah internetno povezanih naprav in družbenih omrežij je omogočil nove poti za odklonska vedenja na spletu, ki učencem omogočajo izvajanje škodljivih dejanj s še nikoli doslej videnim lahkotnim in anonimnim dostopom. Vrste kibernetskega nasilja zajemajo širok spekter dejavnosti, vključno s kibernetskim ustrahovanjem, kibernetskim zalezovanjem ter nadlegovanjem prek sporočilnih aplikacij, širjenjem govoric ali lažnih informacij ter celo ustvarjanjem lažnih profilov za posnemanje ali blatenje drugih. V kontekstu šole, kjer se mladi še razvijajo tako socialno kot

čustveno, ima kibernetsko nasilje še posebej škodljive posledice za njihovo dobrobit in akademski uspeh.

V današnjem digitalnem svetu je kibernetsko nasilje postala resna težava, ki se je dotaknila tudi slovenskih izobraževalnih ustanov. Pojav je še posebej zaskrbljujoč, saj se otroci in mladostniki pogosto ne zavedajo resnosti svojih dejanj na spletu. Kibernetsko nasilje se lahko kaže na različne načine, od žaljivih komentarjev in objav na družbenih omrežjih do zlonamernih sporočil in groženj. V šolah se pojavlja v različnih oblikah, vključno s posredovanjem sporočil, ki so namenjena žaljenju ali poniževanju sošolcev, objavljanjem fotografij ali videoposnetkov brez privoljenja, širjenjem lažnih informacij in še več. Metode, ki se uporabljajo pri kibernetskem nasilju, so raznolike in se nenehno razvijajo, odražajoč prilagodljivost digitalnih platform in komunikacijskih tehnologij. Od žaljivih komentarjev na družbenih omrežjih do distribucije sramotnih fotografij ali videoposnetkov – storilci pogosto izkoriščajo popularnost spletnih vsebin, da povečajo učinek svojega nadlegovanja.

Poleg tega uporaba anonimnih sporočilnih aplikacij ali lažnih računov lahko oteži sledenje in obravnavo primerov kibernetskega nasilja, kar ustvarja občutek nekaznovanosti med storilci. V nekaterih primerih se lahko kibernetsko nasilje stopnjuje v resnejše oblike spletnega zlorabljanja, vključno z doksanjem (javno objavo osebnih informacij) ali spletnim zalezovanjem (plenilsko ciljanje mladoletnih oseb za spolno izkoriščanje), kar predstavlja resne nevarnosti za varnost in dobrobit mladih učencev (Whittaker in Kowalski, 2015).

Kibernetska udeležba mladih prek digitalnih medijev

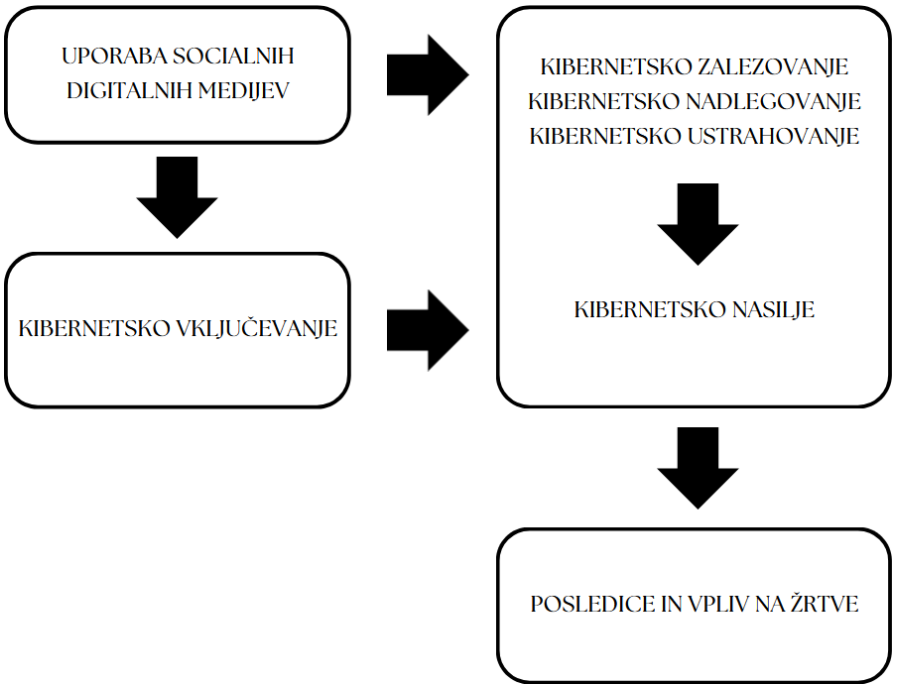
Veliko raziskav ne zajema vseh dejavnikov, ki vplivajo na ali zmanjšujejo kibernetsko nasilje med mladimi. Pomemben del raziskav o kibernetskem ustrahovanju, nadlegovanju in zalezovanju je preučevanje vpliva uporabe digitalnih medijev učencev v izobraževanju. V tem kontekstu je potrebno opraviti temeljito raziskavo, da lahko ugotovimo tudi druge dejavnike, ki vplivajo na kibernetsko nadlegovanje in zalezovanje vključenih v izobraževalni sistem.

