Digitalno nasilje

Klarić-Kukuz, Karlo

SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ak. god. 2022./2023.

Karlo Klarić-Kukuz

Digitalno nasilje

Završni rad

Mentor: prof. dr. sc. Radovan Vrana

Zagreb, rujan 2023

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

1. Uvod

U proteklih 20 godina nas je razvoj informacijske i komunikacijske tehnologije doveo do međusobnog umrežavanja uz pomoć raznih softvera. Informacijska i komunikacijska tehnologija je prema Hrvatskoj enciklopediji (bez dat.) „djelatnost i oprema koja čini tehničku osnovu za sustavno prikupljanje, pohranjivanje, obradu, širenje i razmjenu informacija različita oblika, tj. znakova, teksta, zvuka i slike. Komunikacija putem interneta se odnosi na dijeljenje informacija putem interneta.“ Za komunikaciju putem interneta koristimo elektroničku poštu, izravne poruke, pozive, video pozive te objavljujemo i komentiramo slike, videozapise i tekstove na društvenim mrežama. Mogućnosti interneta su praktički neograničene. Proteklih godina se iz internetske komunikacije razvio fenomen zvan digitalno nasilje.

Digitalno nasilje predstavlja jedan od najvećih problema u internetskom okruženju. U digitalno nasilje spadaju razni fenomeni koji se često isprepliću. Međutim jasno je da je digitalno nasilje krajnje negativno ponašanje u internetskom okruženju. U digitalno nasilje spada govor mržnje, krađa podataka putem interneta, vrijeđanje putem interneta, kibernetičko uhođenje, zlostavljanje putem slika, rodno usmjerena dezinformacija, internetska ucjena, iskorištavanje putem interneta i sadržaj koji prikazuje seksualno zlostavljanje djece. Također u digitalno nasilje spadaju drugi oblici štetnog sadržaja na internetu, koji imaju veliku važnost u suvremenom internetskom okruženju. To su kibernetičko ratovanje, kibernetički kriminal i lažne vijesti. U radu ću objasniti pojmove počevši od digitalnog nasilja i različitih vrsta tog oblika nasilja. Zatim ću tematizirati ostale oblike štetnog sadržaja na internetu. Rad će onda prikazati medije koji se koriste za širenje digitalnog nasilja. Naposljetku će se rad baviti zaštitom i prevencijom od digitalnog nasilja kao i kratko prikazati zakonodavni okvir u kontekstu digitalnog nasilja.

Cilj ovog rada je prikaz digitalnog nasilja kao problem koji se događa uporno i trajno u internetskom okruženju zbog toga što internet radi 0-24 sata i ima neograničenu publiku. Također je cilj prikaz različitih vrsta digitalnog nasilja, kao i prikaz medija putem kojih se vrši digitalno nasilje. Isto tako je cilj rada prikaz posljedica digitalnog nasilja za žrtvu i prikaz zaštite od svakog oblika nasilja u internetskom okruženju.

2. Digitalno nasilje

Digitalno nasilje koje se naziva još virtualno zlostavljanje ili elektroničko nasilje (tzv. *digital violence* ili *cyberviolence*) se definira kao „korištenje računalnih sustava radi izazivanja, olakšavanja ili prijetnje nasiljem prema pojedincima, što rezultira tjelesnom, seksualnom, psihološkom ili ekonomskom štetom ili patnjom i može uključivati iskorištavanje pojedinčeve situacije, osobina ili ranjivosti.“ (Vijeće Europe, bez dat.). To je vrsta nasilja u kojoj su žrtve izložene napadima putem elektroničkih medija, elektroničke pošte, SMS poruka i društvenih mreža (Batori, Ćurlin i Babić, 2020). Za razliku od klasičnog oblika nasilja, digitalno nasilje ima praktično neograničenu publiku. Na primjer grupe na Facebooku i javni profili na Instagramu imaju publiku od više milijuna ljudi. Što ne znači da će toliki broj ljudi vidjeti te profile i objave, ali ta mogućnost postoji i kod žrtve može izazvati anksioznost i nelagodu. S time da internet radi 0-24 bez prestanka, tako i žrtve mogu biti zlostavljanje 24 sata dnevno (Batori i sur. 2020). Uz to što djeca i odrasli sve više koriste internet i društvene mreže razvoj digitalnog nasilja leži i u činjenici da djeca nemaju vizualizaciju načinjene štete na žrtvi. Na primjer fizička tučnjava sa sobom nosi i fizičke rane za žrtvu ili njegov plač, urlik i slično. Na taj način nasilnik postaje svjestan učinjenog te mu se psihološki stvara neka vrsta suosjećanja. U digitalnom svijetu ta svijest izostaje i nasilnik često nije ni svjestan uzrokovane štete (UNICEF, 2010. prema Ciboci, 2014). Između tradicionalnog i digitalnog oblika vršnjačkog nasilja postoje sličnosti i razlike. Djeca i adolescenti digitalno nasilje provode i doživljavaju putem internetskih servisa. Digitalno nasilje se prema profilu dijeli na žrtve, na počinitelje, na reaktivne žrtve i promatrače. Također postoji i podjela na fizičko i ekonomsko nasilje (Batori i sur 2020). Nasilje putem društvenih mreža je postalo najčešći oblik digitalnog nasilja među mladima (Batori i sur. 2020). U svibnju 2021. godine je udruga LET (2021) provela istraživanje o iskustvima mladih u Hrvatskoj na internetu u kojem su sudjelovali mladi s prosjekom od 19 godina. Rezultati tog istraživanja pokazuju da 73% ispitanika zna što je digitalno nasilje. Osobno doživjelo jedan oblik digitalnog nasilja je 31% ispitanika. Motivi za vršenje digitalnog nasilja su različiti a najčešći motivi su zabava, osveta ili pritisak drugih osoba.

Da digitalno nasilje nije samo problem među djecom dokazuju razni radovi, koji su istražili nasilje u radnom okruženju. U organizacijama gdje se uveliko koristi informacijska i komunikacijska tehnologija problem digitalnog nasilja raste i predstavlja najrašireniji oblik nasilničkog ponašanja na radnom mjestu. Zhang i Leidner (2014) definiraju digitalno nasilje na radnom mjestu kao „događaji u kojem je zaposlenik elektroničkim putem sistemski izložen

negativnim postupanjem od strane nadređenih i podređenih kolega na duži vremenski period u situaciji gdje nasilnik ima veću moć od žrtve.“ Pew Research Center je 2021. godine proveo istraživanje u kojem je 41% odraslih američkih državljana bilo žrtva digitalnog nasilja (Pew Research Center, 2021). Žrtve digitalnog nasilja na radnom mjestu su izložene visokim stresom, koji na duži vremenski period može imati izrazito negativan učinak na psihološko, emocionalno i mentalno zdravlje zaposlenika u organizaciji, što će se odraziti na motivaciju i radni uspjeh te na kraju krajeva biti kontraproduktivno za organizaciju (Keskin i sur. 2016). Zbog toga što smo u radnom okruženju primorani primati elektroničku poštu i izravne poruke, izbjegavanje digitalnog nasilja na radnom mjestu se čini nemogućim. Isto tako se digitalno nasilje na radnom mjestu može događati u bilo koje vrijeme i na bilo kojem mjestu. Prema tome nasilje se nastavlja i kada zaposlenik nije više na radnom mjestu. Psihološke posljedice za žrtve digitalnog nasilja na radnom mjestu su stres, tjeskoba, napetost, strah, depresija, gubitak samopouzdanja, i manjak zadovoljstva radnim okruženjem te prema tome i manja predanost tvrtki. Također postoji za svjedoka mogućnost psiholoških posljedica, u kojima se on može smatrati ugroženim i kao posljedicu napustiti poduzeće (Keskin i sur. 2016). U poduzećima u kojima postoji neka vrsta digitalnog nasilja može doći do velike fluktuacije radne snage. Manjak zadovoljstva na radnom mjestu rezultira većim promjenama u samom poduzeću a novu radnu snagu se mora obučiti što samo poduzeće košta vrijeme i novac (Keskin i sur. 2016).

2.1. Podjela digitalnog nasilja

Prema Bijelić (2010) se digitalno nasilje može podijeliti u dvije skupine. To je izravan ili direktan napad i neizravan ili indirektan napad.

2.1.1. Izravan napad

Izravnim ili direktnim napadamo smatramo kada žrtva prima uznemirujuće poruke, mijenja joj se lozinka na društvenim mrežama i elektroničkoj pošti, preuzimaju se privatni podaci, koji se koriste u negativne svrhe, šalje se privatni sadržaj trećim osobama te se lažno predstavlja. Isto tako se izravnim napadom smatra slanje virusa, junk maila i spama na računalo ili mobitel (Batori, Ćurlin i Babić, 2020).

2.1.2. Neizravan napad

Neizravnim ili indirektnim napadom se smatraju napadi putem posrednika tj. treće osobe. Žrtva digitalnog nasilja često nije ni svjesna napada. Primjer toga je kada nasilnik sazna lozinku žrtve te trećim osobama šalje uznemirujući sadržaj (Batori, Ćurlin i Babić, 2020).

