Univerzitet u Beogradu
Fakultet za specijalnu edukaciju i rehabilitaciju

ISTRAŽIVANJA U SPECIJALNOJ PEDAGOGIJI

BEOGRAD 2009.

UNIVERZITET U BEOGRADU -
FAKULTET ZA SPECIJALNU EDUKACIJU I REHABILITACIJU
UNIVERSITY OF BELGRADE -
FACULTY OF SPECIAL EDUCATION AND REHABILITATION

Istraživanja u specijalnoj pedagogiji

Research in Special Pedagogy

Priredio / Edited by
Prof. dr Dobrivoje Radovanović

Beograd / Belgrade
2009

EDICIJA:
RADOVI I MONOGRAFIJE

Izdavač:

Univerzitet u Beogradu - Fakultet za specijalnu edukaciju i rehabilitaciju

Istraživanja u specijalnoj pedagogiji

Za izdavača: Prof. dr Dobrivoje Radovanović, dekan

Urednik edicije: Prof. dr Zorica Matejić-Đuričić

Štampa:
„Planeta print“, Beograd

Tiraž:
150

Objavljivanje ove knjige je pomoglo Ministarstvo za nauku i tehnološki razvoj.

Nastavno-naučno veće Univerziteta u Beogradu - Fakulteta za specijalnu edukaciju i rehabilitaciju donelo je Odluku 3/9 od 8.3.2008. godine o pokretanju Edicije: Radovi i monografije.

Nastavno-naučno veće Fakulteta za specijalnu edukaciju i rehabilitaciju Univerziteta u Beogradu, na redovnoj sednici održanoj 14.4.2009. godine, Odlukom br. 3/54 od 23.4.2009. godine, usvojilo je recenzije rukopisa Tematskog zbornika "Istraživanja u specijalnoj pedagogiji"

ISBN 978-86-80113-83-8

EDITION:
ARTICLES AND MONOGPRAPHS

Publisher:
University of Belgrade - Faculty of Special Education and Rehabilitation

Research in Special Pedagogy

Printing:
„Planeta Print", Belgrade

Circulation:
150

Publication of this Book supported by Ministry of Science and Technology Development.

Scientific Council of the Belgrade University - Faculty of Special Education and Rehabilitation made a decision 3/9 from March, 8th 2008 of issuing Edition: Articles and Monographs.

Scientific Council, Faculty of Special Education and Rehabilitation University of Belgrade, at the regular meeting held on April, 14.th 2009 the Decision № 3/53 of April, 23th 2009, adopted a Thematic review manuscripts collection of "Research in Special Pedagogy "

ISBN 978-86-80113-83-8

INTERPERSONALNO NASILJE U SAJBER PROSTORU

Vesna Žunić-Pavlović, Marina Kovačević-Lepojević
Univerzitet u Beogradu - Fakultet za specijalnu edukaciju i rehabilitaciju,

Razvojem informaciono-komunikacionih tehnologija dolazi do prepoznavanja promena u domenu socijalnih interakcija, pri čemu "fizičko" i "realno" sve više ustupaju mesto "virtuelnom" kao vidu dematerjalizacije u ljudskim odnosima. Iako se na taj način umnogome doprinosi razvoju gotovo svih sfera društvenog života, počevši od obrazovanja, zaposlenja, politike, zabave, sa druge strane, virtuelna kultura otvara prostor za mnoge zloupotrebe. Sajber proganjanje se smatra zločinom koji za osnovu ima interpersonalno nasilje u sajber prostoru, i kao takvo predstavlja ozbiljnu pretnju modernog doba.

Rad ima za cilj da pruži određenje pojma sajber proganjanja i njegovog odnosa sa srodnim pojmovima, prikaže istraživanja koja ukazuju na rasprostranjenost i karakteristike sajber proganjanja, žrtava, učinilaca, odredi vrste sajber proganjanja i tipologiju učinilaca, kao i da da pregled mera koje se preduzimaju u cilju prevencije.

Ključne reči: on-lajn uznemiravanje, sajber proganjanje, kriminlitet, internet

UVOD

Internet kao prvi medij koji podrazumeva interaktivnost u komunikaciji, za mnoge korisnike pruža novi svet otvorene komunikacije, svet koji je umnogome rasterećen moralnih dilema kulturnog nasleđa civilizovanog sveta. Metode savremene komunikacije bacaju sasvim novo svetlo na socijalne interakcije, uz učestalost socijalnih kontakata i čitavih sistema dostupnih usluga i službi. Obrazovanje, zaposlenje, rad, odmor, politika, kultura, zabava egzistiraju u sajber prostoru, prostoru globalnih komunikacionih mreža. Savremeni trend je da realna, fizička komunikacija sve više preti da mesto ustupi virtuelnoj, sajber komunikaciji.

Prema poslednjim istraživanjima, od ukupno 6710029070 stanovnika na planeti 1596270108, odnosno 23,8% koristi internet. Poređenja radi 2000. godine internet je koristilo 360985492 (Internet World Stats, 2009). Podaci potkrepljuju činjenicu da ljudi sve češće obitavaju u različitim vrstama virtuelnih zajednica, što povećava rizik od mogućih zloupotreba. Neki autori smatraju da internet po prirodi stvari promoviše sajber (cyber) proganjanje, podražava lažni osećaj bliskosti, otvara mogućnost za nesporazume po pitanju namera učesnika u komunikaciji (Finn, 2004: 470). Isto tako, relativna anonimnost, brisanje socijalnih razlika i različite devijantne sklonosti mogu da proizvedu rizik za sajber proganjanje.

Teoretičarka kulture Zorica Tomić ukazuje na brojna pitanja o posledicama masovne upotrebe interneta po samu strukturu društvenog, otvarajući teme socijalnog raslojavanja, problem društvenih, etničkih i ekonomskih razlika, izmena u fizionomiji kulture, novoj pismenosti, problemima identiteta, restrukturiranju čitavog kategorijalnog aparata društvene teorije (Tomić, 2004). "Moralni paničari" savremenog doba posebnu pažnju poklanjaju proučanju ovog fenomena i mogućem uticaju pretnji, ucena, povreda privatnosti, časti i ugleda, seksualnog uznemiravanja na psihičko i fizičko zdravlje ljudi.

U domaćoj naučnoj i stručnoj javnosti, fenomen sajber nasilja još uvek nije dobio zasluženu pažnju. Razlog za to verovatno treba tražiti u činjenici da relativno mali broj naših građana koristi računare, kao i da ne postoje razvijeni sistemi sprečavanja i suzbijanja ove negativne pojave. Međutim, opravdano je pretpostaviti da će sajber nasilje kod nas pratiti trendove zapažene u drugim zemljama. Sagledavanje savremenih svetskih dostignuća nauke i istraživanja u ovoj oblasti predstavlja dobru polaznu osnovu za sprovođenje sličnih istraživanja u Srbiji, ali i planiranje uspešnih načina zaštite od sajber nasilja.

Predmet rada je specifičan vid sajber nasilja – sajber proganjanje, odnosno uznemiravanje putem informaciono-komunikacionih tehnologija. Posebna pažnja biće posvećena definisanju osnovnih pojmova i terminološkim razgraničenjima, razmatranju pojavnih oblika, analizi rezultata istraživanja o rasprostranjenosti i karakteristikama, kao i sagledavanju društvene reakcije na sajber proganjanje.