Spletna udeležba in uporaba digitalnih medijev sta opredeljeni kot neodvisna dejavnika v študiji, ki je bila objavljena v Mednarodni reviji za okoljske raziskave (angl. *International Journal of Environmental Research*), medtem ko so kibernetsko

nadlegovanje, ustrahovanje in zalezovanje opredeljeni kot posredne spremenljivke kibernetskega nasilja. Odvisna spremenljivka je moralni učinek dejanja, ki neposredno vpliva na psihološko dobro počutje učencev. Opisan model uporablja izraz kibernetsko nadlegovanje za označevanje tako kibernetskega zalezovanja kot ustrahovanja. Udeležba v različnih spletnih mrežnih organizacijah in interakcije z osebami s sumljivimi identitetami so pomembni napovedovalci povečane občutljivosti na tveganje napadov. Spletno vedenje, imenovano spletna udeležba, se nanaša na kibernetsko zalezovanje. Predlaga se, da šole sprejmejo metodo spletne udeležbe, kjer učenci izrazijo soglasje za usmerjeno rabo oz. spletni dogovor ali pogodbo za uporabo računalnika. Potrebna so ustrezna priporočila o etičnem vedenju pri uporabi digitalnih medijev, saj raziskave kažejo, da mladi učinkovito prepoznavajo kibernetsko nasilje in kako ga prijaviti (Alismaiel, 2023).

Digitalni mediji so opredeljeni kot oblike elektronske komunikacij, kot so spletna mesta za digitalne medije, preko katerih uporabniki ustvarjajo spletne skupnosti za deljenje informacij, idej, osebnih sporočil in druge vsebine. Kibernetsko nasilje prek digitalnih medijev običajno opisujemo kot pošiljanje nezaželene, žaljive, zastrašujoče ali neprijetne vsebine s strani neznancev ali znancev preko mobilnih telefonov, interneta ali drugih oblik informacijsko-komunikacijske tehnologije. Kibernetsko nasilje vključuje kibernetsko nadlegovanje, krajo identitete, kibernetsko zalezovanje, pošiljanje nezaželene pošte, sovražno vsebino, individualne zlorabe in kibernetsko ustrahovanje. Jezikovne ovire lahko poslabšajo težave, saj je angleščina najpogosteje uporabljen jezik na večini spletnih mest digitalnih medijev, prevajalni algoritmi pa pogosto dajejo napačne prevode (Alismaiel, 2023).

V zadnjem letu se je število mladih, ki uporabljajo digitalne medije, znatno povečalo. Raziskava Mednarodne revije za okoljske raziskave, ki vključevala 1388 osnovnošolcev, je pokazala, da 22 % otrok dostopa do spletnih mest večkrat na dan, medtem ko 60 % otrok preverja digitalne medije vsaj enkrat na dan. Posamezne spletne identitete nastajajo zaradi digitalne interakcije. Želja po stalnem stiku s prijatelji je močna motivacija za uporabo digitalnih medijev, ki jih lahko uporabimo tudi za širjenje informacij splošni javnosti. Seksting med mladimi ima lahko nepredvidene posledice, kot so uničenje prijateljstev, odnosov in ugleda (Alismaiel, 2023).



