JAČANJE BEZBEDNOSTI OTVORENIH JAVNIH GRADSKIH PROSTORA PRIMENOM IKT – DRUŠTVENOG RAČUNARSTVA

Milena Vukmirović[1], Miroslava Raspopović Milić[2]
UDK=351.758:004.7
https://doi.org/10.18485/fb_ubur.2018.1.ch16
[1] Univerzitet u Beogradu – Šumarski fakultet
milena.vukmirovic.arch@gmail.com
[2] Univerzitet Metropoliten – Fakultet informacionih tehnologija,
miroslava.raspopovic@metropolitan.ac.rs

Sažetak

Bezbednost se smatra osnovnim kriterijumom kvaliteta otvorenih javnih gradskih prostora i preduslovom za ostvarivanje drugih kriterijuma, poput ugodnosti, atraktivnosti ili životnosti. Kako bi se ostvario navedeni kriterijum, primenjuju se različite strategije u oblasti urbanog dizajna i oblikovanja otvorenih javnih gradskih prostora, koje uglavnom obuhvataju mudre i dugoročne intervencije, čiji su rezultat društvena uključenost i kohezija. Na drugoj strani, otvoreni javni prostori postaju slobodni, pristupačni, demokratski, a, pre svega, usled prisustva ljudi, omogućavaju prirodan oblik nadzora. Gotovo istovremeno sa ponovnim povećanjem značaja i razvojem otvorenih javnih gradskih prostora, pojavljuju se i savremena sredstva komunikacije, koja su otvorila različite mogućnosti kako za korišćenje otvorenih prostora, tako i za postizanje bezbednosti.

Sa napredovanjem informaciono-komunikacionih tehnologija (IKT), kao što su klaud-računarstvo (engl. *cloud computing*), *IoT* (*Internet of Things*) i obrada velike količine podataka (engl. *big data*), pojavile su se i njihove razne primene. Jednu od zapaženijih primena čine i društvene mreže, koje su jedna od tehnologija koje i dalje evoluiraju. Društvene mreže pružaju mogućnost većeg korišćenja interneta za kreiranje, deljenje i učestvovanje u deljenju informacija o sebi ili drugima, o onome što nam se sviđa ili ne sviđa, o našim kretanjima, mislima i transakcijama.

S jedne strane, deljenje svih ovih informacija donosi mogućnost za razvijanje novih aplikacija i mogućnosti, dok, sa druge strane, zbirni pregled podeljenih informacija jednog korisnika ili više korisnika na društvenoj mreži može dovesti i do njihovih korišćenja u neadekvatne svrhe.

Društveno računarstvo predstavlja novi pravac istraživanja za informacione sisteme. Ono podrazumeva prikupljanje podataka o svim aktivnostima korisnika na mreži, kako bi se ti podaci obradili u svrhu analize onlajn ponašanja jednog ili više korisnika u njegovom prirodnom okruženju, kao i kontrolisanim eksperimentalnim uslovima. Onlajn profilisanje (engl. *online profiling*) koristi hronologiju ponašanja korisnika na mreži kako bi predvidelo njegovo buduće ponašanje i njegove afinitete za određene veb-aplikacije, kao što su ciljani

onlajn marketing, personalizacija sadržaja i društvene preporuke. Izvođenje preciznih informacija i tačnih zaključaka iz pregršti podataka o korisnicima na društvenim mrežama važno je za moderne komunikacije prilikom vanrednih situacija. Društvene mreže predstavljaju platformu koja se može koristiti za prikupljanje podataka, efikasno deljenje informacija i izvođenje informacija.

S obzirom na to da putem društvenih mreža korisnici svesno ili nesvesno daju dosta informacija o sebi i tendenciji svog ponašanja, informacije koje se prikupljaju ovim putem nazivaju se „volonterske informacije".

Korišćenje informacija sa društvenih mreža u kriznim situacijama može se klasifikovati u tri grupe: (i) širenje informacija, (ii) geolokacijske informacije, (iii) semantička analiza. Širenje informacija putem društvenih mreža može da poboljša pravovremeno podizanje svesti u kriznim situacijama, zbog toga što one mogu da brzo i efikasno prošire informacije velikoj grupi ljudi. Geolokacijske informacije društvenih medija takođe imaju značajnu ulogu u otkrivanju kriznih događaja i u davanju brzih odgovora. Semantička analiza poruka na društvenim mrežama, kao što su tvitovi/poruke na mreži *Twitter*, mogu pomoći da se saznaju informacije o načinjenoj šteti, potrebnoj pomoći, žrtvama ili primanju pomoći tokom vanredne situacije. Dok se društveno računarstvo i društvene mreže mogu koristiti za brzo reagovanje u vanrednim situacijama, slične metode se mogu koristiti i u negativne svrhe, te je važno i njih napomenuti kao nusprodukt.

Jednostavno rečeno, teroristi imaju dobar razlog da koriste društvene medije. Društvene mreže omogućavaju teroristima da koriste strategiju „sužavanja" (engl. *narrowcasting*). Ova strategija omogućava da se, na osnovu demografskih atributa ili drugih karakteristika, suzi ciljna grupa kojoj se plasiraju određene informacije. U ovom radu se daje pregled kako se informacije društvenih mreža mogu koristiti (i) za upravljanje u kriznim situacijama i (ii) u cilju onlajn profilisanja.

Rad se fokusira na prikaz specifičnih i aktuelnih metoda, na mogućnostima koje one nude i zaključcima koji se mogu formirati na osnovu podataka prikupljenih sa društvenih mreža, kao i etičkih i pravnih pitanja koja se pojavljuju njihovim korišćenjem. Ove metode se smatraju važnima, jer mogu da pomognu u očuvanju bezbednosti u otvorenim javnim prostorima, sprečavajući terorizam i štiteći njihove korisnike. Rad takođe razmatra na koji se način i u kojoj meri navedeni ciljevi mogu postići pomoću sadašnjih tehnologija, imajući u vidu stav javnosti prema njihovom nadzoru na društvenim mrežama. U skladu sa navedenim, rad se bavi pregledom različitih mogućnosti i alata koje nude informaciono-komunikacione tehnologije, sa fokusom na društvenom računarstvu i društvenim mrežama, a koje mogu doprineti ostvarivanju i povećanju bezbednosti otvorenih javnih gradskih prostora.

Ključne reči: *bezbednost, otvoreni javni gradski prostor, društveno računarstvo, IKT*

Bezbednost otvorenih javnih gradskih prostora

Prema svojoj definiciji (Vidanović, 2006), strah predstavlja primarnu emociju koju odlikuje snažno, neprijatno uzbuđenje, a koja nastaje usled opažanja ili očekivanja stvarne ili zamišljene opasnosti, ili ozbiljne pretnje pred kojom je organizam nemoćan. Pored navedenog, to je urođena, genetski programirana adaptivna reakcija na preteći ili bolan stimulus. Shodno tome, strah je ključan, ako ne i najveći motivator određenog ponašanja i jedan od najefikasnijih i najnehumanijih oblika upravljanja ljudima i drugim živim bićima.

Zbog navedenih svojstava, vekovima je korišćen i kao povod, odnosno uzrok kontrole određenog načina življenja i gradnje, što je vrlo često dovodilo do loših ishoda i efekata. Prema evidenciji Projekta za javne prostore (Project for public spaces – PPS), na globalnom nivou, strah od nuklearnog napada bio je „ključni faktor u motivisanju SAD u gradnji međudržavne mreže auto-puteva nakon Drugog svetskog rata, a što je za posledicu imalo razaranje gradskih naselja i širenje predgrađa“ (Project for Public Spaces, 2008). Na nivou manje razmere, strah od „nepoželjnih“ doveo je do pojave otvorenih prostora u kojima nema klupa za sedenje, senila, prodavnica, odnosno bilo kakve pogodnosti koja bi podstakla dolazak i boravak ljudi u otvorenom prostoru. To je rezultovalo stvaranjem praznih, otuđenih, dosadnih gradskih prostora – prostora „izgrađenih pod uticajem straha od 'negativne aktivnosti', straha od interakcije sa bilo kojim drugim ljudima“ (Project for Public Spaces, 2008).