RAZGRANIČENJE OSNOVNIH POJMOVA
(sajber kriminal, on-lajn uznemiravanje, proganjanje, sajber proganjanje)

Termin sajber prostor (*cyber space*), po prvi put se sreće kod Williama Gibsona u naučno-fantastičnoj noveli *Neuromanser* (1984) i upotrebljen je da prikaže nematerijalni prostor nezamislive kompleksnosti u kome računarski podaci putuju kao delići svetlosti (Wikipedia, 2009).

Danas se pod sajber prostorom podrazumeva vrsta „zajednice" sačinjene od mreže kompjutera, u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova, ili prostor koji kreiraju kompjuterske mreže, odnosno globalna informaciona infrastruktura kroz koju se vrši masovna komunikacija i u kojoj istovremeno koegzistiraju virtuelno i realno (Drakulić, Drakulić, 2009). Prema tome, dva ili više informaciono-komunikaciona uređaja, koja su povezana žičnim ili bežičnim spojem čine delić sajber prostora. Internet, kao globalna svetska mreža daje sajber prostoru globalnu dimenziju, odnosno omogućava vezu između bilo koje dve tačke na planeti kroz sajber prostor. Sajber prostor je istovremeno i socijalni prostor koji nastaje spajanjem dva vida komunikacije, i to: komunikacije posredstvom računarskih mreža (Computer Mediated Communication - CMC) i poslovne komunikacije podržane računarskim sistemima (Computer Supported Collaborative Work – CSCW) (Riva, Galimberti, 1997: 142).

Prema Konvenciji Saveta Evrope o sajber kriminalu, pod pojmom sajber kriminal podrazumeva se „svaka aktivnost usmerena protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka, kompjuterskih sistema i kompjuterskih mreža, kao i zloupotreba kompjuterskih podataka, sistema i mreža" (CoE, 2001). U skladu sa tim, sajber kriminal podrazumeva raznovrsne kriminalne aktivnosti

uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu.

Sajber zloupotrebe mogu se odnositi na: interpersonalne relacije, dela protiv svojine i dela protiv javnog reda i mira (TRANSCRIME, 2002, prema Savona, 2004: 14). Prema tome, sajber proganjanje spada u domen zloupotreba na interpersonalnom nivou.

U Konvenciji o sajber kriminalu data je tipologija sajber kriminala u odnosu na kriterijum povrede sajber prostora, i to su:

- dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema (nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme),
- zloupotreba uređaja, programa i šifara (neovlašćena proizvodnja, prodaja, uvoz i distribucija),
- dela vezana za kompjutere (falsifikovanje i krađa kompjuterskih podataka),
- dela vezana za sadržaje (pornografija i dečija pornografija, pri čemu se vrši posedovanje, distribucija, transmisija, čuvanje ili činjenje dostupnim i raspoloživim pornografskih materijala, njihova proizvodnja radi distribucije i obrade u kompjuterskom sistemu) i
- dela vezana za kršenje autorskih i srodnih prava (neautorizovano reprodukovanje i distribucija što se direktno nadovezuje na mogućnost zaštite autorskih prava i intelektualne svojine).

Kako pojedini autori ukazuju (Randy Mc Call, 2004: 3), ne postoji jedinstvena definicija on-lajn (*on-line*) uznemiravanja i sajber proganjanja, pa ni jasna razlika, jer se radi o srodnim pojmovima koji se naizmenično prepliću. Zapravo, može se reći da sajber proganjanje sadrži on-lajn uznemiravanje. Postupci koje karakterišemo kao on-lajn uznemiravanje prerastaju u sajber proganjanje kada se neželjena komunikacija ponavlja, bilo da je ona direktna ili pak indirektna, i kada se vrši u određenom vremenskom periodu, putem jednog ili više sredstava internet ili neke druge vrste elektronske komunikacije. Element izazivanja razumnog straha kod žrtve je takođe neophodan za kvalifikaciju sajber proganjanja (Randy Mc Call, 2004: 3). On-lajn uznemiravanje može biti direktno ili indirektno. Direktno uključuje pretnje, zastrašujuće poruke upućene žrtvi putem e-maila ili nekim drugim vidom internet komunikacije, slanje zaraženih poruka *(junk mail, spamming)* ili kompjuterskih virusa, hakovanje tragova koje žrtva ostavlja putem interneta ili onemogućavanje određene usluge putem napada koji se ostvaruje slanjem velikog broja zahteva sistemu na željenoj adresi, što za posledicu ima blokadu (*DoSa – Denial of services attacks*). Indirektno on-lajn uznemiravanje uključuje, ali nije ograničeno samo na širenje glasina o žrtvi na različitim internet forumima, potpisivanje žrtve na neželjene on-lajn servise, ostavljanje informacija o žrtvi na sajtovima za on-lajn zabavljanje, seksualne usluge ili slanje poruka drugima u žrtvino ime (Ellison, Akdeniz, 1998: 31).

Radi adekvatnog razumevanja pojma sajber proganjanja potrebno je dati određenje proganjanja i tumačenje sličnosti i razlika u odnosu na konvencionalno proganjanje. Uže gledano, proganjanje se smatra „vidom interpersonalnog nasilja i podrazumeva način ponašanja koji uključuje dva ili više incidenta uznemiravanja, koji izazivaju strah, uzbunu ili poremećenost i to putem tri načina: putem telefonskih poziva ili pisama, čekanja ispred kuće ili posla i uništavanja žrtvine

imovine" (Walby, Allen, 2004: 4). Šire i potpunije određenje proganjanja uključuje dve ili više radnji kojima progonitelj direktno, indirektno ili na neki treći način, putem neke akcije, metoda, uređaja ili sredstva, prati, nadzire, posmatra, preti osobi, komunicira sa osobom ili dolazi u kontakt sa svojinom dotične osobe (National Center for Victims of Crime, 2007). Ovakvo određenje uključuje i virtuelno, sajber uznemiravanje, odnosno uznemiravanje putem računara i drugih elektronskih uređaja, koja ne zahtevaju vizuelnu ili fizičku bliskost. Takođe, posledice proganjanja na žrtvu su definisane i obuhvataju ne samo strah za život i telo, sopstveni ili bliske osobe, već i emocionalnu patnju.

Pojedini autori prihvataju šire određenje proganjanja, pa sajber proganjanje smatraju vidom konvencionalnog proganjanja, uznemiravanja u nekonvencionalnom, sajber prostoru koje se vrši posredstvom informaciono-komunikacionih tehnologija (Ogilvie, 2000, D'Ovidio, Doyle, 2003, Finn, 2004, Baum, Catalano, Rand, Rose, 2009). U tom slučaju govorimo o sajber proganjanju koje predstavlja „kontinuiranu upotrebu interneta, i-mejla (e-mail) ili drugih vidova elektronske komunikacije radi uznemiravanja određenog pojedinca ili grupe pojedinaca" (D'Ovidio, Doyle, 2003: 10).

Sa druge strane, neki autori (npr. Bocij, McFarlane, 2002, Southworth, Dawson, Fraser, Tucker, 2005) smaraju da sajber proganjanje treba posmatrati kao nezavistan, izolovan problem, koji ne mora biti uži od pojma proganjanja. Sajber proganjanje ne isključuje i druge uobičajene metode uznemiravanja koje podrazumevaju fizičku bliskost. Informaciono-komunikacione tehnologije ne treba ograničiti samo na upotrebu računara i interneta. Tu treba uključiti i komunikaciju telefonskim uređajima, elektronski nadzor i druge tehnologije za praćenje i nadgledanje. Iako se u literaturi polemike najčešće vode oko toga koji postupci proganjanja pripadaju sajber, a koji konvencionalnom proganjanju, ono što je nesumnjivo zajedničko za ova dva oblika proganjanja je kontinuiranost u postupcima uznemiravanja i izazivanje straha kod žrtve.

