Strategos, 3(2), 2019, 97-102
UDK 32
UDK 355/359

STRATEGOS

Osvrt

Operacije utjecaja: nova ili već poznata paradigma

brg dr. sc. Mladen Viher

Tehnološki razvoj u zadnjih nekoliko desetljeća doveo je ne samo do korjenitih društveno-ekonomskih promjena nego i novih paradigmi, među koje možemo ubrojiti i „operacije utjecaja" (engl. *Influence Operations*). U ovom osvrtu prikazat ćemo njihove temeljne značajke na način kako ih je predložio Bruce Schneier, jedan od najpoznatijih svjetskih zagovornika slobodnog i sigurnog interneta. U svojem eseju objavljenom u časopisu *Foreign Policy* (Schneier, 2019), kao i na svojoj internetskoj stranici (www.schneier.com), predložio je uporabu pojma „operacija utjecaja" i time potaknuo intelektualnu raspravu o njegovu točnom definiranju i prepoznavanju u aktualnim događanjima. Ovim prikazom želimo potaknuti interes i budući znanstveni diskurs o toj temi u okviru našeg časopisa.

Schneier je primijetio da pojam „operacija utjecaja" izmiče strogoj definiciji, ponajprije zbog širokog područja ljudskih djelatnosti koje zahvaća, a to se stanje nije bitno popravilo još od prvih radova o toj temi (Larson et al. 2009). Operacije utjecaja nadmašuju djelovanja definirana kibernetičkim ili hibridnim operacijama, ponajprije stoga što operacije utjecaja zahvaćaju cijelo društvo po širini i dubini, pa čak i nadnacionalne odnose i politike. Unatoč tome možemo se složiti oko inherentne dvosmjernosti operacija utjecaja: one počinju prikupljanjem informacija o protivniku i uočavanjem njegovih slabosti te zatim aktivnim djelovanjem prema njemu kako bi se uočene slabosti iskoristile za postizanje napadačevih ciljeva. Ono što je izvoran doprinos u Schneierovom osvrtu jest precizno opisivanje osam načina provedbe operacija utjecaja preko suvremenih medija, kao i načina učinkovitog djelovanja na suzbijanje ili barem djelomično poništavanje njihova utjecaja. U nastavku ovog osvrta ukratko ćemo proći svih osam

načina, redoslijedom kako ih je naveo Schneier. U svakom slučaju, upućujemo čitatelja na izvornik.

1. Otkrivanje „pukotina u tkanju društva"

Napadač uočava pukotine u „tkanju društva", odnosno uobičajene demografske, socijalne i etničke podjele, koje se sustavno prenaglašavaju kako bi se oslabilo povjerenje u postojeće institucije društva. Pritom se radi većeg učinka najčešće ističe ona podjela od koje se očekuju najveći i najbrži učinci, i to na način koji odgovara napadaču.

Otvorene društvene razlike značajka su svakog razvijenog demokratskog društva, ali one se uobičajeno rješavaju na temelju konsenzusa i neupitnosti temeljnih demokratskih vrijednosti. Razvoj zdrave demokracije preventivna je mjera za operacije utjecaja s obzirom na to da populacija izložena takvim napadima izražava otpor. Naime, lako se prepoznaju neargumentirane i emotivno nabijene lažne informacije te se najprije postavlja pitanje: „*Cui bono?"*.

2. Izgradnja ciljane publike

Ako napadač ima dovoljno vremena, odnosno dalekosežne ciljeve, posegnut će za time da oblikuje publiku koja je sklona prihvatiti njegove poruke, bez obzira na to koliko u početku bila brojčano mala i možda društveno neutjecajna. To se najbolje postiže stjecanjem kontrole nad medijem koji stvara utjecaje i uspostavljanjem društvenih mreža, pri čemu operativci napadača uopće ne moraju biti ljudi, nego to mogu biti i algoritmi (tzv. *botovi*) koji svoj utjecaj šire preko društvenih mreža. Za to su idealna meta pojedinci koji će dalje širiti utjecaj napadača, i to na suptilniji i inteligentniji način od botova. Prednost je botova ta što odjednom mogu pokriti velik broj veza i usklađeno djelovati u više smjerova na topologiji društvene mreže, uz mogućnost trenutačne prilagodbe svakoj situaciji.

Većina populacije u razvijenim zemljama svakodnevno je prijavljena na jednu društvenu mrežu ili više njih. Na svakoj od tih društvenih mreža postoji problem trolova i botova, koji korisnicima stvaraju razne vrste neugodnosti.

