УДК: 004.738.5:351.86

COBISS.SR-ID: 125235721

https://doi.org/10.18485/uunt_pl.2023.2.3.2

Оригинални научни рад

Политикологија

бр. 3/2023, год 2, vol. 1.

стр. 13-27

Рад примљен 24. 04. 2023.

Рад прихваћен 20. 06. 2023.

ДРУШТВЕНЕ МРЕЖЕ КАО ИЗВОР ОБАВЕШТАЈНО-БЕЗБЕДНОСНИХ ПОДАТАКА

Филип, С. Филиповић[1], дипломирани политиколог

Резиме

Друштвене мреже су један од најзначајних извора информисања у савременом друштву. На друштвеним мрежама се објављују различите врсте података. Од приватних и личних, политичких, идеолошких, безбедносних, до разноврсних информација из света економије. Сваки податак може сам за себе, или у једном ширем или ужем контексту, имати одређено обавештајно значење. У раду ће бити објашњено како се друштвене мреже могу користити као обавештајни извор сазнања, колики је значај прикупљања информација из отворених извора, као и који су то изазови са којима се обавештајна заједница суочава када је реч о овом методу прикупљања података. У овом истраживању аутор је покушао да објасни како се друштвене мреже могу користити као извор обавештајних података, који је значај прикупљања података из отворених извора, а посебно са друштвених мрежа, као и то који су изазови са којима се обавештајна заједница суочава када је реч о овом методу прикупљања података. Природа истраживања захтева мултиметодски приступ, који укључује примену разних поступака за систематско прикупљање и интерпретацију података из различитих извора.

Кључне речи: *друштвене мреже, извори обавештајно-безбедносних података, обавештајно-безбедносне службе, сакупљање обавештајно-безбедносних података.*

1 драганстанар@унионниколатесла@еду.рс, драганстанар@уахоо.цом

Увод

Према истраживању *Digital 2019.* скоро половина светског становништва (3,48 милијарди људи) користи друштвене мреже. Према доступним подацима у Србији 2,5 милиона људи има свој налог на некој од друштвених мрежа. Човек у просеку проведе 116 минута дневно на друштвеним мрежама, што употребу друштвених мрежа поставља на друго место најзаступљенијих активности у слободно време - одмах иза гледања телевизије. Очекивано је да ће у будућности, даљим развојем друштвених мрежа и повезаних апликација, њихова употреба наставити да расте, наспрам традиционалног начина информисања као што су телевизија или новине у штампаном облику. Наведени подаци показују значај друштвених мрежа као глобалног комуникацијског феномена.

Потреба човека за разменом информација на дневном нивоу повећава значај друштвених мрежа као базе за постављање и чување огромног броја података. Мерења показују да се у само једном минуту на интернету размени 19 милиона текстуалних порука, постави 194,444 твитова (енг. Twitter), 1,3 милиона људи приступи свом фејбук профилу (енг. *Facebook)*, пошаље 59 милиона порука путем апликације на месенџеру (енг. *Messenger*), те размени преко 190 милиона мејлова (енг. *e-mail*).2 Наведени подаци нам говоре о распрострањености употребе друштвених мрежа међу становништвом.

Значај друштвених мрежа јесте и у чињеници да 1,2 милијарде људи свакодневно користи интернет кроз апликације, блогове и постове, дељења (енг. *Share*) и претраживања - гледања (енг. *View*) различитих садржаја. Друштвене мреже, као интернет платформе, обезбеђују средства којима се интернет све више користи за учествовање, креирање и дељење личних и приватних информација о нама и нашим пријатељима, изражавање мишљења и ставова, кроз опције „свиђа ми се“ као и све видове трансакција (Christopher, Moran & Salisbury, 2014, стр. 24).