Jedna od najšire prihvaćenih definicija sajber proganjanje određuje kao „skup postupaka kojima pojedinac, grupa ili organizacija koristeći informacione i komunikacione tehnologije uznemirava jednu osobu ili više pojedinaca. Takva ponašanja mogu da uključe pretnje i lažne optužbe, krađu identiteta, krađu podataka, uništavanje podataka ili opreme, elektronsko praćenje i nadgledanje, namamljivanje maloletnika u svrhe seksualne eksploatacije i drugo. Kao uznemiravajući definisani su oni postupci koji bi i kod druge osobe u sličnoj situaciji izazvali razuman strah" (Bocilj, McFarlane, 2002: 12).

Namera autora bila je da se ovako obuhvatnim određenjem sajber proganjanja odredi odnos između sajber i konvencionalnog proganjanja. Sudeći po ovakvom definisanju sajber proganjanje nije ograničeno samo na on-lajn uznemiravanje od strane pojedinca, već ukuljučuje i uznemiravanje od strane skupine pojedinaca ili organizacija. Ponašanja koja su definicijom data treba shvatiti uslovno, jer, na primer, „pretnja" može imati različite oblike, a „uništavanje podataka i opreme" može da uključi postupke od vandalizma do prenošenja virusa. Prema ovoj definiciji nije isključena mogućnost fizičkog i seksualnog nasilja nad žrtvama.

Sajber proganjanje, kao kontinuirano on-lajn uznemiravanje može se vršiti na dva nivoa: interpersonalnom - između dva ili više pojedinaca i na korporacijskom - između pojedinaca i institucije ili organizacije. On-lajn uznemiravanje

na nivou pojedinac – institucija ili organizacija može se vršiti u oba smera, od institucije ili organizacije prema pojedincu i od pojedinca prema instituciji ili organizaciji. Motivi za ovakvu vrstu proganjanja mogu biti najrazličitije prirode i to su: osveta, pobeda u nekoj ličnoj igri, kompeticija, sticanje profita, pri čemu organizacija ili institucija ne mora biti upućena u on-lajn uznemiravanje koje zaposleni vrši u ime firme (Bocilj, 2002: 11).

Na osnovu analize postojećih pojmovnih određenja, može se konstatovati da sajber proganjanje za osnovu ima interpersonalno nasilje u virtuelnom prostoru. S obzirom na to da je ovde reč o fenomenu progranjanja upotrebom savremenih sredstava komunikacije, pod sajber proganjanjem podrazumevaće se kontinuirana upotreba informaciono-komunikacionih tehnologija radi uznemiravanja pojedinaca.

OBLICI SAJBER PROGANJANJA

Premda se veliki broj postupaka sajber proganjanja odvija posredstvom računara i interneta, kao najvećeg medija informaciono-komunikacionih tehnologija, nije opravdano zanemariti telefonske mreže i različite tehnologije za praćenje i nadgledanje. U skladu sa širim određenjem sajber proganjanja, posebna pažnja biće posvećena sledećim pojavnim oblicima: sajber proganjanje posredstvom telefonskih tehnologija, sajber proganjanje posredstvom tehnologija za praćenje i nadgledanje žrtve i sajber proganjanje posredstvom računarskih mreža i interneta (adaptirano prema Southworth, Dawson, Fraser, Tucker, 2005: 5-8).

Sajber proganjanje posredstvom telefonskih tehnologija

Kao sredstvo uznemiravanja putem telefonskih tehnologija u upotrebi su pripejd (*prepaid*) kartice za telefoniranje ili pripejd mobilni telefoni, jer je učiniocima tako najteže ući u trag, posebno ako nisu kupljeni pomoću platne kartice. Telefoni koji imaju identifikaciju broja sa kog se poziva ili čak adresu, takođe mogu poslužiti kao pomoćno sredstvo proganjanja. Faks mašine mogu da pokažu identifikaciju broja sa kog je dokument poslat, kao u slučaju žene žrtve proganjanja od strane partnera koja je iz skloništa za žrtve faksirala document svom advokatu koji je prosledio muževljevom advokatu uz pomoć čega je muž uspeo da locira sklonište (Safety Net, 2004). Teleprinteri (TTY) i telekomunikacioni uređaji za osobe sa oštećenjem sluha (TTD), takođe, mogu poslužiti kao sredstvo uznemiravanja.

Sajber proganjanje posredstvom tehnologija za praćenje i nadgledanje žrtve

Progonitelji mogu koristiti sofisticiranu tehnologiju za praćenje i nadgledanje i to: preko sistema za globalno pozicioniranje (GPS) putem koga pozicioniraju žrtvu u realnom vremenu prateći njene dnevne aktivnosti ili preko skrivenih kamera. Sistemi za globalno pozicioniranje koriste satelitske predajnike i na taj način omogućavaju učiniocu da u realnom vremenu locira i prati svoju žrtvu. GPS uređaji variraju prema veličini, ceni, dostupnosti. Mogu biti u malim crnim kutijama ili pak u obliku čipa. Skrivene kamere progoniteljima pružaju mogućnost

da spoznaju žrtvine rutinske aktivnosti i na taj način pomognu u održavanju moći i kontrole nad žrtvom. Male, bežične kamere sa visokom rezolucijom mogu biti smeštene u detektore za dim, lampe, male rupice u zidu, a mogu biti aktivirani sa udaljene tačke.

Sajber proganjanje posredstvom računarskih mreža i interneta

Ovaj vid progranjanja može se ostvariti posredstvom softvera, hardvera, elektronskih poruka, krađe digitalnog identiteta, internet sajtova i baza podataka.

Softveri za praćenje računara (*SpyWare*) isprva su osmišljeni za praćenje aktivnosti dece na internetu, ali je kasnije počela njihova zloupotreba. Ovakav softver može biti instaliran sa distance ili putem fizičkog pristupa žrtvinom računaru. Neki softveri (npr. *Evidence-Eliminator.com*) se reklamiraju kao sredstvo za brisanje tragova ili eliminisanje dokaza o neovlašćenom korišćenju ili krađi tuđih podataka (Wykes, 2007: 171). Većina programa za detekciju softvera za praćenje računara nije dala dobre rezultate.

Osim upotrebe softvera, progonitelji mogu da koriste i hardverske uređaje (tzv. *Keystroke Loggers*) koji se instaliraju pored kabla od tastature na žrtvinom računaru. Uz pomoć takvog uređaja snima se svaki otkucani karakter uz kompletne šifre, PIN-ove, elektronske poruke, sajtove koje žrtva posećuje i drugo. Poput softvera za praćenje, u reklamiranju hardverskih uređaja ističe se da predstavljaju jednostavno rešenje za špijuniranje vlastite supruge i slične aktivnosti.