3. Oblici digitalnog nasilja

Digitalno nasilje je širok pojam i kako postoje različite definicije tako i postoje različite vrste digitalnog nasilja. Točna podjela nije moguća i često se pojmovi isprepliću, međutim digitalno nasilje se može raščlaniti na govor mržnje, krađu podataka putem interneta, vrijeđanje putem interneta, kibernetičko uhođenje, zlostavljanje putem slika, rodno usmjerenu dezinformaciju, ucjenu, iskorištavanje na internetu i sadržaj koji prikazuje seksualno zlostavljanje djece. U sljedećem poglavlju ću definirati i objasniti svaku od podvrsta digitalnog nasilja.

3.1. Govor mržnje

Ne postoji univerzalna definicija pojma govor mržnje. Govorom mržnje prema UN-u smatramo „diskriminirajuće interakcije i ponašanja prema osobi na temelju osobnih karakteristika te osobe.“ (UN, bez dat.). Govor mržnje se temelji na diskriminaciji prema nekoj osobi ili grupi na osnovi rase, nacionalnosti, vjere, spola, seksualne orijentacije i slično (UN, bez dat.). Cilj govora mržnje je vrijeđanje i ponižavanje žrtve. On se razvija iz predrasuda i stereotipa. Predrasude sadrže procjenjivanje i prosuđivanje. Stereotipi su uvjerenja o određenim skupinama koja mogu biti pozitivna ili negativna, međutim u kontekstu govora mržnje ona su negativna (Senta i sur. 2021). U govor mržnje spadaju rasističke, homofobne, islamofobične i antisemitske poruke. Također u govor mržnje spadaju mizogine i transfobne izjave, kao i omalovažavajući komentari prema invalidima. Čak i pozitivne formulacije kao „Afrikanci su dobri u sportu“ u kontekstu mogu upućivati na to da su samo u sportu dobri (Senta i sur. 2021). U Hrvatskoj je govor mržnje česta pojava u svim područjima društva. Poznat je slučaj iz 2022. godine kada je pripadnik Oružanih snaga Republike Hrvatske dijelio i komentirao sadržaj protiv LGBT zajednice. Potom je kazneno prijavljen i određena mu je kazna od 30 000 kuna (danica, 2022).

3.2. Krađa podataka putem interneta

Krađa podataka putem interneta (tzv. *doxing* ili *doxxing*) je pojam koji označava „postupak objavljivanja osobnih podataka o nekoj osobi na internetu bez njene privole kao što su ime, adresa, radno mjesto, broj mobitela, osobne slike i financijske i druge osobne informacije.“ (Kaspersky, bez dat.). Cilj krađe podataka putem interneta je uznemiravanje žrtve, osveta ili narušavanje privatnosti. Krađa podataka putem interneta je problematična jer se osobne informacije određene osobe koriste za zlostavljanje i uznemiravanje putem interneta. Često su žrtve slavne osobe, kojima se objavljuju osobni podaci kao adresa stanovanja, te ih obožavatelji mogu uhoditi u stvarnom svijetu. Objavljivanje osobnih slika slavnih osoba je također problem, međutim taj segment spada već u zlostavljanje putem slika. Poznati primjer krađe podataka

putem interneta je afera Ashley Madison. Ashley Madison je bila internetska stranica za upoznavanje namijenjena ljudima u braku. Grupa hakera je nakon neuspjelog pokušaja ucjene objavila osobne podatke korisnika te mreže i time su milijuni ljudi javno poniženi, što je naštetilo i reputaciji tih osoba (Kaspersky). Žrtva krađe podataka putem interneta je postao i bivši direktor CIA John O. Brennan. Jedan haker je uspješno provalio u elektroničku poštu Brennana. Zatim je objavio njegovu elektroničku poštu, dokumente i osobne podatke. Također žrtvom krađe podataka putem interneta mogu postati i cijele korporacije. Tako su 2014. godine hakeri iz Sjeverne Koreje upali u servere Južno Korejske firme Sony. Pritom su objavili neobjavljene filmove, financijske podatke i osobne podatke zaposlenika (Schneier, 2015).

3.3. Vrijeđanje putem interneta

Vrijeđanje putem interneta (tzv. *flaming*) u internetskom kontekstu se odnosi na agresivno, uvredljivo ili namjerno provokativno ponašanje koje se javlja u internetskim raspravama, forumima, na društvenim mrežama ili drugim platformama (Tech Terms, 2006). Ova vrsta ponašanja često uključuje upotrebu uvredljivog jezika, vrijeđanje, prijetnje ili izazivanje svađe s drugim sudionicima rasprave. Vrijeđanje putem interneta ima za cilj izazvati negativne reakcije, rasprave i konflikte među sudionicima. Primjer vrijeđanja putem interneta je kada zlostavljač vulgarnim rječnikom želi izazvati reakciju na žrtvi. Zlostavljači u ovom kontekstu traže pažnju. Relativna anonimnost na internetu je jedan od uzroka vrijeđanja putem interneta. U stvarnom životu rijetko bi se ljudi vrijeđali intenzitetom kao na internetu. Vrijeđanje putem interneta je odličan primjer kako se internet i stvarni život dijele i kako internet štiti ljude sa lošim namjerama (Christensen, 2023). Rasprave na društvenim mrežama i forumima često prelaze u vrijeđanje onog trenutka kada civilizirani dijalog među sugovornicima više nije moguć. Također se ova vrsta digitalnog nasilja javlja za vrijeme igranja online igrica u kojoj se igrači međusobno verbalno zlostavljaju.

3.4. Kibernetičko uhođenje

Kibernetičko uhođenje (tzv. *cyberstalking*) je „bilo koja uporaba interneta radi uznemiravanja ili proganjanja druge osobe.“ (Kaspersky, bez dat.). Ono se odnosi na praćenje, uznemiravanje i proganjanje neke osobe putem interneta. U kibernetičko uhođenje spada neželjena komunikacija, slanje prijetećih poruka i praćenje žrtvinih aktivnosti na društvenim mrežama. Nasilnik u ovoj vrsti digitalnog nasilja često uhodi žrtvu putem različitih platformi istovremeno. Također kibernetičko uhođenje ne mora nužno zahtijevati direktnu komunikaciju. U takvu vrstu nasilja također spada praćenje žrtvine lokacije pomoću GPSa i digitalna špijunaža. Ovisno o vrsti kibernetičko uhođenje može biti ozbiljno kazneno djelo (Avast academy, bez dat). Na

primjeru žene poznate pod imenom Sara koja je postala žrtva kibernetičkog uhođenja možemo vidjeti na koji način nasilnici vrše uhođenje. Što je počelo kao bezopasan flert putem društvenih mreža je kroz vrijeme preraslo u vrstu internetske veze. Nakon što je Sara pokušala prekinuti vezu, nasilnik poznat pod imenom James Bell joj je krenuo neprestano slati poruke putem različitih servisa, upućivao joj je neželjene pozive i pritom je pokušavao sabotirati druge Sarine odnose. Bell je zatim počeo prijetiti i govoriti laži o Sari na internetu. Na kraju se ispostavilo da je Bell imao bar još deset drugih žrtava, što njega svrstava u serijskog počinitelja (Merlan, 2022).

3.5. Zlostavljanje putem slika i videozapisa

Zlostavljanje putem slika i videozapisa (tzv. *image based abuse*) se definira kao „nesuglasno stvaranje i širenje privatnih seksualnih slika i videozapisa.“ (McGlynn i Rackley, 2016). U tu vrstu nasilja spada osvetnička pornografija (tzv. *revenge porn*) koja se javlja najčešće među bivšim ljubavnicima. To je nasilje u kojoj bivši ljubavnici objavljuju seksualizirani sadržaj koji su dobili od strane bivšeg partnera. Tzv. upskirting je također vrsta zlostavljanja putem slika i videozapisa. To je skriveno snimanje ispod suknje ženske osobe bez pristanka u kojoj se koristi mobitel ili posebne kamere u cipeli. Drugi oblik iznude na temelju intimnog sadržaja je kada haker prijeti objavljivanjem seksualnog sadržaja koji je dobio ulaskom u žrtvine profile (McGlynn i Rackley, 2016). Da žrtva osvetničke pornografije može patiti od dugotrajnih posljedica dokazuje članak o osobi poznatoj pod imenom Ruth King. Ona je žrtva osvetničke pornografije od strane bivšeg partnera. U jednom trenutku ju je prijateljica obavijestila da po internetu kruži njen intimni sadržaj. Bivši partner je taj sadržaj dijelio po pornografskim stranicama, te je isti taj sadržaj podijeljen bezbroj puta. Eksplicitni sadržaj su vidjeli obitelj, prijatelji, poznanici kao i suprugovi kolege s posla. Ruth izjavljuje da se njen život od tada nikad nije vratio na staro i da dan danas trpi od posljedica zlostavljanja putem slika i videozapisa (Moore, 2019).