Slika 1: Posledice in vpliv na žrtve kibernetskega nasilja pri kibernetskem vključevanju in uporabi socialnih digitalnih medijev

Slika 1 prikazuje model kibernetskega nasilja, kjer je kibernetsko vključevanje prek uporabe socialnih digitalnih medijev in medsebojne spletne interakcije glavni dejavnik, ki prispeva k tveganju kibernetskega zalezovanja, nadlegovanja in ustrahovanja (angl. *cyberbullying*). Iz slike lahko razberemo, da pri kibernetskem vključevanju obstaja več odklonskih dejavnikov tveganja, ki lahko v procesu vključevanja in uporabe digitalnih medijev pripeljejo do nastanka vplivov in posledic, ki različno vplivajo na žrtve kibernetskega nasilja. Vpliv in posledice kibernetskega nasilja v izobraževalnem sistemu je možno omiliti z več ustreznimi preventivnimi aktivnostmi, kot so npr. ustrezna ozaveščanja in izobraževanja o tveganjih in drugih grožnjah pri kibernetskem vključevanju.

Center pomoči za zdravljenje odvisnosti od interneta Logout že izvaja izobraževanja, namenjena izboljšanju dobrobiti in duševnega zdravja staršev in otrok. Center nudi podporo in individualno svetovanje posameznikom, ki se soočajo s spletnimi stiskami, kot so razširjanje in prejemanje seksualnih vsebin (seksting), čustveno izsiljevanje (angl. *grooming*), grožnje, zalezovanje, posmehovanje, ustrahovanje, kraja

identitete ter spletno trpinčenje. Preventivne aktivnosti so ključne za zmanjšanje vpliva in posledic kibernetskih groženj, saj omogočajo zgodnje prepoznavanje težav in nudijo potrebna orodja za njihovo učinkovito obvladovanje. Center Logout poleg preventivnih aktivnosti za večjo ozaveščenost o tveganjih in posledicah pri kibernetskem vključevanju izvaja tudi usposabljanja, izobraževanja, seminarje, predavanja in delavnice za učitelje (Logout, 2024).

Žrtve kibernetskega nasilja

Po podatkih raziskave, ki jo je izvedel Inštitut za kriminologijo Pravne fakultete Univerze v Ljubljani, je kibernetsko nasilje med slovenskimi osnovnošolci v porastu. Raziskava, izvedena med več kot 1000 učenci, je pokazala, da je približno 20 % učencev že bilo žrtev kibernetskega nasilja, medtem ko je okoli 10 % priznalo, da so sami sodelovali v takšnih dejanjih (Žorž, 2020).

Žrtve kibernetskega nasilja pogosto doživljajo občutke tesnobe, depresije in nizke samozavesti. Prav tako so bolj nagnjene k samomorilnim mislim in dejanjem. Raziskave kažejo, da so posledice kibernetskega nadlegovanja lahko celo hujše kot posledice tradicionalnega nadlegovanja, saj se kibernetsko nadlegovanje pogosto dogaja neprekinjeno in lahko doseže široko občinstvo (Kovač, 2019).

Preventivne aktivnosti

Šole in učitelji igrajo ključno vlogo pri preprečevanju in obvladovanju kibernetskega nasilja. Pomembno je, da šole razvijejo jasne politike in smernice za ravnanje v primerih kibernetskega nasilja ter da učitelje in starše ustrezno izobrazijo o prepoznavanju in obravnavanju takšnih primerov. Poleg tega je ključno, da se učencem že v zgodnjem otroštvu privzgojijo vrednote spoštovanja, empatije in odgovorne uporabe digitalnih tehnologij. V okviru programa *Varni na internetu*, ki ga izvaja Zavod RS za šolstvo, potekajo različne izobraževalne delavnice in aktivnosti, namenjene ozaveščanju učencev, učiteljev in staršev o nevarnostih kibernetskega nasilja ter o načinih, kako se mu izogniti in kako ravnati v primerih, ko do njega pride. Program spodbuja tudi aktivno sodelovanje učencev pri oblikovanju varnega spletnega okolja in nudi podporo žrtvam kibernetskega nasilja (ZRSŠ, 2021).

Kljub obstoju preventivnih programov in politik je pomembno, da se kibernetskemu nasilju posveti še več pozornosti, saj gre za dinamičen in hitro spreminjajoč se pojav. Nenehno spremljanje trendov in prilagajanje strategij je ključno za učinkovito preprečevanje in obvladovanje kibernetskega nadlegovanja. Prav tako je pomembno, da se v boj proti kibernetskemu nadlegovanju vključijo vse ravni družbe, vključno s starši, šolami, lokalnimi skupnostmi in zakonodajalci. Šole lahko vzpostavijo politike in postopke za preprečevanje in obravnavanje nadlegovanja, vključno s poučevanjem učencev o varni rabi interneta in družbenih omrežij ter spodbujanjem pozitivnih vedenjskih vzorcev. Starši lahko igrajo pomembno vlogo pri nadzoru spletnega vedenja in vzpostavljanju odprte komunikacije o temah, kot so varnost na spletu in odgovorno ravnanje. Skupnost pa lahko prispeva k ozaveščanju o problemu in zagotavljanju podpore žrtvam ter njihovim družinam (ZRSŠ, 2021).

