MOŽNOSTI NAPOVEDOVANJA MNOŽIČNIH KAZNIVIH DEJANJ (MNOŽIČNIH UMOROV, TERORISTIČNIH NAPADOV)

Peter Umek in Jure Mertük

Namen prispevka

Prispevek obravnava teroriste samotarje (Lone Wolf), ki jih je težko odkriti in ravno zaradi tega predstavljajo nevarnost za družbo in posledično za varnostne organe. Glaven namen prispevka je predstaviti možnosti odkrivanja teroristov samotarjev na podlagi digitalnih sledi, ki jih posamezniki z svojim udejstvovanjem puščajo na svetovnem spletu. Tako je v prispevku podrobneje predstavljen celoten proces mogočega odkrivanja potencialno nevarnih posameznikov s pomočjo svetovnega spleta.

Metode

Za potrebe prispevka smo pregledali in analizirali vsebino domačih in tujih pisnih in elektronskih virov. Uporabljena je bila deskriptivna metoda in konceptualna analiza, s katero smo si pomagali pri opredelitvi pomena nekaterih pojmov.

Ugotovitve

Na to temo obstaja veliko tuje literature, kar pomeni, da se po svetu zavedajo nevarnosti, ki jo tako imenovani »Lone Wolf« teroristi oz. teroristi samotarji predstavljajo za družbo. Tako so nekatere države že izoblikovale učinkovite načine odkrivanja teh posameznikov s pomočjo iskanja digitalnih sledi na svetovnem spletu. Dejstvo je, da gre za zelo nepredvidljivo obliko terorizma, za katero je težko napovedati kje in kdaj se bo pojavil, saj teroristi samotarji pripadajo različnim ideologijam, rasam in veram. Kljub temu ugotavljamo, da obstajajo načini odkrivanja posameznikov na podlagi digitalnih sledi na internetu.

Omejitve

Pri pregledu in analizi vsebine pisnih in elektronskih virov smo bili omejeni na uporabo javno dostopnih virov.

Izvirnost/pomembnost prispevka

Prispevek je pomemben predvsem z vidika ozaveščanja oz. opozarjanja na morebitno nevarnost, ki jo predstavljajo teroristi samotarji, pa čeprav živimo v prepričanju, da se kaj takšnega v našem okolju ne more pripetiti. Pomembnost članka pa se kaže tudi z vidika prikaza načina odkrivanja potencialno

nevarnih posameznikov in morebitna implementacija (vzpostavitev) takšnega sistema odkrivanja v naš sistem varnosti.

Ključne besede: teroristi samotarji, svetovni splet, digitalne sledi, spletni pajek, plazenje.

1 UVOD

Terorizem je v današnjem času pogost pojav. Gre za dogodke, ki v družbi povzročajo strah in negotovost, države pa ne morejo zagotavljati varnosti pred različnimi terorističnimi dejanji. Kljub temu, da ne gre za nove pojave, pa jim je posebna pozornost namenjena od l. 2001 oz. od odmevnega napada na World Trade Center v New Yorku. Vse od takrat lahko v medijih redno spremljamo novice o takšnih in drugačnih terorističnih napadih ali morilskih pohodih v različnih krajih sveta. Medtem ko smo bili v preteklosti mnenja, da se kaj takšnega v Evropi ne more zgoditi, pa smo se v zadnjih letih lahko prepričali, da temu ni več tako. Da terorizem predstavlja resno grožnjo tudi na evropskih tleh, pričajo teroristični napadi na javna prevozna sredstva v Londonu in Madridu, med teroristi samotarji pa izstopa predvsem morilski pohod na Norveškem, ki ga je izvedel Anders Behring Breivik. Pred leti so največjo nevarnost predstavljale teroristične organizacije, danes pa največjo grožnjo na področju varnosti predstavljajo tako imenovani »Lone Wolf« teroristi oz. teroristi samotarji. To so posamezniki, ki se iz takšnih ali drugačnih razlogov odločijo, da morajo vzeti stvari v svoje roke in v popolni anonimnosti načrtujejo maščevanje posameznikom in družbi. Razvoj terorizma in množičnih umorov pa seveda pomeni tudi to, da se morajo novim oblikam groženj prilagoditi tudi tisti, ki skrbijo za varnost v družbi. Nove oblike nevarnosti namreč silijo k prilagajanju, kar pomeni, da morajo strokovnjaki iz vseh področij zagotavljanja varnosti odkrivati nove načine, kako v prihodnosti odkrivati in preprečevati morebitna nova hujša kazniva dejanja, predvsem pa morajo v luči učinkovitega boja proti storilcem okrepiti medsebojno sodelovanje.

2 TERORISTI SAMOTARJI

V zadnjih letih se svet srečuje z novo obliko terorizma, in sicer z tako imenovanimi teroristi samotarji oz. »Lone Wolf« teroristi. Gre za eno izmed najbolj nepredvidljivih oblik terorizma, saj teroristi samotarji lahko pripadajo kateri koli ideologiji, veri ali rasi. Za njih je značilno tudi to, da delujejo sami, brez pomoči katere izmed terorističnih organizacij (Kaati in Svenson, 2011). Spaaij (v Nijboer, 2012) definira samotarski terorizem kot teroristične napade s strani posameznika, ki:

a) deluje samostojno,

b) ne pripada nobeni organizirani teroristični mreži ali skupini,
c) si sam izbere način delovanja brez sprejemanja in upoštevanja navodil s strani tretjih oseb.