3.6. Rodno usmjerena dezinformacija

Rodno usmjerena dezinformacija (tzv. *gendered disinformation*) je namjerno širenje dezinformacija o nekoj osobi. Često se ta vrsta nasilja događa ženama na političkim i drugim visokim pozicijama. Cilj rodno usmjerene dezinformacije je manipuliranje javnim mišljenjem tj. diskreditiranje i diskriminacija (HM Government, bez dat.). U to spada širenje lažnih statistika i narativa. Na primjer se žene mogu diskreditirati na način da im se prišiju narativi kao manja sposobnost od muškaraca u određenim područjima, na primjer u političkoj sferi ili da su promiskuitetne. Taktike kojima se služe zlostavljači su objavljivanje lažnih informacija i

manipuliranih slika i videozapisa. Također se u kampanjama koriste narativi o rodnim ulogama i ravnopravnosti kao i seksualnoj orijentaciji, da bi se polarizirale javne rasprave (HM Government). Njemačka ministrica vanjskih poslova Annalena Baerbock je više puta bila žrtva rodno usmjerene dezinformacije. Video montažom njenih intervjua su nasilnici pokušali Baerbock diskreditirati. Neupućeni u montirani sadržaj su mislili da se Baerbock pozicionira na prorusku stranu u rusko-ukrajinskom konfliktu i da ne zastupa interese njemačkog naroda. Time je proizašla velika kampanja protiv ministrice vanjskih poslova Njemačke te se tražila i njena ostavka (Reveland, 2022).

3.7. Ucjena putem interneta

Ucjena putem interneta (tzv. *blackmail*) „je prijetnja otkrivanjem privatnih informacija o osobi u zamjenu za novac ili druge usluge.“ (Simonds, 2022). Počinitelj u ovoj vrsti nasilja ucjenjuje žrtvu objavljivanjem osobnih podataka, eksplicitnih fotografija ili slično. Osim financijskog gubitka, žrtvi može biti oštećena i reputacija (Simonds, 2022). Često oštećena osoba prihvaća zahtjeve nasilnika i plaća traženi iznos iz straha od objavljivanja informacija ili sadržaja na internetu. 2018. godine je u Hrvatskoj kružila masovna poruka putem elektroničke pošte u kojoj je žrtvi rečeno da je na računalo preuzet maliciozni program koji ima pristup kameri te da je počinitelj na taj način došao do eksplicitnog sadržaja žrtve. Zatim se žrtvi prijetilo da će nasilnik objaviti sav prikupljeni sadržaj, ukoliko žrtva ne uplati određeni novčani iznos u obliku Bitcoina. Neupućeni u tu vrstu prevare su iz straha uplatili iznos. Ovaj primjer pokazuje da ucjena može biti lažna ali svejedno učinkovita, ukoliko žrtva nije svjesna prevare (Zaštita, 2018).

3.8. Iskorištavanje putem interneta

Iskorištavanje putem interneta (tzv. *exploitation*) obuhvaća niz seksualno iskorištavajućih i štetnih ponašanja koja se odvijaju ili su omogućena putem interneta i korištenjem digitalnih tehnologija. Često takva vrsta nasilja uključuje djecu kao žrtve. Iskorištavanje na internetu ima široki spektar. U iskorištavanje putem interneta spada kada osoba sa žrtvom razgovara o seksualnim činovima ili šalje seksualizirane slike žrtvi kao na primjer pornografski sadržaj. Također u iskorištavanje putem interneta spada iznuda na temelju seksualnog sadržaja (tzv. *sextortion*). To je vrsta prijetnje u kojoj se žrtvu tjera na seksualne činove ispred kamere te prijetnja objavljivanjem tog sadržaja u javnost. Nasilnici u ovoj vrsti digitalnog nasilja snimaju, izrađuju i dijele sadržaj na raznim platformama na internetu (ACCCE, bez dat.).

3.9. Sadržaj koji prikazuje seksualno zlostavljanje djece

Sadržaj koji prikazuje seksualno zlostavljanje djece je pojam koji je poznat kao dječja pornografija, odnosi se na bilo koji oblik vizualnog prikaza, uključujući slike, videozapise ili druge medije, koji uključuju seksualno iskorištavanje ili zlostavljanje djece (Thorn, bez dat.). To uključuje slike ili videozapise koji prikazuju seksualne radnje s djecom, prikazivanje genitalija djece ili uključivanje djece u eksplicitne ili seksualno sugestivne poze. U tu vrstu nasilja spada svako širenje seksualiziranog sadržaja djece do 18. godine. Nasilnici su često osobe koje poznaju žrtvu, kao obitelj ili uski krug poznanika. U 80% slučajeva su žrtve djevojčice. Takav sadržaj se najčešće dijeli putem internetskih stranica, elektroničke pošte i razmjenom izravnih poruka (National center for missing & exploited children, bez dat.). U Europskoj uniji je 2010. godine bilo 2300 prijava vezano uz djecu zlostavljanom putem interneta. U 2020. godini se ta brojka popela na preko milijun prijava, uz pretpostavku da se veliki broj slučajeva ne otkrije niti prijavljuje (DW, 2022).

4. Ostale vrste štetnog sadržaja

Sljedeće poglavlje se bavi nekim od ostalih vrsta štetnog sadržaja u internetskom okruženju. Sljedeći pojmovi nisu digitalno nasilje u smislu cyberbullyinga, ali svejedno predstavljaju veliku opasnost u internetskom okruženju. Time ih se može smatrati jednom vrstom digitalnog nasilja. Opasnost za građane u internetskom okruženju predstavljaju kibernetičko ratovanje, kibernetički kriminal i lažne vijesti. Te fenomene ću detaljno obraditi u sljedećem poglavlju.

4.1. Kibernetičko ratovanje

Kibernetičko ratovanje se definira kao „postupci države, organizacije ili pojedinca protiv suverene države za prodor u njene računalne i ostale mrežne sustave s ciljem disrupcije, onesposobljavanja ili onemogućavanja korištenja informacijskih resursa, financijskih mreža ili kritične infrastrukture s ciljem jačanja političke agende putem računalnih sustava i mrežne tehnologije.“ (Applegate, 2012). Prema Brzici (2021) u pojam kibernetičkog ratovanja spadaju kibernetički napadi, kibernetički terorizam i kibernetički kriminal. Kibernetičko ratovanje se dijeli na interpersonalne, korporacijske i međunarodne operacije (Brzica, 2021). Interpersonalne operacije imaju za cilj nanijeti štetu pojedincu u što spadaju svi oblici uznemiravanja, gubitak privatnosti i krađa osobnih podataka. Korporacijske operacije imaju za cilj države i poslovne subjekte, krađom hardvera, softvera i servisnih usluga. A međunarodne operacije imaju za cilj destabilizaciju društva i ekonomije, u što spadaju teroristički napadi i međudržavna špijunaža (Brzica, 2021). Metode koje se koriste u kibernetičkom ratovanju su manipulacija internetskih anketa, masovno slanje elektroničke pošte i SMS poruka, ometanje

internetskih stranica, degradacija objava koje se odnose na protivničku stranu i povezano s time umjetno povećavanje vlastite popularnosti kroz objavljivanje bilo to slika, videozapisa ili tekstualnih poruka (Brzica, 2021). Gledajući na trenutna ratna događanja u Ukrajini stručnjaci pretpostavljaju da bi kibernetički rat između Ukrajine i Rusije doveo do potpunog uništenja informacijske i informatičke infrastrukture jedne i druge strane. Rusija, koja je poznata kao država koja vješto koristi informacijsku infrastrukturu za promidžbu njenih vojnih i ekonomskih ciljeva, bi mogla odgovoriti na daljnje vojne sukobe kibernetičkim napadima, a Ukrajina uz pomoć ponajprije SAD-a odgovoriti istom mjerom, što bi zbrojivši stanovnike ove države u kameno doba vratilo oko 200 milijuna stanovnika (Rukavina, 2022).

4.2. Kibernetički kriminal

Jedna od grana kibernetičkog ratovanja je kibernetički kriminal. Kibernetički kriminal se definira kao „kriminal počinjen pomoću računala ili nekog drugog elektroničkog medija i za kriminalne radnje specifične računalima i elektroničkim medijima.“ (Bača, 2004. prema Brkić, Babić i Blažević, bez dat.). Pretpostavlja se da je u 2019. godini putem društvenih mreža kroz kriminalne aktivnosti generirano otprilike 3,25 milijardi dolara (McGuire, 2019). Najrašireniji oblici internetskog kriminala su prodaja medikamenata, prodaja podataka i financijske prevare. Primjer jedne vrste financijske prevare je investicijska prevara, koja se često odvija na društvenim mrežama. Putem oglasa se nudi jedinstvena prilika kojom se navodno možemo brzo i lako obogatiti. Navodno nam se uplatom određenog novčanog iznosa za kupnju najčešće kriptovaluta vraća deseterostruki iznos. Komentari na tim oglasima su uvijek pozitivni i pozivaju da se također okušamo u ulaganju (HANFA, 2022). Prevare u obliku online ljubavnih veza i romansa su također vrlo raširene. U današnjoj informacijskoj ekonomiji najvrjednija stvar su postali podaci. Društvene mreže skupljaju i pohranjuju podatke njihovih korisnika na serverima i time postaju cilj kibernetičkih kriminalaca. Istraživanje Bromiuma je pokazalo da je u zadnjih 5 godina preko 1.3 milijarde korisnika društvenih mreža postalo žrtvom krađe podataka svjesno ili nesvjesno (McGuire, 2019).