Komuniciranje putem i-mejl (*e-mail*) poruka podrazumeva mogućnost da se drugoj osobi prenese slika, tekst, video ili audio materijal. Pri upotrebi i-mejl poruka radi uznemiravanja, sajber progonitelj kreira i šalje žrtvi tekstualne, grafičke, video ili audio poruke preteće, zastrašujuće ili na neki drugi način za žrtvu uznemiravajuće sadržine (D'Ovidio, Doyle, 2003: 16). I-mejl poruke mogu biti upućene žrtvi u cilju započinjanja ili obnove ljubavne veze ili radi pretnje (Ogilvie, 2000: 2). Osim u svrhu pretnje i drugih vidova uznemiravanja, upućivanjem i-mejl poruka mogu se slati zaraženi fajlovi (*junk mail*) ili softveri za praćenje računara (*SpyWare*). Instant poruke podrazumevaju interakciju (tekstualnu, video ili audio) između dve osobe u realnom vremenu, pri čemu je komunikacija moguća samo dok su obe osobe konektovane na internetu.

Pod krađom digitalnog identiteta žrtve podrazumeva se neovlašćeno korišćenje žrtvine i-mejl adrese radi prijavljivanja za korišćenje različitih servisa i usluga u njeno ime; slanje pogrešnih informacija ili lažnih poruka na sajtove za grupnu interakciju (*chat room, usenet*), slanje demografskih informacija ili slika seksualno orjentisanim ili pornografskim sajtovima ili pak upućivanje poruka žrtvinom poslodavcu/instituciji u kojoj je zaposlena (Finn, 2004: 469).

Učinilac može postaviti sajt koji je preteći po žrtvu ili koji ohrabruje druge da kontaktiraju, uznemiravaju i na drugi način povređuju žrtvu. To mogu biti sajtovi koji omogućavaju grupnu tekstualnu, video ili audio interakciju (*chat room*) u realnom vremenu koja je obično organizovana oko specifičnih tema vezanih za politiku, religiju, zabavljanje i drugo. Ovi sajtovi mogu biti javni, odnosno dostupni svim korisnicima ili privatni sa ograničenim pristupom. Učinilac u cilju uznemiravanja žrtve može slati poruke uznemiravajuće sadržine vidljive svim korisnicima sajta, a može i otkriti žrtvine lične podatke ostalim učesnici-

ma i time podstaći druge na uznemiravanja putem interneta, telefona ili slično (D'Ovidio, Doyle, 2003: 16).

Putem on-lajn baza podataka i on-lajn agencija koje trguju podacima učinioci mogu pronaći privatne informacije o žrtvama. Neretko, dostupna im je sudska dokumentacija i statistika, kao što su baze osuđenih lica ili prikazi pojedinih slučajeva. Primera radi, u okrugu Mongomeri u Pensilvaniji sud je čak objavio imena i adrese žrtava i njihove dece, kojima su izrečene zaštitne mere (Webster, 2003, prema Southworth, Dawson, Fraser, Tucker, 2005).

Napadi poput socijalnog projektovanja (*social engineering*) i DoSa (*denial of services*) retko se koriste kod uznemiravanja pojedinca, već su karakteristični pretežno za napade na sisteme različitih institucija ili organizacija. Socijalno projektovanje podrazumeva infiltriranje u organizaciju koja predstavlja metu napada, pri čemu se putem intervjuisanja zaposlenih ili drugim metodama dolazi do osetljivih podataka. Napadi pod oznakom DoS se često koriste kao sredstvo sajber ratovanja, jer omogućavaju napade na sisteme državnih uprava od strane „neprijateljskih" država (Fenz, 2005: 6-8)

RASPROSTRANJENOST I KARAKTERISTIKE SAJBER PROGANJANJA

Na osnovu pregleda savremene literature, primećuje se da su istraživanja koja se bave isključivo sajber proganjanjem retka, da pružaju oskudne podatke o pojavi i oblicima sajber proganjanja, o žrtvama, učiniocima i društvenoj reakciji. S druge strane, određeni podaci o sajber proganjanju mogu se naći u istraživanjima konvencionalnog proganjanja. Postoje izvesne teškoće u poređenju i sumiranju podataka iz različitih studija, jer ne postoji jasna i univerzalno prihvaćena definicija sajber proganjanja, niti jasni kriterijumi na osnovu kojih se ono identifikuje. Poseban problem predstavljaju neka metodološka ograničenja u istraživanju ovog fenomena.

U narednom delu biće prikazani rezultati nekoliko najpopularnijih savremenih studija o sajber proganjanju.

Nacionalno istraživanje o proganjanju u SAD u 2006. godini identifikovalo je 3424100 žrtava proganjanja, od kojih je 677870 osoba, odnosno gotovo svaka četvrta osoba (26%) bila izložena sajber proganjanju (Baum, Catalano, Rand, Rose, 2009). U 83% žrtve su trpele on-lajn uznemiravanje putem i-mejl poruka, u 35% putem instant poruka, blogova i oglašivača u 12%, a putem veb sajtova u 9%. Jedna od 13 identifikovanih žrtava proganjanja bila je elektronski praćena. U gotovo podjednakom broju slučajeva žrtve su praćene putem video ili digitalnih kamera (46%) i putem uređaja za prisluškivanje (42%). Sistem za globalno pozicioniranje kao sredstvo praćenja upotrebljen je u nekoliko slučajeva. Zapaža se da autori istraživanja pod pojmom sajber proganjanja nisu podrazumevali i elektronsko praćenje. Pored toga, podaci o oblicima sajber proganjanja su vrlo oskudni i nema informacija o karakteristikama žrtava i učinilaca, njihovom međusobnom odnosu i drugo.

Studija o sajber proganjanju u Velikoj Britaniji pokazala je da su žrtve najčešće bile uznemiravane putem i-mejla i to u 79%, preko instant poruka u 13%, putem soba za čet (*chat room*) u 8%, dok su interaktivni sajtovi (*message board* i *guest book*) i veb sajtovi bili korišćeni u 4 i 2% slučajeva. Progonitelji su najmanje kori-

stili *newsgroup-e* i lažne korisničke profile i to u oko 1% slučajeva. U 92% slučajeva žrtve su uznemiravane jednom metodom proganjanja. Sajber proganjanje je u 56 mesečnom periodu praćenja (1996-2000) policijskih slučajeva koji su imali veze sa upotrebom računara i interneta u kriminalne svrhe, činilo 42% od ukupnog broja slučajeva. U 80% učinioci su bili muškarci, prosečnog uzrasta od 24 godine, s tim što je najstariji prestupnik imao 53, a najmlađi 10 godina. U 26% slučajeva počinitelji su bili mlađi od 16 godina. Od ukupno 201 registrovanih slučajeva 192 je rešeno za vreme sprovođenja studije. Žrtve su u 87% bile fizička lica, i to 52% bile ženskog pola, a u 35% slučajeva muškog pola, dok su u 13% žrtve bile pravna lica, i to obrazovne ustanove u 8%, a privatne firme u 5%. Žrtve su u proseku bile 32 godine stare, sa najstarijom žrtvom od 62 godine, a najmlađom od 10 godina (D'Ovidio, Doyle, 2003: 13).

