Fakultet za kriminalistiku, kriminologiju i sigurnosne studije
Univerziteta u Sarajevu
KRIMINALISTIČKE TEME, Godina XIX, Broj 5
Zbornik radova
XVIII DANI KRIMINALISTIČKIH NAUKA
Međunarodna naučna konferencija
„Savremeni izazovi u cyber sigurnosti" – CFS 2019
Sarajevo, 2019.

Izdavač: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije
Za izdavača: prof. dr Nedžad Korajlić, dekan
Gost urednik: prof. dr Jasmin Ahić
Redakcija: Naučni i programski odbor Konferencije
predsjednik Odbora: prof. dr Jasmin Ahić (BiH), prof. dr Nedžad Korajlić (BiH), prof. dr Dina Bajraktarević Pajević (BiH), prof. dr Marija Lučić-Ćatić (BiH), prof. dr Muhamed Budimlić (BiH), prof. dr Lada Sadiković (BiH), prof. dr Sakib Softić (BiH), prof. dr Haris Halilović (BiH), dr.sci. Beba Ešrefa Rašidović (BiH), profesor emeritus Mirsad Abazović (BiH), dr.sci. Itamara Lochard (USA), prof. dr Samim Konjicija (BiH), prof. dr Jasmin Azemović (BiH), prof. dr Ratko Duev (S. Makedonija), prof. dr Oliver Bakreski (S. Makedonija), prof. dr Vančo Kenkov (S. Makedonija), prof. dr Andrej Sotlar (Slovenija), prof. dr Gorazd Meško (Slovenija), doc. dr Ivan Toth (Hrvatska), doc. dr Ivan Nađ (Hrvatska), prof. dr Lulzim Tafa (Kosovo), dr.sci. Krunoslav Borovec (Hrvatska), prof. dr Želimir Kešetović (Srbija), prof. dr Zoran Keković (Srbija), prof. dr Nikola Dujovski (S. Makedonija), prof. dr Marjan Gjurovski (S. Makedonija), prof. dr Milan Žarković (Srbija), prof. dr Zvonimir Ivanović (Srbija), mr. Nenad Sikirica (Hrvatska); sekretar Odbora: Ermina Bakić
Organizacioni odbor Konferencije
predsjednik Odbora: prof. dr Admir Hadžikadunić, prof.dr. Goran Kovačević, prof.dr. Almir Maljević, prof. dr Muamer Kavazović, doc. dr Elvira Čekić, doc. dr Armin Kržalić, dr.sci. Adnan Fazlić, Sandra Kobajica, MA, dr.sci. Nerma Halilović-Kibrić, Kenan Hodžić, MA, Predrag Puharić, Amra Hodo; sekretar Odbora: Mirza Buljubašić, MA

Lektor: Nizama Hodžić
Štampa: _____

ISSN: 1512-5505

XVIII Dani kriminalističkih nauka

Međunarodna naučna konferencija

„Savremeni izazovi u cyber sigurnosti“ – CFS 2019

ZBORNIK RADOVA

Sarajevo, 3-4. oktobar 2019.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

METODOLOŠKA ISTRAŽIVANJA U POLITICI I SIGURNOSTI KAO DIO KOMPJUTERSKE MANIPULACIJE PODACIMA U KREIRANJU SIGURNOSNE PERCEPCIJE JAVNOSTI

Stručni rad

Vanredni profesor dr Oliver Andonov[479]
Vanredni profesor dr Toni Georgiev[480]
Mr sc. Monika Andonova[481]

Sažetak

Uobičajeno kad govorimo o sajber sigurnosti (prevedeno kao kompjuterska sigurnost sa uticajem u sajber prostoru), mislimo na hakerske napade na kompjuterske sisteme ili na sigurnost podataka, pojedinih informacija, ličnih podataka i informacija.

U ovom radu naš cilj je da otvorimo jedno uslovno rečeno novo pitanje sajber sigurnosti, a koje se odnosi na metodologiju istraživanja političkih i sigurnosnih pojava sa aspekta naučnog pristupa i korišćenje suvremene kompjuterske tehnologije u kreiranju percepcije javnosti. Svakako da kreirana percepcija javnosti jeste i kreriranje javnog mnjenja, a to utiče na kretanje u društvu, ili kreiranje sigurnosne politike.

Pristup metodologije istraživanja političkih i sigurnosnih nauka i njihovo prevođenje u praksi veoma često se svodi na političku pragmu sa kojom se manipuliše u okviru naučne zasnovanosti prikazanih rezultata o društvenim kretanjima ili najviše u odnosu na percepciju sigurnosnih prijetnji i izazova. Jedan takav primer uslovljavanja kreiranja sigurnosne politike jeste „sekuritizacija" sigurnosnih problema kroz stvaranje percepcije javnosti kao uslov sekuritizacije. Sigurno da se ova percepcija ne može isključiti u odnosu na kreiranje javne komunikacije ili medija, ali smatramo da osnov upravo potkrepljivanja takvih stavova i percepcija jeste naučna potpora dobivenih rezultata.