Tvrtke koje su vlasnici tih mreža razvile su standardne postupke za suzbijanje tih utjecaja, a katkad se za pomoć obraćaju i nadležnim državnim tijelima. Zasad je utvrđena velika razlika u pristupu sigurnosnih agencija u odnosu na privatne tvrtke u borbi protiv pokušaja formiranja zlonamjernih skupina. U suzbijanju ove vrste operacija utjecaja potrebno je bolje uskladiti i zakonski regulirati javni i privatni interes na društvenim mrežama, ali isključivo uz aktivan i otvoren civilni nadzor nad metodama i protumjerama koje se provode.

3. Stvaranje zamjenske priče

Jedan od preduvjeta za uspješne operacije utjecaja jest prethodno pripremanje „zamjenske priče" (engl. *alternative narrative*) koja unosi zabunu, sumnju i u svakom slučaju otežava i izobličava svaki oblik rasprave. Suvremeno širenje informacijskih tehnologija omogućuje laku provedbu stvaranja zamjenske priče, pri čemu je napadaču zapravo veći problem prikrivanje izvora, a to se obično izvodi navođenjem lažnog izvora i tehničkom pripremom same informacije, koja tada ima sva obilježja lažnog izvora (krivotvorena svojstva i oznake na multimedijskim datotekama tako profesionalno krivotvorene priče nazivaju se engl. *deepfakes*).

Tvrtke koje održavaju društvene mreže i mrežne usluge stalno prate i djeluju protiv zamjenskih priča, onemogućujući njihovo širenje u samom začetku. Najbolji je način zaštite podizanje razine osviještenosti i pravovremena prijava administraciji mrežnih usluge. Zamjenske priče vrlo je teško uočiti i utvrditi algoritmima s obzirom na to da je uvjerljivost njihova osnovna značajka. Društvena osviještenost i izvaninstitucionalna djelovanja osnova su obrane od zamjenskih priča, koje je potrebno učiniti nedostupnima u što ranijoj fazi.

4. Manipulacije izvornim podatcima

Manipuliranje izvornim podatcima ne podrazumijeva njihovo krivotvorenje, nego ostavljanje izvorne informacije u nepromijenjenom obliku, ali uz interpretaciju i temelj za stvaranje utjecaja na način kako to najbolje odgovara napadaču. Nedavni primjer manipuliranja izvornim podatcima

jest objavljivanje sadržaja elektroničke pošte utjecajnih osoba ili povjerljivih podataka koje su objavili zviždači. Izvornim podatcima često se manipulira na način da ih se pogrešno obrađuje, a jedan je od poznatih primjera takve manipulacije „korelacija" ovisnosti o pušenju i pojave malignih bolesti. U tom je slučaju postavljeno pogrešno pitanje: „Kolika je vjerojatnost da će pušači oboljeti od malignih bolesti?", na što je propisno obrađen statistički podatak dao razmjerno malu vjerojatnost. Međutim, postavimo li pitanje ispravno: „Koliki je postotak pušača u uzorku osoba oboljelih od malignih bolesti?", dobit ćemo sasvim suprotan odgovor, odnosno da doista postoji značajna korelacija između pušenja i malignih bolesti. Slične primjere opažamo u poricanju klimatskih promjena.

U obrani od manipuliranja izvornim podatcima potreban je ozbiljan pristup i visoka stručnost. Izvornu informaciju potrebno je predočiti i zatim praktično predstaviti kako se ne bi mogla iskoristiti za manipulaciju te naposljetku obvezno donijeti zaključak u obliku prezentacije ishoda koji ne odgovara napadaču. Pritom se svakako mora upotrijebiti isti medij koji je koristio napadač, ali i mediji koji su najzastupljeniji u napadnutoj populaciji (na manipuliranje izvornim podatcima mora se reagirati promptno i na širokom polju najzastupljenijih medija). Dobar primjer obrane od manipuliranja izvornim podatcima bila je televizijska emisija „Slikom na sliku", koju je tijekom Domovinskog rata prikazivala Hrvatska televizija.

5. Prikrivanje stvarnog izvora

Preduvjet je uspješne operacije utjecaja skrivanje stvarnog izvora. Vješt napadač nastojat će krivotvoriti izvor, i to na način da oslabi cilj ili uvede zabunu i sumnju među saveznike.

Otkrivanje stvarnog izvora zadaća je specijalista iz sigurnosnih službi i civilnih stručnjaka za informacijsko djelovanje. Važno je reagirati brzo i poricati navodni izvor kako bi se umanjio učinak osjećaja izdaje u vlastitim ili savezničkim redovima. Pozitivna atribucija stvarnog izvora operacije utjecaja jedini je pozitivan ishod za branitelja u operaciji utjecaja, no ne treba računati na to da će do nje doći s obzirom na to da je danas vrlo lagano

potpuno sakriti stvarni izvor uporabom nekoliko slojeva mrežnih posrednika. Usporedni napori u obavještajnom radu i aktivna suradnja s pružateljima mrežnih usluga, uz informiranje populacije da je izvor informacija namjerno krivotvoren, mogu djelomično poništiti učinak prikrivanja stvarnog izvora.