Na osnovu istraživanja koje je za predmet imalo ispitivanje karakteristika sajber progonitelja i pravljenje tipologije, na osnovu 24 slučaja došlo se do podataka o karakteristikama žrtava i učinilaca i njihovom međusobnom odnosu, postupcima sajber proganjanja i dugo (McFarlane, Bocilj, 2004: 6-8). U 91% žrtve su bile ženskog pola, dok je 85% učinilaca bilo muškog pola. Žrtve su prosečno bile uzrasta 32 godine, pri čemu je najmlađa žrtva imala 14 godina, a najstarija 53. Učinioci su u proseku imali 41 godinu, pri čemu je najmlađi imao 18, a najstariji 67 godina. Sajber proganjanje je u zavisnosti od slučaja do slučaja trajalo od 17 dana do 5 godina, prosečno 11,5 meseci. U najvećem broju, odnosno u 10 slučajeva žrtve su uznemiravane putem i-mejl poruka. U ostalim slučajevima uznemiravanje je vršeno putem *usenet* grupa i oglašivača, veb sajtova za upoznavanje osoba za čet, poslovnih mreža i drugo. U 13 slučajeva on-lajn uznemiravanje je bilo praćeno oflajn (*offline*) uznemiravanjem. U više od polovine slučajeva progonitelji su pretili žrtvama ili njihovoj porodici i prijateljima. U najvećem broju slučajeva ni žrtve ni učinioci nisu bili u braku ili vezi. Istraživanje je pokazalo da je 12 od ukupno 24 učinilaca imalo istioriju sajber proganjanja od kojih je tri četvrtine bilo procesuirano. Žrtve su učinioce u trećini slučajeva upoznale putem informaciono-komunikacionih tehnologija. U 22% radilo se o potpunim strancima, a u po 12% o bivšim partnerima i kolegama. U tri četvrtine slučajeva radi se o muško-ženskom sajber proganjanju, a u preostalim slučajevima o žensko-ženskom ili muško-muškom sajber proganjanju.

Istraživanje koje je rađeno 2002. godine na univerzitetu Nju Hempšir imalo je za cilj dolaženje do podataka o učestalosti sajber proganjanja kod studenata, o karakteristikama sajber progranjanja i progonitelja. Istraživanje je rađeno na uzorku od 339 studenata, u 65% ženskog pola, prosečnog uzrasta 20 godina, koji su u 97% komunicirali mejlovima jednom ili više puta nedeljno, a u 81% instant porukama. Njih 7% (23), odnosno svaki deseti student je imao loše iskustvo u komunikaciji i-mejlovima ili putem instant poruka. Studenti su najčešće bili uznemiravani od strane nepoznatih osoba, u 16% putem i-mejlova, u 19,3% putem instant poruka. U 14% uznemiravanje i-mejlovima prestaje nakon upozorenja od strane žrtve, kao i u 13% uznemiravanje putem instant poruka. U najvećem broju slučajeva, odnosno u 59% studenti su prijavili slanje neželjenih pornografskih materijala kao vid uznemiravanja. Istraživanje je pokazalo da su GLBT (Gay-Lesbian-Bisexual-Transexual) studenti u većem broju slučajeva prijavljivali on-line uznemiravanje u odnosu na heteroseksualne studente (Fin, 2004: 474-480).

Na osnovu i-mejl istraživanja sprovedenog na uzorku od 169 ispitanika iz Velike Britanije, SAD i Kanade došlo se do podataka o rasprostranjenosti sajber proganjanja i posledicama koje ono ostavlja na žrtve (Bocilj, 2003). Od ukupnog broja učesnika, 82% svakodnevno koristi internet, a 14% barem jednom nedeljno. Učesnici su u 58% prošli neku vrstu obuke za rad na računaru, u istom procentu imali svoj veb sajt ili veb stranu, pri čemu 60% učesnika koristi softver koji gradi „zaštitni zid" oko računara i sprečava upad malicioznih softvera (*firewall*). Od ukupnog uzorka jedna trećina se izjasnila da je trpela sajber proganjanje, pri čemu je od tog broja 26% sajber proganjanje trpelo za vreme popunjavanja upitnika. Oko četvrtine žrtava je prijavilo da je istovremeno trpelo šest i više različitih oblika sajber proganjanja, dok je 17% bilo žrtva samo jednog oblika. Najzastupljeniji oblici sajber uznemiravanja bili su: on-lajn uznemiravanje putem sajtova za grupnu interakciju (*chat room*) (47%), uznemiravanje putem i-mejl poruka (40%), slanje malicioznih programa (40%) i upotreba softvera za komuniciranje putem instant poruka (39%). Otkrivena je manja zastupljenost uznemiravanja putem postavljanja „Trojanskog konja" - programa za infiltriranje i nadgledanje tuđeg računarskog sistema (27%), putem širenja negativnih komentara i glasina o žrtvama (24%), putem ohrabrivanja drugih da uznemiravaju žrtvu (23%), dok je 9% ispitanika bilo žrtva krađe identiteta. U najvećem broju slučajeva, odnosno u 65%, žrtve su bile ženskog pola, prosečne starosti oko 30 godina. Četvrtina uzorka je na pitanje o emotivnoj patnji koja im je naneta postupcima sajber proganjanja na skali od 1 do 10, odgovorila sa 10. Žrtve u 42% nisu znale identitet progonitelja, u 16% to su bili prijatelji, 9% bivši partneri, 2% kolege i drugo. U 33% žrtve su prijavljivali proganjanje organizacijama koje se bave očuvanjem bezbednosti na internetu (npr. *CyberAngels*), dok je 14% prijavilo napad policiji.

Rezultati istraživanja sajber proganjanja predstavljaju osnovu za uspešno sprečavanje i suzbijanje ove negativne pojave. U tom smislu, poseban značaj ima unapređivanje saznanja o karakteristikama učinilaca.

TIPOLOGIJA SAJBER PROGONITELJA

Na osnovu sprovedenog istraživanja koje je imalo za cilj izvođenje tipologije učinilaca, uzimajući kao kriterijum vezu između žrtava i učinilaca mogu se razlikovati četiri tipa sajber progonitelja, i to su: osvetnički, strpljiv, romantični i sajber progonitelj koji deluje u grupi (McFarlane, Bocilj, 2004: 8-10).

Osvetnički tip

Naziv „osvetnički" proizlazi iz motivacije za proganjanjem, pa u skladu sa tim pripadnici ovog tipa u odnosu na ostale najčešće prete i zastrašuju žrtve, pri čemu se u većini slučajeva proganjanje odvija i van virtuelne stvarnosti (*offline*). Trećina progonitelja iz ove grupe ima kriminalni dosije, dok je za druge dve trećine utvrđeno da su bili u poziciji zlostavljača i ranije. Osvetnički tip sajber progonitelja ima srednji ili viši nivo obuke za rad na računaru. „Osvetnici" koriste naširi opseg informaciono-komunikacionih metoda u svrhu uznemiravanja žrtve (*spamming*, *mailbombing*, ugrožavanje identiteta žrtve). Prema podacima istraživanja, oni su bili jedina grupa progonitelja koja je koristila tzv. „Trojanskog konja" u cilju neovlašćenog pristupa žrtvinom računaru i/ili prenošenja virusa. Prema

rečima žrtava, od ove grupe progonitelja često su dobijale bizarne, nepovezane poruke i komenatare, preteće multimedijalne poruke (slika/zvuk), kao na primer mrtvačke glave, fotografije leševa, vrisak i slično. Navedeni postupci mogu biti indikativni za mentalne poremećaje.