Veoma interesantan pristup koji ćemo pokušati da otvorimo kao dilemu u ovom radu, jeste pristup u mjerenju laži u politici povezanih sa realnosti sigurnosnih ugrožavanja društva. Upravo prikazivanje ove realnosti i poticanje lažnih informacija jeste deo kreiranja javne percepcije o sigurnosti, a tome pridonosi sajber prostor kao glavni medij suvremenih društava i kreiranju percepcije građana o sigurnosti na svim nivoima.

Ovaj rad nema tendenciju da uradi cjelosnu elaboraciju i naučno istraživanje koje će u potpunosti determinirati korišćenje metodologije naučnog istraživanja i kreiranja željenih naučnih podataka radi stvaranja uticaja kroz sajber prostor na percepciju javnosti o sigurnosti i politici, već da pored tradicionalnih pogleda na sajber sigurnost u suvremenom svijetu i izazovima sajber sigurnosti pokušamo da pionirski otvorimo jedno novo

[479] Vojna akademija „General Mihailo Apostolski" –Skopje, andonov.oliver@yahoo.com
[480] Vojna akademija „General Mihailo Apostolski" – Skopje,tonigjorgiev@yahoo.co,uk
[481] Skopje, monika92andonova@gmail.com

poglavlje u kome je sajber sigurnost dio uticaja na društvena kretanja i kreiranju sigurnosne politike na svim nivoima.

Ključne reči
sajber prostor, metodologija političkih i sigurnosnih nauka, laži u politici, sigurnosna politika, percepcija javnosti

Uvod

Pisati znanstveni rad o sajber sigurnosti u vremenu razvijene informatičke tehnologije i dostupnosti informacija i pri tome se ograničiti isključivo na sajber terorizam ili upade u kompjutorske sigurnosne mreže jeste uobičajeni pristip ovom sigurnosnom problemu.

Upravo ovaj rad će pokušati da prezentuje jedan drugačiji pristup sajber sigurnosti u svjetlu sigurnosti građana i države, odnosno cjelokupnog društva. Korišćenje kompjuterskih tehnologija, informacionih sistema i tehničkih dostignuća u odnosu na ugrožavanje sigurnosti ne odnosi se uvijek i samo na tehničko-tehnološkom nivou ugrožavanja sigurnosti. Više nego ikada sajber sigurnost se ugrožava suptilnim korišćenjem znanstvenih dostignuća u cilju kreiranja javnog mnjenja i usmjeravanja političkih tokova i donošenja odluka.

Ovakav pristup ugoržavanja sigurnosti i to na državnoj razini (možemo da govorimo o državnoj sigurnosti) u svakom njenom segmentu, a da pri tome ne mislimo isključivo na zaštitu državnosti od direktnih ugrožavanja, jeste izraženo prisutan u suvremenim izvorima ugrožavanja sigurnosti.

Vidljivo je da akter ugrožavanja primenjuje suptilne metode i instrumente ugrožavanja objekta sa jedinstvenim ciljem da ostvari svoje interese, odnosno tradicionalno pitanje zaštite – „sigurnost od koga i od čega“ jeste poticaj za otvaranje različitog pristupa prema izvoru ugrožavanja.

Ciljevi koje izvor ugrožavanja želi da postigne u suvremenim okolnostima nisu puno različiti od onih povjesnih, odnosno zavladavanje ili potčinjavanje države i naroda. Različne su metode i pristipu koji su takoreći manje nasilni, ali ne imanje pogubni za napadnutu državu ili društvo. Jedan od isključivo važnih pristupa jeste ovladavanje političkom sferom uticaja države, a to se može pokriti demokratskim izborom građana te države koji na osnovu dobivenih informacija glasaju na izborima i na taj način na vlast dovode političku strukturu koja rukovodi državom. Ubjeđeni u najbolji izbor i vjerujući svemu rečenom i pretstavljenom kao i prikazanim „istraživačkim“ prikazima o tendencijama ko je u prednosti, raznim lažnim vijestima i kreiranim informacijama, potpuno i metodički pristupajući kroz sajber prostor kreira se javno mnijenje koje u datom trenutku donosi odluku koju upravo izvor ugrožavanje želi da bude donesena. Pri tome sve je to izraz demokarcije i volje naroda.

Da bi ovaj izraz demokracije i da bi ta i takva volja naroda mogli da budu obezbjeđeni i verifikovani, kretorima javnog mnijenja potrebni su mnogi elektronski obrađeni podaci koji imaju statističku osnovu i koji služe za obradu terena. Neizostavni dio te zloupotrebe podataka jeste i korišćenje ličnih podataka, a sa ciljem praćenja individualnih aktivnosti na socijalnim mrežama i u sajber prostoru i sprovođenje anketa i testiranja javnog mnijenja po opredjeljenim pitanjima oko kojih će se izraditi strateški pristup za kreiranje osnovnog javnog mnijenja.