Gre za posameznike, ki so se radikalizirali s pomočjo interneta, brez pomembnejšega vpliva drugih posameznikov ali skupin. Posamezniki sicer črpajo voljo in inspiracijo s strani terorističnih organizacij in skupin, vendar pa niso z njimi v nobenih stikih in z njihove strani ne sprejemajo nobenih navodil. Njihova dejanja so politično ali versko motivirana in jih posamezniki izvajajo z namenom vplivanja na javno mnenje ali z namenom vplivanja na sprejemanje političnih odločitev. Glavna značilnost teroristov samotarjev je, da delujejo sami, brez pomoči drugih in da gre za verjetno najbolj nepredvidljivo in zapleteno obliko terorizma (Bakker in de Graaf, 2010). Pantucci (2011) opisuje štiri tipe teroriste samotarje:

- *Samotar (Loner):* posameznik, ki načrtuje ali izvede teroristično dejanje pod pretvezo ekstremistične ideologije. Tak posameznik izkoristi ideologijo kot razlog za napad, ni pa v nikakršni povezavi ali stikih z ekstremistično skupino. Pri njih je težko oceniti, v kolikšni meri je določena ideologija prispevala k načrtovanju in izvedbi napada, ali pa je bila uporabljena zgolj kot izgovor z namenom prikrivanja psiholoških ali drugih težav posameznika.
- *Osamljeni volk (Lone Wolf):* posameznik, ki samostojno izvede teroristično dejanje, je pa povezan s člani teroristične skupine. Sami načrtujejo in izvajajo svoja dejanja, so pa pri tem predvsem s pomočjo interneta v stiku z drugimi ekstremisti.
- *Trop osamljenih volkov (Lone Wolf Pack):* gre za posameznike z lastnostmi predhodno omenjenih osamljenih volkov, združenih v skupino. Gre torej za manjšo skupino ideološko motiviranih posameznikov s podobnim načinom razmišljanja, ki se odloči izvesti teroristično dejanje. Čeprav ima ta skupina stike z večjimi terorističnimi skupinami (Al Kaida), ki v glavnem potekajo s pomočjo interneta, se zdi, da od njih ne sprejemajo nobenih navodil in usmeritev.
- *Osamljeni napadalec (Lone Attacker):* v to skupino spadajo posamezniki, ki delujejo samostojno, njihova dejanja usmerja Al Kaid ali druge teroristične organizacije. Ti posamezniki so torej v neprestanem stiku z drugimi ekstremističnimi skupinami in posamezniki, kar jih razlikuje od osamljenih volkov, kjer sodelovanje z drugimi ekstremisti predstavlja zgolj šibka internetna komunikacija.

3 MOŽNOSTI ODKRIVANJA POTENCIALNIH TERORISTOV (MORILCEV) SAMOTARJEV

Ena od številnih nalog, s katerimi se soočajo organi pregona in obveščevalne službe, je iskanje in identifikacija nasilnih skrajnežev, da bi tako preprečili povzročanje škode družbi. Pri tem se poleg uporabe tradicionalnih metod, kot je infiltriranje posameznika v neko skupino ali prisluškovanje, vedno pogosteje uporabljajo tudi metode odkrivanja skrajnežev na svetovnem spletu oz. internetu. Veliko ekstremističnih in terorističnih skupin namreč uporablja internet kot orodje za vodenje in organizacijo delovanja neke skupine. Tako se s pomočjo interneta rekrutirajo novi člani, pridobivajo se finančna sredstva za delovanje skupine, objavlja se literaturo, povezano z delovanjem skupine, izmenjujejo se mnenja in posledično krepi njihova prepričanja ipd. Zaradi tega predstavlja spremljanje in analiza internetnih vsebin pomembno nalogo obveščevalnih služb, saj bi lahko tako v prihodnosti lažje odkrivali posameznike ali skupine, ki so za uresničitev svojih ali nekih višjih ciljev pripravljeni škodovati družbi.

3.1 Zbiranje in analiza šibkih signalov za potrebe odkrivanja teroristov samotarjev

Eno izmed najbolj nepredvidljivih in nevarnih oblik terorizma predstavljajo teroristi samotarji. Gre za dokaj novo obliko grožnje, kar posledično pomeni, da so zmožnosti odkrivanja in preprečevanja teh terorističnih napadov omejene, saj je njihovo odkrivanje z tradicionalnimi metodami skoraj nemogoče. Po mnenju številnih strokovnjakov se problem teroristov samotarjev povečuje in trenutno predstavlja družbi večjo nevarnost kot organizirane teroristične skupine. Razpoložljivi statistični podatki kažejo, da so teroristi samotarji odgovorni za manjše število terorističnih napadov kot organizirane skupine, vendar imajo s svojimi napadi veliko večji vpliv na družbo. Čeprav torej velja, da so tradicionalne metode odkrivanja pri teroristih samotarjih v glavnem neučinkovite, to še ne pomeni, da jih obveščevalne službe ne morejo odkriti. Večina teroristov samotarjev je aktivna na internetu, kjer sodelujejo na raznih forumih in so aktivni uporabniki socialnih omrežij. Na internetu brez težav širijo svoja prepričanja in z lahkoto dostopajo do različnih informacij in znanj, kar pa posledično pomeni, da tam tudi puščajo svoje sledi. Internet zato predstavlja pomemben vir pri iskanju potencialnih morilcev samotarjev, naloga varnostnih organov pa je, da te tako imenovane digitalne sledi oz. šibke signale zberejo, združijo, analizirajo in posledično odkrijejo nevarne posameznike (Brynielsson et al., 2013). Šibek znak oz. signal (indikator) je nekaj, kar samo po sebi še ne pomeni ničesar, vendar postane pomemben oz. močnejši v povezavi z drugimi signali. Npr. informacija, da je nekdo kupil strelno orožje, še ne pomeni nič posebnega, če ob tem nimamo na voljo nobenih drugih informacij. Če pa

podatek o strelnem orožju ni edini, in vemo, da je ta ista oseba kupila tudi velike količine amonijevega nitrata in poleg tega na internetu izražala svoja radikalna prepričanja, pa to pomeni, da je takšnemu posamezniku potrebno posvetiti dodatno pozornost (Dahlin, Johansson, Kaati, Martenson in Svenson, 2012).

