УДК: 355.358.014
316.472.4:004.738.5]:327
351.861

Врста рада:
СТРУЧНИ РАД

Примљен: **24.10.2022.**
Прихваћен: **15. 11. 2022.**

Дарко ОБРАДОВИЋ
Центар за стратешку анализу
Београд, Србија
контакт: **darko@czsa.org**

ОПЕРАЦИЈЕ УТИЦАЈА НА ДРУШВЕНИМ МРЕЖАМА КАО ХИБРИДНА ПРЕТЊА

Апстракт: Друштвене мреже као феномен свакодневно креирају свој утицај на реалан живот. Одређене друштвене појаве и процеси започети на друштвеним мрежама своје последице испољавају на живот изван сајбер простора. Многи друштвени покрети своје зачетке су имали управо на друштвеним мрежама, многе иницијативе и политички захтеви прво су иницирани на друштвеним мрежама. О томе нам сведоче онлајн петиције, позиви на протесте и демонстрације, указивање на постојеће и „постојеће" друштвене противуречности.

Оно чиме се бавимо у овом раду јесте колико су одређени дискурси и мишљења спонтана на друштвеним мрежама, а колико су плод координираних акција које имају јасно зацртане краткорочне и дугорочне циљеве. Да ли иза таквих активности стоје појединици, интересне групе и државне институције. За нашу анализу је нарочито важно како изгледају активности иза којих стоје државе. Којим методима се може на време открити такав извор угрожавања као појава и процес. Шта нам је доступно од техника којима се може недвосмислено установити да иза одређене активности стоји одређене држава. Посебну важност у овом контексту има тзв. „приписивање" односно изношење оптужби које са собом носе политичку одговорност. Због свега наведеног у данашњем тренутку је веома исплативо изводити овакве операције. Литература препознаје таква дејства као „операције утицаја". Међутим, како би се разумела ова безбедносна појава важно је баратати компетентним алатима који нам омогућавају да разумемо сам полигон на коме се одвија дејство – друштвене мреже, али и да разумемо шири контекст због чега је одређено дејство мање или више успешно. У овом раду сагледаћемо нову реалност људског друштва и због чега су данас операције утицаја успшеније, динамичније и економичније него што су биле пре 50 година.

Рад настоји да анализира хибридне претње, односно операције утицаја, у једном „уском" домену друштвених мрежа. Могућности извођења операција утицаја су веома изазовне. Али није свака дезинформација или кампања на друштвеним мрежама уједно операција утицаја.

Фокусираћемо се на операције утицаја као информационе и психолошке операције које представљају безбедносну претњу за савремене државе.

Кључне речи: ХИБРИДНИ РАТ, ДРУШТВЕНЕ МРЕЖЕ, ПРОПАГАНДА, ЛАЖНЕ ВЕСТИ, ДЕЗИНФОРМАЦИЈЕ, БЕЗБЕДНОСТ.

Дефинисање хибридних претњи као безбедносне појаве

Хибридни рат као појам доживео је своју потпуну медијску афирмацију у 21. веку. Поједини теоретичари указују да је исправније говорити о хибридним претњама, уместо о хибридном рату. Своје становиште заснивају на томе да је рат насилна интеракција између две или више организоване политичке групације. Док хибридне претње могу постојати и деловати независно од тога да ли је објекат угрожавања свестан њиховог постојања или не. Често су сами мотиви за извођење хибридних претњи и засновани на елементима прикривености у смислу безбедносног угрожавања одређеног друштва. Настоји се да се прикрије и само постојање мотива према којима би били идентификовани налогодавци, а целокупна друштвена противуречност која би настала, била би приписана ткз. објективним друштвеним околностима. Одсуство препознавања појава које се манифестују као угрожавање даје могућност нападачу да неометано врши оперативну експлоатацију до тренутка када штетна дејства развију свој пун потенцијал и прећу у категорију неуправљивог безбедносног ризика. Управо касно откривање хибридних дејстава, као и њихова мултидисциплинарна комплексност, чини их атрактивним за употребу у околностима када се процењује да би директан оружани конфликт био неисплатив или ризичан подухват. Хибридне претње често се налазе на граничној линији између конвенционалног кинетичког сукоба, економског и дипломатског корозивног дејства, сајбер напада и пласмана дезинформација. Заједнички чинилац свега наведеног је постојање политичке одлуке и координације од стране обавештајних служби. Нарочито са аспекта када се свесно прелази у фазу непријатељстава. То отворено непријатељство се увек избегава, јер са собом носи читав низ последица – раскидање економских веза, ограничење трговине, неповољан положај у међународним организацијама, смањење политичке сарадње, нарушавање односа са другим државама до избијања оружаног конфликта и рата. Хибридна дејства су те активности које обликују дихотомију између рата и мира чије поимање у потпуности редефинишу.