Poleg tega je pomembno, da se žrtvam zagotovi ustrezna podpora in pomoč. To lahko vključuje psihološko svetovanje, podporne skupine in druge oblike pomoči, ki lahko pomagajo žrtvam pri obvladovanju stresa in izboljšanju njihovega počutja. Prav tako je pomembno, da se storilcem zagotovi ustrezna vzgoja in podpora, da se prepreči nadaljnje neželeno vedenje. V zaključku je treba poudariti, da je kibernetsko nadlegovanje resen problem, ki zahteva celost pristop in sodelovanje vseh deležnikov. Z ozaveščanjem, izobraževanjem in podporo lahko skupaj preprečimo in zmanjšamo pojav v slovenskih šolah ter zagotovimo varno in prijetno okolje za vse učence (ZRSŠ, 2021).

Vzroki za kibernetsko nasilje so lahko različni, vključno s socialnimi in čustvenimi dejavniki, kot so nizka samopodoba, pomanjkanje empatije in želja po priljubljenosti. Prav tako lahko vplivajo tudi družbeni dejavniki, kot so pritiski vrstnikov in želja po pripadnosti določeni skupini. Pomembno je, da se zavedamo, da je kibernetsko nasilje resen problem, ki lahko ima dolgoročne posledice za žrtve, vključno s psihološkimi težavami, kot so depresija in anksioznost, ter težavami v šoli in socialnih odnosih. Motivacije za kibernetsko nasilje med učenci so raznolike in pogosto izvirajo iz kompleksnih dinamik. Medtem ko nekateri primeri izvirajo iz osebnih sporov ali nesoglasij med vrstniki, drugi izvirajo iz ljubosumja, negotovosti ali želje po družbenem ugledu. Poleg tega relativna anonimnost spletnih interakcij omogoča učencem, da se vključijo v vedenje, ki ga morda ne bi razkrili v osebnih interakcijah, kar vodi v povečano distanco in nezadržnost. Ta anonimnost lahko

žrtvam tudi oteži prepoznavanje storilcev ali iskanje pomoči odraslih, kar dodatno poveča občutek izolacije in nemoči.

V odziv na naraščajočo grožnjo kibernetskega nasilja morajo izobraževalne institucije sprejeti celovite strategije za preprečevanje, posredovanje in podporo. Izobraževanje igra ključno vlogo pri opolnomočenju učencev z znanjem in veščinami za varno in odgovorno krmarjenje po digitalni pokrajini. Z vključevanjem kurikuluma digitalnega državljanstva v svoje programe šole lahko spodbujajo kritično mišljenje, empatijo in etično odločanje med učenci, kar ustvarja kulturo spoštovanja in tolerance na spletu. Poleg tega morajo šole vzpostaviti jasne politike in protokole za odzivanje na primere kibernetskega nasilja, zagotavljajoč, da se žrtve počutijo podprte in opolnomočene za prijavo svojih izkušenj brez strahu pred maščevanjem. Skupni napori med izobraževalci, starši, strokovnjaki za duševno zdravje in pravosodnimi organi so ključni za obravnavo mnogoplastnih izzivov, ki jih predstavlja kibernetsko nadlegovanje, in za ustvarjanje varnejših, bolj vključujočih učnih okolij za vse učence.

6 Nacionalni program SAFE.SI

V Sloveniji je bil uveden nacionalni program in pobuda za boj proti kibernetskemu nasilju. Projekt se imenuje *Safe.si* in ponuja izobraževalne vsebine, nasvete in delavnice za učence, starše in učitelje o varni uporabi interneta in preprečevanju kibernetskega nasilja. Kljub tem prizadevanjem pa ostaja kibernetsko nasilje kompleksen problem, ki zahteva stalno pozornost in prilagajanje novim izzivom, ki jih prinaša tehnološki razvoj. Zato je ključnega pomena nadaljnje raziskovanje in razvoj učinkovitih strategij za preprečevanje in obvladovanje tega pojava v izobraževalnem okolju.