Ena od glavnih težav pri analiziranju podatkov z interneta je, da gre za veliko količino podatkov, kar analitikom onemogoča, da bi sami zbrali in analizirali vse za njih pomembne informacije. Poleg podatkov, ki jih analitiki lahko najdejo z uporabo različnih internetnih iskalnikov, pa obstaja tudi ogromna količina podatkov, ki se nahaja v tako imenovanem globokem oz. nevidnem spletu, delu interneta, ki ni indeksiran in ga internetni iskalniki zaradi različnih razlogov ne zajamejo. Varnostni organi (obveščevalne službe) tako v zadnjem času veliko truda vlagajo v razvoj programov, ki bi omogočali spremljanje dogajanja v internetnem okolju. Dogajanje spremljajo z pomočjo analize vsebin na spletnih straneh, kjer računalniški programi iščejo za njih relevantne internetne vsebine. Kar se tiče programske opreme, ki bi bila v pomoč varnostnim organom, je treba omeniti, da razvoj popolnoma samostojnih oz. avtomatskih računalniških programov oz. orodij za iskanje podatkov ni možen, tako zaradi velike količine podatkov, kot zaradi poglobljenega znanja, ki je potrebno za resnično razumevanje stvari, ki se jih raziskuje. Dodati je potrebno, da ne gre zgolj za analizo pisanega besedila, ampak je potrebno pozornost nameniti tudi posnetkom in slikam. Ob vsem tem je potrebno opozoriti še na pasti, ki jih lahko prinašajo raziskave takšnih razsežnosti in s takšno programsko opremo. Preden se začne dejansko izvajanje takšnih raziskav, je potrebno postaviti jasna pravila delovanja, da bi se s tem čim bolj zaščitila zasebnost in integriteta državljanov. Že v začetku je torej potrebno vzpostaviti učinkovit nadzor, ki čim bolj omejuje možnosti zlorab. Še en problem pa predstavlja dejstvo, da je to, kaj nekdo dojema kot skrajno mnenje, različno od uporabnika do uporabnika (Brynielsson et al., 2013).

3.1.1 Digitalne sledi na internetu

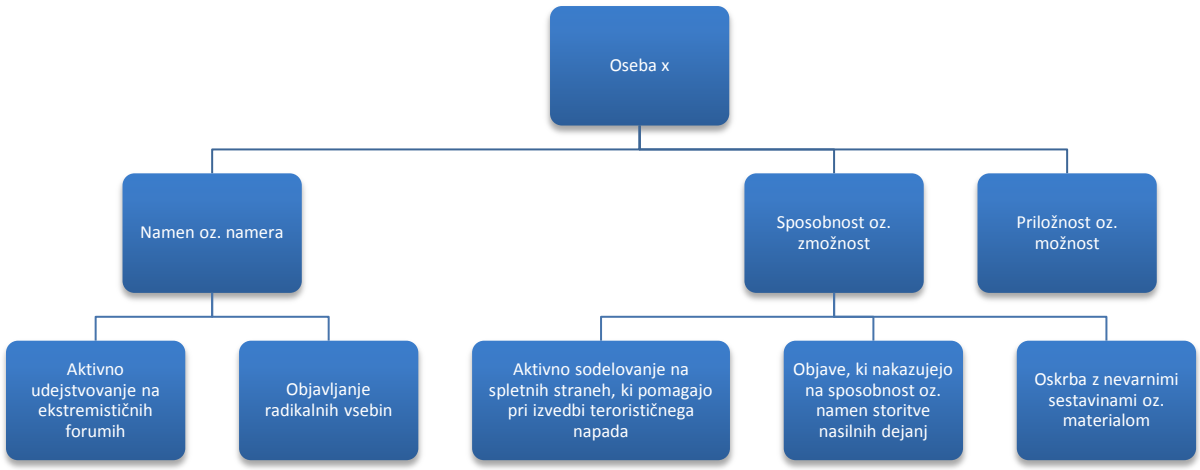
Teroriste samotarje je zelo težko odkrivati z običajnimi metodami, kot je infiltracija, na internetu pa je pogosto na voljo veliko šibkih signalov, ki lahko v primeru, da so odkriti in primerno analizirani, predstavljajo pomembno pomoč in vodilo pri odkrivanju sumljivega vedenja, ki ga je potrebno dodatno raziskati. Večina radikalizacije teroristov samotarjev namreč poteka na internetu, zato je internet ključen pri odkrivanju teh posameznikov. Ko pride do terorističnega napada, ni nič nenavadnega, da mediji začnejo z zbiranjem takšnih digitalnih sledi za nazaj in se potem kritizirajo neučinkovitost in pomanjkanje sposobnosti policije in obveščevalnih služb. Po storjenem terorističnem napadu je veliko lažje poiskati signale, saj so zadeve veliko bolj jasne in razumljive. Veliko težje pa je iskanje ustreznih sledi (šibkih signalov), še preden pride do izvedbe napada. Signali, ki jih je relativno

lahko odkriti, so npr. aktivno sodelovanje na ekstremističnih forumih in žaljivo oz. sovražno izražanje na spletnih straneh oz. forumih. Za lažje prepoznavanje znakov nasilnega vedenja je bilo predstavljenih nekaj vedenjskih znakov, ki jih je možno prepoznati v besedilih na internetu, in ki se lahko uporabijo kot kazalci pri prepoznavanju posameznikov, ki nameravajo izvesti teroristični napad. Vedenjski znaki so naslednji:

- *Razkritje:* komunikacija s tretjo osebo glede svojih namenov škodovanja drugim posameznikom ali skupinam oseb, kot so recimo objave številnih šolskih strelcev pred samo izvedbo napada.
- *Fiksacija:* patološka obsedenost z neko osebo ali stvarjo.
- *Identifikacija:* želja biti vpliven vzornik. Gre za identifikacijo z nekim posameznikom, skupino ali poslanstvom (Brynielsson et al., 2013).