Анализа остварених активности на друштвеним мрежама широко се користи у маркетингу и менаџменту, током политичких избора, у академским заједницама за изучавање одређених тема, али и у систему безбедности. Бизнис модели многих компанија се данас ослањају управо на податке које друштвене мреже прикупљају о својим корисницима (Spinello, 2011, стр. 43). Корисници на друштвеним мрежама излажу приватне информације о себи како би били у могућности да комуницирају са својим пријатељима, члановима породице и колегама. То је формула која представља почетну базу за трговинску трансакцију, која омогућава кориснику да бесплатно користи друштвену мрежу, а за узврат да лични подаци који се прикупљају буду доступни маркетинг компанијама које на тај начин таргетирају кориснике ради промоције

2

производа различитих компанија кроз тзв. додатке или рекламне поруке (Harris, 2008, стр. 45). У стручној и грађанској јавности, друштвене мреже се критикују као један од начина на који се данас најлакше крши право на приватност и личну сферу појединца. Прописивањем посебних одредби о заштити права на личне податке и имплементацијом тих прописа кроз посебна правила приватности на друштвеној мрежи, иде се за тим да се права корисника друштвених мрежа заштите у мери у којој је то могуће.

Друштвене мреже представљају својеврсне савремене медије 21. века. С тим у вези, медији представљају значајан део демократског друштва јер представљају један од главних извора информисања грађана. Они су битан посредник између демократске власти и народа (Стојадиновић, 2014, стр. 133). Како професор Стојадиновић наводи, „медији имају великог утицаја у усмеравању савремених друштвених процеса, тако да они могу служити развоју демократске свести и културе мира, али уједно и распиривати расну, верску и националну мржњу својим једностраним извештавањем о битним догађајима у друштву, а под утицајем одређених интересних група. Моћ медија се нарочито огледа у томе што они могу утицати на обликовање свести а да грађани тога не буду ни свесни. Снага масовних медија, као што су друштвене мрежем је у присутности у свим сегментима живота, од информисања па све до забаве. Телевизија, радио, новине, интернет постају кључни чиниоци који значајно утичу на начин на који интерпретирамо догађаје који су изван нашег директног окружења. Ово доводи до тога да медији добијају значајну улогу у обликовању друштвене свести форсирањем одређених информација“ (Стојадиновић, 2014, стр. 135)

Поред позитивних страна које коришћење друштвених мрежа има за појединце, организације и друштво у целини, у информатичкој ери, када је брз проток информација изузетно значајан у свим аспектима живота, кршење приватности у виду злоупотребе података у различите сврхе, несумњиво је једна од негативних страна друштвених мрежа.

Злоупотреба друштвених мрежа у илегалне сврхе

Са повећањем популарности друштвених мрежа, растао је и број корисника, што је довело до појаве негативних последица и настанка посебног облика криминалитета који се манифестује преко друштвених мрежа и у виртуелном простору уопште, као и до стварања новог облика зависности – зависности од интернета и друштвених мрежа. У литератури су заступљена различита схватања о утицају интернета на кориснике у смислу подстицања агресивности и вршења кривичних дела уз помоћ информационих технологија. Заступљена су и таква схватања која негирају криминални утицај интернета

и истичу да је његов утицај на осећања, ставове и понашање људи много више позитиван него што има етиолошки значај криминогеног фактора.

Са фреквентнијом употребом интернета и са повећањем броја корисника, веће су и разноврсније могућности за злоупотребу интернет мреже. У вези са злоупотребама поставило се питање заштите појединачног личног права - права на приватност. Током времена, правила приватности на друштвеним мрежама су мењана. Под утицајем концепта заштите личних података, на коме почива владавина права у многим савременим демократским државама, политика друштвених мрежа је кренула истим стопама. Ипак, уз одређене технике и методе обавештајне аналитике, сваки објављени податак може у оквиру датог контекста имати одређени обавештајни значај.

Друштвене мреже се користе за организовање терористичких акција, ширење пропаганде, неморалних садржаја, разних националистичких, дискриминаторских и других друштвено неприхватљивих идеја. Напади на друштвеним мрежама подразумевају прикупање података о појединцима или групама или организацијама, у виду недозвољене аналитике, неовлашћеног прислушкивања, анализу саобраћаја, ради имитације (нпр. лажирање идентитета на друштвеним мрежама, лажирање ИП адресе, клонирање, *Sibil* напади – иза једне ИП адресе се налази велики број рачунара и др) (Стевановић и Ђурђевић, 2016, стр. 117).

Свака организација (терористичке групе, криминалне организације) користи друштвене мреже како би организовала и лакше спровела своје операције (Крстешић, 2016, стр. 171). Напади на друштвеним мрежама, уколико су почињени од стране недржавних актера, ради остваривања политичких или циљева националне безбедности, представљају, тзв. сајбер нападе (Милошевић, Матић и Мијалковић, 2017, стр. 545).