Хибридне претње спадају у претње невојним средствима. Разне дефиниције које би требале да пруже транспарентност у разумевању ове безбедносне

Дарко ОБРАДОВИЋ
Центар за стратешку анализу
Београд, Србија

појаве, често не подразумевају исти контекст зависно од државе и њеног политичког уређења.

Европски центар изузетности за супротстављање хибридним претњама[1] (*Hybrid CoE*) дефинише хибридне претње као акцију коју спроводе државни или недржавни актери, чији је циљ да поткопају или нашкоде мети утичући на њено доношење одлука на локалном, регионалном, државном или институционалном нивоу. Такве акције су координисане и синхронизоване и намерно циљају на рањивост демократских држава и институција.

Дејвид Катлер, асистент Генералног секретара НАТО-а за обавештајни рад и безбедност одређује хибридне претње као комбинацију војних и невојних, јавних и тајних деловања, укључујући и дезинформације, сајбер нападе, економске притиске, размештање нерегуларних оружаних група и употребу регуларних снага.

Европска комисија се према хибридним претњама одређује као активностима када, државни или недржавни, актери настоје да искористе рањивост ЕУ у своју корист користећи на координисан начин мешавину мера (тј. дипломатских, војних, економских, технолошких) док остају испод прага формалног ратовања.

У документу Европске комисије[2] под називом „Заједничка комуникација у европском парламенту и већу, заједнички оквир за сузбијање хибридних претњи, одговор Европске уније" наводи се да хибридне претње настоје да искористе слабости поједине државе и често угрозе темељна демократска права и слободе. На трагу овог документа склони смо да одржимо своју тезу да се хибридне претње појављују у областима у којима је већ присутна одређена друштвена противуречност са циљем продубљивања стања и проширења подела између одређених друштвених група. Те друштвене групе могу бити државне институције и синдикати, здравствени систем и родитељска удружења, еколошки покрети и стране корпорације. У проучавању феномена операција утицаја као једног од сегмената хибридних претњи сматрамо за важним да хибридна дејства сагледамо на начин како их сагледавају државне и међународне организације. Из разлога што онако како се претња перципира од политичких доносилаца одлука, зависи и какав ће одговор бити, и управо зато је неопходно разумети тежишта дефиниција ових претњи.

За целокупно разумевање хибридних претњи као безбедносних појава осврнућемо се и на документ Централне војне комисије НР Кине из 2003. године под називом „Политичке смернице за Народну ослободилачку Армију". Документ[3] препознаје три врсте ратовања психолошки рат који укључује при-

1 https://www.hybridcoe.fi/about-us/

2 https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

3 Central Military Commission (2003): *Political Work Guidelines of the People's Liberation Army*; Beijing: CMC.

мену војних и дипломатских мера да би се пореметио противник који се супротставља кинески м спољнополитичким циљевима, затим рат „мишљења"[4] који обухвата јавне и тајне медијске манипулације са циљем утицаја на домаћу и страну јавност у погледу спољнополитичких циљева, и трећи је регуларни рат. Чини се логичним да подела на три облика рата, уједно се узима и као офанзивна и као дефанзивна одредница у политичком доношењу одлука. Заправо, видимо да и НАТО, ЕУ и НР Кина борбу за наративе односно операције утицаја доживљавају као безбедносне појаве. И сва је прилика да активности, онако како су их дефинисали, сматрају за изворе угрожавања који са собом носе одређене последице.

Серђио Маракола са Италијанског института за међународне и политичке студије у свом раду[5] о Кинеском хибридном рату констатује да Кина, такође захваљујући својој историјској способности да изводи асиметрично ратовање, што је потврђено током грађанског рата и шире, постаје кључни актер у примени способности хибридног ратовања. Домени у којима улога Пекинга постаје централна су: кинеске поморске акције у Јужном кинеском мору; кинеска дипломатија; и коначно, пекиншка доктрина сајбер ратовања.

Руска војска дефинише „хибридни рат" као напор на стратешком нивоу да се обликује управљање и геостратешка оријентација циљне државе у којој су све акције, укључујући употребу конвенционалних војних снага у регионалним сукобима, подређене информацијама (Kagan, 2020). Начелник генералштаба Руске Федерације генерал армије Валери Герасимов у свом разматрању савременог рата као сукоба истиче информациону компоненту. Све ово је допуњено војним средствима а прикривеног карактера, укључујући извођење радњи информационог сукоба и дејства снага за специјалне операције. Отвореној употреби снага често под маском очувања мира и регулисања кризе прибегава се само у одређеној фази, пре свега за постигнуће коначног успеха у сукобу (Герасимов, 2013) .