Pored navedenih, kao poseban oblik pretnje i problema, javio se strah od sve učestalijih i surovijih terorističkih napada, koji teži da se transformiše u nešto što se naziva „mentalitetom utvrđenja“. Naročito je važno navesti da je strah od mogućeg ugrožavanja bezbednosti i sigurnosti pojedinca mnogo izraženija pojava od samog čina koji bi doveo do toga. Međutim, upravo taj strah i utiče na ponašanje ljudi kako u pogledu korišćenja određenih prostora, tako i uopšte.

U urbanom dizajnu bezbednost je osnovni kriterijum kvaliteta otvorenih javnih gradskih prostora, pa čak i preduslov za njihovo funkcionisanje. Ovo se može sagledati kroz normativne teorije u urbanom dizajnu, odnosno analizom nekoliko okvira[1] kojima se definišu kriterijumi, aspekti, zahtevi i principi za vrednovanje kvaliteta otvorenih javnih gradskih prostora, a koje je neophodno dostići u cilju stvaranja kvalitetnog prostora. Navedeni okviri posmatraju različite teritorijalne nivoe.

Tako, na nivou grada Gel (Gehl, 2010) smatra da se bezbednost grada može generalno uvećati kada se veliki broj ljudi kreće i provodi vreme u otvorenim gradskim prostorima. Okviri za vrednovanje kvaliteta otvorenih javnih gradskih prostora bezbednost posmatraju kao preduslov za korišćenje određenog gradskog prostora, pa je usled toga među kriterijumima uspostavljena hijerarhija. U tako

[1] Allan Jacobs (1995), Martinchigh (2002), Project PROMT (2003), Bazik (2008), NYC DoT (2009), Gehl (2010), Gerlach (2010), Vukmirovic (2013).

definisanom kontekstu, bezbednost je primarni kriterijum koji je neophodno ostvariti, da bi se dostigli drugi kriterijumi koji slede, a to su: pristupačnost i protočnost, čitljivost, ugodnost, inspirativnost i životnost (Bazik, 2008; Bazik & Vukmirović, 2006).

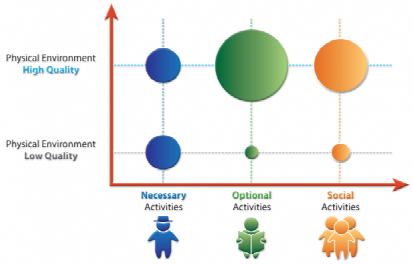
Iz ugla PPS-a, a posmatrajući bezbednost i strah kao objektivnu i stvarnu pojavu, metode koje se primenuju u njihovom suzbijanju ne moraju svuda da dovedu do pojave otuđenih i praznih gradskih prostora. Njima bi trebalo ohrabriti boravak u otvorenom prostoru, različitost, raznovrsnost, itd. U skladu sa tim, a govoreći o različitim „svrhama trotoara", Džejn Džejkobs navodi kako je „glavna odlika uspešnog dela grada da se čovek mora osećati bezbedno i sigurno" te da ukoliko se u tom domenu podbaci, neće biti uspešan ni u drugim. Kao moguće strategije da se doprinese osećaju bezbednosti i sigurnosti Džejkobs (2011) navodi potrebu za postojanjem jasne demarkacije između onog što je javni i onoga što je privatni prostor, potrebu za postojanjem „očiju koje gledaju na ulicu", tj. prirodnog nadzora ulice i stalnog prisustva ljudi. Ovo se ujedno može opisati i kao jedan od principa izgradnje grada „po meri čoveka", a pri kojoj se uspostavlja i najdirektnija interakcija sa njim.

Stavljanje težišta u urbanom dizajnu na ljudsku meru ima zadatak da podstakne povećanje broja ljudi u otvorenim prostorima u vidu integralne gradske politike čiji je cilj razvijanje živahnih, bezbednih, održivih i zdravih gradova. Ovo je podjednako važno i za jačanje društvene funkcije gradskog prostora kao mesta za sastajanje, a koja doprinosi socijalnoj održivosti i stvaranju otvorenog i demokratskog društva.

Uspostavljanjem relacije između kvaliteta otvorenih prostora i broja ljudi koji provode vreme u njima Gel (Gehl, 2010) uočio je da se povećanjem kvaliteta spoljnog okruženja povećava nivo pratećih aktivnosti. Navedeni odnos je predstavljen dijagramom (Slika 1) na kojem se uočava da se nivo nužnih aktivnosti ne menja zavisno od kvaliteta spoljašnjeg okruženja, ali da se unapređenjem kvaliteta otvorenih prostora znatno povećava nivo pratećih, a samim tim i društvenih aktivnosti. Društvene aktivnosti[1] su plod kvaliteta i dužine trajanja druga dva tipa aktivnosti, jer se zbivaju spontano prilikom susreta. Upotreba javnog prostora se na ovaj način može shvatiti kao posredнички faktor u smislu definisanja fizičkih i društvenih uslova koji utiču na stvarnu precepciju sigurnosti u nekom prostoru.

Međutim, ranjivost otvorenih javnih gradskih prostora dodatno je usložnjena u savremenom periodu koji karakteriše globalizacija kriminala, nasilja i konflikata. Posebnu pretnju predstavljaju terorizam i uvećan strah od njegove pojave, jer je upravo veliki broj osoba koje vrše svakodnevne aktivnosti i provode slobodno vreme u otvorenim javnim gradskim prostorima i drugim mestima gde se ljudi okupljaju, relaksiraju i zabavljaju verovatna meta terorista.

[1] One se odnose na igru dece, pozdravljanja i konverzaciju među ljudima, zajedničke aktivnosti različitih vrsta ili jednostavno posmatranje i slušanje drugih ljudi.



Slika 1: Kvalitet spoljnog okruženja doprinosi
povećanju neobaveznih aktivnosti (Gehl, 2010)

Ranjivost otvorenih javnih gradskih prostora

Primena različitih strategija u dizajnu otvorenih prostora koja ima za cilj porast intenziteta njihovog korišćenja, sa jedne strane, i urbani terorizam, čiji je cilj da se ostvari veća stopa smrtnosti i povreda ljudi, kao i oštećenja imovine, sa druge, predstavljaju ozbiljan problem, koji je neophodno prevazići a da se pri tome ne stvori atmosfera straha i „mentalitet utvrđenja“. U literaturi koja se bavi temom borbe protiv terorizma mesta koja privlače teroriste nazivaju se prometnim mestima (engl. *crowded places*), a „smatraju se 'atraktivnom metom', jer im se može lako pristupiti, imaju manji stepen zaštite i u njima se, usled uspešno realizovanog napada, može ostvariti veća stopa žrtava i političkog uticaja“ (Royal Institute of British Architects, 2010).

Po definiciji, pod prometnim mestom se smatraju „lokacije ili okruženja dostupne javnosti, koja se mogu tretirati i kao potencijalne mete terorističkog napada, a usled veće gustine ljudi koji su prisutni na tome mestu“ (Home Office in partnership with the Department for Communities and Local Government, 2012). Shodno tome, to mogu biti sportski stadioni, tržni centri, klubovi, bioskopi, pozorišta, kafei, restorani, ali i svakodnevni otvoreni javni gradski prostori, kao što su trgovi, ulice ili parkovi. Prema svojim fizičkim atributima, prometna mesta se dele na dve kategorije: stalna i povremena (Tabela 1).

Ova podela je vrlo važna i treba je imati u vidu, jer, za razliku od ranijih terorističkih praksi, koje su uglavnom bile usmerene protiv ekonomskih i vojnih ciljeva, kao i državnih, prostornih simbola, a koje su imale za cilj stvaranje pometnje i osvajanje medijske pažnje umesto izazivanja velikog broja žrtava (Royal Institute of British Architects, 2010), nedavni događaji pokazuju da su sve više meta terorista upravo prometna mesta, gde se okuplja veliki broj ljudi. Imajući u vidu nedavne događaje u evropskim gradovima, teroristi napadaju upravo mesta gde ljudi dolaze da se opuste i zabave (gledanje fudbalske utakmice, slušanje koncerta omiljenog muzičkog izvođača, sedenje u lokalnom kafeu ili restoranu sa prijateljima, javna proslava državnog praznika itd.).