С друге стране, сајбер криминалне активности које се не врше зарад остварења политичких или национално безбедносних циљења, као што су интернет преваре, крађе идентитета и интелектуалне својине, представљају акт сајбер-криминала (Милошевић, Матић и Мијалковић, 2017, стр. 545). Суштина је да се и једне и друге активности врше злоупотребом друштвених мрежа и да се на тај начин крше права и интереси појединаца или државе, односно угрожава јавна безбедност.

Начин понашања корисника на друштвеним мрежама може много да олакша или отежа рад обавештајним службама. Од пресудног значаја су она понашања и активности које у себи могу садржати одређени податак или информацију о криминалним активностима. Иако су могућности злоупотреба друштвених мрежа огромне, истовремено друштвене мреже су користан извор прикупљања података о криминалним активностима.

Са појавом интернета, пренос дигиталних података и информација постао је још лакши. У почетку је интернет омогућавао корисницима анонимност – информације су прослеђиване преко IP адреса које нису могле да препознају ни ко је пошиљалац нити ко је прималац информације (Spinello, 2011, стр. 13). Данашњи модел интернет комуникација је у потпуности другачији и опаснији по приватност својих корисника. „Колачићи" (енгл. *Cookies*) и „бубе" (енгл. *Bugg*) створили су виртуелни простор који не штити приватне интересе, већ фаворизује и намеће као императив принцип сталног посматрања свих корисника. Овакви рачунарски програми сакупљају са интернета информације попут лозинки, који интернет садржај је прегледан, које поруке су послате, који сајтови су посећени и сл. Резултат је немогућност корисника интернета да се неприметно и анонимно креће виртуелним простором (Мијалковић, 2015, стр. 18).

Са сваком својом активношћу на мрежи, корисник оставља својеврсни траг, у виду електронског записа, који омогућава обавештајној заједници да њиховим праћењем прикупи податке који су од значаја за обавештајни рад. Питање које се намеће јесу правила приватности, као невидљиви круг ограничења, у коме се креће обавештајна делатност прикупљања података са друштвених мрежа.

Друштвене мреже као извор обавештајних података

Друштвене мреже се могу дефинисати као услуга која је заснована на коришћењу интернета, а која дозвољава појединцу да направи (полу)јавни профил и у оквиру ограниченог садржаја, направи листу других корисника са којима дели повезаност, те види и упореди своју листу контаката који су направили други корисници у оквиру истог садржаја. Прикупљање података из отворених извора обавештајних сазнања - OSINT (*Open Source Intelligence*) подразумева анализу садржаја писаних медија и електронских извора доступних јавности, а прикупљање података са друштвених мрежа, као посебне подврсте отворених извора обавештајних сазнања – SOCMINT (*Social Media Intelligence*) подразумева прикупљање и обраду у обавештајне сврхе личних података које корисници друштвених мрежа, намерно или случајно, откривају о себи кроз употребу одређене друштвене мреже. Прикупљање података, њихова анализа и обрада, подразумева посебан обавештајни процес који има за циљ долажење до информација које имају обавештајни значај.

У литератури се сматра да један догађај представља прекретницу у коришћењу друштвених мрежа као отворених извора обавештајних сазнања. Верује се да су управо дешавања у Ирану током 2009. године, позната као „Зелена револуција" (низ протеста грађана против тадашњег владајућег режима), допринела схватању да су друштвене мре-

же нови облик отворених извора обавештајних података. 3 Милиони младих Иранаца координисали су своје активности преко интернета, тако што су делили виралне садржаје и охрабривали друге да се придруже кампањи. Први пут интернет је био преплављен информацијама око политичких догађаја, већином захваљујући комбинацији паметних телефона, интернет конекцијама и друштвеним мрежама. Током прве недеље протеста око 60% од свих линкова који су постављени на енг. *Twitter-y* били су повезани са иранском политиком. Иако је Зелена револуција била неуспешна, јер је држава успела да поврати контролу над интернетом ограничавањем и контролом његовог садржаја, за кратко време, друштвене мреже су успеле да покажу колико велики може бити утицај отворених извора података за обавештајну анализу. У ограниченом времену, уз употребу паметних телефона, интернет мреже, малог броја апликација кроз које се велики број података делио, први пут, сваки појединац широм света могао је да тако доступне податке користи за анализу и обраду. У историји развоја отворених извора обавештајних сазнања, овај догађај доказује колико је велики значај друштвених мрежа као извора обавештајних података.