4.3. Lažne vijesti

Lažne vijesti se definiraju kao „nevjerodostojne informacije čiji je cilj uvjeriti javnost u željeni sadržaj odnosno manipulirati javnim stavovima i razmišljanjima.“ (Topić Crnoja i Palić, 2022). Pojam lažna vijest ili (tzv. *fake news*) se raširio 2016. godine kao reakcija na navodno namještanje predsjedničkih izbora u Sjedinjenim Američkim Državama od strane ruskih hakera. Vijest kao takva se definira kao novost i informativnost za određenu publiku. Kulić (2019) klasificira lažne vijesti u tri različite kategorije koje se razlikuju po istinitosti informacija

i namjeri. Time dobivamo netočne vijesti (tzv. *false news*), lažne vijesti (tzv. fake news) i satirične vijesti (tzv. news satire). Satirična vijest nije nužno lažna vijest. Lažna vijest kao takva ima zadaću obmane tj. ona tek postaje vijest ako ju čitatelj prihvati kao istinitu. Netočna vijest je jednostavno kriva informacija, koja nema za cilj obmanu nego je kod prijenosa informacija došlo do pogreške od strane stvaratelja informacije. Lažna vijest je digitalna manipulacija, koja ima za cilj obmanu, stvaranje sukoba, i širenje propagande. Isto tako one usmjeruju komunikaciju na društvenim mrežama u jednom smjeru (Grmuša i Prelog, 2019).

Marco Chacon je jedan od stvaratelja lažnih vijesti. On je za The Daily Beast priznao da je lažirao sve svoje članke. A vrhunac njegovog stvaralaštva je bio trenutak kada je novinarka Megyn Kelly s Fox Newsa povjerovala u njegove tekstove te ih je i sama iznosila u eteru. Autori tih portala i članaka zarađuju putem Googleovog Ad Sense servisa, koji funkcionira na način da se po posjeti stranici dobiva određeni novčani iznos od prikazanih reklama na stranici. Svoje stranice promoviraju najčešće putem Facebooka tako da plaćaju određeni iznos Facebooku za plaćeno oglašavanje. Stvaratelji lažnih vijesti plaćanjem oglasa povećavaju publiku, a ta publika dijeli lažne vijesti sa svojim poznanicima i zatim se lažna vijest eksponencijalno širi među svim korisnicima društvenih mreža (Kovačić i Baran, 2018).

Usko povezano sa lažnim vijestima je i ideološka propaganda. Propaganda ili dezinformacija je pojam koji označava „specifično provjerljivo neistinite ili zavaravajuće informacije stvorene, prezentirane i proširene s namjerom stjecanja ekonomske, političke ili neke druge koristi ili radi zavaravanja publike, a koje mogu prouzročiti štetu javnosti.“ (Cert, 2019). Ona se većim dijelom širi putem društvenih mreža. Zbog komora jeka i personaliziranih sadržaja društvene mreže djeluju u službi radikalnih i ekstremističkih skupina koje šire svoja mišljenja s ciljem da utječu na individualca i populaciju. Cilj propagande je nanijeti štetu demokraciji, zdravlju, sigurnosti i ekonomskom blagostanju građana (Cert, 2019). Dezinformacija se većinom širi putem članaka. Često se prilažu i slike izvan konteksta. Zapravo je istinitost takvog članka lako provjerljiva, međutim čitatelj istinitost često ne provjerava. Napredna tehnologija kao umjetna inteligencija (tzv. *AI* ili *artificial intelligence*) nam omogućuje i uvjerljivo objavljivanje dezinformacija kroz manipulaciju slike i zvuka (tzv. *deepfake*) (Cert, 2019).

5. Digitalno nasilje putem raznih medija

Kao što je kroz rad naznačeno, se digitalno nasilje provodi putem različitih internetskih servisa. Digitalno nasilje se provodi putem različitih servisa, zbog toga što internet nudi razne mogućnosti za komunikaciju s drugim ljudima. Mediji kojima se koriste nasilnici su mrežni

forumi, elektronička pošta, sms poruke, izravne poruke i društvene mreže. U sljedećem poglavlju ću kratko objasniti svaki od medija u kontekstu digitalnog nasilja.

5.1. Mrežni Forumi

Mrežni forum „je stranica s aplikacijama koje omogućuju slanje kraćih, uglavnom tekstnih poruka, koje svi korisnici mogu čitati i komentirati slanjem vlastitih poruka.“ (Hrvatska enciklopedija, bez dat.). Obilježja mrežnog foruma su ta da je forum javan i dopušta bilo kome objavljivanje. Forum je zapravo medij u kojem se raspravlja i iznosi stajališta o nekoj temi (Hrvatska enciklopedija, bez dat.). Na forumima se digitalno nasilje provodi vrijeđanjem i objavljivanjem uvrjedljivih poruka i komentara. Često se žrtvu pokušava osramotiti, blatiti i diskreditirati. Isto tako se na forumima šire dezinformacije s ciljem štete reputaciji. Rasprave na forumima mogu poprimiti i ružan rječnik i osobne napade između sudionika, što onemogućava argumentiranu raspravu.

5.2. Elektronička pošta

Elektronička pošta je još uvijek jedan od glavnih komunikacijskih kanala kojim se služimo putem interneta. Postoje različiti pružatelji usluge elektroničke pošte koji se ne razlikuju previše. Najpoznatiji pružatelji elektroničke pošte su Googleov Gmail, Microsoftov Outlook, Yahoo Mail i Apple Mail. Razni oblici digitalnog nasilja se šire elektroničkom poštom. Isto tako elektronička pošta nudi mogućnost slanja masovne pošte putem koje se može dijeliti nasilni sadržaj ili ucjenjivati više žrtava od jednom. Postoji i drugi način vršenja digitalnog nasilja elektroničkom poštom. Dijeljenjem lozinke za pristup računu elektroničkoj pošti nasilnici omogućavaju širenje štetnog sadržaja putem skica (tzv. *draft*) koje sigurnosni filteri ne mogu pratiti, zato što pošta nikad nije bila poslana, ali je spremljena na serveru pružatelja elektroničke pošte (learn safe, 2018).

5.3. SMS poruke

SMS poruke se također koriste za provođenje digitalnog nasilja i širenje štetnog sadržaja u kontekstu digitalnog nasilja. Porukama nasilnik direktno napada žrtvu ili indirektno piše poruke o žrtvi trećoj osobi. Ukoliko žrtva nema spremljen broj nasilnika neće ni znati tko je osoba koja vrši nasilje nad njom. Često se SMS porukama širi govor mržnje, vrijeđanje kao i oblici seksualnog uznemiravanja.

5.4. Izravne poruke

Razmjena izravnih poruka (tzv. *instant messagin*g) je sličan oblik komunikacije kao i komunikacija putem SMS poruka. Međutim putem izravnih poruka se lakše i brže širi vizualni

sadržaj kao slike i videozapisi, bez dodatnih troškova te je ona suvremenija metoda slanja poruka od SMS poruka. Razmjena izravnih poruka se odvija putem aplikacija kao što su WhatsApp, Facebook Messenger, Viber, Signal, Telegram i ostali. Prednost izravnih poruka je ta što se komunikacija odvija trenutačno. Zbog jednostavnosti uporabe i koristi takvih aplikacija, one su postale jedan od glavnih oblika komunikacije putem interneta (Beal, 2022). Zbog toga što su najrašireniji oblik komunikacije putem interneta, tako su i glavni medij za vršenje digitalnog nasilja te je potrebno sagledati ih u kontekstu digitalnog nasilja.

WhatsApp i drugi servisi za razmjenu poruka su jedni od glavnih platforma za provođenje digitalnog nasilja, zbog mogućnosti slanja više vrsta poruka na primjer teksta, slike, videozapisa i zvuka. Postoji i mogućnost stvaranja grupa kao na primjer grupe mržnje ili se određena osoba isključuje iz grupe i tako bude žrtva digitalnog nasilja. Po tome se većina vrsta digitalnog nasilja može provoditi putem razmjene izravnih poruka. Najčešći oblici su ipak govor mržnje, vrijeđanje putem interneta, zlostavljanje putem slika, iskorištavanje i širenje sadržaja koji prikazuje seksualno zlostavljanje djece.

5.5. Društvene mreže

Društvena mreža je internetska usluga u obliku platforme. Ona služi za međusobno povezivanje korisnika (Wikipedija, bez dat.). S time da postoji veliki broj društvenih mreža, tako se razlikuju i načini povezivanja. Na Instagramu se dijele slike sa pratiteljima. X, koji je donedavno bio poznat kao Twitter, se koristi za kratke poruke do 280 znakova koje se dijele sa pratiteljima (Twitter Developer Platform, bez dat.). Facebook umrežuje prijatelje i najraznovrsnija je društvena mreža, zbog toga što ima mogućnost dijeljenja slika, videozapisa, teksta, linkova, prodaje i kupnje na Marketplaceu, traženja novih poznanstva i ljubavnih veza, igranja mrežnih igrica itd. Iako je često u kritici Facebook je postao neizostavan dio privatnog i poslovnog života. Zbog toga što su društvene mreže jedan od glavnih medija za provođenje digitalnog nasilja ću u sljedećem poglavlju kratko predstaviti najkorištenije društvene mreže na svijetu i u kratko prikazati probleme, koji nastaju korištenjem istih.