Без жеље да дужимо, уочавамо да сви актери перципирају информације као средство вођења сукоба. Хибридне претње ће настојати да искористе медије, технологију и позицију унутар политичке, војне и друштвене инфраструктуре државе у своју корист (TC 7-100, 2010).

Хибридне претње карактерише координисано коришћење различитих мера за постизање нелегитимног мешања (дипломатског, војног, економског или технолошког) од стране државних или недржавних актера, уз задржавање испод прага формалног ратовања наводи у својој дефиницији[6] Федерално министарство за европске и међународне односе Аустрије.

4 Ово може потпасти под когнитивни рат који НАТО дефинише као обликовање и утицај на индивидуална и групна уверења и понашања која иду у прилог агресоровим тактичким или стратешким циљевима. Више се може погледати на овом линку: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

5 https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853

6 https://www.bmeia.gv.at/en/european-foreign-policy/global-issues/hybrid-threats/

Дарко ОБРАДОВИЋ
Центар за стратешку анализу
Београд, Србија

Кембриџ речник (*Cambridge Dictionary*) наводи да је хибридни рат коришћење низа различитих метода за напад на непријатеља, на пример, ширење лажних информација, или напад на важне компјутерске системе, као и, или уместо, традиционалне војне акције.

Аутор овог рада ће у наставку користити дефиницију хибридног дејства као планског, организованог, унапред припремљеног, координисаног, економичног деловања државних актера против цивилног становништва, институција и интереса суверених држава, уз саставну употребу принципа војне тактике и обавештајног рада, у првом реду субверзивног деловања са коначним циљем паралисања друштва, државног система срачунатог у принуди ради остварења одређених уступака и жељеног поступања државе у целини (Животић, Обрадовић, 2022).

Хибридне претње у великој мери се ослањају на примену дезинформација као покретача одређених промена у држави мети напада. Видимо да све дефиниције у већини сматрају дезинформације као алат, а информационе операције као средство за вршење хибридних дејстава. Само присуство дезинформација, уколико је координирано, сматра се за хибридну претњу која може угрозити виталне државне вредности.

Савремено окружење и хибридне претње – друштвене мреже

Експлоатација различитих облика хибридних претњи данас увелико представља област истраживања која је сама по себи посебна. Анализирање читавог спектра доступних тактика и метода са собом повлачи укључење читавих научних области, од кибернетике, психологије, безбедности, међународних односа, комуникологије, менаџмента до војне науке. Тешко је и замислити да је рационално очекивати примени уских научних области. Што представља додатни изазов за сваког истраживача који би одлучио да се упусти у разматрање свих појавних облика хибридних претњи.

Као истраживачи на задатку смо да проникнемо у основне поставке неких од претњи и на такав начин дамо свој допринос заједници. Употреба друштвених мрежа у сврху политичког деловања је више него позната, као и употреба истих у сврху извођења превrата или организације легитимних протеста широм света. Друштвени медији су обликовали дигитални свет до те мере да је то сада неизоставни део живота за већину нас (Gazi, Cetin, 2017).

Кроз овај рад желимо да установимо у којој мери су друштвене мреже подложне за информационе операције и који ефект се могу измерити од таквих дејстава. Велике силе несумњиво користе друштвене мреже као полигон за примену хибридних дејстава односно покретање информационих операција. Како је свет ушао у нову еру такмичења великих сила током протекле деценије,

националне државе све више воде стране пропагандне кампање на платформама друштвених медија као што су Фејсбук и Твитер, ефективно претварајући такве платформе у технологије утицаја (Nemr, Gangware 2019). Ресурси који су на располагању државама превазилазе било ког недржавног актера. Могућност за координацијом, материјалним ресурсима као и доступност разноврсних специјалности су још увек на страни савремених држава. Одржавање комплексних циклуса који чине фалсификати, полуистине и истинити али тајни подаци као и аналитичке способности увезане са другим методама обавештајног рада издвајају државне операције утицаја од неких локалних политичких или комерцијалних кампања. Координација и синхронизација са високим степеном економичности представљају само неке од атрибута приликом анализе ове безбедносне појаве, а о чему ће бити речи нешто касније. Докази о организованим кампањама манипулације друштвеним медијима које су се одвијале у 70 земаља, у односу на 48 земаља у 2018. и 28 земаља у 2017. У свакој земљи постоји најмање једна политичка партија или владина агенција која користи друштвене медије да обликује ставове јавности у земљи (Bradshaw, Howard, 2021). Као основа за манипулације на друштвеним мрежама користе се дезинформације као намерно ширење нетачних вести, прича или фабрикованих документарних формата са задатком остварења политичких циљева (Бенет, Ливингстон 2018).