6. Izgradnja mreže posrednika

Za razliku od stvaranja ciljane publike, koja je većinom pasivna te je samo primatelj u operaciji utjecaja, mreža posrednika (u engl. žargonu *useful idiots*) dalje prenosi i promiče operaciju utjecaja. Posrednik (engl. *proxy*) na taj način i sam postaje sudionik u operaciji utjecaja. Posrednici su vrlo opasni jer djeluju iz same ciljane skupine, koju dobro poznaju i mogu pametno iskoristiti njezine slabosti.

Posrednici su često nagli i emotivno motivirani te se može očekivati da ih većina nema dovoljnu razinu stručnog znanja o prikrivanju na internetu te ih se može detektirati, locirati i onemogućiti sinkroniziranim djelovanjem sigurnosnih službi i pružatelja mrežnih usluga, uz primjenu punog civilnog nadzora nad planovima i provedbama ovih mjera. Široka informiranost o ovoj metodi operacija iznimno je važna u preventivnim mjerama.

7. Poricanje kampanje operacija utjecaja

Odlučan napadač u svakom će slučaju poricati postojanje kampanje operacija utjecaja, kao i svaku svoju ulogu i umiješanost. Iznimka je od tog načela namjera zastrašivanja, demonstracije sposobnosti i snage napadača.

Nije za očekivati da će napadač priznati svoju ulogu u provedbi operacija utjecaja. Za identifikaciju i obrazloženje cilja kampanje operacija utjecaja potreban je širok odgovor koji obuhvaća mnoge segmente društva. Također, ne može se očekivati da će sigurnosne službe javno identificirati napadača jer bi time otkrile svoje sposobnosti i metode. U svakom slučaju, odgovor na poricanje napadača prilika je za pokazivanje vlastite demokratske orijentiranosti i volje za postizanjem mirnog rješenja svake nesuglasice na svima prihvatljiv i civiliziran način.

8. Težnja prema dugoročnim ciljevima

Operacije utjecaja mogu imati kratkoročne i dugoročne ciljeve. One će zbog svoje prirode, ukratko opisane u prethodnih osam značajki, imati najveći uspjeh kao dugoročne kontinuirane kampanje.

Dugoročno je potrebno realno procijeniti opasnosti moguće kampanje operacija utjecaja. Na osnovi studija i ozbiljnih igara potrebno je upoznati se s mogućim ishodima i posljedicama. Na temelju njih potrebno je organizirati protumjere, te formirati i opremiti stručne timove za učinkovit odgovor koji će nastaviti razvijati doktrinu operacija utjecaja. U ove je aktivnosti potrebno uključiti što šire segmente društva. To je ujedno prilika za afirmaciju neborbene pričuve obrambenog i sigurnosnog sustava zemlje, koju je moguće organizirati, razvijati i aktivirati na temelju stvarnih potreba. Strategije i doktrine obrane od kampanja operacija utjecaja, uključujući postojeće mehanizme demokratskog nadzora nad obrambenim i sigurnosnim sustavom, potrebno je učiniti javno dostupnima i izložiti ih konstruktivnoj kritici.

Nadamo se da smo ovim kratkim osvrtom na Schneierov esej potaknuli zainteresiranu stručnu javnost na diskurs o operacijama utjecaja, pri čemu je ponajprije potrebno odgovoriti na pitanje treba li operacije utjecaja definirati i istraživati odvojeno od postojećih kibernetičkih i hibridnih operacija. Ovim putem upućujemo poziv na stručnu raspravu o ovoj temi, za koju su stranice našeg časopisa otvorene.

Literatura

1. Schneier, Bruce. 2019. *Eight Ways to Stay Ahead of Influence Operations*. https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/ ili https://www.schneier.com/essays/archives/2019/08/8_ways_to_stay_ahead.html (pristupljeno 10. prosinca 2019.).

2. Larson, Eric V.; Darilek, Richard E.; Gibran, Daniel; Nichiporuk, Brian; Richardson, Amy; Schwartz, Lowell H.; Quantic Thurston, Cathryn. 2009. *Foundations of Effective Influence Operations, A Framework for Enhancing Army Capabilities*. RAND Corp. ISBN 978-0-8330-4404-4. Santa Monica, CA. 227 str.