U osnovi ovih operacija jeste poznavanje metodologije političkih znanosti i upotrebi sajber prostora u prikupljanju i slanju informacija prema strateškoj procjeni izvora ugrožavanja. Ovaj rad neće obuhvatiti metode suprotstavljanja već samo sistem metodološkog pristupa istraživanja u politici i pri tome zloupotrebe ličnih podataka i aktivnosti na socijalnim mrežama. Ovakav pristup radu daje karakter preglednog rada u klasifikaciji znanstvenih radova, ali nadamo se da će u budućnosti prouzrokovati interes za konkretno znanstveno istraživanje.

1. Sajber prostor i mogućnosti njegove zlouporabe

U zavisnosti od različitih perspektiva i društveno socijalnih gledišta, ne postoji jedinstvena ili unificirana definicija o tome što predstavlja sajber proctor. Sama riječ smatra se nasljednikom riječi kibernetika (cybernetic), a koja što semantički potiče od grčke riječi "kybernetes", koju prvi put spominje Norbert Winner prilikom njegovog rada sa elektronskim komunikacijama i avtomatizacijom. Sajber prostor kao pojam je najviše povezan sa informatičkim i telekomunikaciskim tehnologijama. Svakako njihovim razvojem godinama je mijenjana percepcija o tome što obuhvata sajber prostor kao pojam.

Jedna od većinom definicija o sajber prostoru daje Internacionalna Telekomunikacijska Jedinica (International Telecommunication Union – ITU), koja je specijalizirana agencija Ujedinjenih naroda namjenjena za informaciske i komunikaciske tehnologije. Prema definisanju ove Agencije, sajber prostor predstavlja: „skup korisnika, mreža, uređaja, softverskih procesa, informacija koji su sačuvani ili koji su u tranzitu, aplikacija i sistema koji mogu direktno ili indirektno da se povežu na mreži".[482]

Još jednu definiciju daje Talinski priručnik, koji pomoću međunarodnih zakona daje legalnu i nepolitičku perspektivu rješavanja sajber konflikata. U osnovi priručnik predstavlja pravni kodeks, uređen sa strane međunarodne grupe pravnih stručnjaka. Pri tome, sajber prostor se definiše kako: „sredina oformljena od fizičkih i abstraktnih

[482]International Telecommunication Union: **"Series X: Data networks, open system communications and security: overview of cybersecurity"**, 2008, str. 2

komponenata, koja se karakterizuje upotrebom kompjutorskih i elektronskih komponenata, sa ciljem očuvanja, modifikovanja i razmjene podataka upotrebom kompjutorskih mreža".[483]

Potrebno je napraviti distinkciju između poima internet i sajber prostor, koji su sasvim različiti ali su tijesno povezani. Sam internet i svi njegovi elementi (web strane, aplikacije) su komponente koje između ostalog formiraju sajber prostor gdje se odvija ogromna razmjena informacija. Sve većim porastom upotrebe interneta, povećava se sajber prostor koji se stalno puni podacima i informacijama svakakvog sadržaja. Ovakvim pristupom, sajber prostor ulazi u sve aspekte današnjeg društva i svakodnevnog života, a porastom njegove kompleksnosti raste i opasnost od njegove zlouporabe.

Prateći zadnju definiciju sajber prostora, možemo zaključiti da kada postoji sajber prostor postoje i sajber konflikti, a samim tim i različiti oblici napada i narušavanja ove sredine, odnosno razni načini njene zlouporabe posebno za nelegalna i protuzakonita dejstva.

Sajber napad predstavlja: „neovlaščeni pokušaj otkrivanja, krađe, pristupa do podataka, informacija ili kompjutorskih sustava i mreža, a najčešće sa malicioznim ciljem. Pre nego što klasifikujemo sajber napade, uradićemo pregled klasifikacije prijetnji u sajber prostoru. Pretnje mogu da budu slučajne ili namjerne i aktivne ili pasivne.

Slučajne prijetnje su rezultat ne namjernog pronalaženja defekata u softveru ili sustavu. Namjerno - planirane prijetnje, klasifikuju se različito od slučajnih upotrebom ureda za monitoring, pa sve do napada koji uključuju ozbiljna poznavanja sustava. Namjerne ili planirane prijetnje tretiraju se kao sajber napadi.

Pasivne prijetnje su one koje ukoliko se realizuju neće rezultirati nikakvim promjenama u sustavu, softveru ili te podataka sačuvanih u samom sustavu. Aktivne prijetnje uključuju promjenu informacija koje sadrži sustav ili promjenu u načinu rada samog sustava.

Prilikom dizajniranja sustava i produkta koje mogu biti cilj sajber prijetnji, potrebno je utvrditi mesta u sustavu kdje može doći do ovakvih napada i adekvatno ih zaštititi. Ipak moramo biti svjesni toga da uvjek postoji mogućnost i pored zaštite, sustavi i softveri da postanu žrtve sajber prijetnji, ali se ipak ovim pristupom zaštite smanjuju posljedice za realizaciju prijetnje.

Kada govorimo o sajber napadima, u zavisnosti od cilja koji se želi realizovati, mogu se klasifikovati u napade koji imaju za cilj da onemoguće rad napadnutog sustava, ili napad

[483]Michael N. Schmidt: **"Tallinn Manual on the International Law applicable to cyber warfare"**, Cambridge University Press, New York, str. 278

sa ciljem pristupa podacima koji su skaldirani u sustavu koji je napadnut ili dostup drugim informacijama, administratorskih prava i slično.