3.2 Model analize

Kadar se soočimo z kompleksnimi problemi, jih je najlažje reševati tako, da jih razčlenimo na več manjših, bolj obvladljivih problemov. Ta pristop je primeren tudi za analizo šibkih internetnih signalov. Za vsakega potencialnega storilca, ki se skriva za enim ali več uporabniškimi imeni, se izvede tako imenovano razvijanje temeljnih hipotez na več manjših hipotez oz. pod-hipotez. Slika 1 prikazuje poenostavljen model raziskave, kjer se osnovna hipoteza glasi: »Oseba X je potencialni terorist samotar«. Na prvi stopnji se postavljeno hipotezo razdeli na tri splošne kriterije ocenjevanja nevarnosti: motiv oz. namen, sposobnost in priložnost. Če se v analizi izkaže, da so vsi trije kriteriji izpolnjeni, potem velja, da obstaja potencialno tveganje za napad. Naslednja stopnja razgradnje prikazuje različne kazalnike, ki se lahko odkrijejo preko opazovanja dogajanja in posameznikovega obnašanja na internetu. Ko opravimo začetno razčlenjevanje, lahko vzporedno začnemo z nadaljnjim procesom razčlenjevanja na različne podskupine hipotez. Rezultati različnih postopkov se nato združijo in uporabijo za oceno, kjer se ugotavlja, če pri katerem posamezniku obstaja povečana možnost za izvedbo terorističnega napada. Temu sledi izdelava seznama potencialno nevarnih posameznikov, ki se jim v nadaljevanju posveti dodatna pozornost analitikov (Brynielsson et al., 2013).

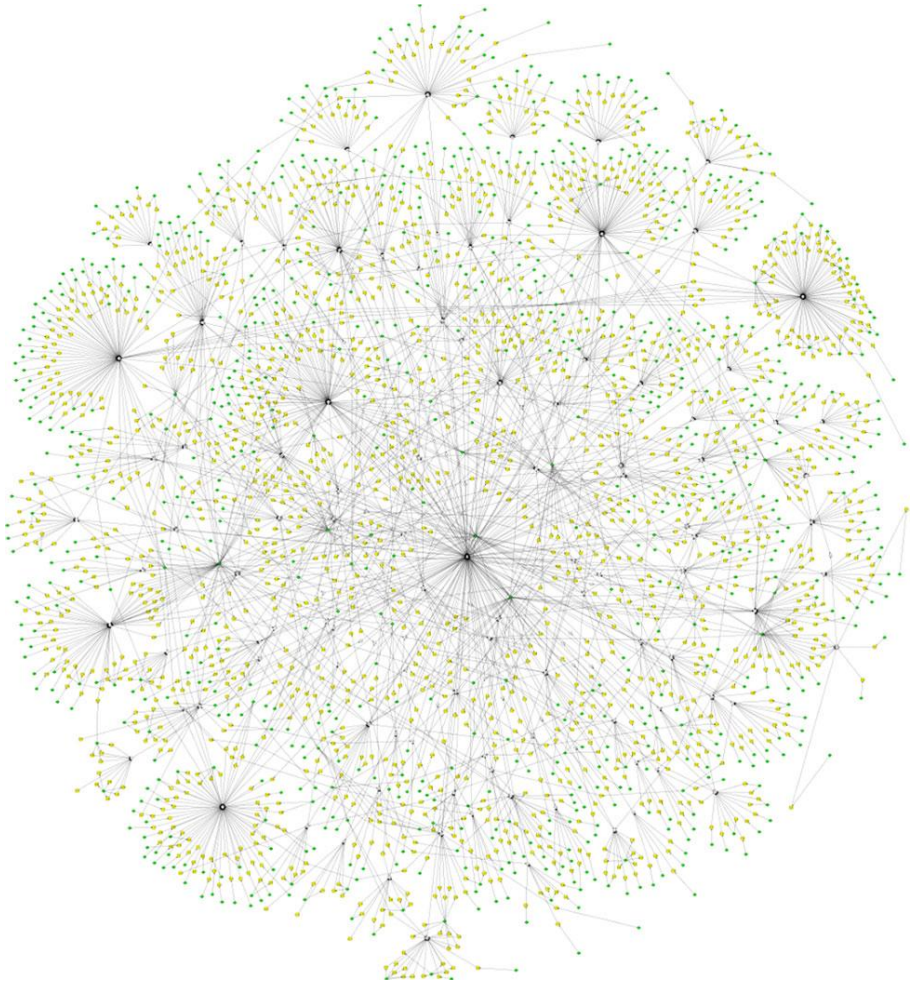


Slika 1: Pregled postavljanja in razvijanja hipotez v zvezi z potencialnim teroristom samotarjem (vir: Brynielsson et al., 2013).

3.3 Identifikacija izhodiščnih spletnih strani in filtrirano zbiranje podatkov

Ker je količina vsebine na internetu ogromna, nima iskanje digitalnih sledi potencialnih teroristov samotarjev brez kakršnih koli usmeritev nobenega smisla, kar pomeni, da je potrebno omejiti iskanje in se osredotočiti zgolj na najpomembnejše izsledke. Čeprav obstaja velik del spleta, ki ni dostopen preko internetnih iskalnikov, kot so Google in podobni, je vseeno večina ekstremističnih forumov dobro poznanih, saj je ideja sodelujočih na teh forumih, da njihova sporočila in ideje dosežejo čim večje število ljudi. Prav tako večina teh ekstremističnih internetnih strani vsebuje povezave do spletnih strani z podobno vsebino, kar pomeni, da je smiselno uporabiti te spletne strani kot izhodišče oz. začetno točko pri odkrivanju novih spletnih strani z podobno vsebino. Z analizo hiperpovezav na spletnih straneh je namreč mogoče odkriti veliko novih ekstremističnih forumov. Ta proces sistematičnega zbiranja spletnih strani s tako imenovanim spletnim pajkom se imenuje plazenje (crawling). Proces plazenja se začne z eno ali več določenimi spletnimi stranmi, ki predstavljajo vir, na katerem program išče hiperpovezave, da bi tako našel nove spletne strani. Proces plazenja se ponovi na vsaki spletni strani posebej in se nadaljuje dokler na neki strani ne zmanjka povezav do novih spletnih strani oz. se lahko proces konča tudi z najdbo predhodno določenega števila spletnih strani. Z obdelavo zbranih spletnih strani in analizo povezav med posameznimi spletnimi stranmi dobimo mrežo, iz katere lahko z nadaljnjo analizo ugotovimo, katere spletne strani so najbolj pomembne z vidika analize. S takšnim iskanjem zanimivih spletnih strani pa pride tudi do tega, da je veliko tako najdenih spletnih strani nepomembnih za obveščevalne analitike. Zato je v interesu analitikov, da računalniški program samodejno loči med za njih relevantnimi in irelevantnimi