Са становишта безбедности, друштвене мреже су показале да су користан извор података када треба предвидети одређене догађаје или активности који могу бити перципирани као угрожавајући по питању безбедности појединаца или друштва. У теорији се закључује да је допринос друшвених мрежа пресудан у очувању јавне безбедности и поузданости у предвиђању и тачности информација за крајње кориснике који доносе тешке одлуке у кратком временском року. То се постиже у три нивоа анализе (Christopher, Moran & Salisbury, 2014, стр. 13).

Први и основни ниво јесте да помогне овлашћеним огранима да формирају свест о ситуацији и догађају који се одвија. То значи да се анализом социјалних мрежа, сви кључни догађаји у свету могу идентификовати са питањима „Када се догађај десио“, „Шта се тренутно дешава“, „Где се догађај десио“ и „Ко је учесник догађаја“. Следећи ниво анализе подразумева објашњење догађаја који је посматран, кроз одговоре на питања „Зашто“ и „Како“ се посматрана активност одиграла, што се односи како на терористичке нападе, тако и на ситуациони криминал. Други ниво анализе је сложенији и захтева високи ниво разумевања и познавања феномена који се посматра у корелацији са околностима у којима појединци себе редовно изражавају. Адекватним сагледавањем целокупног догађаја и мотива учесника, могуће је предвидети како ће се догађаји одвијати. Трећи ниво анализе укључује најсложенији употребу обавештајних знања и примену метода испитивања, укључујући и податке прикупљене на друштвеној мрежи,

3

како би се дао одговор на питања „Шта даље“ и „Где даље“, која најчешће и постављају политички и владајући ауторитети (Christopher, Moran & Salisbury, 2014, стр. 13).

Друштвене мреже као извор података о криминалним активностима

Друштвене мреже представљају потенцијални простор за криминалне активности. Организоване криминалне групе, терористичке групе и појединци своју комуникацију обављају управо преко друштвених мрежа. *Facebook* је у једном случају употребљен да би се ангажовао плаћени убица (Christopher, Moran & Salisbury, 2014, стр. 13).

До 1999. године скоро све познате терористичке групе су успоставиле своје присуство и на друштвеним мрежама. У то време је још било нејасно како терористичке и екстремистичке групе користе погодности друштвених мрежа, али је чињеница да су друштвене мреже коришћене у великом броју терористичких напада у Великој Британији.

Познато је да у својим активностима терористичке огранизације и организоване криминалне групе, користе готово све методе обавештајних служби, од непосредног опсервирања и сарадничког/агентурног метода, преко метода псеудоислеђивања, па до најсавременијих и најсуптилнијих метода (злоупотреба савремених научних и технолошких достигнућа) (Мијалковић, 2019, стр. 106).

Тако, друштвене мреже су се данас сврстале у средство комуникације које омогућава слободан и релативно лак начин комуникације и логистике у организовању нелегалних активности. Напретком информатичког друштва и развојем технике, аналитичари у оквиру обавештајних служби свој рад све више окрећу ка друштвеним мрежама.

Са становишта безбедности, праћење активности ових група на друштвеним мрежама, уз адекватну примену знања, метода и адекватну анализу прикупљених података, може бити ефикасно средство у борби против свих облика криминала. У обавештајној пракси и теорији прикупљање информација о криминалитету и учиниоцима кривичних дела сврстава се у посебне облике обавештајне активности, криминалистичко-обавештајну активност. Као облик анализе, представља сложени процес прикупљања, анализе и процене информација у циљу спречавања криминалних активности и њихових учинилаца (Бајагић, 2015, стр. 23). Разликује се од традиционалног полицијског рада по томе што је усмерена на истраживање образаца криминалних понашања и активности како би се исте предупредиле.

SOCMINT олакшава полицији откривање и гоњење учинилаца кривичних дела на тај начин што примена овог метода омогућава да се докази прикупљају на друштвеним мрежама. Такав вид прикупљања података, који касније могу имати доказни значај у поступку, посебно је карактеристичан за друштвену мрежу *Twitter*, која делује као нови канал комуникације, дозвољавајући широј јавности односно корисницима мреже да објављују све познате информације, па чак и слике и видео снимке о критичним догађајима, што омогућује снагама безбедности да прате ситуацију у реалном времену (Christopher, Moran & Salisbury, 2014, стр. 13).