Strpljiv tip

Naziv „strpljiv" odražava cilj i metode proganjanja. Postupci učinilaca ovog tipa usmereni su ka konstantnom dosađivanju i iritiranju žrtava. Ovaj tip sajber progonitelja ne želi da ostvari emotivnu vezu sa žrtvom, ali želi da je duboko uznemiri. U odnosu na ostale tipove, "strpljiv" progonitelj pretežno upućuje pretnje žrtvama. "Strpljiv" sajber progonitelj najčešće ima srednji ili viši nivo obuke za rad na računaru. Prema rezultatima istraživanja, progonitelji iz ove grupe retko kada imaju kriminalni dosije i predistoriju ranijeg zlostavljanja. Ovaj tip nije indikativan za psihijatrijsku dijagnozu.

Romantičan tip

Pipadnici ove grupe bore se za osećanja, naklonost, pažnju svoje mete. Kako žrtve procenjuju, nivo obučenosti za rad na računaru kod ovog tipa učinilaca varira od veoma slabog do izuzetno visokog nivoa znanja. Od postupaka proganjanja koriste se: i-mejlovi, veb grupe za diskusiju, sajtovi za upoznavanje i drugo. Sajber progonitelji romantičnog tipa imaju uvid u detalje iz žrtvinog života. U okviru ovog tipa, razlikujemo dva podtipa. Prvo, to su bivši partneri ili bivši poznanici – prijatelji žrtve i, drugo, osobe koje su žrtvi nepoznate, a koje žele da ostvare intimnu vezu sa njom. Postupci proganjanja od strane bivših partnera ili prijatelja kreću se od jednostavnih poruka koje imaju za cilj obnovu veze do surovih pretnji žrtvama i njima dragim osobama. Prema rečima žrtava, uznemiravanje od strane bivših partnera je započinjalo i završavalo se u virtuelnom svetu. Oni koji su težili započinjanju romantične veze sa žrtvom, podizali su nivo pretnje i zastrašivanja nakon što bi shvatili da su odbijeni. Prema rezultatima istraživanja, ova podgrupa može da uključi i postupke konvencionalnog proganjanja. Prema tipologiji proganjanja koju daje Mullen, sajber progonitelj koji je bio u prethodnoj vezi sa žrtvom podseća na "odbačenog" progonitelja, koji ne može da prihvati završetak veze, dok njegovo ponašanje predstavlja mešavinu želje za pomirenjem i želje za osvetom. Isto tako, postoji sličnost između sajber progonitelja koji teže da ostvare intimnu vezu sa žrtvom i "romantičnog" progonitelja ili "nesposobnog udvarača" (npr. intelektualna ili socijalna ometenost) kod konvencionalnog proganjanja u tipologiji progonitelja datih prema Mullen-u (Mullen i dr., 1999: 1247).

Tip koji deluje u grupi

Za ovaj tip sajber progonitelja karakteristično je da deluje u grupi (dva ili više progonitelja). Obučenost za rad na računaru kod ovog tipa varira od slabog do veoma visokog nivoa. Karakteristični postupci proganjanja su: pretnje (multimedijalne i druge poruke), slanje opasnih poruka (*spamming, mailbombing*) i pretnje identitetu žrtve. Za ovu grupu nije specifičnio da on-lajn uznemiravanje bude praćeno proganjanjem izvan virtuelnog sveta, ali su poznati slučajevi ohrabrivanja drugih da uznemiravanje žrtve na ovakav način. U ovkviru ovog tipa treba

razlikovati učinioce takozvanog korporacijskog proganjanja, pri čemu institucija/organizacija preuzima odgovornost za proganjanje (Bocilj, 2002).

DRUŠTVENA REAKCIJA NA SAJBER PROGANJANJE

Zakonodavstvo

Premda se sajber proganjanje sve više prepoznaje kao specifičan i nezavistan problem, i dalje ne postoji posebna legislativa u cilju regulisanja ove pojave. Kao posledica toga, sajber proganjanje najčešće ulazi u zakonsku definiciju konvencionalnog proganjanja.

Prvi zakon protiv proganjanja (California Penal Code, 1990) donet je u Kaliforniji 1990. godine kao reakcija na ubistvo glumice Rebeke Šefer koje je bilo posledica proganjanja. Ovo ubistvo je usledilo nakon ubistava četiri žene u Kaliforniji koja su, takođe, bila povezana sa proganjanjem. Do kraja devedesetih godina i ostale američke države izgradile su svoja zakonodavstva protiv proganjanja, a 1996. godine donet je zakon o proganjanju na federalnom nivou.

Al Gore je u Americi krajem devedesetih godina prvi skrenuo pažnju na opasnost od sajber proganjanja, na čiji zahtev je sačinjen izveštaj o rasprostranjenosti i karakteristikama sajber proganjanja i o mogućnostima adekvatne društvene zaštite (U.S. Attorney's office, 1999). Iako gotovo sve američke države imaju legislativu protiv proganjanja, pri čemu zakonodavstva čak 42 države prepoznaju upotrebu elektronske komunikacije kao sredstva proganjanja, svega nešto manje od trećine država eksplicitno uključuje pojavu sajber proganjanja u svoje zakonske definicije. Juta, Nju Džersi, Novi Meksiko, Ajdaho i Nebraska još uvek nemaju zakonodavstva koja tretiraju sajber proganjanje. Prva država koja je 1993. godine donela zakon protiv proganjanja, a koji uključuje uznemiravanje putem elektronske komunikacije bila je država Mičigen (Fullerton, 2003).

Veći gradovi u SAD poput Los Anđelesa i Njujorka imaju specijalizovane jedinice obučene za adekvatnu istragu i optuženja u slučajevima sajber proganjanja. Na primer, u Los Anđelesu od pripadnika policije i tužilaštva formiran je tim specijalizovan za rad na slučajevima sajber proganjanja, pod nazivom tim za otkrivanje i gonjenje slučajeva proganjanja i pretnji. Slično tome, u Njujorku formiran je odred policije specijalizovan za informacione tehnologije. Ovaj odred pruža redovne obuke za policajce i tužioce uključujući i obuku za rad sa slučajevima sajber proganjanja. Polaznici se obučavaju za to kako da pribave i obrade elektronske dokaze, kako da sačine nalog za pretres, poziv za sud i slično. FBI ima jedinice za kompjuterski kriminalitet širom zemlje koje su obučene i za postupanje u slučajevima sajber proganjanja (U.S. Attorney's office, 1999). Nauka koja se bavi otkrivanjem incidenata počinilaca, prikupljanjem, analizom i rekonstrukcijom dokaza dobijenih iz računarskih mreža korišćenjem multidisciplinarnih znanja, a kojima se omogućava rešavanje krivičnih slučajeva naziva se sajber forenzika (Vuletić, 2008: 35).

Iako je prvi zakon protiv proganjanja donet u Americi, evropske zemlje nisu zaostajale u izradi relevantne legislative protiv proganjanja. Od zemalja koje pripadaju Evropskoj Uniji, svega osam država ima posebne zakone protiv proganjanja, i to su: Austrija, Belgija, Danska, Nemačka, Holandija, Malta, Irska i Velika

Britanija. Neke države sa izgrađenom legislativom protiv proganjanja (Austrija, Danska, Nemačka, Vellika Britanija), imaju dovoljno široke zakonske definicije da ih mogu primeniti na slučajeve sajber proganjanja, dok, primera radi, Irska daje najužu definiciju proganjanja, nudi tumačenje pojave ograničeno na fizičko praćenje i posmatranje žrtve, koja se tako smatra pretesnom za regulaciju sajber poroganjanja. U Begiji (*Harassment by phone, e-mail, text message law*) i na Malti (*Electronic communications (Regulation) Act*) postoje posebni zakoni kojima se posredno može regulisati uznemiravanje u sajber prostoru (Modena group on stalking, 2007).