5.5.1. Facebook

U Hrvatskoj je najpopularnija društvena mreža Facebook. Prema statistici iz 2022. godine otprilike 2 605 600 hrvatskih građana ima profil na Facebooku (Internet World Stats, 2022). Uzmemo li u obzir najnoviji popis stanovništva Hrvatske u kojem u Hrvatskoj živi 3 888 529 stanovnika (Državni zavod za statistiku, 2022), možemo paušalno reći da u Hrvatskoj gotovo 68% stanovnika ima profil na Facebooku. Kao domena Facebook je registriran 11. siječnja 2004. i od tada raste kao najveća i najmoćnija društvena mreža (Singer i Brooking, 2018). S

2,96 milijardi korisnika je Facebook najraširenija društvena mreža (Statista, 2023). Uz širenje lažnih vijesti, Facebook također ima problem sa grupama mržnje, krađom identiteta, financijskim prevarama i dijeljenjem virusa (Perinic, 2021). Grupe mržnje su posebno problematične. Grupa Exposing the Rothschilds ima 130 000 članova (ADL, 2020). U toj se grupi redovito šire teorije zavjere, antisemitizam i govor mržnje. Obitelj Rothschild je poznata židovska obitelj povezana s bankarstvom i često je povezana u negativnom kontekstu (ADL, 2020). Takozvanu bjelačku nadmoć veliča grupa White Lives Matter. Grupa je pokrenuta početkom 2015. godine kao odgovor na pokret Black Lives Matter. Grupa pretežito sadrži rasističke objave prema Afro-Amerikancima i Južno-Amerikancima a veliča bijelu populaciju i fašizam (ADL, 2020).

5.5.2. X (Twitter)

X je donedavno bio poznat kao Twitter. On je također jedna od najpoznatijih društvenih mreža. Jack Dorsey, Biz Stone, Noah Glass i Evan Williams stvorili su X pod imenom Twitter, kao tekstualnu aplikaciju u kojoj u nekoliko znakova korisnici dijele svoja mišljenja sa drugima. Twitter je zatim postao najpopularnija aplikacija za političke poruke (Singer i Brooking, 2018). S time da je X stvoren za objavljivanje tekstualnih poruka bez cenzure, javio se problem govora mržnje na platformi. Zatim je rasla kritika društvenoj mreži X i veliki broj kontroverznih profila je uklonjeno, kao na primjer profil Donalda Trumpa (Singer i Brooking, 2018). 27. listopada 2022. godine Elon Musk, inženjer i investitor, je za 44 milijardi dolara kupio većinski dio dionica Twittera (Conger i Hirsch 2022). Musk je 22. srpnja 2023. Twitter preimenovao u X (Silbering, Stringer, 2023). Musk je nakon preuzimanja te društvene mreže otpustio 6500 zaposlenika, ujedno i odjel za ljudska prava. Nakon toga je govor mržnje protiv Afro-Amerikanaca u prosjeku sa 1282 objava porastao na 3876 objava dnevno. Broj dnevnih objava protiv gej populacije je porastao sa 2506 na 3964. A antisemitske poruke su porasle za 61%. Također su opet dozvoljeni profili povezani sa islamskom državom i krajnjom desnicom (Frenkel i Conger, 2022). S uplatom od 8 dolara moguće verificirati profil tj. priložiti mu plavu kvačicu pored korisničkog imena, time profili dobivaju na vjerodostojnosti (Rosenblatt, 2023). Musk ima velike planove sa samom aplikacijom te želi stvoriti aplikaciju za sve prema uzora na kineski WeChat, s kojim je moguće vršiti platne transakcije (National, 2023). X ima u planu onemogućiti blokiranje drugih profila, što je upitno za djelovanje protiv digitalnog nasilja, zbog toga što se na primjer govor mržnje neće moći ograničiti (Riordan, 2023). Sve u svemu će se daljnji razvoj X-a i dalje gledati pod povećalom.

5.5.3. YouTube

YouTube je društvena mreža za dijeljenje videozapisa i ima 2,562 milijardi korisnika. YouTube je od 2006. godine u vlasništvu Googlea tj. krovne organizacije Alphabet (Ruby, 2023). Svatko sa internetskim pristupom ima mogućnost objavljivanja videozapisa na YouTubeu i dijeljenja sadržaja sa ostalim korisnicima te platforme. Od privatnih korisnika do velikih organizacija svi su prepoznali važnost YouTubea, tako se na njemu mogu pronaći najrazličitiji sadržaji od zabavnih, do obrazovnih videozapisa, snimke i prijenosi sportskih manifestacija, glazbe ali i propagande (Ruby, 2023). Na YouTubeu se mjesečno pregledava 6 milijardi minuta sadržaja u obliku videozapisa te se objavljuje 100 sati video sadržaja svake minute (GCF Global, bez dat.). S time da svatko ima mogućnost objavljivanja sadržaja na YouTubeu postoji i veliki broj videozapisa koji veličaju ideologiju, bave se teorijama zavjera kao i rasizmom. Na primjeru Stefana Molyneuxa, koji je desničar i antisemit i redovno objavljuje video sadržaj na YouTubeu možemo vidjeti širenje rasizma na toj platformi. Molyneux je poznat po širenju lažnih narativa a milijunska publika vjeruje Molyneuxu i neki vide i uzor u njemu, time prihvaćaju njegova mišljenja kao nešto dobro. Pojavom na podcastu Joe Rogana, koji je jedan od najpoznatijih ličnosti u sferi podcasta, si je Molyneux samo povećao publiku, kojoj može isprati mozak pozivanjem na ekstremizam i na govor mržnje (Lewis, 2020).

5.5.4. Instagram

Instagram broji preko 2 milijarde mjesečnih korisnika i time je na četvrtom mjestu najkorištenijih društvenih mreža. To je platforma za dijeljenje slika i kratkih videozapisa sa pratiteljima. Pokrenuta je 2010. godine nakon razvoja pametnih telefona, u njih ugrađenih kamera i većim hardverskim i softverskim mogućnostima uređaja (Ruby, 2023). Mark Zuckerberg je prepoznao potencijal Instagrama te je 2012. godine za 1 milijardu dolara kupio tu društvenu mrežu (Ghaffary i Heath, 2022). Pogotovo mladi su osjetljivi na izgled, a s time da je Instagram aplikacija za razmjenu slika, ona postaje centar za digitalno nasilje. Na jednom primjeru je adolescentica koja vodi stranicu sa 15 000 pratitelja, preimenovala vlastitu stranicu u ime osobe s kojom je u sukobu, te je na tu stranicu objavila obrađene slike žrtve da joj našteti ugled. Osim stranica mržnje, najveći broj nasilničkog ponašanja se događa putem direktnih poruka, komentara na priču (tzv. story) i komentara na objavama (Lorenz, 2018).

6. Posljedice digitalnog nasilja

Prepoznati žrtvu digitalnog nasilja je teže od klasičnog oblika nasilja. Prema Batori, Ćurlin i Babić (2020) znakovi pokazatelji da osoba trpi neki oblik digitalnog nasilja su depresija,

anksioznost, socijalna izolacija, uznemirenost nakon korištenja računala ili mobitela, manjak samopoštovanja, lošiji školski i poslovni uspjeh i narušeno zdravlje.

Osoba koja trpi bilo koji oblik negativnog ponašanja na internetu može patiti od trajnih posljedica. To mogu biti emocionalne, psihološke, fizičke, društvene posljedice i promjene u ponašanju. Najčešće emocionalne posljedice za žrtvu mogu biti ljutnja, osramoćenost i osjećaj nemoći. Psihološke posljedice su anksioznost, depresija i nisko samopoštovanje. Fizičke posljedice se mogu javljati u obliku migrena, poremećaja sna i manjka apetita. Društvene posljedice za žrtvu digitalnog nasilja se vide u dva oblika a to su manjak povjerenja u druge osobe i time otežano stvaranje novih odnosa i namjerna izolacija. Drugi oblik se odnosi na isključivanje iz društva. Promjene u ponašanju mogu uključivati korištenje droge ili alkohola, izbjegavanje škole ili drugih mjesta gdje žrtva trpi nasilje. Ekstrem je i činjenica da žrtve digitalnog nasilja često nose i oružje sa sobom zbog misli da su u bezizlaznoj situaciji te se drugačije ne znaju obraniti (Gordon, 2022). Također imamo i posljedicu financijskog gubitka, kod na primjer iznude. Najveći ekstrem predstavljaju posljedice u obliku samoozljeđivanja i suicidalnih misli i naposljetku suicid (Gordon, 2022). Zabrinjavajuće je što treće osobe koje ne poznaju žrtvu također mogu biti zlostavljači. Putem javnih grupa na Facebooku ili otvorenih stranica na Instagramu i drugim društvenim mrežama početno zlostavljanje se može proširiti na višemilijunsku publiku. Žrtva se nakon toga osjeća bespomoćno, zbog nemogućnosti brisanja sadržaja s interneta nakon objavljivanja (Batori, Ćurlin i Babić, 2020).

7. Prevencija i zaštita od digitalnog nasilja

Vršnjačko digitalno nasilje se može prevenirati tako da se školsko osoblje osvijesti tj. educira o problemima digitalnog nasilja. Zatim osoblje mora aktivno djelovati u prevenciji od digitalnog nasilja (Olweus, 1998. prema Batori, Ćurlin i Babić, 2020).

Buljan Flander (2010) navodi četiri točke koje su potrebne za suzbijanje vršnjačkog nasilja u internetskom okruženju.