spletnimi stranmi. Pri tem si pomagajo z analizo besedila, kar pomeni, da program v besedilih na spletnih straneh samodejno išče predhodno izbrane ključne besede. To pomeni, da če program na neki strani najde zadostno število ključnih besed, označi to stran kot pomembno, če pa se ključne besede ne pojavljajo v zadostnem obsegu, je spletna stran označena kot nepomembna, kar pomeni, da jo program zavrže in ne sledi povezavam iz takšne spletne strani. Prav tako pa analitiki tekom raziskave izločijo spletne strani, ki sicer izpolnjujejo pogoje o številu ključnih besed, vendar pa so z vidika nadaljnje raziskave kljub temu nepomembne oz. manj pomembne (spletne strani namenjene boju proti ekstremizmu). V analizi je najdenih tudi veliko spletnih strani, katerih vsebina je zaščitena z geslom. Takšno spletno stran se izloči, ali pa analitik opravi registracijo in tako ročno dostopa do vsebine na spletni strani. Opisan postopek iskanja spletnih strani je v mnogih pogledih podoben pristopu, ki se uporablja za odkrivanje otroške pornografije na spletu (Brynielsson et al., 2013). Na spletu lahko najdemo veliko programov, tako imenovanih spletnih pajkov, ki nam omogočajo iskanje spletnih strani. Na sliki 2 je prikazan primer uporabe spletnega pajka (Crawler4J) in končni rezultat takšnega iskanja. Mreža na sliki 2 prikazuje končni rezultat iskanja spletnih strani na podlagi enega samega semena oz. izhodiščne spletne strani. Vozlišča v mreži predstavljajo forume, objave in uporabniška imena.



Slika 2: Končni rezultat iskanja spletnih strani z spletnim pajkom (vir: Brynielsson et al., 2013)

3.4 Tehnike za analizo zbranih podatkov

Ko je zbiranje ustreznih podatkov iz interneta zaključeno, je potrebno zbrane podatke analizirati. V nadaljevanju bomo predstavili tehnike, ki jih lahko obveščevalni analitiki uporabijo za analizo zbranih podatkov, da bi tako odkrili kazalnike, ki kažejo, da ima neka oseba namen storiti teroristično dejanje. Primarni cilj tega postopka je pridobiti imena potencialnih teroristov samotarjev, katerim je v nadaljevanju raziskave potrebno posvetiti dodatno pozornost. Brynielsson in sodelavci (2013) v svojem prispevku o odkrivanju teroristov samotarjev uporabljajo nekoliko drugačen pristop od do sedaj znanih in opisanih postopkov drugih avtorjev. Pri tem pristopu je poudarek na teroristih samotarjih namesto na terorističnih organizacijah, zagovarjajo uporabo pol-avtomatiziranih orodij za podporo analitikom in ne v celoti avtomatiziranih orodij. Poleg tega, da je izdelava zanesljivih avtomatskih iskalnikov zelo težavna, obstajajo tudi kulturne in etične zahteve, zaradi katerih velja razmisliti o uporabi programskega orodja v povezavi s človeškim uporabnikom.
Ko torej zberemo za obdelavo zanimive spletne strani, sledi poglobljena analiza besedil na teh straneh. Uporabni sta predvsem dve metodi, in sicer obdelava naravnega jezika in rudarjenje besedil. Ena izmed oblik rudarjenja besedil je analiza čustev, kot koristna analiza za merjenje prisotnosti sovraštva in nasilja na ekstremističnih forumih. Opredeljenih je niz kazalnikov, ki lahko pomenijo, da ima neka oseba naklep, da stori teroristično dejanje oz. da postane terorist samotar. Seznam kazalnikov ni popoln in služi zgolj za ponazoritev, kako je mogoče z tehnikami analize besedil samodejno zaznati nekatere izmed njih. Kazalniki, ki jih uporabljamo, so:

- posameznikova aktivnost na radikalnih spletnih straneh,
- radikalno izražanje v objavah,
- razkritje,
- fiksacija oz. obsedenost,
- identifikacija.

3.4.1 Posameznikova aktivnost na radikalnih spletnih straneh

Za vse, v procesu tako imenovanega plazenja, zbrane spletne strani se predvideva, da so radikalne spletne strani, kar posledično pomeni, da so takšni tudi njeni uporabniki. Obstajajo pa tudi izjeme, kar pomeni, da obstajajo posamezniki, ki objavljajo stvari na ekstremističnih straneh, vendar sami niso ekstremisti. V takih primerih obstaja velika verjetnost, da pri posamezniku ne bodo prisotni tudi drugi kazalniki, zato se ga izloči iz nadaljnje analize (Brynielsson et al., 2013).

3.4.2 Radikalno izražanje v objavah

Gre za ocenjevanje oz. merjenje stopnje radikalnih besed v besedilu izbrane spletne strani. Pred samo analizo se sestavi seznam besed, ki jih program potem prepoznava oz. išče. Na podlagi prisotnosti teh besed v besedilu se označi spletne strani kot radikalne ali ne-radikalne oz. kot zanimive oz. nezanimive za nadaljnjo raziskavo. Večji kot je delež predhodno izbranih besed v besedilu, višja je raven zanimivosti takšne spletne strani za obveščevalce. Slabost takšnega načina merjenja radikalnosti spletnih strani je, da je potrebno seznam besed vedno znova dopolnjevati, saj se izrazi za izražanje ekstremističnih mnenj sčasoma lahko spremenijo (Brynielsson et al., 2013).