Tabela 1: Kategorije prometnih mesta utvrđene prema svojim fizičkim atributima (Royal Institute of British Architects, 2010)

STALNA MESTA	**Otvoreni prostori**	Stadioni, trkališta, veliki sportski kompleksi
	Zatvoreni prostori	Saobraćajna čvorišta (aerodromi, železničke stanice itd.), arene, pozorišta, koncertne dvorane, izložbeni centri, tržni centri, noćni klubovi, sakralni objekti itd.
POVREMENA MESTA	**Događaji na koje se ulazi sa ulaznicom**	Festivali, godišnje izložbe, umetničke izložbe
	Događaji na kojima je pristup slobodan	Parade, trke, izložbe

U takvim prilikama niko od prisutnih ljudi i ne očekuje da će se dogoditi nešto tragično, pa se ljudi koji su bili žrtve napada na ovakvim mestima često nazivaju i mekim metama (engl. *soft targets*). Kao ključna posledica ovakvih tragičnih događaja, a što je ujedno i cilj napadača, nastaje strah od boravka u javnom prostoru, a što je karakteristično kako za pojedince koji su preživeli napad, tako i za opštu populaciju. Stvara se strah od moguće ponovne pojave nečega takvog.

Karakteristike nedavnih terorističkih napada u Evropi

Istražujući teroristički napad koji se odigrao u Parizu, početkom 2015. godine, Salivan i Eklus (Sullivan & Elkins, 2015) identifikovali su tri vrste terorističkih napada koje je definisao Vots (Watts, 2015): usmerene, umrežene i inspirisane. Usmereni napadi pretpostavljaju visok stepen centralne organizacije spoljne grupe, visok nivo smrtnosti i posedovanje određenih veština i sposobnosti za realizaciju napada. Usled unapređenja rada policije, obaveštajnih službi i vojnih napora, značajno je otežana realizacija ove vrste napada, posebno njene organizacije od vrha ka dnu, pa je samim tim i njihova pojava proredjena.

Za razliku od usmerenih, umrežene napade realizuju grupe ili pojedinci sa određenim stepenom obučenosti, ali i povezanosti sa terorističkim organizacijama i zajednicama. Vots (Watts, 2015) ih poistovećuje sa „rojem koji okuplja operativce, resurse i 'počinioce po potrebi'". Na kraju, inspirisane napade odlikuje „nejasna šema i organizacija i nasumično nasilje 'samoproklamovanih džihadista'[1]" (Watts, 2015). Ako se posmatra sâm napad koji se odigrao početkom januara 2015. godine u Parizu, napadači na časopis *Šarli ebdo* (*Charlie Hebdo*) i prodavnicu košer-hrane

[1] "jihadi wannabees"

bili su deo mreže inspirisanih i usmeravanih od ideološki suprostavljenih terorističkih organizacija, prva od strane Islamske države (ID), a druga od Al kaide.

Zbog navedenih karakteristika, ova vrsta napada se može sve više očekivati u budućnosti, naročito imajući u vidu uticaj društvenih mreža, interneta i elektronskog novinarstva, koji poseduju potencijal da motivišu i usmeravaju slabo povezane pokrete i pojedince (Vukmirović, 2017). Kao prekretnica ovog fenomena navodi se smanjenje uticaja usled uništavanja mreže koju je razvila Al kaida. Pored navedenog, Islamska država se veoma brzo prilagođava ovoj situaciji i smatra se njenim „najuspešnijim praktičarem, zbog svog onlajn prisustva, aktivnosti na društvenim mrežama, filmova visoke produkcije, kao i užasavajućih video-snimaka koji vode ka onlajn propagandnim materijalima i vodičima za učenje tehnika, procedura i taktika“ (Kilcullen, 2015).

Isti autor smatra da je upravo koristeći digitalne resurse Islamska država uspela da napadne različite ciljeve, tj. prostore koji se svakodnevno koriste, služeći se neuobičajenim sredstvima za svrhu napada, bez koordinacije sa drugim učesnicima. Posebno treba imati u vidu da će ova vrsta napada sve više da evoluira, da će biti sve više napada koji uključuju mali broj pojedinaca, nizak nivo tehničke opremljenosti, ali i ne nužno i manji broj žrtava, da napadači ne odgovaraju terorističkom stereotipu[1] i da još nisu razvijeni i usavršeni tehnološki uređaji i nadzor, niti stvoreni kadrovi u vidu supervojnika koji bi mogli da spreče i zaštite građane od ovakve vrste pretnje. Zato ne iznenađuje činjenica da se u poslednjem periodu u Evropi dogodio niz ovakvih napada u javnim gradskim prostorima (Tabela 2).

Tabela 2: Pregled napada[2] koji su se desili u Evropi u periodu od 7. januara 2015. zaključno sa 19. avgustom 2017. godine

No.	Mesto	Datum	Vrsta napada	Lokacija
1.	Turku (Finska)	19. avgust 2017.	napad nožem	pijaca
2.	Barselona (Španija)	17. avgust 2017.	napad kombijem	šetalište
3.	London (VB)	19. jun 2017.	napad automobilom	džamija
4.	London (VB)	4. jun 2017.	napad kombijem	most
5.	Mančester (VB)	23. maj 2017.	bombaš samoubica	koncertna dvorana
6.	Pariz (Francuska)	21. april 2017.	napad vatrenim oružjem	šetalište
7.	Stokholm (Švedska)	7. april 2017.	napad kamionom	šetalište, pešačka zona
8.	London (VB)	22. mart 2017.	napad automobilom i nožem	most
9.	Pariz (Francuska)	3. februar 2017.	napad nožem	muzej
10.	Berlin (Nemačka)	20. decembar 2016.	napad kamionom	božićna pijaca na trgu

[1] Vojno sposoban muškarac koji je član tajne organizacije, usamljenik, radikalnih stavova, koji je prošao specijalizovanu obuku, sa unapred određenim planom napada [12].

[2] *Napomena:* Broj navedenih napada nije konačan. U istom ili u sličnom periodu odigrali su se još neki napadi koji su bili povezani sa navedenim, ali za potrebe ovog pregleda istraživanja nisu bili relevantni.

11.	St Etjen di Rovr (Francuska)	26. jul 2016.	napad nožem	crkva
12.	Nica (Francuska)	14. jul 2016.	napad kamionom	šetalište
13.	Brisel (Belgija)	22. mart 2016.	bombaški napadi	aerodrom, metro
14.	Pariz (Francuska)	13. novembar 2015.	bombaški napadi i napadi vatrenim oružjem	koncertna dvorana, kafei, restorani
15.	Pariz (Francuska)	7. januar 2015.	napad vatrenim oružjem	redakcija časopisa, prodavnica

Ako se analizira sadržaj pregledne tabele, može se zaključiti da su se svi napadi odigrali na lokacijama koje imaju karakter „prometnog mesta“, od čega 8 napada na lokacijama na kojima se kreću pešaci (4 na šetalištima i u pešačkoj zoni, 2 na mostu i 2 na pijaci/trgu), 2 napada u koncertnoj dvorani, 2 u sakralnim objektima, 1 u muzeju, 1 na saobraćajnom čvorištu (metro i aerodrom), 1 u redakciji časopisa, 1 u restoranima i kafeima i 1 u prodavnici. S druge strane, ako se posmatra način na koji je izvršen napad, naveći broj njih (7) izveden je motornim vozilom (kamionom, kombijem ili automobilom), 3 napada su izvedena hladnim oružjem (nožem), 3 napada bombom i 3 napada vatrenim oružjem. Navedeni rezultati, ali i druge pojedinosti koje se vezuju za ove napade, govore u prilog tezi da ovi napadi imaju karakter inspirisanih. Tu je i CNN-ova (CNN, 2017) hronološka analiza događaja koji su prethodili ovim napadima, a koja navodi i obraćanje portparola Islamske države, Abu Muhameda al-Adnanija, koji poziva „usamljene vukove“ da izvedu napade koristeći improvizovano oružje, među kojim navodi i automobil kao moguću opciju.