1. Podizanje svijesti
2. Školska pravila o nultoj toleranciji na nasilje
3. Nadzor u domovima i školama
4. Adekvatni programi koji imaju za cilj smanjenje vršnjačkog nasilja.

Nužno je educirati i roditelje o internetu i društvenim mrežama, jer jedino kroz informatičku pismenost mogu kvalitetno zaštiti djecu od opasnosti koje pruža internet (Ciboci, 2014). Registracijom i prijavom na platformu ili društvenu mrežu svaka osoba postaje javna za druge

korisnike te platforme. Time se izlažemo svim opasnostima koje društvene mreže mogu izazvati. Međutim, na svim velikim društvenim mrežama se možemo i zaštititi. UNICEF (bez dat.) je dao nekoliko smjernica za zaštitu od napada na društvenim mrežama. U postavkama možemo podesiti privatnost i sigurnost. Na primjer profil na Instagramu možemo zaključati, tako da samo osobe koje se međusobno prate mogu vidjeti objave. Ista postavka postoji i na Facebooku. Komentari se mogu izbrisati i prijaviti administratoru, ukoliko doživimo nasilje putem komentara od osobe koja nas prati. Također možemo i ograničiti komentiranje, time je određenim osobama onemogućeno komentiranje. Vrlo efikasna i laka metoda ograničiti nasilnika od našeg profila je blokiranje drugih profila. Blokirane osobe nam ne mogu ući u profil niti nas kontaktirati na bilo koji način putem određene društvene mreže.

Hrvatska policija je kroz dugogodišnju praksu dala nekoliko smjernica za samozaštitno ponašanje na internetu. Tako povodom dana sigurnijeg interneta koji se ove godine održavao 7.2. Hrvatska policija daje preventivne savjete i edukativne aktivnosti pod temom „Zajedno za bolji Internet.“ Dan sigurnijeg interneta se održava od 2004. godine svakog drugog utorka u veljači (MUP, 2023). Policija godinama daje opće smjernice kako bi se trebalo ponašati u internetskom okruženju. U glavnu točku spada samozaštita uz poslovicu: „Ne čini ništa u virtualnom svijetu što ne bi učinio u stvarnom svijetu.“ (MUP, 2013). Druga točka govori o opreznosti s kontaktom s nepoznatim osobama. Važno je pažljivo promotriti nove „prijatelje“ i u razgovore treba uvijek ulaziti s nekom dozom skepticizma, ukoliko nismo stopostotno sigurni u namjere tih osoba. Sljedeća smjernica za sigurno ponašanje je svijest da svaki privatni i intimni razgovor s osobom može postati javan. Ukoliko imamo razgovor s osobom koja nas uznemiruje odmah trebamo prekinuti razgovor s njome. Također treba uzeti u obzir da nam se nepoznate osobe mogu predstaviti kao poznate i od nas tražiti povjerljive podatke te nas na taj način ucijeniti, prema tome je uvijek potrebna doza skepticizma za vrijeme razgovora putem izravnih poruka (Matijević, 2014). Red Button je aplikacija koju je razvila Hrvatska policija s ciljem prijavljivanja negativnog ponašanja u internetskom okruženju, koji se prvenstveno odnosi na iskorištavanje djece, ali i svih drugih oblika digitalnog nasilja. Aplikacija je puštena u javnost 2013. godine i do sada je zaprimljeno preko 2500 prijava u vezi s nasiljem (Roda, 2018). Putem Red Buttona žrtva ili treća osoba ima mogućnost anonimno prijaviti zlostavljanje djeteta. U to spada svaki oblik nasilničkog ponašanja putem interneta kao vrijeđanje putem interneta, krađa podataka putem interneta, iskorištavanje, ucjena ili seksualno zlostavljanje. Red Buttom nije samo aplikacija kojom se prijavljuje nasilje na internetu nego i u stvarnom

životu. Nakon prijave policijski službenici za mladež prijavu obrađuju u skladu sa zakonom, da bi spriječili zlostavljanje djece (Ministarstvo unutarnjih poslova, bez dat.).

Hrvatski zakonodavni okvir kažnjava kriminalne radnje na internetu prema Prekršajnom zakonu Republike Hrvatske i Kaznenom zakonu Republike Hrvatske. Većina kaznenih djela je potrebno privatno prijaviti, kao što je kazneno djelo protiv časti i ugleda. U to spadaju uvrede, sramoćenje i kleveta. Isto tako imamo i kaznena djela protiv privatnosti. U to spada nedozvoljena uporaba osobnih podataka, neovlašteno snimanje te povreda privatnosti djeteta. Kažnjivo je i nametljivo ponašanje, prijetnja i poticanje na nasilje i mržnju, kao i rodna diskriminacija. Također su definirana i kaznena djela spolnog zlostavljanja i iskorištavanja djeteta. U većini slučajeva dolazi do novčane kazne za počinitelja, a u krajnjim ekstremnim slučajevima može doći i do zatvorske kazne za počinitelja (Matijević, 2014).

8. Zaključak

Digitalno nasilje je kao na početku rada navedeno suvremeni problem u internetskom okruženju. Sama definicija digitalnog nasilja da je to „korištenje računalnih sustava radi izazivanja, olakšavanja ili prijetnje nasiljem prema pojedincima, što rezultira tjelesnom, seksualnom, psihološkom ili ekonomskom štetom ili patnjom i može uključivati iskorištavanje pojedinčeve situacije, osobina ili ranjivosti“ (Vijeće Europe, bez dat.), nam daje široku lepezu ponašanja, koja se mogu svrstati u digitalno nasilje. Rad je podijelio digitalno nasilje u 9 različitih kategorija koje se ponekad međusobno isprepliću. Govor mržnje kao diskriminirajuća komunikacija vrijeđa žrtvu na osnovi vanjskih karakteristika i uvjerenja. Krađa podataka putem interneta se u digitalno nasilje svrstava kao povreda zaštite privatnosti i informacija. Vrijeđanje putem interneta je zapravo vrsta nasilja u kojoj se žrtva ismijava, ponižava i blati korištenjem uvredljivog jezika. Kibernetičko uhođenje kao i krađa podataka putem interneta je povreda privatnosti, međutim taj oblik nasilja može i u stvarnom svijetu poprimiti ozbiljne posljedice za žrtvu. Zlostavljanje putem slika je širenje seksualno eksplicitnog sadržaja i ono nanosi veliku štetu žrtvi, kojoj je objavljena intima. Rodno usmjerena dezinformacija se provodi radi diskreditiranja druge osobe na način da se šire razni netočni narativi. Ucjena putem interneta za cilj ima financijsku dobit, dok se iskorištavanje putem interneta češće manifestira u krađi podataka. Sadržaj koji prikazuje seksualno zlostavljanje djece je jedan od najozbiljnijih kriminalnih činova u internetskom okruženju, a za žrtvu su posljedice vrlo ozbiljne. Kibernetičko ratovanje, kibernetički kriminal i lažne vijesti također predstavljaju ozbiljan negativan čin, jer te oblike nasilja često provode organizacije, koje imaju za cilj oštetiti druge organizacije ili pojedince. Digitalno nasilje se provodi putem svih mogućih medija i često nasilnik ne bira ni vrijeme ni sredstvo. Veliki problem digitalnog nasilja je internet sam po sebi. Jednom objavljeni sadržaj na internetu se gotovo ne može izbrisati. Digitalno nasilje koje se događa na internetskim forumima, putem direktnih poruka i na društvenim mrežama često i godinama nakon objavljivanja ostaje vidljiv. Pogotovo su društvene mreže postale glavni katalizator za provođenje negativnog ponašanja na internetu. Posljedice za žrtvu mogu biti kobne. Žrtva digitalnog nasilja može trpiti trajne emocionalne, psihološke, fizičke i društvene posljedice, a sama spoznaja da žrtvama dolazi u obzir čak i suicid bi nas sve trebala osvijestiti o realnom problemu digitalnog nasilja. Iako se putem raznih programa obrazovanja pokušava prevenirati svaki oblik digitalnog nasilja to često jednostavno nije moguće. Zakonodavni okvir je takav da se najčešće samo uz privatnu tužbu nasilnik može prijaviti, međutim sudski procesi su često dugotrajni, naporni, skupi i neisplativi, ukoliko je žrtva uopće spremna na tužbu zbog mogućeg srama.

Uzevši sve to u obzir digitalno nasilje postaje jedan od najvećih problema današnjice. S time da se internet koristi gotovo u svim segmentima privatnog i poslovnog života mora se naći način za bolje suzbijanje svakog oblika nasilja u internetskom okruženju. Preventivne mjere nisu dovoljne, već je potreban suvremeni zakon koji će adekvatno kazniti počinitelja. A osobe koje primijete nasilje se moraju osvijestiti, prijaviti nasilje i stati u obranu žrtvi.