3.4.3 Razkritje

Oseba v pogovoru tretjo osebo namerno ali nenamerno obvesti o svojih namerah. Pomembna značilnost velike večine teroristov samotarjev je, da že vnaprej razglašajo oz. sporočajo svoje poglede in namere. Tako je analiza strelcev v šolah pokazala, da je večina storilcev svoje namere še pred izvedbo napada razkrila oz. napovedala na socialnih omrežjih. V izdanih podatkih o posameznikovi nameri se skupaj z besedami, ki izražajo nasilna dejanja, nahajajo tudi pomožni glagoli, ki izražajo posameznikov namen (npr. bom, grem, bi moral). Razkritje bi zato lahko odkrivali na enostaven način, kjer se po opravljenem procesu lematizacije[1] v analiziranem besedilu iščejo predhodno določene besede, ki označujejo nasilna dejanja. Se pa ob tem lahko pojavi še ena težava, saj se lahko za opisovanje nasilnih dejanj uporabljajo različne sopomenke. V teh primerih je priporočljiva uporaba baze podatkov oz. leksikonov, kot je npr. WordNet[2], kjer so izraženi semantični odnosi med sopomenkami. Primer takšnih semantičnih odnosov je npr. beseda masaker, namesto katere bi v besedilu lahko uporabili druge besede, kot so pokol, klanje ali prelivanje krvi. Z uporabo teh semantičnih odnosov se število besed, ki jih je potrebno predhodno eksplicitno definirati v seznamu iskanih besed, močno zmanjša. Ob tem velja povedati, da ena sama nasilna beseda v besedilu še ne zadošča, da bi lahko takšno besedilo označili kot kazalnik za razkritje, ampak je za to potrebnih ali več takšnih besed ali pa mora obstajati povezava z drugimi kazalniki. Pri tej vrsti analize besedil se lahko pojavijo tudi problemi z ironičnimi izjavami posameznikov, saj so lahko šale prepoznane kot potencialni znaki razkritja. Vendar pa se z omejevanjem pozornosti na spletne strani ali forume z nasilnimi ekstremističnimi vsebinami, ki jih predhodno poiščemo z spletnim pajkom, takšni neupravičeni pozitivni rezultati obdržijo na sprejemljivi ravni. Kot primer razkritja so Brynielsson in

[1] Lematizacija je ročno ali računalniško podprt postopek določanja osnovne oblike posameznim besedam, ki jih najdemo v besedilu.

[2] WordNet je velika baza angleških besed, ki so jo razvili študentje Univerze v Princetonu. Samostalniki, glagoli, pridevniki in prislovi so združeni v sklope kognitivnih sinonimov, od katerih vsak izraža poseben koncept.

sodelavci (2013: 9) uporabili stavek iz Breivikovega objavljenega manifesta 2083: Evropska deklaracija neodvisnosti, kjer navaja: »*Zagotovili bomo, da bodo vsi izdajalci, ki omogočajo Islamizacijo in uničevanje naše kulture, naroda in družbe, usmrčeni*«. V stavku se pojavlja signalizacija namena (bomo), kateremu sledi izraz za nasilno dejanje (usmrčeni) (Brynielsson et al., 2013).

3.4.4 Fiksacija oziroma obsedenost

Fiksacija se kaže kot obsedenost z osebo ali višjim ciljem oziroma poslanstvom. Fiksacijo lahko opazimo kot težnjo k ponavljajočemu se komentiranju določene teme, pri čemer se v primerjavi z drugimi uporabniki neko osebo, skupino ali težavo omenja pogosteje. Fiksacijo v besedilih je možno iskati tudi s štetjem pojavljanja ključnih izrazov (oseb, organizacij) v določenem besedilu. Primer fiksacije so Brynielsson in sodelavci (2013: 9–10) našli v Breivikovem manifestu 2083: Evropska deklaracija neodvisnosti: *»Ne gre le za našo pravico, ampak tudi za našo dolžnost, da prispevamo k ohranitvi naše identitete, kulture in suverenosti, zato je potrebno preprečiti proces Islamizacije. Ni odporniškega gibanja, če posamezniki, kot smo mi zavrnejo svoj prispevek … Čas je pri tem ključnega pomena. Imamo le nekaj desetletij za utrditev zadostne stopnje odpora, preden bodo naša glavna mesta demografsko preplavljena z muslimani. Zagotavljanje uspešne distribucije tega manifesta med čim večje število Evropejcev, bo bistveno prispevalo k našemu uspehu. To je mogoče edini način, da se v prihodnosti izognemo suženjstvu islamske vladavine v naših državah«*. V besedilu je mogoče opaziti, da se besede povezane z Islamom (Islamizacija, muslimani, islamske) pojavljajo zelo pogosto (Brynielsson et al., 2013).

3.4.5 Identifikacija

Identifikacija je opozorilno vedenje, ki se kaže kot posameznikova identifikacija z prejšnjimi napadalci ali morilci ali identifikacija samega sebe kot tistega, ki mora nadaljevati neko poslanstvo. Gre torej za identifikacijo z radikalnimi aktivnostmi ali za identifikacijo s kakšnim vzornikom. Identifikacija s skupino ali poslanstvom se izraža z uporabo pozitivnih pridevnikov v povezavi z omembo skupine in z uporabo zaimkov prve osebe množine (mi, nas, nam), medtem ko uporaba zaimkov tretje osebe množine (oni) kaže na sovražno nastrojenost proti neki skupini. Identifikacijo z bojevnikom oziroma z bojevniško miselnostjo se da opaziti z uporabo določene terminologije, medtem ko se občutek moralne dolžnosti izraža z uporabo besed v povezavi z dolžnostjo, častjo in pravičnostjo. Identifikacija z drugim radikalnim mislecem se poleg citiranja in omenjanja le-tega, kaže

tudi v podobnosti pisanja. Uporabljajo se isti izrazi, v nekaterih primerih pa se pojavlja tudi podobna struktura stavkov. Obstajajo številni primeri slik in posnetkov objavljenih na internetu, kjer morilci samotarji pozirajo z orožjem že pred samim napadom. Tako je tudi Breivik že pred izvedbo napada posnel serijo fotografij, na katerih pozira z avtomatskim orožjem (Brynielsson et al., 2013).