Једна анализа коју је спровела организација Демос показала је да 20,000 твитова који су послати Метрополитен полицији у Лондону између 17. и 24. маја 2009. године, око 20% њих се односило на податке који су имали доказни кредибилитет, укључујући сведоке и доказе о криминалним активностима на самој мрежи (Christopher, Moran & Salisbury, 2014, стр. 13). Информације које се деле на друштвеној мрежи најчешће се односе на притужбе грађана упућене полицији поводом говора мржње, расне и друге облике дискриминације, саобраћајне удесе, преваре, крађе, предофилију, трговину опојним дрогама, злостављање животиња и сл. Ради се о подацима који могу утицати или чак преусмеравати деловање снага безбедности у одређеном правцу. Истиче се и да је у томе недостатак друштвених мрежа, будући да често малициозни подаци буду објављени са намером да заварају трагове или пак одведу истрагу у погрешном смеру. Без обзира на то, истиче се велики значај друштвених мрежа у прикупљању података који су од значаја у свакодневном деловању полиције и снага безбедности у борби против различитих облика криминалитета.

У 2009. години, полиција у Великој Британији је креирала систем приступа друштвеним мрежама као што је *Facebook* који је имао за циљ да открива криминалну активности кроз идентификовање држалаца оружја, што је за резултат имало испитивање преко 400 лица. Систем је коришћен као компјутерски програм у откривању несталих особа и за идентификацију непознатих лица. Полиција у Канади је друштвене мреже користила како би сакупила податке о криминалним активностима група као што је нелегално држање оружја.

Ово су само неки од примера који показују значај и сврху које друштвене мреже имају са становишта гоњења учинилаца кривичних дела, откривања и спречавања различитих облика криминалне активности, а у ширем смислу успостављања и одржавања безбедности друштва и заједнице.

Друштвене мреже као извор података о односима и повезаности појединаца и група

Сврха друштвених мрежа јесте у међусобном повезивању њихових корисника. Мотиви повезивања су различити. Било да је реч о индивидуалним потребама које се огледају у контакту са пријатељима, породицом, колегама или пак групним повезивањама у циљу пословних контаката или пак неких других хуманих циљева, свака од таквих релација је легитимна док циљеви и сврха повезивања не поприме облике одређених активности чији су циљеви неспојиви са становишта закона и морала. Стога се истиче да су друштвене мреже битан фактор снагама безбедности у стицању сазнања о релацијама и повезаности појединаца и група, оних чија природа и намена постојања није у складу са законом, односно које настају ради незаконитог, криминалног или неког другог облика нелегалне активности.

Анализа друштвених мрежа **(***Social Network Analysis*) је приступ који комбинује социолошке и математичке методе да опише природе, интензитет и учесталост, веза између индивидуалних елемената, појединаца или мањих група. Темељи се на претпоставци да су људи под моћним утицајем психолошких и начина понашања у социјалним односима који их окружују. Да би објаснила ове везе, анализа друштвених мрежа полази од испитивања начина понашања на мрежи уопштено гледано, као и испитивања понашања појединаца на бази локације где се налазе, као и праћење понашања тзв. инфлуенсера, посебних група као и везе које се успостављају међу њима (Christopher, Moran & Salisbury, 2014, стр. 13). Суштина је да се применом социолошких метода испитују везе између појединаца и група, како би се дошло до података на основу којих би се могло предвидети одређено понашање у будућности. Ово је посебно значајно са становишта безбедности. Анализа веза је једна од изузетно ефикасних метода за приказ и интеграцију великог броја података о организованим криминалним групама и њиховим везама у форми дијаграм везе (Бошковић и Ђурђевић, 2011, стр. 125).

Дијаграм веза је графички метод који омогућава организацију великог броја података на такав начин да се у кратком временском интервалу стекне увид у комплексну ситуацију. Посебно када се ради о подацима који се прикупљају са друштвених мрежа, имајући у виду њихову масу и сложеност, дијаграм веза је један од начина који омогућава ефикасније и брже сагледавање релација између појединаца и група на мрежи.