Postoji više tipova sajber napada koji se često nadopunjavaju i mijenjaju posebno razvojem tehnologije i samim tim se međusobno isprepliću pri čemu ne postoje koncizne granice. Postoji nekoliko njih i neke ćemo da objasnimo.

Malware – kovanica engleskog pojma malicious software ili takozvani „zlunamjerni softver". Bez obzira na to kakav je softver i kako je upravljan i dizajniran, ukoliko je cilj nanošenja štete targetovanom sustavu taj softver se smatra malicioznim, zlunamjernim. Ovim softverom može se napravite šteta funkcionalnosti sustava, mreže ili izvršilac napada se može ugnjezditi u korjen sustava odakle će moći da kontroliše cijeli sustav sa daljine.

Phishing – Fišing je tehnika kojom sajber kriminalci šalju mail poruke pokušavajući da obmanu subjekat. Subjekat koji je primio poruku može biti obmanut i sam izvrši skidanje malicioznih datoteka koje će uništiti rad sustava. Veoma često u ovakvim mailovima postoje linkovi do web sajtova koji traže podatke, senzitivne informacije, passworde, korisnička imena, bakovne račune ili nude anketne upitnike u vezi neke aktualne društvene teme. Ove informacije napadači kasnije koriste za opredjeljene ciljeve. Uobičajeno ovi email napadi se šalju ljudima slučajnim izborom, ali često su ljudi i grupa unaprijed targetirani sa ciljem sondaže terena ili dobijanja neke informacije koju ta grupa ljudi ima ili je važna za ostvarivanje ciljeva.

Negiranje usluge – Ovaj napad se upotrebljava da bi se zaustavio pravilan rad nekih internet usluga. Naprimjer, šalje se ogromna količina zahtjeva na neki web sajt ili na neku bazu podataka čime se opterećuje sustav i dovodi do toga da usluga bude nedostupna za sve korisnike. Vrlo često prilikom ovakvih napada upotrebljava se veliki broj kompjutora koji prije toga su napadnuti malicioznim softverima i stavljeni su pod kontrolom sajber kriminalaca radi preusmjeravanja saobraćaja sa svih prema ciljanom sustavu.

Čovjek u sredini – jeste metod kada se napadač tajno umiješa između korisnika i web usluge kojoj korisnik pristupa. Kao primjer može se uzeti zlouporaba wi-fi mreže gdje sajber kriminalac imitira mrežu na kojoj ukoliko se korisnik konektuje, napadač može da pristupi do sve informacije koje korisnik ispraća ili prima, uključujući passworde, bankovne i lične podatke.

Cryptojacking – je specijalizirani napad pri čemu se uzima neki kompjuter koji treba da generira kriptovalute za potrebe napadača (proces nazvan „mining" ' rudarenje). Napadač instalira maliciozni softwere u kompjuter žrtve ili startuje kod u Java skript koji se realizuje u pretraživaču žrtve.

SQL injection – napadač preko eksploatacije neke slabe točke u bazi podataka ili sustava preuzima cjelu bazu podataka žrtve napada. Najveći broj data baza su dizajnirane da reaguju na komande napisane strukturnim jezikom za pretragu (Structured Query Language), a ogromni broj web strana koje na bilo kakav način uzimaju određene podatke od svojih korisnika šalju te podatke u SQL bazi podataka. U ovakvim tipovima napada, napadač može da napiše nekoliko komandi u web formatu gdje može tražiti određene informacije kao što su imena, prezimena, adrese i drugo. Ukoliko baza podataka i web strana nisu adekvatno programirani i zaštićeni, ovakve komande može da daje i napadač i samim tim da dođe do podataka i ličnih informacija korisnika.

Danas, kada sajber prostor predstavlja našu svakodnevicu, napadi i zlouporaba su sve češći i razvijeniji. Pored standardnih ekonomskih, financiskih ili obavještajno-sigurnosnih ciljeva napada u kojima nerijetko učestvuju i vladine službe, sve je češća pojava da svaka individua postaje cilj sajber zlouporabe. Sve većim tempom razvoja znanosti povezanih za podatke – Data Science, svako od nas pojedinačno postaje potencijalna žrtva. Svakidašnjem korišćenjem socijalnih mreža i uopšte internet pristupa i internet tehnologija svi podaci koje slučajno ili namjerno unesemo u sajber prostor mogu biti zlopuptrebljeni za različite ciljeve.

Jedan od veoma čestih ciljeva zlouporabe ličnih podataka jeste i istraživanje u cilju kreiranja javnog mnijenja za političke ciljeve, odnosno odrešivanja ciljnih grupa i interesnih zajednica.

2.Uticaj na kreiranje javnog mnjenja za političke ciljeve kroz upotrebu kompjuterskih instrumenata metodologije znanstvenih istraživanja

2.1. Analiza, konstrukcija instrumenata, navođenje na željene odgovore, obrada podataka i njihova upotreba

Prilikom istraživačkih postupaka u cilju stvaranja relevantnih rezultata sasvim je normalno da se pojave greške. Ove greške mogu biti nenamerne, i njihovo odstranjivanje jeste permanentni zadatak istraživača ukoliko nam je tendencija da dobijemo znanstveno relevantne, potvrđene i proverljive rezultate istraživanja.