Države Viktorija i Kvinsland u Australiji jedine su države koje neposredno uključuju on-lajn uznemiravanje kao vid proganjanja. Većina ostalih država u Australiji, daju šire definicije proganjanja koje uključuju i sajber proganjanje uz izuzetak države Novi Južni Vels i Zapadne Australije koje metode proganjanja sužavaju na fizičko praćenje i nadziranje kuće ili radnog mesta žrtve što isključuje sajber prostor (Ogilvie, 2000: 5).

Analizom legislative protiv proganjanja zapaža se da je većina država u svetu koja tretira proganjanje kao posebno krivično delo širinom svojih zakonskih definicija obuhvatila i sajber proganjanje. U preostalom broju država (Irska, Zapadna Australija, Novi Južni Vels), usled preuske definicije proganjanja i njegovog ograničavanja svođenjem na fizičku bliskost, dolazi do svojevrsnog negiranja virtuelne stvarnosti i samim tim do onemogućavanja regulacije sajber proganjanja. Osim toga, neki autori ističu i mnoge druge nejasnoće koje proizlaze iz trenda da se sajber proganjanje u reči zakona smatra vidom konvencionalnog proganjanja (Bocilj, Griffiths, McFarlane, 2002: 5).

Zakonske definicije tradicionalnog proganjanja najčešće podrazumevaju da je proganjanje moguće vršiti isključivo od strane pojedinca, uz zanemarivanje proganjanja od strane grupa pojedinaca ili pravnih lica (organizacija i institucija), što je neretko slučaj kod sajber proganjanja. Zakonski uslov „izazivanja straha" kod žrtve u slučajevima sajber proganjanja ne mora biti zadovoljen, jer postupci često uključuju mnogo sofisticiranije metode ugrožavanja žrtava od prostih pretnji ugrožavanjem fizičkog integriteta žrtve. Usled upotrebe interneta i kataktera globalnosti pri vršenju sajber proganjanja često je problematično utvrditi nadležnost suda, s obzirom na to da nisu retka i prekookeanska uznemiravanja. Aspekt „neželjenosti komunikacije" od strane žrtve je, takođe, teško dokazati, jer žrtva sajber proganjanja često ne može ni da utvrdi identitet učinioca, niti da mu skrene pažnju o neželjenosti komunikacije. Većina zakonskih definicija proganjanja uključuje uslov kontinuiranosti uznemiravanja, dok se sajber proganjanjem smatra i aktivnost gde se samo jednom radnjom može poslati više poruka. Učinioci mogu upotrebiti aplikaciju posredstvom koje se uznemiravanje kontinuirano vrši i bez fizičkog pristupa računaru. Isto tako, zakonski opisi proganjanja u većini slučajeva ne uključuju elektronsko praćenje i nadgledanje žrtve u realnom vremenu.

Preporuke za zaštitu od sajber proganjanja

Preporuke za zaštitu od sajber proganjanja mogu se podeliti na opšte, koje imaju preventivni karakter i specijalne, koje treba da zaštite pojedince od daljeg proganjanja.

Opšte preporuke se upućuju internet korisnicima u preventivne svrhe. Potencijalnim žrtvama sajber proganjanja preporučuje se: upotreba druge e-mail adrese pri poseti sobama za čet, blogovima, grupama za diskusiju i drugo; ograničavanje komuniciranja putem ličnog mejla (samo porodica i prijatelji); izbor korisničkog imena koje je neutralno po polu; biranje nelogičnog sleda karaktera pri kreiranju šifre; često menjanje šifara, lozinki; vođenje računa o elementima lične zaštite pri izboru internet provajdera i opreznost pri upoznavanju „on-lajn prijatelja". Dodatno, programi za enkripciju („zaključavanje") poruka poput programa *Pretty Good Privacy* preporučuju se kao programi koji pružaju pouzdanost, autentičnost i privatnost on-lajn komunikacije (Ellison, Akdeniz, 1998: 14).

Specijalne preporuke se upućuju osobama koje su već postale žrtve proganjanja. U slučajevima kada je identitet progonitelja dostupan žrtvi, potrebno je staviti mu do znanja da je svaka dalja komunikacija nepoželjna. Bazična preporuka, odnosi se na neophodnost čuvanja istorije komunikacije sa učiniocem, kopija poruka, radi eventualnog korišćenja u istrazi i gonjenju. Žrtva može prijaviti uznemiravanje internet provajderu učinioca, policiji i zatražiti zaštitu od organizacija koje se bave pružanjem zaštite na internetu (WHOA, NCVC, *CyberAngels, GetNetVice*). Poželjno je korišćenje programa koji blokiraju napade od strane nepoželjnih ili nepoznatih adresa ili sajtova sa nepoželjnim sadržajem (*CyberSitter, Netnanny*) (U.S. Attorney's office, 1999).

Posebnu pažnju treba posvetiti zaštiti prilikom korišćenja sajtova za umrežavanje. Danas u svetu funkcioniše oko 150 sajtova baziranih na principu socijalnog umrežavanja koji okupljaju milionske grupe korisnika poput Facebook-a (200 miliona), My Space-a (250 miliona), Wayn-a (10 miliona), Linkedln-a (40 miliona) i drugih (Wikipedia, 2009). Korisnici ovih i sličnih sajtova neretko ostavljaju veliku količinu osetljivih podataka na mreži i tako se izlažu riziku od proganjanja. Prema istraživanju kompanije *Sophos* koja se bavi zaštitom na internetu, 41% korisnika Facebook-a čini dostupnim lične podatke, što omogućava zloupotrebu poput krađe identiteta, praćenja korisnika i drugo; 87% korisnika ostavlja informacje o svom obrazovanju ili radnom mestu; 84% datum rođenja; 78% adresu stanovanja; 72% jednu ili više e-mail adresa, dok je 23% spremno da ostavi svoj broj telefona (Sophos, 2007). Radi izbegavanja opasnosti od sajber proganjanja, ova kompanija preporučuje upotrebu naprednih opcija za zaštitu privatnosti, pooštravanje kriterijuma pri izboru sajber prijatelja i korišćenje skraćene (limitirane) verzije ličnog profila.

ZAKLJUČNA RAZMATRANJA

Na osnovu pregleda relevantne svetske literature iz oblasti sajber proganjanja zaključuje se da ono predstavlja kompleksnu pojavu, koju treba posmatrati samostalno i izolovano od drugih fenomena i koja pre svega zahteva multidisciplinarnost kako u prevenciji, tako i prilikom pružanja pomoći i podrške žrtvama i tretmanu učinilaca. Naime, reč je o krajnje složenoj, dinamičnoj pojavi koja je direktno uslovljena razvojem informaciono-komunikacionih tehnologija i podrazumeva kontinuiran i sistematski pristup u proučavanju, jer se iz časa u čas menjaju načini on-lajn uznemiravanja, širi virtuelni prostor, grade nove veze sa fizičkom, on-lajn realnošću.

Napredak saznanja i razmenu iskustava o sajber proganjanju i adekvatnom načinu reagovanja u velikoj meri ograničava nepostojanje opšteprihvaćene definicija. U radu se zagovara prihvatanje šireg određenja sajber proganjanja koje, osim računara i interneta, uključuje telefonske i druge elektronske tehnologije za praćenje i nadgledanje potencijalnih žrtava.