9. Izvori

1. Applegate, S. (2012). Cyber Warfare addressing new threats in the information age. Academia. Preuzeto 15.2.2023 s https://www.academia.edu/1098261/Cyber_Warfare_Addressing_New_Threats_in_the_Information_Age
2. Batori, M, Ćurlin, M. i Babić D. (2020). Nasilje putem interneta među adolescentima, Mostar: Zdravstveni glasnik, 2020. Vol. 6 No. 1. str. 104-114
3. Beal, V. Types of Internet Communications (2022, srpanj). Webopedia.com. Preuzeto 15.1.2023 s https://www.webopedia.com/insights/internet-communications/
4. Brkić, A. Babić, Š. Blažević (2013), A. Kibernetički kriminal/cyber kriminal. Preuzeto 15.2.2023 s https://security.foi.hr/wiki/index.php/Ra%C4%8Dunalni_kriminal/cyber_kriminal.html
5. Child pornography is sexual abuse material. Thorn. Preuzeto 10.6.2023 s https://www.thorn.org/child-pornography-and-abuse-statistics/
6. Christensen, T. (2023, svibanj). What ist Flaming? Easy Teck Junkie. Preuzeto 10.6.2023 s https://www.easytechjunkie.com/what-is-flaming.htm
7. Ciboci, L. (2014) Grupe mržnje na društvenim mrežama – novi oblici nasilja među djecom i mladima. Zbornik radova konferencije nasilje na Internetu među i nad djecom i mladima (13-27). Zagreb: Društvo za socijalnu podršku
8. Conger, K. i Hirsch L. (2020, listopad). Elon Musk Completes $44 Billion Deal to Own Twitter. The New York Times. Preuzeto 1.2.2023 s https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html
9. Coping with Cyberbullying. The Bury Dictionary. Preuzeto 3.2.2023 s https://theburydirectory.co.uk/coping-with-cyberbullying
10. Cyberbullying a problem around the globe: poll (2012, siječanj). Reuters. Preuzeto 16.2.2023 s https://www.reuters.com/article/us-cyberbullying-poll-idUSTRE80A1FX20120111
11. Dan sigurnijeg Interneta (2023). Ministarstvo unutarnjih poslova. Preuzeto 2.6. s https://mup.gov.hr/policijske-uprave/dan-sigurnijeg-interneta-203647/200270
12. Daniel (2022, listopad). Cyberbullying on Twitter: Examples, Statistics & Policy. Qwitter. Preuzeto 1.2.2023 s https://useqwitter.com/cyberbullying-on-twitter/

13. Defining online sexual harassment. deShame. Childnet. Preuzeto 15.1.2023 s https://www.childnet.com/what-we-do/our-projects/project-deshame/defining-online-sexual-harassment/
14. Desjardins N. (2022, prosinac). Creepshots a perverted menace. Fonsly.com. Preuzeto 5.2. s https://fonsly.com/en/creepshots-a-perverted-menace/
15. Downey, L. (2021, rujan). Google's Incredible YouTube Purchase 15 Years Later. Investopedia. Preuzeto 3.2.2023 s https://www.investopedia.com/google-s-incredible-youtube-purchase-15-years-later-5200225
16. Društvena mreža (2021, srpanj). Wikipedija Preuzeto 7.2.2023. s https://hr.wikipedia.org/wiki/Dru%C5%A1tvena_mre%C5%BEa
17. Edukacija djece o sigurnosti na društvenim mrežama i internetu (2013, studeni). Ministarstvo unutarnjih poslova. Preuzeto 10.6.2023 s https://mup.gov.hr/vijesti-8/edukacija-djece-o-sigurnosti-na-drustvenim-mrezama-i-internetu/170653
18. EU cracks down online child sexual abuse (2022, studeni). Deutsche Welle. Preuzeto 10.6.2023 s https://www.dw.com/en/eu-plans-crackdown-on-online-child-sexual-abuse/a-61758237
19. Fifteen ways Elon Musk has changed Twitter, now X, since taking over (2023, kolovoz). The National News Business Preuzeto 27.8.2023 s https://www.thenationalnews.com/business/technology/2023/08/19/fifteen-ways-elon-musk-has-changed-twitter-now-x-since-taking-over/
20. Flaming (2006). Tech Terms. Preuzeto 10.6.2023 s https://techterms.com/definition/flaming
21. Frenkel S. i Conger K. (2022, Prosinac) Hate Speech's Rise on Twitter Is Unprecedented, Reaserchers Find. The New York Times. Preuzeto 30.4.2023 s https://www.nytimes.com/2022/12/02/technology/twitter-hate-speech.html
22. Gender and countering disinformation. HM Government. Preuzeto 10.6.2023 s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866353/Quick_Read-Gender_and_countering_disinformation.pdf
23. Ghaffary S. i Heath A. (2022, srpanj) The Facebookification of Instagram. Vox.com. Preuzeto 15.1.2023 s https://www.vox.com/recode/23274761/facebook-instagram-land-the-giants-mark-zuckerberg-kevin-systrom-ashley-yuki
24. Gordon, S. (2022, srpanj). The Real-Life Effects of Cyberbullying on Children. Very well family. Preuzeto 7.6.2023 s https://www.verywellfamily.com/what-are-the-effects-of-cyberbullying-460558

25. Grmuša, T. i Prelog, L. (2020). Uloga novih tehnologija u borbi protiv lažnih vijesti – iskustva i izazovi hrvatskih medijskih organizacija, Medijske studije, Vol.11 No.22, 2020, str. 62-80
26. Hateful and Conspiratorial Groups on Facebook (2020, ožujak). ADL.org. Preuzeto 3.2.2023 s https://www.adl.org/resources/blog/hateful-and-conspiratorial-groups-facebook
27. Informacijska i komunikacijska tehnologija. enciklopedija.hr. Preuzeto 15.1.2023 s https://www.enciklopedija.hr/natuknica.aspx?id=27406
28. Internet prijevare. Republika Hrvatska Ministarstvo unutarnjih poslova Ravnateljstvo policije. Preuzeto 3.2.2023 s https://policija.gov.hr/prevencija/racunalna-sigurnost/internet-prijevare/456
29. Internet World stats (2022, siječanj). Preuzeto 15.2.2023 s https://www.internetworldstats.com/europa.htm
30. Jesu li i vas ucijenili preko interneta? (kolovoz, 2018). Zaštita. Preuzeto 10.6.2023 s https://zastita.info/hr/novosti/jesu-li-i-vas-ucijenili-preko-interneta,25222.html
31. Keskin H. Akgün A. E. Ayar H. i Kayman S. S. (2016). Cyberbullying victimization, counterproductive work behaviours and emotional intelligence at workplace, Antalya: Procedia - Social and Behavioral Sciences 235, 281 – 287
32. Kovačić, S. i Baran, T. (2018) Novi mediji – generator novih tehnika manipulacija; HUM: časopis Filozofskog fakulteta Sveučilišta u Mostaru, Vol. 13 No. 19, 2018. str. 271-294
33. Lewis, B. (2020, siječanj). All of YouTube, Not Just the Algorithm, is a Far-Right Propaganda Machine. FFWD. Preuzeto 1.2.2023 s https://ffwd.medium.com/all-of-youtube-not-just-the-algorithm-is-a-far-right-propaganda-machine-29b07b12430
34. Lorenz, T. (2018, listopad). Teens Are Being Bullied ‘Constantly’ on Instagram. The Atlantic. Preuzeto 1.2.2023 s https://www.theatlantic.com/technology/archive/2018/10/teens-face-relentless-bullying-instagram/572164/
35. Matijević, A. (2014). Nasilje nad i među mladima na Internetu. Zbornik radova konferencije nasilje na Internetu među i nad djecom i mladima (39-50). Zagreb: Društvo za socijalnu podršku
36. McGlynn C. i Rackley E. (2016). Image-based abuse: More than just „Revenge porn.“ Research Spotlight. Preuzeto 10.6.2023 s https://www.birmingham.ac.uk/Documents/college-artslaw/law/research/bham-law-spotlight-IBSA.pdf

37. McGuire, M. (2019). Social media platforms and the cybercrime economy. Bromium. Preuzeto 21.4.2023 s https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf
38. Merlan. A (2022, lipanj). These Women Say One Man Terrorized Them Online for Years. Then, They Decided to Band Together. Vice. Preuzeto 11.6.2023 s https://www.vice.com/en/article/m7gq8a/james-bell-cyberstalking-harassment-catfishing
39. Mjera opreza pri korištenju društvenih mreža (2014). Ministarstvo unutarnjih poslova. preuzeto 14.4. s https://mup.gov.hr/vijesti-8/mjere-opreza-pri-koristenju-drustvenih-mreza-159539/156741
40. Moore, A. (2019, rujan). „There's no end and no escape. You feel so, so, exposed“: life as a victim of revenge porn. The Guardian. Preuzeto 10.6.2023 s https://www.theguardian.com/lifeandstyle/2019/sep/22/theres-no-end-and-no-escape-you-feel-so-so-exposed-life-as-a-victim-of-revenge-porn
41. Objavljeni konačni rezultati Popisa stanovništva (2022, rujan). Državni zavod za statistiku. Preuzeto 15.2.2023. s https://dzs.gov.hr/vijesti/objavljeni-konacni-rezultati-popisa-2021/1270
42. Online prijava zlostavljanja djeteta – Red Button. Ministarstvo unutarnjih poslova. Preuzeto 10.6.2023. s https://mup.gov.hr/online-prijave/online-prijava-zlostavljanja-djeteta-red-button/281667
43. Online sexual exploitation and abuse: A Glossary of Terms. Equality now. Preuzeto 10.6.2023 s https://www.equalitynow.org/online-sexual-exploitation-and-abuse-a-glossary-of-terms/
44. Perinic, M (2021, svibanj). Facebook is the Place to Go for Cybercrime Services. Secure Thoughts. Preuzeto 3.2.2023 s https://securethoughts.com/facebook-cybercrime-services/
45. Preventivne aktivnosti policije povodom Dana sigurnijeg interneta 2023 (2023, veljača). Republika Hrvatska Policijska uprava vukovarsko-srijemska. Preuzeto 8.2.2023 s https://vukovarsko-srijemska-policija.gov.hr/vijesti/preventivne-aktivnosti-policije-povodom-dana-sigurnijeg-interneta-2023/20281
46. Research & statistics (2022). Australian Center to Counter Child Exploitation. Preuzeto 5.2.2023 s https://www.accce.gov.au/resources/research-and-statistics
47. Reveland, C. (2022, rujan). Eine pro-russische Kampagne? Tageschau. Preuzeto 9.6.2023 s https://www.tagesschau.de/faktenfinder/baerbock-zitat-101.html
48. Riordan, A. (2023, kolovoz). ‘X’ To Remove Ability To Block Users. Channelnews. Preuzeto 27.8.2023 s https://www.channelnews.com.au/x-to-remove-ability-to-block-users/