Program *Safe.si* je nacionalni program, ki se osredotoča na ozaveščanje in izobraževanje otrok, mladostnikov, staršev, učiteljev ter drugih strokovnih delavcev o varni in odgovorni uporabi interneta in mobilnih naprav. Namen programa je zmanjšati tveganja, povezana z uporabo digitalnih tehnologij, in preprečiti pojav kibernetskega nasilja ter drugih spletnih nevarnosti. *Safe.si* je bil ustanovljen leta 2005 in deluje pod okriljem Fakultete za družbene vede Univerze v Ljubljani. Program se financira preko Evropske komisije in je del širše evropske mreže INSAFE, ki združuje podobne iniciative iz drugih evropskih držav (Safe.si).

Ena izmed ključnih dejavnosti programa *Safe.si* so izobraževalne delavnice in predavanja, ki so namenjena različnim ciljnim skupinam. Za učence osnovnih in srednjih šol organizirajo interaktivne delavnice, kjer se učenci seznanijo s tveganji na spletu in se naučijo, kako se varno in odgovorno obnašati v digitalnem okolju. Posebna pozornost je namenjena temam, kot so kibernetsko nasilje, varovanje zasebnosti, spletne prevare in varna uporaba družbenih omrežij. Za starše in učitelje *Safe.si* ponuja posebna predavanja in delavnice, kjer so predstavljeni načini, kako lahko odrasli učinkovito podpirajo in usmerjajo otroke pri uporabi interneta. Staršem svetujejo, kako postaviti pravila za varno uporabo interneta doma, učiteljem pa nudijo orodja in metode za obravnavo spletnih nevarnosti v šolskem okolju. Poleg delavnic *Safe.si* razvija in ponuja različna izobraževalna gradiva, kot so spletni vodiči, priročniki, video vsebine in interaktivne spletne igre, ki so prosto dostopni na njihovi spletni strani (Safe.si).

Ta gradiva so zasnovana tako, da so razumljiva in privlačna za vse starostne skupine, ter pokrivajo širok spekter tem, povezanih z varno rabo interneta. *Safe.si* tudi redno izvaja raziskave in spremlja trende na področju uporabe interneta med mladimi v Sloveniji. Rezultati teh raziskav so pomemben vir podatkov, ki pomagajo pri oblikovanju učinkovitejših preventivnih strategij in politik na nacionalni ravni. Program *Safe.si* igra ključno vlogo pri izobraževanju in zaščiti mladih v digitalnem svetu. S svojimi dejavnostmi in resursi prispeva k večji ozaveščenosti o spletnih nevarnostih ter spodbuja varno in odgovorno uporabo interneta med mladimi in njihovimi starši (Safe.si).

7 Zaključek

Osebe ki so med seboj danes prijatelji, se lahko že naslednji dan spremenijo v nasprotnike. Za profilno sliko domnevnega sošolca se lahko skriva povsem neznana oseba. Ta tako imenovani 'prijatelj' lahko dostopa do občutljivih podatkov in jih brez našega vedenja posreduje tretjim osebam. Pri kibernetskem vključevanju posameznikov vedno obstaja dovzetnost za odklonska ravnanja ter tveganje za zlorabo osebnih podatkov, ki jih mladi delijo na spletnih omrežjih. Tako kot v vsakdanjem življenju tudi na internetu in družbenih omrežjih ne obstaja popolna varnost. Zato je ključnega pomena, da izobraževalni sistem vzpostavimo tako, da kurikularno vseskozi omogoča pridobivanje dodatnega znanja o uporabi digitalnih

medijev in usposabljanje o varni rabi interneta ter pasteh, ki jih prinaša uporaba družbenih omrežij.

Posledice kibernetskega nasilja v izobraževalnem sistemu so lahko globoke in dolgoročne, prizadevajo ne le neposredne žrtve, temveč tudi njihove širše socialne mreže in izobraževalne skupnosti. Za žrtve se lahko psihološki pritisk kibernetskega nasilja kaže na različne načine, vključno z večjo anksioznostjo, depresijo in nizkim samospoštovanjem. Poleg tega prevladujoča narava digitalne komunikacije pomeni, da lahko nadlegovane žrtve spremlja izven šolskega dvorišča, vstopa v njihove domove in osebna življenja skozi konstantno povezanost. Ta občutek stalnega nadzora lahko prispeva k občutkom strahu in ranljivosti, dodatno oslabi občutek varnosti učencev tako v fizičnih kot tudi virtualnih prostorih.