Imajući navedeno u vidu, kompleksnost zadatka u pogledu odbrane prometnih mesta saglēda se u potrebi da se ovi svakodnevni prostori nadziru putem neinstitucionalizovanih i aktera civilnog društva (Coaffee, O'Hare, & Hawkesworth, 2009) i da je potrebno uključiti brojne aktere i organizacije (Home Office in partnership with the Department for Communities and Local Government, 2012). To podrazumeva dva oblika intervencija – prve imaju za cilj odbranu od napada, a druge imaju svrhu ublažavanja efekata napada. Imajući u vidu da se i teroristi koriste savremenim tehnologijama kako bi instruisali i inspirisali pojedince za buduće napade, neophodno je razmotriti njihov potencijal za potrebe sprečavanja i ublažavanja efekta napada, kao vid mere bezbednosti otvrenih javnih gradskih prostora.

Društveno računarstvo

Sa napredovanjem informaciono-komunikacionih tehnologija (IKT), kao što su klaud-računarstvo (engl. *cloud computing*), IoT (*Internet of Things*) i obrada velike količine podataka (engl. *big data*), pojavile su se i njihove razne primene. Jednu od zapaženijih primena čine i društvene mreže, koje su tehnološke platforme kakve i

dalje evoluiraju i usavršavaju se. Društvene mreže pružaju mogućnost za veće korišćenje interneta, za kreiranje, zajedničko deljenje i učestvovanje u deljenju informacija o sebi ili drugima, o onome što nam se dopada ili ne dopada, o našim kretanjima, mislima i transakcijama. Razašiljanje svih ovih informacija daje mogućnost za razvijanje novih aplikacija. Sa druge strane, zbirni pregled podeljenih informacija jednog ili više korisnika na društvenoj mreži može dovesti i do korišćenja tih informacija u neadekvatne svrhe.

Društveno računarstvo predstavlja novi pravac istraživanja za informacione sisteme. Društveno računarstvo podrazumeva prikupljanje podataka o svim aktivnostima korisnika na mreži, kako bi se ti podaci obradili u svrhu analize onlajn ponašanja jednog ili više korisnika u njegovom prirodnom okruženju, kao i kontrolisanim eksperimentalnim uslovima (Xu, Zhang, Sugumaran, Choo, Mai, & Zhu, 2016).

Izvođenje preciznih informacija i tačnih zaključaka iz pregršti podataka o korisnicima na društvenim mrežama vrlo je važno za moderne komunikacije prilikom vanrednih situacija. Društvene mreže predstavljaju platformu koja se može upotrebljavati za prikupljanje podataka, efikasno deljenje informacija i izvođenje drugih informacija. S obzirom na to da putem društvenih mreža korisnici svesno ili nesvesno daju dosta informacija o sebi i tendenciji svog ponašanja, tako se informacije koje se prikupljaju ovim putem nazivaju „volonterske informacije“, a korisnici društvenih mreža često se nazivaju „društvenim senzorima“. Društveni senzor (engl. *social sensor*) definisan je kao delatnik koji pruža informacije o svom okruženju na društvenoj mreži nakon interakcije sa drugim agentima (Krishnamurthy & Poor, 2014).

Neke od analiza koje se mogu sprovesti nad podacima društvenih mreža predstavljaju:

- vremenska analiza (tvitovi, ključne reči, broj aktivnih korisnika u nekom intervalu, prosečan broj objava tokom određenog vremenskog perioda);
- prostorna analiza (informacije koje se mogu povezati sa određenom lokacijom ili regionom);
- topološka analiza (istaknute ključne reči ili URL, korelacija između podataka/informacija);
- analiza aktivnosti korisnika (aktivnost specifičnih korisnika ili grupe korisnika).

Korišćenje društvenih mreža u vanrednim situacijama

Sa porastom popularnosti društvenih mreža otvorila su se mnoga nova pitanja i mogućnosti, u pravcu njihovog korišćenja, kao i analize podataka koji potiču od aktivnosti korisnika društvenih mreža. Istraživači su izučavali podatke sa društvenih mreža kako bi ispitali njihov uticaj na specijalne događaje i lokalizaciju prirodnih katastrofa (Trusov, Bodapati, & Bucklin, 2010). Sakaki je ispitao Twitter u realnom vremenu kako bi detektovao neki događaj (Sakaki, Okazaki, & Matsuo, 2013). Poruke s Twitter-a su se koristile u svrhu detektovanja zemljotresa, koristeći

prostorne i vremenske karakteristike tvitova (Crooks, Croitoru, Stefanidis, & Radzikowski, 2013). Longvil je koristio tvitove tokom požara u šumi, kako bi pokazao da je moguće podržati aktivnosti planiranja, rizika i procene štete (De Longueville, Smith, & Luraschi, 2009).

Obrada i analiza podataka tokom vanrednih situacija predstavlja tipičan scenario u kojem je potrebno obraditi veliku količinu podataka i iz njih izvesti pravovremene zaključke i doneti adekvatne mere pomoći i saniranja nastale štete. Brojni društveni senzori i uređaji za nadzor prikupljaju podatke iz fizičkog sveta, dok internet predstavlja repozitorijum za veliku količinu podataka, koji mogu da reflektuju različita stanja sajber-sveta i našeg sveta. Efikasna obrada podataka predstavlja jedan od izazova u korišćenju društvenih mreža u vanrednim situacijama. Zbog toga je važno razviti napredne mehanizme za upravljanje podacima i obradu podataka koji podržavaju otkrivanje katastrofa, reagovanje na katastrofu i njenu kontrolu, planiranje resursa za spasavanje i njihovu efikasnu distribuciju u slučaju vanredne situacije.

Priprema adekvatnih koraka za reagovanje tokom vanredne situacije predstavlja veliki izazov, zbog nedostatka informacija, nepredvidivosti situacije, kratkog vremenskog intervala za donošenje odluka i reagovanje. Tačne i pravovremene informacije su od vitalne važnosti tokom vanredne situacije. Društvene mreže predstavljaju dobrog kandidata za platformu koja može, uz podesne metode, da upravlja, sakuplja i obradi relevantne podatke.

Korišćenje informacija društvenih mreža u kriznim situacijama može se klasifikovati u tri grupe: (i) širenje informacija, (ii) geolokacijske informacije, (iii) semantička analiza. Širenje informacija putem društvenih mreža može da poboljša pravovremeno podizanje svesti u kriznim situacijama, zbog toga što mogu brzo i efikasno da prenesu informacije velikoj grupi ljudi. Geolokacijske informacije društvenih mreža takođe imaju značajnu ulogu u otkrivanju kriznih događaja i u davanju pravovremenih informacija. Geolokacijske informacije se odnose na lokaciju baziranu na sadržaju, postavljanje lokacije, registrovanje lokacije, koje se mogu koristiti u određivanju geografske lokacije kriznog događaja. Semantička analiza poruka na društvenim mrežama, kao što su tvitovi na mreži Twitter, mogu pomoći da se saznaju informacije o pričinjenoj šteti, potrebnoj pomoći, žrtvama ili primanju pomoći tokom vanredne situacije.