3.5 Razvrstitev in ocena uporabniških imen

Po tem, ko se s tematsko oziroma vsebinsko filtriranim iskanjem spletnih strani zbere potrebne podatke, je potrebno te podatke še ustrezno analizirati. Prvi korak analize je identifikacija vseh zaznanih uporabniških imen, sledi analiza besedila, kot je bila opisana v prejšnjih poglavjih, cilj katere je iskanje kazalnikov, ki nakazujejo namen storitve terorističnega dejanja. Ko se v raziskavi zazna uporabniško ime, se ga uvrsti na seznam uporabnikov, ki jih je potrebno podrobneje spremljati in raziskati. Če je pri nekem uporabniku zaznan eden izmed indikatorjev, to po navadi še ne zadošča, da bi takšnega uporabnika označili kot možnega terorista samotarja, daje pa neko osnovo, na podlagi katere se sproži iskanje novih oziroma dodatnih potencialnih kazalnikov. Da bi lahko natančneje ocenili določenega uporabnika, si pomagamo z modelom ocenjevanja grožnje (Slika 1) in razvijanjem hipotez, s pomočjo katerih ugotavljamo morebitno grožnjo družbi, pri čemer si pomagamo z vsemi, do tega trenutka znanimi informacijami, ki so povezane z določenim uporabniškim imenom. Ker torej en sam kazalnik ne zadošča za oceno posameznika kot terorista samotarja, je treba združiti informacije različnih kazalnikov, da bi lahko nato podali ustrezno oceno. Za takšno združevanje obstaja več načinov. Eden izmed načinov je, da iščemo pozitivne dokaze za vse kazalnike, da bi lahko potem zaključili, da ima posameznik namen izvesti teroristično dejanje. Naslednji način je, da ugotovimo, če so npr. trije od petih kazalnikov izpolnjeni v zadostni meri, da lahko rečemo, da ima neka oseba namen izvesti teroristični napad.

Kadar analiziramo podatke iz interneta lahko naletimo še na en problem. Tako ni nič nenavadnega dejstvo, da posamezniki za pisanje po internetu uporabljajo različna uporabniška imena, zato je eden izmed najpomembnejših delov tega procesa ugotavljanje, če kateri izmed avtorjev za svoje udejstvovanje na internetu uporablja različne vzdevke. Če tega ne storimo, obstaja tveganje, da bodo šibki signali s strani istega avtorja končali v ločenih modelih in se ne bodo združili v skupni imenovalec. To bi lahko pomenilo, da bi bili določeni akterji spregledani, zato je naloga združevanja uporabniških imen še kako pomembna, saj zaznani šibki signali šele nato dobijo pravo vrednost (Dahlin et al., 2012). Posameznik lahko sodeluje v razpravah na različnih internetnih straneh ali forumih z različnimi vzdevki oziroma uporabniškimi imeni ali uporablja različne vzdevke oziroma uporabniška imena na enem spletnem mestu. Do tega pride, če posameznikov prvi vzdevek iz takšnih ali drugačnih razlogov izključijo iz razprave, ali da avtor enostavno pozabi geslo za svoje uporabniško

ime. Prav tako se lahko zgodi, da avtor izgubi zaupanje drugih članov razprave, ali da je avtor razvil slabe odnose z nekaterimi drugimi člani razprav in se zato odloči za uporabo novega uporabniškega imena. Lahko pa uporablja različna uporabniška imena z namenom podpiranja lastnih argumentov in tako razširja zavest o pravilnosti svojega mnenja. Johansson in sodelavci (Johansson, Kaati in Shrestha, 2013) so na podlagi teh razlogov identificirali dva glavna primera, v katerih je preverjanje ujemanja uporabniških imen lahko koristno. Prvi primer je, ko si nek uporabnik ustvari novo uporabniško ime, vendar tega nima namena prikriti, do česar pride predvsem takrat, ko se uporabniku zaradi neaktivnosti staro uporabniško ime izbriše, če pozabi geslo za staro uporabniško ime, ali če mu zaradi takšnih in drugačnih razlogov uporabniško ime zablokirajo. Drugi primer pa je, ko uporabnik ne želi razkriti, da različna uporabniška imena pripadajo isti osebi in je pogosto v primerih, ko posameznik izgubi zaupanje ali ima slabe odnose z drugimi uporabniki, ali ko želi z novim uporabniškim imenom okrepiti svoje argumente. Koliko truda bo posameznik vložil v prikrivanje tega dejstva, je seveda odvisno od vsakega posameznika posebej, je pa za pričakovati, da uporabnik ne bo uporabil podobnega vzdevka oz. uporabniškega imena. Ne glede na to, kaj je vzrok za to, da posamezniki za svoje udejstvovanje v internetnih razpravah uporabljajo različna uporabniška imena oz. vzdevke, le-to predstavlja veliko težavo za analitike v obveščevalnih in drugih službah, saj otežuje zaznavanje in združevanje šibkih signalov s strani določenega posameznika. Načini za odkrivanje in posledično združevanje različnih uporabniških imen enega posameznika so naslednji:

- podobnosti uporabniških imen,
- stilometrija ,
- časovne informacije,
- podobnosti v različnih socialnih omrežjih.

Če uporabnik uporablja isto uporabniško ime, ali če obstajajo le majhne razlike v uporabniških imenih, je prepoznavanje dokaj preprosto. S stilometrijo poskušamo kvantitativno določiti karakteristike nekega besedila, s katerimi lahko ločimo besedilo enega avtorja od besedila nekega drugega avtorja. Gre torej za analizo stila pisanja, ki temelji na predpostavki, da ima vsaka oseba svoj individualen način pisanja. Individualnost se ustvarja z značilnostmi, ki jih lahko odkrijemo v besedilu. Analiziramo lahko frekvenco in naravo napak, ki se pojavljajo v besedilu, frekvenco značilnosti stila pisanja (povprečna dolžina besed, stavkov) in različna razmerja (med glagoli in pridevniki, glagoli in samostalniki) (Rožej, 2010). Za namene identifikacije različnih uporabniških imen so uporabni tudi časovni podatki. Gre za informacije o tem, kdaj tekom dneva nekdo objavlja svoja sporočila in o frekvenci sporočil v nekem časovnem obdobju. Pri prepoznavanju si lahko pomagamo tudi z analizo socialnih omrežij. Če dve različni uporabniški imeni objavljata na istih forumih, na iste teme in redno komentirata iste vrste objav, je zelo verjetno, da gre za isto osebo. Z združevanjem različnih informacij o uporabniških imenih in analizo njihovih sporočil namreč lahko povečamo možnosti za identifikacijo uporabnikov z različnimi uporabniškimi imeni (Brynielsson et al., 2013). Dokazano je,

da je identifikacija uporabniških imen še najučinkovitejša, ko gre za kombinirano uporabo vseh naštetih tehnik, še najbolj učinkovita pa je kombinacija časovnega ujemanja in stilometrije (Johansson et al., 2013).