Upravo kao znanstvena suprotnost ovakvog pristupa, imamo tendencioznu pojavu grešaka koje kao posljedica projektiranja i realizacije istraživanja prouzrokuju namjerne sistematske „pogreške“ u istraživanju.

Ovakve namerne greške u okvirima potrebe sprovođenja istraživanja sa ciljem stvaranja lažne slike i kreiranja percepcije javnog mnijenja najčešće nisu rezultat neznanja, već namerno pogrešno konstruisanog teoriskog koncepta istraživanja, unapred određenog cilja rezultata istraživanja, pri čemu se neprimjenjuju pravila modela istraživanja, metodskih

postupaka, upotreba instrumenata i što je najvažnije, nepoštovanje etičkih načela u istraživanju. Ovo je rezultat unapred određenih „neophodnih" istraživačkih rezultata, a greške su katastrofalne i tendenciozno se izbegava logička analiza i ukrštanje podataka, već se upravo usmjerava ceo proces ka kreiranju istraživačkih podataka odnosno rezultata istraživanja. Ovakav pristup istraživanju jeste uvod ka stvaranju rezultata „željenih odgovora" i time otvaranje mogućnosti da se kroz pseudo znanstvene podatke i metodološki koncept prezentuju „relevantni" rezultati koji će imati uticaj na kreiranju javnog mnijenja u politici.

Nakon uvoda u istraživanje i tendenciozno stvaranje sistematske greške kroz ekspoloataciju pogrešnog teoriskog koncepta i samim tim i pogrešnog metoda i instrumenata dolazi do obrade dobivenih rezultata.

Obrada podataka se determinira „konzistentan sistem logičkih, epistemioloških, statističkih (matematičkih) i tehničkih postupaka kontrole, klasifikacije, grupisanja, prikazivanja, upoređenja, povezivanja, ukrštanja i kombiniranja podataka svih vidova u suglasnosti sa osnovnom idejom predmeta istraživanja i prema odredbama pravila istinskog mišljenja, dokazivanja i provjeravanja".[484]

Upravo polazeći od premise istinosti i znanstvene relevantnosti istraživanja druga faza istraživačkog procesa nakon sređivanja dobivenih podataka jeste analiza podataka. Cilj ove faze jeste izvođenje analize kao misaonog procesa u kome trebamo razlučiti istinitost i kvalitet istraživanja posebno preko provjere postavljenih hipoteza i upotrebe analitičkih tehnika. Ovo je u suštini faza u kojoj je veoma lako doći do istine, odnosno utvrditi validnost dobivenih podataka koje bi trebalo da se prezentuju u javnosti i prikazati kao javno mnijenje u vezi neke društvene pojave, rejting političkih stranaka ili stav građana o nekom događaju u društvu. Interesantno je što najčešće zbog tendencije stvaranja javnog mnijenja i pored dobro postavljenih hipoteza korektne obrade podataka i dobivenih rezultata, u ovoj fazi analize, postoji isključivo velika mogućnost namještanja podataka, odnosno njihovog prepravljivanja u okvirima korišćenja softverskih rešenja za obradu podataka. U praksi ovo znači vraćanje unatrag u prethodnoj fazi pri čemu analiza podataka utiče direktno na sređivanje podataka, izbegavanje njihove logičke kontorle i karaktera podataka. Pri tome, veoma je lako staviti bilo koje podatke u okvirima tabela, grafikona, dijagrama i slično koristeći bilo koji kompjuterski sistem za obradu podataka (MS Excel, SPSS, Statistica, StatGraf i sl.). Iskusne istraživačke agencije za mjerenje javnog mnijenja I stavova građana u politici još tokom sakupljanja podataka na terenu znaju da na osnovu konstrukcije istraživačkih instrumenata mogu sukcesivno i simultano da prate trend odgovora ispitanika, pri čemu se faze istraživačkog procesa uopšte ne moraju dijeliti već se u nekim momentima koriste zajedno. Informacije prikupljene istraživačkim

[484]Cane T.Mojanoski, **"Metodologija na bezbednosnite nauki-analitički postapki"**, Kosta Abraš, Ohrid-Skopje, 2015, str.31

instrumentima (anketni list, ček lista, intervju, protokol o osmatranju pojava i slično), unose se u kompjuterski sistem kroz izabrano softversko rješenje, ali te podatke unosi istraživački tim koji ima uvid u hipoteze i prije svega u cilj istraživanja, tako da sistematska-katastrofalna greška se prilagođava potrebama rezultata istraživanja, odnosno političkih ciljeva. Ovde se ne izvode logički zaključci o mogućim greškama, već se greške prilagođavaju željenim rezultatima, a time se stvara pogrešna slika o javnom mnijenju građana ili se na osnovu prikazanih rezultata kreira pogrešno javno mnijenje. Možemo uzeti primjer upotrebe sekuritizacije nekog sigurnosnog problema za potrebe kreiranja sigurnosne politike i kreiranja prijetnji od nekih izvora ugrožavanja koji ne mora da su upravo aktuelni ili direktno ugrožavajući.