49. Rosenblatt K. (2023, ožujak) Some of Twitter's top users aren't afraid of losing their blue check marks. NBC News. Preuzeto 30.4.2023 s https://www.nbcnews.com/tech/internet/twitter-blue-check-mark-cost-how-much-verified-rcna77432
50. Ruby, D. (2023, siječanj). YouTube Statistics (2023) – Trending Facts & Figures Shared! Demandsage. Preuzeto 1.2.2023 s https://www.demandsage.com/youtube-stats/
51. Ruby, D. (2022, prosinac). 71+ Essential Instagram Statistics for 2023 (Updated Dana & Trends). Demandsage. Preuzeto 1.2.2023 s https://www.demandsage.com/instagram-statistics/
52. Rukavina, Damir (2022, Ožujak) Stručnjaci: Katastrofalan kibernetički rat između Rusije i Ukrajine još nije počeo, ali... tportal. Preuzeo 30.4.2023 s https://www.tportal.hr/tehno/clanak/strucnjaci-katastrofican-kiberneticki-rat-izmedu-rusije-i-ukrajine-jos-nije-poceo-ali-foto-20220310
53. Schneier, B. (2015, listopad). The Rise of Political Doxing. Vice. Preuzeto 11.6.2023 s https://www.vice.com/en/article/z43bm8/the-rise-of-political-doxing
54. Senta, C. Bačić, L. Sigeti, V. Valić Nedeljković, D. Jovović, J. Zdravković, L. Valentič, U. (2021). Sprečavanje govora mržnje na internetu. Centar za mirovne studije. Preuzeto 6.6.2023 s https://www.cms.hr/system/publication/pdf/159/Sprecavanje_govora_mrznje__Priru_nik_za_nastavnike_HR.pdf
55. Sigurnost djece na Internetu. (2008) CARNet, CERT i LS&S; preuzeto 21.4.2023 s https://safetynet-kviz.skole.hr/Assets/Documents/sigurnost_djece_na_internetu.pdf
56. Silberling, A. i Stringer A. (2023, kolovoz) Elon Musk’s Twitter (now X): Everything you need to know, from layoffs to verification. Techcrunch. Preuzeto 27.8.2023 s https://techcrunch.com/2023/08/11/elon-musk-twitter-everything-you-need-to-know/
57. Simonds, W. (2022, kolovoz) Proven Strategies for Dealing with Online Blackmail
58. Singer, P. W. i Brooking, E. (2021). Rat lajkova. Zagreb: Fokus
59. Statista (2023). Number of monthly active Facebook users worldwide as of 4th quarter 2022. Preuzeto 15.1.2023 s https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
60. Što je digitalno nasilje i kako da ga zaustavimo? (2019). Preuzeto 15.1.2023 s https://www.unicef.org/serbia/zaustavimo-digitalno-nasilje

61. Što je Red Button aplikacija i kako se koristi (2018, Siječanj). Preuzeto 10.6.2023 s https://www.roda.hr/udruga/projekti/razmisli-pa-klikni/sto-je-red-button-aplikacija-i-kako-se-koristi.html
62. Topić Crnoja, M. i Palić, M. (2022) Politička propaganda i lažne vijesti: Trendovi na društvenim mrežama. Ekonomski fakultet u Zagrebu; International journal of multidisciplinarity in business and science, Vol. 8 No. 13, 2022. str. 36-41
63. Twitter developer Platform. Counting characters when composing Tweets https://developer.twitter.com/en/docs/counting-characters
64. The State of Online Harassment (2021, siječanj). Pew Research Center.
65. So schützen Sie sich effektiv vor Cyberstalkern. Kaspersky. Preuzeto 10.6.2023 s https://www.kaspersky.de/resource-center/threats/how-to-avoid-cyberstalking
66. Vojnik na Facebooku homoseksualce nazvao nakazama, sudac ga brutalno kaznio (2022, studeni). Danica. Preuzeto 10.6.2023 s https://danica.hr/vojnik-na-facebooku-homoseksualce-nazvao-nakazama-sudac-ga-brutalno-kaznio/
67. What is hate speech? United Nations. Preuzeto 10.6.2023 s https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech
68. What is Cyberviolence? Council of Europe. Preuzeto 10.6.2023 s https://www.coe.int/en/web/cyberviolence
69. Was ist Cyberstalking und wie können Sie es unterbinden? Avast Academy. Preuzeto 10.6.2023 s https://www.avast.com/de-de/c-cyberstalking
70. What is doxing – Definition and Explanation. Kaspersky. Preuzeto 6.6.2023 s https://www.kaspersky.com/resource-center/definitions/what-is-doxing
71. What is YouTube. GCF Global. Preuzeto 15.1.2023 s https://edu.gcfglobal.org/en/youtube/what-is-youtube/1/
72. Zaštitite se od investicijskih prijevara putem interneta (2022, rujan). HANFA. Preuzeto 3.2.2023 s https://www.hanfa.hr/vijesti/za%C5%A1titite-se-od-investicijskih-prijevara-putem-interneta/#
73. Zhang, S. i Leidner, D. „Workplace Cyberbullying: The Antecedents and Consequences" (2014). AMCIS 2014 Proceedings 18. preuzeto 21.4.2023 s https://aisel.aisnet.org/amcis2014/Posters/SocioTechnicalIssues/18

Digitalno nasilje

Sažetak

Razvoj informacijske i komunikacijske znanosti u obliku društvenog povezivanja putem foruma, elektroničke pošte, izravnih poruka i društvenih mreža donio nam je razne opasnosti. Suvremene pojave kao digitalno nasilje, i s time povezane opasnosti kao govor mržnje, vrijeđanje putem interneta, krađa podataka putem interneta, kibernetičko uhođenje, zlostavljanje putem slika, rodno usmjerena dezinformacija, ucjena, iskorištavanje putem slika i sadržaj koji prikazuje seksualno zlostavljanje djece za korisnike interneta predstavljaju veliki problem. Ti fenomeni su se proširili na sve grane interneta i nasilje se većinom provodi putem foruma, elektroničke pošte, izravnih poruka i društvenih mreža Također i cijele organizacije vrše digitalno nasilje među građanima u obliku kibernetičkog ratovanja, kibernetičkog kriminala i lažnih vijesti.

Posljedice digitalnog nasilja su za žrtvu često teške i dugotrajne. Posljedice mogu biti emocionalne, psihološke, fizičke, društvene prirode. A u najveću i najkritičniju posljedicu spada i suicid. Zbog toga se u školama i drugim obrazovnim ustanovama vode programi za prevenciju i suzbijanje digitalnog nasilja. Međutim se digitalno nasilje ne odnosi samo na djecu i adolescente. Odrasle osobe također mogu biti žrtva digitalnog nasilja. Zbog toga je potrebno uvijek pažljivo korištenje interneta, pogotovo u kontaktu sa nepoznatim osobama.

Ključne riječi: digitalno nasilje, štetan sadržaj, govor mržnje, krađa podataka, vrijeđanje putem interneta, izravne poruke, društvene mreže

Digital violence

Summary

The development of information and communication science in form of social networks like forums, e-mails, instant messaging, and social media has brought various risks for their users. Contemporary phenomena like digital violence, in which we classify hate speech, flaming, doxing, cyberstalking, image-based abuse, gender-based disinformation, extortion, exploitation and child abuse material represent a significant problem. These phenomena have spread across all branches of the internet and violence is mostly carried out through forums, instant messaging, and social media. Moreover, also organizations engage in digital violence in the form of cyberwarfare, cybercrime, and fake news.

The consequences of digital violence for the victim are often severe and long-lasting. The consequences can be of an emotional, psychological, physical, or social nature. The most severe and critical consequence can be suicide. Therefore, prevention and combating programs against digital violence are implemented in schools and other educational institutions. However, digital violence is not limited to children and adolescents. Adults can also be6+ victims of digital violence. So, it is necessary to always use the internet witch care, especially when interacting with unknown individuals.

Key words: digital violence, harmful content, hate speech, doxing, flaming, instant messages, social media