Што се прикупи више података о везама појединаца и група, о њиховим међусобним релацијама, начинима понашања на друштвеној мрежи, али и ван ње, то ће у каснијим фазама обавештајног процеса, обрађени подаци добити обавештајни значај за предвиђења будућих активности.

Анализа садржаја друштвених мрежа укључује: праћење пораста садржаја насталог поводом одређеног питања или места; праћење ширења одређеног дела информације; праћење дељења **(***share*) информације између корисника; сагледавање и разумевање сложених структура насталих понашањем појединаца који утиче на информације које примају други корисници и понашања која те заједнице усвајају (Бошковић и Ђурђевић, 2011, стр. 125).

У пракси се користе разне методе статистичке и математичке природе које аналитичари користе како би издвојили значење из података. Једна од метода која се користи у процесу таргетирања организованих криминалних и терористичких група је тзв. рударење података **(***eng. data maning*). Тражење података изводи се скенирањем података у сајбер простору да би се пронашла места (веб локације, портали, форуми, друштвене мреже и друге безбедносно занимљиве дигиталне локације), које садрже одређене кључне речи и фразе које указују на одређену криминалну активност. На тај начин се објекат од интереса означава као потенцијална мета за даљу анализу. Када објекат буде означен као потенцијални комуникациони портал за терористе или друге криминалне ентитете, тада сва комуникација на том порталу постаје предмет интересовања. Детаљном анализом података о активностима корисника утврђује се постојање одређених малициозних активности, док се дубља анализа података постиже уз помоћ вештачке интелигенције. На тај начин аналитичари добијају све неопходне податке и информације за даљу анализу (Крстешић, 2016, стр. 20).

За службе безбедности, анализа друштвених мрежа помаже бољем разумевању понашања јавности током криза, али се користи и за прикупљање информација о људима кроз разумевање односа који појединци и групе формирају у циљу стицања и размене информација и знања (Крстешић, 2016, стр. 20).

Доступност информација као предуслов за превенцију и прогнозирање безбедносно значајних догађаја

Предикција догађаја и њихов значај за безбедност темељи се на примени посебних техника које користе статистичке моделе који омогућавају коришћење, селекцију и чување свих података на друштвеним мрежама који би могли бити предиктивни сигнал за будућа понашања како на друштвеним мрежама тако и у реалном свету. Коришћење друштвених мрежа за предикцију догађаја широко се примењују у одређеним областима, политици, јавном здрављу, и криминалитету. Као доминантан метод који се користи у праћењу понашања на друштвеним мрежама, а у вези са тим и предвиђањима догађаја,

јесте анализа језика тј. употреба речи које се користе на мрежи (Christopher, Moran & Salisbury, 2014, стр. 14).

Када је реч о друштвеној мрежи *Twitter*, која се у суштини своди на објављивање кратких текстова у виду порука, метода анализе речи и садржаја текста се примарно примењују. У првом кораку анализе врши се класификација објављених твитова са становишта социолошких информација које садрже, на позитивне, негативне и неутралне: као што су упозоравајући, смирујући, насилни и ненасилни. Друга фаза се своди на примену квалификатора језичких значења да би се проценило да ли су посматрани садржаји релевантни или не. Трећа фаза је још увек експериментална и подразумева креирање слојева више фактора квалификације језичких значења који би требало да производе чиниоце који су способни да праве софистицираније разлике између значења речи (Christopher, Moran & Salisbury, 2014, стр. 14).

Прављењем софтвера који ће на брз и поуздан начин, применом одређеног алгоритма, ефективно тумачити значење употребљених речи, у једном одређеном контексту, предуслов је да се друштвене мреже оцене као потпуно поуздан начин и средство за предикцију понашања и активности појединаца и група, како на мрежи тако и ван ње. На тај начин и време које је од круцијалног значаја у обавештајном циклусу бива мање варијабилан фактор. Овде се ради о такозваној *Media Intelligence* или *Press Inteligence* анализи података. *Media Intelligence* анализира јавни, друштвени и уређивачки медијски садржај ван заштитног зида, што омогућава компанијама да мере и управљају својим перформансама као бренда у ширим водама маркетинга. Открива иначе скривена понашања потрошача, омогућавајући бренду да доноси интелигентне и информисане одлуке које ће довести до већег успеха. Ову врсту анализе и прикупљања података користе платформе *Facebook* и *Instagram,* а обавештајно-безбедносне службе моу затражити приступ прикупљених података уколико имају основану сумњу и дозволу надлежног органа, углавном суда.