Da bi se cijela ova operacija sprovela i ista izgledala logično posebno za javnost, neophodno je da se kreiraju adekvatni istraživački instrumenti koji bi sugerisali željene odgovore ispitanika. Na ovaj način kreiranje lažnih znanstvenih istraživačkih podataka biće olakšano jer će kroz instrument istraživanja i poticanje očekivanih odgovora ispitanika biti lakše unositi podatke u softverski sistem bez logičke kontrole. Teži put je da se nakon korektno realizovanog istraživanja bukvalno falsifikuju dobiveni podaci da bi se u javnosti prikazao željeni rezultat i time uticalo na kreiranje javnog mnijenja u politici.

Rezultata ovoga jeste upotreba simulacije, prije i za vrijeme istraživanja, a u pravcu političkih očekivanja ispitanika po određenom društvenom pitanju pri čemu je upotreba suvremenih kompjuterskih tehnologija neophodna.

2.2. Simulacija političkih očekivanja i kreiranje javnog mnijenja

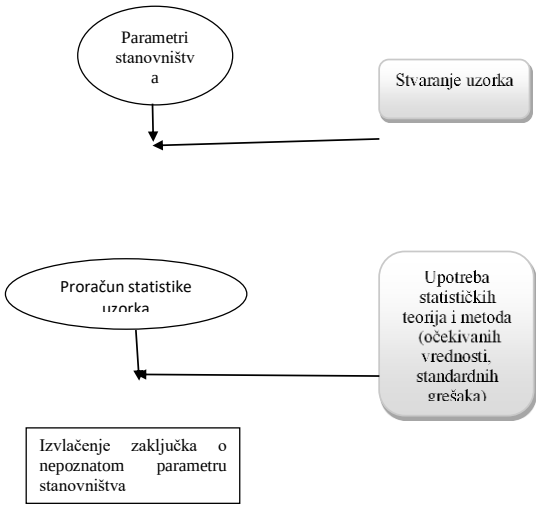
Politička očekivanja su sublimirana u dobivenim efektima reklamiranja političkih kampanja i kroz njih kreiranju javnog mnijenja. Reklame mogu imati i veoma slab efekat na populaciju, ali upravo zato kreiranje lažnih vjesti ili cjelih informacija, a posebno kreiranje kvazi znanstvena istraživanja i njihovi rezultati mogu preusmjeriti javno mnijenje i cjelovite rezultate političke kampanje. Upravo ovakvi ciljevi traže simulaciju mogućih odgovora ispitanika i njihovo usmjeravanje ka istima. Kako doći do željenih rezultata upravo definiše simulacija političkih očekivanja. Svakako da ova simulacija u osnovi ima realno i kvalitetno znanstveno istraživanje i točne proračune statističkih podataka, ali upravo zato sljedeći korak jeste manipulisanje podacima i opet simulacija podataka. U tome kontekstu jedan od najznačajnih istraživačkih ciljeva jeste: „istražiti vezu između karaktera kampanja i tendencije glasanja“, a pri tome se u osnovi nalazi tonalitet kampanja, a sve to ovisi od legitimiteta kritike u javnim medijima što je istraživački zaključak Kana i Kenedija.[485] Upravo zbog ovakvog mogućeg ponašanja ispitanika možemo modelirati ili maksimizirati (subjektivno ili psihološki) korisnost dobivenih odgovora ili ponašanja ispitanika

[485]Jannet Buttolph Johnson and H.T.Reynolds, **“Political Science Research Methods”**-Sixth Edition, Akademski pečat, Skopje, 2012, str.39-40

u korist našeg cilja istraživanja, što svakako nije etički a ponajmanje metodološki i istraživački ispravno. Supstituirajući modeliranje upotrebljavamo simulaciju mogućnosti i uticaja odgovora ispitanika i korišćenju njihovih ličnih podataka, a u čemu potpuno zavisimo od upotrebe kompjuterskih odnosno sajber znanja i tehničkih mogućnosti.

Simulacija jeste reprezent sistema kroz koji se povremeno studira sam sistem i njegovo ponašanje. Jadinice analize nisu diskretne individue, a fundament interesa jeste proces ili struktura kao što je to partička struktura ili društvo, koja što sadrži nekoliko ili mnoštvo komponenata. Do onog momenta kada individue ulaze u simulaciju, njihovo ponašanje kao kolektiv jeste glavni interes. Osnovno sredstvo istraživanja jeste kompjuterski program sa raznim i velikim mogućnostima, a što omogućava istraživaču da vidi kako se komponente sustava odnose i mjenjaju.[486] Osnovni faktor simulacije jeste vrijeme koje ističe dinamične interakcije unutrašnjih elemenata i njihovu kauzalnost prije svega recipročnu. Posebno je važno i cjelokupna tendencija simulacije jeste utvrđivanje mogućnosti da li sustav izlazi iz kontrole. Ovo je ustvari i glavni faktor koji utiče na intenzitet i veličinu kreiranja lažnih podataka, lažnih vijesti ili drugih tendencioznih informacija koje trebaju biti predstavljene javnosti i uticati na kreiranje javnog mnijenja.