Postoji malo empirijskih podataka o fenomenu sajber proganjanja. Ipak, na osnovu pregleda savremenih istraživanja može se izvesti nekoliko zaključaka:

- prevalencija sajber proganjanja je u kontinuiranom porastu;
- žrtve su najčešće uznemiravane jednim oblikom proganjanja;
- najčešći oblik proganjanja je slanje uznemirujućih elektronskih poruka;
- žrtve su najčešće ženskog pola, prosečne starosti oko 30 godina;
- učinioci su u najvećem broju slučajeva muškog pola različitog uzrasta.

Veliki broj razvijenih zemalja prepoznaje proganjanje kao posebno krivično delo, a zakonsko određenje je dovoljno široko da obuhvati i sajber proganjanje. U nekim zemljama osavremenjivanje krivičnopravne reakcije dobija svoj odraz i u formiranju specijalno obučenih policijskih odreda za sprečavanje ovog vida sajber nasilja. Manje formalnu, ali prilično efikasnu pomoć pružaju internet provajderi i organizacije koje se bave pružanjem zaštite na internetu.

Na području Srbije, sajber proganjanje predstavlja još uvek nedovoljno istraženu oblast. Evidentna je potreba za prikupljanjem osnovnih empirijskih podataka o rasprostranjenosti i osnovnim karakteristikama sajber proganjanja, kao i potreba za osmišljavanjem i primenom adekvatnog društvenog odgovora u cilju prevencije i zaštite žrtava.

Savremene informaciono-komunikacione tehnologije omogućavaju masovno povezivanje i komunikaciju između osoba koje ne moraju da otkriju svoj identitet. Sajber prostor ne poznaje granice između država i naroda, odnosno omogućava ostvarivanje kontakta između najrazličitijih osoba. Praktično, to znači da građani Srbije, bez obzira na političku izolaciju, nisu bezbedni od različitih vidova sajber nasilja. U sadašnjoj situaciji naši građani moraju sami da brinu o svojoj bezbednosti. Jedan od prvih koraka u izgradnji razvijenog sistema zaštite trebalo bi da bude informisanje građana o merama prevencije sajber nasilja, a posebno o aktuelnoj pojavi socijalnog umrežavanja i bezbedonosnom riziku koje ono nosi.

LITERATURA

1. Baum, K., Catalano, S., Rand, M., Rose, K. (2009). Stalking victimization in the United States. Washington, DC: Bureau of justice report, US Department of justice.
2. Bocilj, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. First Monday, 8(10).
3. http://firstmonday.org/issues/issue8_10/bocij/index.html, pristupljeno 27. aprila 2009.
4. Bocilj, P., McFarlane, L. (2002). Online harassment: Towards a definition of cyber stalking. Prison Service Journal, 139, 31-8.
5. Bocilj, P., Griffiths, M., McFarlane, L. (2002). Cyberstalking: A new challenge for Criminal law. The Criminal Lawyer, 122, 3-6.

6. Convention on Cyber crime (CoE) (2001).
7. http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc, pristupljeno 27. aprila 2009.
8. D'Ovidio, R., Doyle, R. (2003). A study on cyber stalking: Understanding investigative hurdles. FBI Law Enforcement Bulletin, 73(3), 10-17. www.fbi.gov/publications, pristupljeno 10. 09. 2007.
9. Ellison, L., Akdeniz, Y. (1998). Cyber-stalking: The regulation of harassment on the Internet. Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, 29-48.
10. Finn, J. (2004). A survey of online harassment at a university campus, Journal of Interpersonal Violence, 19, 468-483.
11. http://jiv.sagepub.com/cgi/content/abstract/19/4/468, pristupljeno 27. aprila 2009.
12. Fullerton, F. (2003). Cyber age stalking. Law and technology resources for legal professionals. http://www.llrx.com/node/1114/print, pristupljeno 7. maja 2009. godine.
13. GetNetWise, www.getnetwise.com, pristupljeno 8. maja 2009. godine.
14. McFarlane, L., Bocilj, P. (2004). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. Firstmonday, 8(9), 1-12.
15. McCall, R. (2004). Online harassment and cyber stalking: Victim access to crisis, referral and support services in Canada - concepts and recommendations. Victim Assistance Online Resources, www.vaonline.org, pristupljeno 27. aprila 2009.
16. Modena group on stalking (2007). Protecting woman from the new crime of stalking: comparison of legislative approaches within the European Union
17. http://stalking.medlegmo.unimo.it, pristupljeno 5. juna 2008. godine.
18. Mullen, P., Pathé, M., Purcell, R., Stuart, G. (1999). A study of stalkers. American Journal of Psychiatry, 156, 1244-1249.
19. National Center for Victims of Crime (2007). The model stalking code revisited: Respondings to the new realities of stalking, www.ncvc.org, pristupljeno 26. septembra 2007. godine.
20. Ogilvie, E. (2000). Cyberstalking. Trends and issues in crime and criminal justice, 166, 1-6.
21. Pretty Good Privacy, www.pgp.com, pristupljeno 5. maja 2009. godine.
22. Riva, G., Galimberti, C. (1997). The psychology of cyberspace: A socio-cognitive framework to computer-mediated communication. New ideas in psychology, 15(2), 141-158.
23. CyberAngels, www.cyberangels.org, pristupljeno 8. maja 2009. godine.
24. Southworth, S., Dawson, T., Fraser, C., Tucker, C. (2005). A high-tech twist on abuse: technology, intimate partner stalking and advocacy. Family Violence Prevention and Health Practice, 3, 1-6.
25. Sophos, http://www.sophos.com, pristupljeno 9. maja 2009. godine.
26. Tomić, Z. (2004). Sajber-prostor i problemi razgraničenja, Kultura, 107/108. http://www.zaprokul.org.rs/kultura/broj107.html, pristupljeno 9. maja 2009. godine.
27. U.S. Attorney's Office (1999). Cyberstalking: A new challenge for law enforcement and industry, www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, pristupljeno 1. maja 2009. godine.
28. Vuletić, D. (2008). Šerlok Holms u virtuelnom svetu. Internet ogledalo, 93, 34-39.

29. Walby, S., Allen, J. (2004). Domestic violence, sexual assault and stalking: findings from the British Crime Survey. London: Home office.
30. Working to Halt Online Abuse (WHOA), www.haltabuse.org, pristupljeno 8. maja 2009. godine.
31. Wykes, M. (2007). Constructing crime: Culture, stalking, selerity and cyber. Crime, media culture, 3(2), 158-174.

INTERPERSONAL VIOLENCE IN CYBER SPACE

Vesna Žunić-Pavlović, Marina Kovačević-Lepojević
University of Belgrade - Faculty for Special Education and Rehabilitation

Summary

Within the strong development of ICT techologies, there are many changes in the fild of social interactions, where the „physical" and „real" are more often replaced with „virtual" as a kind of dematerialization in human relationships. Even it is the way for society development, starting with education, employment, politics, entertainmet, at the other side virtual culture opens the space for different abuses. Cyber stalking, as huge treat in modern age, is the crime based upon the interpersonal violence in cyber space.

This paper is aimed to determine the notion of cyber stalking and its relationship with similar phenomenas, to give the cyber stalking and perpetrators typology, to review the research about the prevalence and impact of cyber stalking, victims and perpetrators and to review the measures for its prevention.

Key words: on-line harassment, cyber stalking, crime, internet.