4 ZAKLJUČEK

Terorizem predstavlja veliko grožnjo celemu svetu, saj na tovrstne dogodke ni odporna nobena država. Tako lahko v zadnjem času ob vsakem večjem dogodku, pa naj bo to politično srečanje, športni dogodek ali podobno, spremljamo razne debate o varnosti, saj venomer obstaja nevarnost, da bodo teroristične skupine ali teroristi posamezniki izkoristili odmevnost takšnih dogodkov za uresničitev svojih ciljev. Med tem ko so v preteklosti največjo nevarnost predstavljale organizirane teroristične skupine, v zadnjih letih največjo nevarnost predstavljajo teroristi samotarji, ki so v zadnjih letih odgovorni za nekaj najbolj odmevnih terorističnih dejanj. Ti tako imenovani »Lone Wolf« teroristi oziroma teroristi samotarji zaradi svojega načina delovanja predstavljajo pravo uganko varnostnim organom, kajti tradicionalne metode odkrivanja (prisluškovanje, infiltracija), ki so uporabne pri odkrivanju organiziranih skupin, pri njih niso učinkovite. Ena izmed značilnosti teroristov samotarjev je namreč nezaupljivost, kar ima za posledico, da z nikomer ne komunicirajo o svojih namerah, kar možnosti njihovega odkritja močno zmanjša. Dodatno oteževalno okoliščino pa predstavlja dejstvo, da lahko teroristi samotarji pripadajo kateri koli ideologiji, rasi in veri.

Vendar pa ni vse tako črno, kot se zdi na prvi pogled. Ena izmed značilnosti teroristov samotarjev je namreč ta, da medtem ko v resničnem življenju živijo odtujeno, jim internet omogoča povezovanje s podobno mislečimi posamezniki po celem svetu. Internet jim torej ponuja okolje, v katerem se počutijo varno in udobno, najdejo zagovornike njihovega razmišljanja, lahko pa najdejo tudi napotke glede organizacije samih napadov. Ob tem pa za sabo puščajo tako imenovane digitalne sledi, ki preiskovalcem ponujajo možnost zgodnjega odkrivanja potencialnih teroristov samotarjev. Zato so v zadnjih letih varnostni organi posebno pozornost začeli posvečati razvijanju programske opreme, ki bi omogočala zbiranje sledi, ki jih nekdo pusti na svetovnem spletu. Vendar pa se ob tem seveda pojavlja tudi vprašanje varovanja zasebnosti uporabnikov svetovnega spleta. Pri uporabi takšnih spletnih orodij namreč vedno obstaja nevarnost prekoračenja pooblastil in posledično kršenja zasebnosti. Zato je potrebno stremeti k doseganju ravnotežja med varnostjo državljanov na eni strani in varovanjem zasebnosti na drugi strani. K temu lahko veliko pripomoremo z uporabo kombiniranega spletnega iskanja potencialnih napadalcev, kar pomeni, da v kombinaciji s programsko opremo pri iskanju hkrati sodeluje tudi izkušen analitik. Računalniški programi so lahko precej togi, medtem ko lahko analitiki na podlagi svojih izkušenj dodatno presojajo uvrstitev ali umik posameznika iz liste potencialnih teroristov samotarjev.

LITERATURA

Bakker, E. in de Graaf, B. (2010). *Lone Wolves: How to Prevent This Phenomenon?* International Centre for Counter-Terrorism – The Hague. Pridobljeno na http://www.icct.nl/download/file/ICCT-Bakker-deGraaf-EM-Paper-Lone-Wolves.pdf

Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Martenson, C., Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics 2*(1). Pridobljeno na http://www.security-informatics.com/content/pdf/2190-8532-2-11.pdf

Dahlin, J., Johansson, F., Kaati, L., Martenson, C. in Svenson, P. (2012). *Combining Entity Matching Techniques for Detecting Extremist Behavior on Discussion Boards.* Division of Automatic Control. Linköpings University. Pridobljeno na http://users.isy.liu.se/en/rt/johda87/publications/Dahlin2012-EntityMatching.pdf

Johansson, F., Kaati, L. in Shrestha, A. (2013). *Detecting Multiple Aliases in Social Media.* International Conference on Advances in Social Networks Analysis and Mining. Pridobljeno na http://www.academia.edu/5117526/Detecting_Multiple_Aliases_in_Social_Media

Kaati, L. in Svenson, P. (2011). *Analysis of Competing Hypothesis for Investigating Lone Wolf Terrorists.* European Intelligence and Security Informatics Conference. Pridobljeno na http://scholar.google.si/scholar_url?hl=sl&q=http://www.researchgate.net/publication/221400254_Analysis_of_Competing_Hypothesis_for_Investigating_Lone_Wolf_Terrorist/file/9

Nijboer, M. (2012). A Review of Lone Wolf Terrorism: the Need for a Different Approach. *Social Cosmos, 3*(1). Pridobljeno na http://socialcosmos.library.uu.nl/index.php/sc/article/viewFile/43/38

Pantucci, R. (2011). *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists.* The International centre for the study of radicalisation and political violence. Pridobljeno na http://icsr.info/wp-content/uploads/2012/10/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf

Pantucci, R. (2011). What Have We Learned about Lone Wolves from Anders Behring Breivik? *Perspectives on Terrorism, 5*(5–6). Pridobljeno na http://www.terrorismanalysts.com/pt/index.php/pot/article/view/what-we-have-learned/332

Rožej, T. (2010). *Psiholingvistična analiza dokumentov pri preiskovanju kaznivih dejanj* (Diplomsko delo). Ljubljana: Fakulteta za varnostne vede.