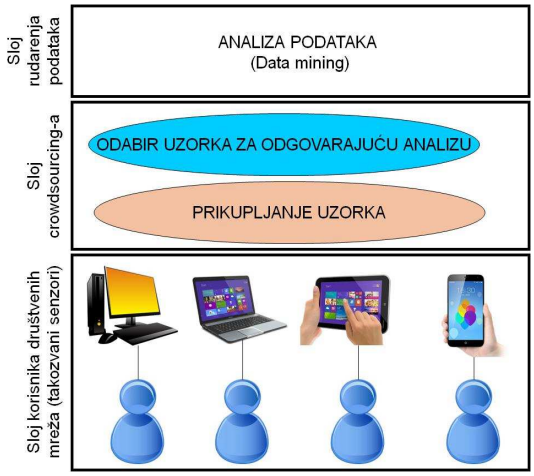
Jedan od načina da se sakupi velika količina podataka tokom vanredne situacije jeste i korišćenje velikog broja društvenih senzora, što se naziva "crowdsourcing". Od momenta sakupljanja podataka, pa do njihove analize, podaci prolaze kroz različite slojeve u "crowdsourcing"-u. Različiti slojevi su prikazani na Slici 2:

- **Sloj korisnika društvenih mreža.** Na ovom sloju se sakupljaju podaci koji se odnose na određeni događaj, odnosno na nastalu vanrednu situaciju. Na primer, ako korisnik postavi tvit o požaru koji se desio, tada ovaj tvit treba da bude sačuvan.
- **Sloj *crowdsourcing*-a.** Na ovom sloju se prikuplja uzorak koji je pogodan za analizu. Pošto se teži automatskom prikupljanju podataka, veoma je važno da su prikupljani podaci relevantni za događaj koji želimo da analiziramo.

Automatsko prikupljanje relevantnih podataka predstavlja jedan od izazova u ovom polju.

- **Sloj rudarenja podataka (engl. *data mining*).** Na ovom sloju se analiziraju relevantni podaci, upoređuju se, traže se različite korelacije i, što je najvažnije, iz njih se izvode zaključci relevantni za događaj koji se analizira.

Postoji nekoliko korisnih načina da se pristupi i obradi velika količina podataka direktno sa društvenih mreža koristeći Application Programming Interfaces (API). Međutim, svaka od društvenih mreža ima svoju strukturu podataka i način na koji koristi te iste podatke. Iako ovo otežava postavljanje standardnih procedura za prikupljanje i obradu podataka, podaci sa društvenih mreža sve su dostupniji i sve se više koriste u različite svrhe.



Slika 2: Hijerarhijski model podataka

Jednu od široko primenjenih tehnika za obradu podataka sa društvenih mreža sačinjava Natural Language Processing (NLP). NLP predstavlja disciplinu koja sakuplja i obrađuje prirodne jezike, što se u stvari odnosi na softverske i hardverske funkcije koje mogu da obrade i analiziraju govorni i pisani jezik. Termin „prirodni“ odnosi se na jezik koji ljudi svakodnevno koriste, a ne na programski jezik ili jezike matematičkih iskaza. NLP sa svojim metodama postaje sve razvijeniji i sofisticiraniji. Tendencija NLP-a je da se upotrebljava u protivterorističkim aktivnostima, prevashodno tokom ili odmah nakon samog napada. Tokom samog događaja korisnici na društvenim mrežama obično postavljaju mnogo sadržaja. NLP može da omogući relativno brzu obradu podataka koji se prikupe iz tih aktivnosti, a koji su korisni u kriznim situacijama za brze reakcije.

Još jedna od metoda za analizu podataka i korisnika na društvenim mrežama jeste analiza mreža (engl. *network analysis*). Ova metoda se često koristi kako bi ukazala na samu strukturu mreže i povezanost njenih korisnika, kao i za analizu

njihovog onlajn ponašanja. Međutim, postoji određena doza neusaglašenosti naučnika kod korišćenja ove metode u pogledu definisanja kako se relacije i povezanosti između korisnika mere i tumače. Analiza mreže se koristi često kao metoda kada se želi da se bolje razumeju informacije i odnosi unutar jedne onlajn zajednice, odnosno grupe.

Otkrivanje zločina

Većina radova koji su se bavili predviđanjem kriminalnih događaja zasnivala se na istorijskim dosijeima, geoprostornim informacijama i demografskim informacijama, ne uzimajući u obzir dostupne i brzo rastuće podatke društvenih mreža, na kojima se mogu pronaći mnogi slučajevi od interesa. Postoje inicijative koje analiziraju tvitove kako bi predvideli buduće kriminalne događaje.

Umesto analize velikog broja ključnih reči i analize osećanja (engl. *sentiment analysis*), koje nisu korisne za predviđanje diskretnih kriminalnih incidenata koji nisu ranije spomenuti, moguće je primeniti NLP tehnike kako bi se izvukli sadržaji semantičkih događaja tvitova. Identifikacija tema baziranih na nekom događaju korišćena je za predikciju kriminalnih incidenata. Primer ovakve analize je obrada specifične kategorije saobraćajnih nesreća u slučaju kada vozač pobegne sa mesta udesa (Wang, Gerber, & Brown, 2012).

Još jedno istraživanje koje je vredno spomenuti u predikciji kriminalnih događaja upotrebom podataka društvenih mreža ispitalo je niz 25 zločina, uključujući prostituciju, štetu nastalu krivičnim delom i provalu. Istraživanje je utvrdilo da se, ako se uključe i podaci sa Twitter-a u uobičajenom modelu predviđanja zločina (kernel density estimation), tačnost predviđanja 19 zločina može poboljšati (Gerber, 2014).

Prikupljanje podataka sa društvenih mreža

Moguće je ručno prikupljanje podataka sa društvenih mreža različitim metodama, kao što su: kopiranje, hvatanje beležaka, slikanje pojedinačnih stranica i čuvanje veb-stranica. Međutim, ovaj način prikupljanja podataka nije praktičan kada se radi o velikoj količini podataka i podesnije je korišćenje neke automatizovane metode. Ovo se najčešće radi konekcijom na društvenu mrežu koristeći API.

Neki API mogu da prikupe starije podatke koji su stari nekoliko meseci ili godina, dok druge nude samo „svež“ sadržaj. S druge strane, postoje mreže koje isporučuju nasumično podatke, dok druge omogućavaju pristup samo podacima koje zahtevamo, na osnovu našeg postavljenog upita (engl. *query*). Upit se obično sastoji iz nekoliko ključnih reči, koje istraživač sâm precizira u zavisnosti od potrebnog sadržaja. Na primer, ako želimo da pristupimo podacima s Twitter-a u vezi sa napadom u Parizu, prvo bismo pokušali sa ključnim rečima “Paris attack”.

U načelu, većina API-ja društvenih mreža omogućava da se preuzmu strukturirani podaci u velikim količinama. Facebook i Twitter, pored podataka, prosle-

đuju i metapodatke, uključujući informacije o korisniku, njihovim prijateljima (ili pratiocima) i profilu. Metapodaci su veoma koristan izvor informacija, s obzirom na to da često sadrže informacije koje olakšavaju karakterizaciju korisnika (na primer, obaveštenja o uređaju koji koristi korisnik, lokaciju korisnika, datum kreiranja naloga i slične podatke).

Kako bi se započelo sakupljanje podataka, često se kreira korisnički interfejs koji je projektovan tako da u svojoj pozadini koristi API. Na taj način korisnik može da pošalje zahtev za prikupljanje podataka, koji se obično šalju kao serija HTTP-zahteva. Twitter ima dva često korišćena API-ja, koji omogućavaju prikupljanje tvitova na osnovu postavljenog upita:

- *streaming API* – pristup globalnim Twitter-podacima sa kašnjenjem;
- *search API* – ograničena količina podataka iz arhive; često daje podatke jednu nedelju unazad. "Search" API se zasniva na relevantnosti, a ne kompletnosti, što znači da neki tvitovi i korisnici mogu izostati iz ovog uzorka.

Treba napomenuti da ovo nisu jedini API-ji koje koristi Twitter, pošto Twitter ima veću ponudu API-ja kako bi omogućio efikasnije i preciznije prikupljanje podataka u različitim situacijama. Međutim, većina ovih API-ja ograničena je sa količinom podataka koji mogu da se prikupe. Javni nalozi obično mogu da prikupe oko 1% od ukupnih dnevnih tvitova, dok komercijalni nalozi, kao što su oni koji koriste "decahose" Gnip Twitter platform, mogu da pribave 10% dnevnih tvitova i "full firehose" Gnip Twitter API-i, koji mogu da sakupe 100% tvitova. Kada uzmemo u obzir da dnevno ima preko 500 miliona tvitova, što je često 350.000 tvitova u minutu, ova ograničenja često ne predstavljaju problem da bi se prikupio adekvatan uzorak.