Slika br. 1 Proces donošenja zaključaka na osnovu istraživačkog uzorka



[486]Ibid, str.192

Upravo zbog ostvarenje cilja uticaja na javno mnijenje i njegovo kreiranje u procesu simulacije mora se izabrati pravi ili istiniti primjerak istraživanja, a da bi ukazivalo na istinitost i znanstvenu istinitost istraživanja. Kreiranje javnog mnijenja traži donošenja zaključaka na osnovu iskorišćenog istraživačkog uzorka. Ovo donošenje zaključka jeste proces koji prikazujemo na slici br.1.

Upravo nam ova slika pokazuje kako se stvara primjerak istraživanja kao uzorak odabira onog djela stanovništva kroz koji hoćemo da nametnemo svoje stanovište i kreiramo javno mnijenje, a da u cjelome kontekstu imamo znanstvenu podlogu istraživanja.

Ovakav pristup izvlačenja zaključaka traži od kreatora lažnih vjesti ili lažnih istraživanja prije nego što krenu u simulaciju da imaju dostupnost do baze ličnih podataka ispitanika kako bi lakše opredijelili primjerak uzorka (N). Ovu bazu podataka mogu obezbijediti u državnim sustavima baze podataka (svakako ako se radi o vlasti) ili u vlastitim stranačkim bazama podataka. Svakako da ovi podaci mogu biti zlouporabljeni pa čak i sami kreirani u nekim segmentima koji direktno utiču na istraživačke rezultate.

3. Zaštita ličnih podataka u sajber prostoru i objavljivanje lažnih vijesti kao dio zloupotrebe kompjuterskog prostora

Proces koji nas okupira novom erom digitalizacije i digitalnog čuvanja podataka sve više postaje ozbiljan problem ne samo sa sigurnosne točke gledišta već i sa pravnog aspekta zaštite podataka. Zaštita ličnih podataka predstavljaju formalno-pravni i društveni fundament svakog fizičkog i pravnog lica, a u isti vrijeme predstavlja i sve vaća opasnost zbog otežavajuće kontrole mogućnosti da ovi senzitivni podaci dođu u nečije ruke i kako će i u koje svrhe biti upotrijebljeni. Formiranje državnih agencija za zaštitu ličnih podatka, prosljeđeno zakonski uređenim nadležnostima nije dovoljno, posebno gledano sa stanovišta njihovog postojanja kao čuvari. Potrebno je napraviti korak dalje u oblasti izvještavanja, ranog upozorenja i uzbunjivanja na nivou brze reakcije da je izvršen upad (bez obzira na razlog istog) u bazu ličnih podataka.[487]

U tom širokom prostoru zlouporabe ličnih podataka jeste i kreiranje lažnih profila koji se u strogo određenim ciljevima upotrebljavaju u okvirime socijalnih mreža, upravo koriste pravnu prazninu tipa neregulisane legislative, a to je ozbiljan problem koji omogućava zlouporabu ličnih podataka za krieranje politički motivisanog javnog mnijenja. Na račun sigurnosti, lišavamo se privatnosti, što postavlja dilemu „gdje je pravo privatnosti ili građanske i ljudske slobode“? Upravo zlouporaba ličnih podataka jeste pravni problem ne samo fizičkih već i pravnih lica i pitanje „od čega se trebaju oni odreći da bi sačuvali svoju sigurnost“? Samim ovim pitanjem ulazimo u sferu ekonomske sigurnosti, sigurnosti

[487] B. Pavišić, **„Kazneno pravo Vijeca Europe, Izvori, komentari, praksa”**, Golden marketing, Tehnička knjiga, Zagreb, 2006, str. 58

tržišta i jednakih mogućnosti, a svakako da biznis sektor ima veliki uticaj na politiku i političke odluke i stavove glasača. Ovo nas uvodi u razmišljanje da se lični podaci u cilju kreiranja javnog mnijenja veoma uspješno mogu upotrebiti i kriz podatke pravnih lica i to u biznis sektori i svakako u svim sektorima u zavisnosti od ciljane grupe.

Zbog svega što smo nabrojali i naveli kao mogućnost zloupotrebe ličnih podataka, postavlja se još jedan problem, a to je zaštita ličnih podataka pravnih lica, ne samo u okviru njihove elektronske korespodencije ili prava inovacija i industriskog vlasništva, transakcija već i intelektualna prava. Svakako da je velikim dijelom zaštita svih ovih aspekata regulisana u međunarodnom kompjuterskom pravu i zaštita žigova i drugih oblika elektronskog vlasništva, ali zaštititi podatke od zlouporabe za političke ciljeve je veoma teško.