Организовани криминалитет и терористичке организације користе друштвене мреже за огранизовање својих активности и окупљање својих чланова, што је данас опште позната чињеница. Међутим, нове технологије, разни видови прикривања података, клонирање IP адреса, коришћење псеудонима, лажних профила и идентитета, само су неки од чинилаца који отежавају рад обавештајним службама у прикупљању података.

У маси објављених информација, задатак обавештајне службе јесте да изврши селекцију оних који у себи садрже обавештајну информацију која има конкретан значај. Сваки извор, па и када долази од сведока, често је непоуздан и лажан, чиниоци који на то утичу су разноврсни и могу се јавити у различитим фазама обавештајног деловања, стога је од пресудног значаја део обавештајног рада који се односи на проверу и упоређивање

добијених података са информацијама које су доступне из других извора, јер једино тако може као крајњи производ добити информација која је поуздана и на којој се може базирати предикција активности и деловања.

За разлику од истинитих или неважних података на друштвеним мрежама, дезинформације су подмуклији и опаснији проблем за рад обавештајних служби. Дезинформација је начин ометања противника или непријатеља тако што ће ширити лажне приче обмотане око језгра истине, чинећи тако целу ствар веродостојном (Johnson, 2010, стр. 235).

Други потенцијални ризик са *SOCMINT* јесте посебно ситуација са прикупљањем информација из објављених видео клипова. У пракси се показало да се кроз објављене видео клипове шаљу скривене поруке, које нису одмах видљиве просечним корисницима, али су препознатљиве оним корисницима којима су и намењене. Познате су ситуације после 11. септембра 2001. године, када су Осама бин Ладен и његови слебеници користили видео преносе како би послали скривене поруке другим следбеницима, а које су имале за циљ, како се веровало, узроковање нових теротистичких напада свуда по свету (Johnson, 2010, стр. 235). Слање скривених порука кроз отворене изворе и медије је стара техника обавештајних служби. На крају, то је један од разлога који указује на значај отворених извора обавештајних сазнања, посебно друштвених мрежа које организоване криминалне и терористичке групе користе у свом раду, у циљу планирања активности, окупљање масе следбенике за реализацију својих планова, а на темељу технике и метода рада које су обавештајне службе развијале од њиховог настанка (Christopher, Moran & Salisbury, 2014, стр. 14).

Закључак

Друштвене мреже су основно средство комуникације модерног друштва. Користе се у разноврсне сврхе, за приватне, пословне или пак вођења државне политике. Данас се не може замислити ниједан догађај у друштву, унутрашњој или спољној државној политици и међународним односима у глобалу, а да није забележен на друштвеним мрежема. Изношење мишљења је део слободе говора и изражавања и данас је једно од неприкосновених људских права које се и у ратним или ванредним околностима не могу ограничити. Међутим, изношење мишљења и говора је слободно у границама права других лица. То значи да изражена реч, у зависности од садржине, али и контекста у коме је дата, може довести у питање националну безбедност и безбедност лица и група, тј. углавном јавних личности и највиших државних функционера, који су због природе посла изложени критикама јавности, а често и претњама појединаца. Стога је значај друштвених мрежа као отворени извор обавештајних сазнања велики.

Сматра се да друштвене мреже као отворени извор обавештајних сазнања, уз примену знања, правила и метода прикупљања, анализе и обраде података, поседују потенцијал да унапреде наведени систем анализе и на тај начин омогуће ефикасно и поуздано предвиђање догађаја у циљу очувања јавне и националне безбедности. Отворени извори обавештајних сазнања, па и онда када се прикупљају од стране обавештајних служби, подразумевају искључиво обраду података који су јавно доступни, у складу са законом, овлашћењима која служба поседује, а у складу са правилима приватности друштвене мреже која се обрађује. Такав начин прикупљања информација из отворених извора јесте у складу са дефиницијом отворених извора коју даје америчка обавештајна заједница, а која је прихваћена и у нашој обавештајној пракси. У зависности од адекватности примењених метода рада и стручности оперативних радника, зависиће и квалитет обавештајне анализе. Препреке са којима се суочава обавештајна заједница у раду са друшвеним мрежама, у пракси се могу ефикасно превазићи, због чега друштвене мреже могу имати велику улогу у обавештајном процесу.