Svaki od Twitter API-ja nude različite medapodatke, koji su često mnogo duži od samog sadržaja tvit-poruke, uključujući lokaciju autora (geografska širina i dužina) kada je dostupna, kao i lokaciju korisničkog profila u tekstualnoj formi, vremensku zonu, broj pratilaca koje korisnik ima, broj tvitova koje je korisnik postavio, datum postavljanja tvita, korisnikov URL, datum kreiranja Twitter-naloga i druge informacije. U zavisnosti od naloga, u prikupljenim metapodacima tvita može biti više od 30 stavki. Tokom godina se menjao način na koji je Twitter omogućavao pristup podacima. Izmene API pristupa Twitter-mreži postavljaju se na Twitter-ov blog za programere.

Loše strane društvenog računarstva

Dok se društveno računarstvo i društvene mreže mogu koristiti za brzo reagovanje u vanrednim situacijama, slične metode se mogu koristiti i u negativne svrhe, te je važno i njih pomenuti kao nusprodukt. Jednostavno rečeno, teroristi imaju dobar razlog da koriste društvene mreže. Društvene mreže omogućavaju teroristima da koriste strategiju „sužavanja" (engl. *narrowcasting*). Ova strategija omogućava da se na osnovu demografskih atributa ili drugih karakteristika suzi ciljna grupa kojoj se plasiraju određene informacije.

Ekstremističke i terorističke grupe već dugo koriste internet u razne svrhe, uključujući međusobnu komunikaciju i propagandu, razmenu tehničkih informacija, prikupljanje obaveštajnih podataka, za zapošljavanje, obuku, finansiranje i nabavku opreme. Međutim, sa brzim razvojem tehnologija i pojavom društvenih mreža njihovo korišćenje interneta se promenilo i razvilo. Ne samo što su ekstremističke grupe počele da koriste društvene mreže u svoje svrhe, nego su počele da kreiraju i postavljaju veliku količinu sadržaja na društvene mreže. Iako je propagandu terorističkog pokreta uvek kontrolisao sâm pokret, društvene mreže su omogućile individuama iz celog sveta da prave i dele ovaj sadržaj. Samim tim je porasla i količina dostupnog sadržaja vezanih za terorizam.

Većina ekstremističkih i terorističkih organizacija koristi društvene mreže u svoje svrhe: kao sredstvo za promovisanje grupe, ali i sredstvo koje olakšava njihovu neformalnu komunikaciju i druženje između članova; kao način širenja propagande ne samo među svojim pripadnicima, nego i među drugim onlajn zajednicama, posebno delimično radikalizovanim pojedincima, ekstremističkim simpatizerima, ljudima koji su podložni radikalizaciji i medijima (Bartlett & Reynolds, 2015).

Stav javnosti prema nadzoru na socijalnim mrežama

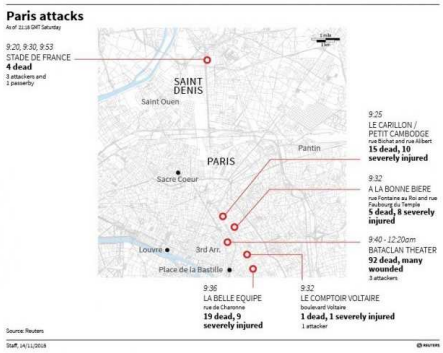
Javna briga o ličnim podacima i privatnosti delom je povećana pošto je Edward Snowden objavio zbirku dokumenata koji su razotkrili niz tajnih projekata za nadgledanje javnosti, ali i delimično zbog sve veće svesti o vrednosti ličnih podataka. Zbog povećane svesti javnosti može doći do promene načina na koji se koriste društvene mreže i oblika kako uopšte društvene mreže funkcionišu. Kompanije su odgovorile na zabrinutost javnosti na četiri načina:

- Korisnici društvenih mreža su počeli da se više brinu o svojoj privatnosti. Anketa koju je sproveo Ask Your Target Market 2013. godine, pokazala je da 46% korisnika društvenih mreža drži svoje naloge kao privatne, kako ih drugi korisnici ne bi mogli naći običnom pretragom interneta. Samo je 9% reklo kako bi nastavilo da koristi društvene mreže, ukoliko bi društvena mreža ugasila mogućnost privatnosti naloga, a 46% je reklo da u tom slučaju više ne bi koristili tu mrežu. Ispitivanje koje je sprovelo preduzeće Consumer Reports u SAD pokazalo je da je 37% korisnika podesilo koliko informacijâ može aplikacija na Facebook-u da vidi na njihovom nalogu.
- Društvene mreže primenjuju usluge enkripcije. Na primer, Facebook omogućava da se koriste tajne poruke, dok Apple i Google pružaju kompletnu enkripciju upotrebljavajući SSL.
- Internet-korisnici koriste sve više razne enkripcione metode, koje će se neizbežno koristiti i na društvenim mrežama. Anonimni veb-čitači, kao što je "Tor", koriste se za pretraživanje interneta bez odavanja lokacije korisnika. Tor ima preko 3 miliona korisnika, a društvene mreže polako dozvoljavaju pristup ovom veb-čitaču.

- Pojavljuju se novi tipovi društvenih mreža, kao što su "anti-Facebook", društvena mreža Ello, koja ne koristi reklame. Ovaj sajt navodi da su prikupljanje i prodaja ličnih podataka, čitanje korisničkih objava i mapiranje društvenih povezanosti sa prijateljima radi profita kako jezivi tako i neetični. Rast društvenih mreža i softvera koji vode računa o enkripciji i privatnosti sve je veći.

Studija slučaja: Napad u Parizu – analiza haštagova

Teroristički napad u Parizu odigrao se 13. novembra 2015. U periodu od 21.20 do 21.53 h, napad se odigrao na 6 lokacija (videti Sliku 3), od kojih sve imaju karakter „prometnog mesta" i obuhvatale su restorane, muzičku dvoranu i nacionalni fudbalski stadion.



Slika 3: Mesta i vreme odigravanja pojedinačnih napada u Parizu, 13. novembra 2015. Izvor: Reuters

Prateći Google-trendove na temu „Kako se u svetu pretraživao napad u Parizu?", dolazi se do podatka da se prva pretraga o ovom događaju desila u 21.21 h, i to sa lokacije na teritoriji Pariza (Google Trends 2015). Do 22.34 h, širom sveta, vest o ovom nemilom događaju munjevito se pronela. Jedna od najviše pretraživanih tema glasila je „Šta je *Pray for Paris*?", što je ujedno bio i najviše korišćen metapodatak u formi haštaga, tokom i nakon napada.

Haštagovi i njihov uticaj

Tokom noći 13. novembra i narednih dana[1] nekoliko haštagova je korišćeno na Twitter-u sa ciljem da se ukaže na opasnost, ponudi pomoć, pošalje podrška žrtvama i njihovim porodicama itd (Vukmirović & Raspopović Milić, 2016). Prvi od navedenih haštagova bio je #fusillades, što predstavlja reč na francuskom jeziku

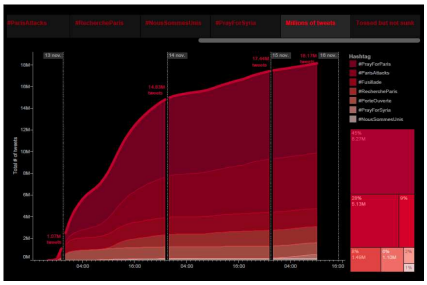
[1] Obuhvata period od 13. novembra 2015. oko 21 h do 16. novembra iste godine u 12 h.

koja u prevodu znači pucnjava. Broj tvitova sa ovim haštagom dostigao je svoj maksimum oko 23 h. Sledeći haštag koji je korišćen u najvećem broju tvitova bio je #PrayForParis, što u prevodu znači „moli se za Pariz". Koristili su ga ljudi[1] širom sveta u nameri da iskažu kako su u svojim mislima i molitvama sa tragedijom koja se dogodila. Treći haštag bio je #PorteOuverte, što na fracuskom znači „otvorena vrata". Ovaj metapodatak imao je cilj da skrene pažnju na ljude (i lokacije) koji su tokom napada, odnosno tokom noći kada se odigrao napad, nudili smeštaj ljudima koji su se u to vreme našli na mestima napada, odnosno na ulici.