Pravni pristup sajber kriminalu se uglavnom svodi na krađu kao definisani i krivično-pravni prekršaj učinjen sa strane jednog ili više lica, radi ostvarivanja određenog cilja, ali korišćenje podataka u okvirima istraživanja ili kvazi znanstvenog istraživanja koji mogu biti izmišljeni ili djelomično tačni nije pravno regulisano u okvirima sajber kriminala i samim tim se teško sankcioniše. Možemo govoriti o krađi podataka, ali to ne mora da bude direktno i potpuno obavljeno i vidljivo iskorišćeno, tako da je samim tim i teško utvrditi osnov kazneno-pravnog djela koje bi bilo kaznivo sankcionisano.

Jedan takav primjer zlouporabe ličnih podataka u cilju „istraživanja“ jeste lažno reklamiranje u ime T'mobila, pri čemu se telefon vrijednsoti 500 eura prodaje za samo 1 euro, ali prije toga se treba odgovoriti na desetak pitanja koja imaju za cilj ulaz u lične podatke financiske prirode.

Kao rezultat upravo jednog ovakvog primjera možemo zakjučiti da pravo ne može samo da reguliše već da preveniše i usaglasi nacionalno i međunarodno pravo.

Zaključak

Kroz rad koji smo prezentirali možemo da sagledamo nekoliko aspekata uticaja na sajber sigurnost i mogućnost kaznenih djela kako sa strane kazneno-pravnog aspekta, tako i sa strane isključivo stručnih postupaka i determiniranih načina upada u sajber prostor radi nanošenja štete i preuzimanja podataka.

Postojanje čvrste povezanosti zaštite ličnih podataka i njihovo korišćenje u cilju političke manipulacije i metodologije političkih istraživanja i stvaranja javnog mnijenja jeste vidljivo i pručavanjem podataka u jednom preglednom znanstvenom radu kao što je ovaj.

Zlouporaba ličnih podataka, upadanje u kompjutorski sustav, neregulisane pravne procedure i posebno ne tretiranje ovog tipa manipulacija kao krađa zbog ostvarivanja

imovinsko-financiske koristi, predstavlja ozbiljan problem sankcionisanja ovakvog tipa zlouporabe podataka. U suštini, radi se o korišćenju kompjutorskih tehnika i sajber prostora da bi se njima manipulisalo sa ciljem ostvarivanja političkih ciljeva, a sve to pokriveno znanstvenim (pseudo znanstvenim) istraživanjem.

Suvremena stvarnost je isključivo podložna ovakvom manipulacijom sajber prostora i znanstvenih istraživanja. U nekim slučajevima to su takozvane lažne vijesti, ali glavni cilj metodološke manipulacije u sajber prostoru jeste da se takozvanim znanstvenim autoritetom može manipulisati javnim mnijenjem i u isto vrijeme vršiti uticaj na njega, odnosno kreirati ga u pravcu ostvarenja vlastitih političkih ciljeva i to najčešće samo u datom trenutku i na kratkom periodu.

Postavlja se jednostavno pitanje. „Kako se odupreti ovoj pojavi i zlouporabi“? Odgovor je višeslojan i nalazi se u rješenju kazneno-pravnih regulativa ne samo u krađi ličnih podataka ili imovinsko-financiske koristi počinioca djela, već i u bilo kakvom obliku (makar i šaljivom) uzimanja tuđih ličnih podataka bez saglasnosti, zabrane kreiranja lažnih profila na socijalnim mrežama iako je to teško utvrditi, ali nije nemoguće pronaći ih i blokirati, ojačati kontrolu i zaštitu sustava u domenu sajber prostora od nanošenja štete upadima.

Ipak najvažnija je etika znanstvenika i njihova istraživačka djelatnost bazirana na točnim metodološkim postupcima i prezentiranju točnih znanstveno izdržanih podataka koji su lako provjerljivi. Svakako da je i ovo teško u realnosti ostvarljivo, jer ovaj tip pseudo znanstvenih istraživanja najčešće rade ljudi koji nisu u znanosti ili ljudi iz znanosti kojima je važnije ostvarivanje političkih ciljeva koje podržavaju.

Sukob etike u znanosti i želja za ostvarivanje vlastitih političkih ciljeva i interesa je uvjek prisutan i tako će i ostati. Ostaje na svima nama koji smo prisutni u sajber prostoru i koji smo “bombardovani“ informacijama potkrepljenih znanstvenim istraživanjem da provjerimo verodostojnost ovih informacija, mišljenja, stavova i anketa javnog mnijenja i da nakon toga donesemo vlastiti sud o društvenoj temi koja se obrađuje u sajber prostoru.

Bibliografija

1. Branislav Pavišić, „Kazneno pravo Vijeca Europe, Izvori, komentari, praksa", Golden marketing, Tehnička knjiga, Zagreb, 2006.
2. Cane T.Mojanoski, "Metodologija na bezbednosnite nauki-analitički postapki", Kosta Abraš, Ohrid-Skopje, 2015.
3. Jannet Buttolph Johnson and H.T.Reynolds, "Political Science Research Methods"-Sixth Edition, Akademski pečat, Skopje, 2012 .
4. Michael N. Schmidt: "Tallinn Manual on the International Law applicable to cyber warfare", Cambridge University Press, New York 2013.
5. International Telecommunication Union: "Series X: Data networks, open system communications and security: overview of cyber security", 2008.