На основу изнетог, може се закључити да су друштвене мреже један од најважнихих полазних извора података помоћу којих се долази до обавештајних информација. Најобимнији извори безбедносно значајних информација су друштвене мреже *Facebook i Twitter,* али које касније буду верификоване провером из других извора. И поред тога *Facebook i Twitter,* представљају најефикасније отворене изворе јер пружају могућност за правовремено организовање мера на сузбијању и спречавању безбедносно ризичних догађаја.

Литература

Бајагић, М. (2010). *Методика обавештајног рада*. Београд: Криминалистичко-полицијска академија.

Бошковић, Г. и Ђурђевић, З. (2011): Примена графичких метода за приказ информација у истрагама огранизованог криминала, *Безбедност*, 3/2010, Криминалистичко-полицијска академија, Београд.

Крстешић, А. (2016). Примена обавештајне анализе у борби против савремених изазова, ризика и претњи, Теорија и пракса безбедност за будућност. Београд: Безбедност и кризни менаџмент.

Мијалковић, С. (2019). Обавештајне структуре терористичких и криминалних организација. *Журнал за криминалистику и право*, Београд: Криминалистичко полицијска академија.

Милошевић, М., Матић, Г. и Мијалковић, М. (2017). *Класификација малициозних активности у сајбер простору и организација сајбер безбедности у Републици Србији*. Београд: Факултет безбедности.

Стевановић, Д. и Ђурђевић, М. (2017). *Интернет ствари, лична и материјална безбедност*. Београд: Академија за националну безбедност.

Стојадиновић, М. (2014). *Ноам Чомски и савремено друштво*. Београд: Институт за политичке студије.

Christopher H., Moran M., Salisbury D. (2014): *Open Source Intelligence in the Twenty First Century- New Approaches and Opportunities*, (ed. Croft S.), Center for Science and Security Studies, King's College London, UK.

Harris, P. (2008): *Here Comes Everybody - The Power of Organizing Wthout Organizations*, CRM.

Johnson, L.K., (2010): *The Oxford Handbook National Security Intelligence*, Oxford University Press.

Mijalković, S. (2015). *Trash Intelligence kao metod obaveštajno-bezbednosnog rada*. Beograd: Kriminalističko-policijska akademija.

Spinello, R. (2011): Privacy and Social Networking Technology, *International Review of Information Ethics*, Vol. 16: .

На друштвеним мрежава проведемо 116 минута дневно", Доступно на: https://www.danas.rs/tehnologije/nadrustvenim-mrezama-provedemo-116-minuta-dnevno/ посећено 11.05.2022.

„*Преглед тржишта телекомуникација у Републици Србији у 2011 години*", РАТЕЛ, *Доступно на:* https://www.ratel.rs/upload/documents/Pregled_trzista/Pregled%20trzista%20telekomunikacija%20u%20 Republici%20Srbiji%20u%202011_godini.pdf *посећено* 11.05.2022.

„A Brief History of Open Source Intelligence" *Доступно на:* https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ *посећено* 20.05.2022.

„*What happens online in 60 seconds 2020*" *Доступно на:* https://www.google.com/search?q=what+happens+online+in+60+seconds+2020&source=lmns&client=o pera&hl=en-US&ved=2ahUKEwjVhPzTw5PqAhUN7xoKHZcbD48Q_AUoAHoECAEQAA *посећено 10.05.2022.*

Resume

Social networks are one of the most important sources of information in modern society. Various types of data are published on social networks. From private and personal, political, ideological, security, to various information from the world of economics. Each piece of information can have a certain intelligence meaning by itself, or in a wider or narrower context. The paper will explain how social networks can be used as an intelligence source of knowledge, the importance of collecting information from open sources, as well as the challenges that the intelligence community faces when it comes to this method of data collection. In this research, the author tried to explain how social networks can be used as a source of intelligence data, what is the importance of collecting data from open sources, and especially from social networks, as well as what are the challenges that the intelligence community faces when it comes to this data collection method. The nature of the research requires a multimethod approach, which includes the application of various procedures for the systematic collection and interpretation of data from different sources.

Key words: *social networks, sources of intelligence and security data, intelligence and security services, collection of intelligence and security data.*