Četvrti haštag bio je #ParisAttack, odnosno „napad na Pariz". Korisnici društvenih mreža su ga uglavnom upotrebljavali za praćenje i plasiranje novih informacija o napadu. Svoje dijagramske maksimume dostigao je dva puta, i to prvi put oko 1.00 h 14. novembra 2015, a drugi put oko 18.00 h 15. novembra 2015, kada se pojavila iznenadna panika tokom protestnog marša na Trgu Republike.

Tvitovi sa haštagom #RechercheParis, što u prevodu znači „pronađi Pariz", imali su svrhu da pomognu ljudima koji su nakon napada tražili svoje rođake i prijatelje. Šesti i konačni haštag koji se pojavio tokom noći i narednih dana otkada se odigrao napad bio je #NousSommesUnis („Mi smo ujedinjeni"). Imao je cilj da skrene pažnju na tvitove podrške građana širom Francuske koji su se okupljali u svojim gradovima na šetnjama solidarnosti sa građanima Pariza.

Posmatrano u odnosu na vremenski interval, koji je obuhvatio 63 časa praćenja komunikacije putem društvene mreže Twitter, zabeleženo je da je 18,17 miliona tvitova objavljeno sa nekim od navedenih haštagova. Posmatrajući ukupan broj pojedinačnih tvitova, najbrojniji su bili tvitovi sa #PrayForParis (8.27 M), a za njim i #ParisAttack (5.13 M), #fusillade (1.66 M), #RechercheParis (1.49 M), #PorteOuverte (1.10 M) i, na kraju, #NousSommesUnis (0.18 M). Pored navedenog, neophodno je ukazati i na činjenicu da je samo u periodu trajanja napada objavljeno 1,7 miliona tvitova koji su sadržali neki od navedenih haštagova.



Slika 4: Broj tvitova i njihova distribucija posmatrana u odnosu na pojedinačne haštagove (Trajkovic 2015)

Ako se posmatraju uticaj navedenih haštagova i njegovi ključni nosioci, analiza pomoću platforme *hashtagify.me* pokazala je da su najveći uticaj na širenje

[1] Neki novinari su ih nazivali „posmatračima".

tvitova sa #PrayForParis vršile popularne javne ličnosti, poput Džastina Bibera, Kejti Peri, Kendal Džener i Džastina Timberlejka. Haštag #Fusillades najviše su upotrebljavali francuski elektronski mediji, poput *Le Figaro*-a, radio-voditelja Jeremstar i Francuske novinarske agencije. Imajući u vidu ozbiljnost sadržaja koji su koristili metapodatak #RechercherParis, ne iznenađuje činjenica da su najuticajniji za njihovo širenje bili mediji poput CNN-a, novina *Le Monde* i *Le Figaro*, kao i portal SOS Paris. Treba spomenuti i da su najuticajniji u bodrenju građana da se hrabro suoče sa onim što se desilo, kao i u podršci porodicama i prijateljima žrtava, bili pariska gradonačelnica An Idalgo, francuska televizija TF1, francuski nacionalni fudbalski tim i njihov igrač Karim Benzema, kao i zvaničan tviter-nalog Republike Francuske.

Pored tvitova sa haštagovima koji su se pojavili tokom i neposredno nakon tragičnog događaja, dva meseca kasnije, a usled opšte atmosfere koja je vladala na ulicama Pariza, kružili su i tvitovi koji su imali cilj da pozovu ljude da izađu izvan stana i vrate se svojim redovnim aktivnostima i navikama. U nastojanju da se podigne moral, poveća odlučnost za odlazak na koncerte, vrate ljudi u bašte kafea i restorana, te na taj način izbegnu strah od napuštanja kuće, javili su se haštagovi poput #resiste (koji je dobio – osim svog osnovnog, „izdrži“ – i novo značenje u vidu „ne boj se da izađeš napolje i popiješ piće“), praćen s #JeSuisEnTerrasse („Ja sam u bašti / na terasi“) i #TousAuBistro („Svi u bar“) – ovi poslednji uglavnom kreirani od strane vlasnika ugostiteljskih objekata. Međutim, imajući u vidu atmosferu u kojoj su vladali strah i tuga, ovaj način delovanja na društvenim mrežama takođe se može posmatrati kao neka vrsta doprinosa u smanjenju posledica terorističkog napada.

Zaključak

Društveno računarstvo predstavlja oblast koja podrazumeva prikupljanje podataka o svim aktivnostima korisnika na društvenim mrežama, kao i obradu i analizu tih podataka. Glavne izazove društvenog računarstva predstavljaju automatizovano prikupljanje adekvatnog uzorka za analizu, kao i efikasna obrada i tumačenje podataka u realnom vremenu, radi pravovremenog donošenja odluka i pravljenja plana aktivnosti. U radu su navedeni neki od primera primene društvenog računarstva u detekciji kriminala i reagovanju u vanrednim situacijama.

Iako predikcija događaja korišćenjem podataka sa društvenih mreža nije savršena metoda, ona ipak pruža dodatnu vrednost već ustaljenim standardnim metodama. Takođe, korišćenje informacija (sa) društvenih mreža tokom vanredne situacija može da olakša brz i efikasan prenos informacija velikoj grupi ljudi. Pored pomenutih dobrih strana društvenog računarstva i društvenih mreža, rad je pružio osvrt i na loše strane društvenog računarstva, gde su, pored aktivnosti ekstremističkih i terorističkih grupa, spomenuti i zabrinutost javnosti o zloupotrebi ličnih podataka i privatnosti na društvenim mrežama.

U skladu sa navedenim, oblast društvenog računarstva može biti od velikog značaja za unapređenje bezbednosti otvorenih javnih gradskih prostora. Sa jedne strane, imajući u vidu da se i teroristi služe društvenim mrežama u širenju poruka i inspirisanju napadâ, ona može služiti za detektovanje takvog ponašanja i

eventualno uklanjanje pretnje i sprečevanja napada. Na drugoj strani, društveno računarstvo može biti od velike koristi prilikom samog napada i nakon njega, kako bi se smanjili njegovi efekti – tokom napada kao medijum kojim se ostvaruje poziv u pomoć i lociranje kriznih mesta, a kasnije za jačanje morala i smanjenje opšteg straha od boravka u otvorenim javnim prostorima.