Večje znanje, bogatejše izkušnje, višja stopnja ozaveščenosti in boljša zaščita računalnikov z osnovnimi zaščitnimi programi zmanjšujejo tveganje. Otroci in mladostniki, ki v šoli redno delajo z računalniki in se zavedajo pomena varnosti ter vrednosti shranjenih podatkov, namenijo del svojega časa tudi urejanju in zaščiti teh podatkov. Zaradi tega se, kljub večji izpostavljenosti, počutijo manj ogrožene.

Tržna konkurenca omogoča dostop do požarnih zidov, antivirusnih programov in programov za filtriranje neprimerne vsebine po dostopnih cenah. Na voljo so tudi brezplačne aplikacije za varno uporabo interneta. Z obstoječimi programi za ozaveščanje in vključevanje starejših ter mlajših oseb v delavnice varne rabe interneta lahko to znanje prenesemo tudi na otroke in mladostnike v izobraževalnem sistemu.

Pomembno je spremeniti splošno prepričanje, da smo na internetu vedno varni. To bi zmanjšalo prostovoljno dodajanje osebnih podatkov v baze družbenih omrežij in otežilo delo storilcem, ki čakajo na trenutek nepremišljenega vedenja uporabnikov (Brečko, 2013).

Viri in literatura

Alismaiel, O. A. (2023). Digital Media Used in Education: The Influence on Cyberbullying Behaviors among Youth Students. *Int. J. Environ. Res. Public Health*, 20, 1370. https://doi.org/10.3390/ijerph20021370

ANSA, dpa, MIA in STA (2023). Slovenia saw an increase in the number of cyber attacks last year. European Newsroom. Pridobljeno 1. 6. 2024 na https://europeannewsroom.com/europe-in-brief-slovenia-sees-rise-in-cyber-attacks/

Bernik, I. (2014). *Cybercrime and cyberwarfare*. Great Britain, Croydon: CPI Group Ltd.

Bernik, I. & Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, 62, 242–252.

Bernik, I. & Prislan, K. (2012). Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem. Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.

Brečko, L. (2012). Raba spletnih socialnih omrežij med otroki (diplomsko delo). Ljubljana: Fakulteta za varnostne vede.

Brečko, L. (2013). Raba socialnih omrežij med otroki in nevarnosti. 14. Slovenski dnevi varstvoslovja, Fakulteta za varnostne vede.

Dimc, M. & Dobovšek, B. (2012). Kriminaliteta v informacijski družbi. Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18(3), 199–210.

Europol (2023). Internet Organised Crime Threat Assessment (IOCTA). Europol. Pridobljeno 3. 6. 2024 na https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 Fakulteta za družbene vede. (2005). Nacionalni program proti kibernetskemu nasilju Safe.si. Pridobljeno 5. 6. 2024 na https://safe.si

Ivanuša, T. (2013). Kibernetika varnostnih sistemov. Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Kovač, M . (2019). Posledice kibernetskega nasilja na duševno zdravje otrok. *Psihološka obzorja*, 28(2), 105–120.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N. & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137.

Logout - Center pomoči za zdravljenje odvisnosti od interneta. (2024) Pridobljeno 1. 6. 2024 na https://www.logout.org/sl/

SI-CERT. (2023). Poročilo o kibernetski varnosti 2023. Pridobljeno 28. 5. 2024 na https://www.cert.si/wp-content/uploads/2024/05/Porocilo-o-kibernetski-varnosti_2023_SI-CERT_web.pdf

Whittaker, E. & Kowalski, R. M. (2015). Cyberbullying via social media. *Journal of School Violence*, 14(1), 11–29.

Zavod RS za šolstvo. (2021). Varni na internetu: Program ozaveščanja o kibernetskem nasilju. Zavod RS za šolstvo.

Završnik, A. (2013). Spletno in mobilno nadlegovanje: pojem, oblike, posledice in soočanje s kazenskim pravom. Zbornik znanstvenih razprav, LXXIII, 219–252.

Žorž, B. (2020). Kibernetsko nasilje med slovenskimi osnovnošolci: Raziskava Inštituta za kriminologijo. Inštitut za kriminologijo pri Pravni fakulteti Univerze v Ljubljani.