Literatura

1. Bartlett, J., & Reynolds, L. (2015). *The State of the Art 2015: A Literature Review of Social Media Intelligence Capabilities for Counter-terrorism.* London: Demos.
2. Bazik, D. (2008). *Relacijski prostor grada: projekat_tekst_realizacija.* Beograd: Univerzitet u Beogradu – Arhitektonski fakultet.
3. Bazik, D., & Vukmirović, M. (2006). *Oblikovanje otvorenih javnih gradskih prostora.* Lična karta predmeta. Belgrade: University of Belgrade – Faculty of Architecture.
4. CNN. (2017, Avg 17). *Terrorist Attacks by Vehicle Fast Facts*. Retrieved Avg 18, 2017, from CNN: https://amp.cnn.com/cnn/2017/05/03/world/terrorist-attacks-by-vehicle-fast-facts/index.html
5. Coaffee, J., O'Hare, P., & Hawkesworth, M. (2009). 'The visibility of (in)security: The aesthetics of urban defences against terrorism'. *Security Dialogue*, *40* (4–5), 489–511.
6. Crooks, A., Croitoru, A., Stefanidis, A., & Radzikowski, J. (2013). "#Earthquake: Twitter as a distributed sensor system". Transactions in GIS, Vo.17 Iss. 1, Wiley Online Library,124–147.
7. De Longueville, B., Smith, R., & Luraschi, G. (2009). Omg, from here, i can see the flames!: a use case of mining location based social networks to acquire spatio-temporal data on forest fires. *Proceedings of the 2009 international workshop on location based social networks* (pp. 73–80). ACM.
8. Džejkobs, D. (2011). *Smrt i život velikih američkih gradova.* (M. Janković, Trans.) Novi Sad: Mediterran Publishing.
9. Gehl, J. (2010). *Cities for People.* Copenhagen: Gehl Architects.
10. Gerber, M. S. (2014). Predicting crime using Twitter and kernel density estimation. *Decision Support Systems*, 115–125.
11. Google Trends. (2015). *How the world searched for Paris attacks.* Retrieved January 10, 2016, from https://googletrends.github.io/parisattacks/
12. Home Office in partnership with the Department for Communities and Local Government. (2012). *Crowded Places: The Planning System and Counter-Terrorism*. London: Home Office.
13. Harvey, D. *Spaces of Hope.* Berkeley: University of California Press, 2000.
14. Jacobs, J. *The death and life of great American cities.* New York: Peregrin, 1961.
15. Kilcullen, D. (2015, Jan 17). *New terror paradigm after Charlie Hebdo raids.* Retrieved July 10, 2016, from The Australian: http://www.theaustralian.com.au/in-depth/terror/new-terror-paradigm-after-charlie-hebdo-raids/news-story/ac0dd5f5a7f-387b4d0140180d351b14e
16. Krishnamurthy, V., & Poor, V. H. (2014). A tutorial on interactive sensing in social networks. *IEEE Transactions on Computational Social Systems*, 3–21.
17. Leykin, Dmitry, Limor Aharonson-Daniel, and Mooli Lahad. "Leveraging social computing for personalized crisis communication using social media." *PLoS currents* 8 (2016).
18. Muggah, R. (2016, January 17). *Is Urban Terrorism the New Normal? Probably.* Retrieved February 10, 2016 from World Economic Forim. Davos: http://www.weforum.org/agenda/2016/01/is-urban-terrorism-is-the-new-normal-probably

19. Project for Public Spaces. (2008, Jan 1). *Safety & Security in Public Space*. Retrieved Apr 10, 2017, from Project for Public Spaces: https://www.pps.org/reference/safetysecurity/
20. Royal Institute of British Architects (2010). *RIBA Guidance on Designing on Counter-terrorism*. London.
21. Sakaki, T., Okazaki, M., & Matsuo, Y. (2013). Tweet analysis for real-time event detection and earthquake reporting system development. Transactions on Knowledge And Data Engineering Vol 25 No 4, 919–931.
22. Sullivan, J. P., & Elkins, A. (2015). Urban Siege in Paris: A Spectrum of Armed Assault. *Small War Journals*.
23. Trajkovic, J. (2015, November 16). *Analysis of Twitter Hashtags Following the Paris Attack*. Retrieved January 30, 2016, from Tips & Viz: http://tipsandviz.blogspot.fr/2015/11/parisattacks-how-twitter-tells-story.html
24. Trajković, J. (2015, Nov 16). *Analysis of Twitter Hashtags Following the Paris Attack*. Retrieved Jan 30, 2016, from Tips and Viz: http://tipsandviz.blogspot.fr/2015/11/parisattacks-how-twitter-tells-story.html
25. Trusov, M., Bodapati, A. V., & Bucklin, R. E. (2010). Determining influential users in internet social networks. Journal of Marketing Resarch, 47(4), 643–658.
26. Vidanović, I. (2006). *Rečnik socijalnog rada*. Beograd: Autorsko izdanje.
27. Vukmirović, M. (2017). The role of urban design and strengthening social inclusiveness in the prevention of the terrorist attacks and related crises. In S. Stanarević, I. Đorđević, & V. Rokvić (Ed.), *3rd International Conference on Human Security* (pp. 99–113). Belgrade: University of Belgrade – Faculty of Security Studies and Human Research Center.
28. Vukmirović, M., & Raspopović Milić, M. (2016). Vulnerability of Public Space and the Role of Social Networks in Crisis. *Proceedings of the 3rd International Academic Conference on Places and Technologies* (pp. 769–779). Belgrade: University of Belgrade – Faculty of Architecture.
29. Wang, X., Gerber, M., & Brown, D. (2012). Automatic Crime Prediction Using Events Extracted from Twitter Posts. *SPB*, 231–238.
30. Watts, C. (2015, Jan 12). *Inspired, Networked, and Directed: The Muddled Jihad of ISIS and Al-Qaeda Post-Hebdo*. Retrieved Jul 10, 2016, from War on the Rocks: http://warontherocks.com/2015/01/inspired-networked-directed-the-muddled-jihad-of-isis-al-qaeda-post-hebdo/?singlepage=1
31. Xu, Zheng, et al. "Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media." *EURASIP Journal on Wireless Communications and Networking* 2016.1 (2016): 1–9.

INCREASING SECURITY IN OPEN URBAN PUBLIC SPACES BY THE APPLICATION OF ICT AND SOCIAL COMPUTING

Summary

Security is considered a basic criterion of the quality of open public spaces and a prerequisite for achieving the other criteria, such as comfort, attractiveness and vitality. In order to achieve the above criteria, different strategies in the field of the design of open public spaces have been applied. They mainly include wise and long-term interventions which result in social inclusion and cohesion. On the other hand, open public spaces become visible, accessible, democratic and, above all, due to the presence of people, provide a natural

form of control. Almost simultaneously with the re-development and increasing the importance of open public spaces, there are contemporary tools of communication that have opened up various possibilities both for ways to use open public spaces, and how to achieve security. With the development of information communication technologies (ICT) such as cloud computing, IoT (Internet of Things) and big data analysis, ICT applications have been rapidly developed as well. One of the well-known ICT applications are social networks, which represent one type of technology that is still evolving. Social networks provide means for better Internet usage for creating, sharing and participating in sharing of information about oneself and others, about what one likes or dislikes, about one's travels, thoughts and transactions. On the one hand, sharing the information provides opportunity to create new applications and their possibilities, while on the other, results of analysis of all shared data of one or more users on social networks can be used inadequately. Social computing represents new area of research for information systems. Social computing represents data collection containing all user activities on the network, so that this data can be processed for the purpose of online behaviour analysis of one or more users in their natural environment, as well as in the controlled experimental scenarios. Online profiling uses chronology of user behaviour on the network for the purpose of predicting user's future behaviour and his/her preferences for the specific web applications such as targeted online marketing, content personalization and social recommendations. During a crisis situation, extraction of the precise information and conclusions from large data set on social network users is very important for modern communications. Social networks represent a platform that can be used for data collection, effective data sharing and information extraction. Keeping in mind that users on social networks consciously or subconsciously provide a lot of data about themselves and their behavioural tendencies, this information is referred to as "volunteered information." Using information from social networks in a crisis situation can be classified in three categories: (i) information spreading, (ii) geolocation information, (iii) semantic analysis. Information spreading through social networks can improve timely awareness raising in a crisis situation, since information can be spread to a wide group of people fast and effectively. The geolocation information of social media also has important role in detecting emergencies and in giving a quick response. Semantic analysis on social network messages, such as tweets on Twitter, can help in extracting information on damages, necessary assistance, casualties or receiving assistance during crisis. While social computing and social networks can be used for quick response in crisis, they can also be used for negative purposes, so it is important to address them as by-products. Simply put, terrorists have a good reason to use social media. Social networks provide terrorists with the opportunity to use narrowcasting. This method provides means to narrow down the target group for placement of specific information based on their demographic attributes or other characteristics. This work gives an overview of how social network information can be used for (i) managing a crisis situation and (ii) for online profiling. The focus of this paper is on presentation of specific and state of the art methods, their possibilities and conclusions that can be extracted based on the collected data from social networks, as well as ethical and legal questions that can arise. These methods are of importance as they can help preserve safety in public spaces by preventing terrorism and by protecting users of public spaces. This paper also considers in which way and how much stated goals can be achieved using existing technologies, keeping in mind the public attitude towards their surveillance on social networks. Accordingly, the paper offers and overview of different possibilities and tools provided by information communication technologies, with the focus on social computing and social networks that can contribute to achieving and increasing the security of open public spaces.

Keywords: *security, open public spaces, social computing, ICT*