Близу 5, тачније 4,7 милијарди људи односно 59% светске популације[7] данас користи друштвене мреже закључно са јулом 2022. Сваки други човек наше планете има приступ милијарди података у свакој секунди који циркулишу друштвеним мрежама. Фејсбук има 2,9 милијарди корисника што га сврстава у најактивнију друштвену мрежу. Апсолутна већина корисника других друштвених мрежа обавезно поседује[8] и Фејсбук. Што нас упућује да Фејсбук можемо посматрати као врсту чворишта путем кога се повезују остали интернет садржаји и друге друштвене мреже. Када разматрамо феномен друштвених мрежа слободни смо да наведемо да их треба посматрати као врсту посредника између интернет садржаја и нашег утиска. Ову тврдњу баштинимо на квантификованим чињеницима. Пев истраживачки центар у својој студији[9] под називом „Употреба вести широм платформи друштвених медија у 2020" наводи да 53% одраслих американаца долази до вести преко Фејсбука, док Твитер као извор вести користи свега 15% одраслих Американаца. Док уколико се дубље размотре објављени статистички подаци, видимо да 59% корисника Твитера користи ту мрежу као примани извор вести, док Фејсбук 54%. Центар за медијску ангажованост из Тексаса у свом емпиријском истраживању долази до закључка[10] да

7 https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

8 https://datareportal.com/reports/digital-2022-favourite-social-platforms

9 https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/

10 https://mediaengagement.org/wp-content/uploads/2016/03/ENP-News-Commenters-and-Comment-Rea-ders1.pdf

55% америчких корисника оставља онлајн коментаре, а 77,9% чита коментаре, од оних који оналјн коментаришу 77,9% то чине преко друштвених мрежа.

Скоро 2 милијарде (1,8)[11] милијарди корисника учествује у Фејсбук групама и тренд раста овакве интеракције забележен је са избијањем пандемије корона вируса.

Твитер има 340 милиона корисника и испоручује 500 милиона твитова дневно, а 200 милијарди твитова годишње (Aslam, 2018).

Друштвене мреже данас имају одлике једне велике друштвене заједнице без баријера и граница. Садржај који се објави у једној Индији, ништа не ограничава да му се приступи у једној Србији. Целокупан онлајн микрокосмос је постао макрокосмос, са могућношћу превода 100 различитих језика у реалном времену на Фејскубу више нема ограничења ни у погледу језичке баријере. Садржаји крстаре друштвеним мрежама у промилима секнуди. У зависности од виралности алгоритам их може пласирати знатно брже. Како се овај рад бави операцијама утицаја и дезинформацијама ми ћемо разматрати друштвене мреже као полигон за извођење хибридних претњи.

Информација као оружје

У претходном поглављу стекли смо увид у окружење за које тврдимо да је феномен без премца за пласман дезинформација и пројектовање спољнополитичких утицаја, изазивање друштвених нереда и конфликата. Ова технологија је драматично преобликовала индустрију вести и медија откако је постала доминантан и растући извор вести и информација за стотине милиона људи (Kaplan, 2015). Друштвене науке већ дуго воде академску дебату да ли живимо у свету истине или пост истине, или можда чак у свету где је важна само перцепција а не суштина. Пред нама је дилема да ли је важнија перцепција одређеног догађаја или сам догађај. Да ли вредносни суд према одређеном актеру одређује и перцепцију деловања тог актера. Увиђамо да се велике силе боре у информационом простору са неколико циљева. Први је представити себе бољим од других – мека моћ. Други, представити противника као „злог" . Трећи, паралисати противника и окренути његово јавно мнење против друштвеног уређења.

Несумњиво лажне вести прете вишеструким сферама живота и могу донети девастацију не само економским и политичким аспектима, већ и добробити и животима људи (Khan, Michalas, Akhunzada, 2021). Приликом пандемије корона вируса и државни и недржавни актери су угрозили јавно здравље људи широм света. Из лукративних мотива појединци су завели милионе људи који су због њихових активности одбили да се повинују упутствима ради заштите сопственог здравља.

11 https://blog.hootsuite.com/facebook-statistics/

Од кључног значаја је да ли информације које се користе могу остварити ратне циљеве без испаљеног метка. Америчка војска информациони рат дефинише у задњих 30 година на различите начине. Што је и разумљиво из разлога технолошког напретка, односно промена безбедносног окружења, али и од природе угрожавања националне безбедности. Једна од понуђених дефиниција, можда није идеална, али са базичним елементима даје нам могућност теоријске надоградње овог концепта уз поседовање методолошких алата.

Акције предузете у циљу информационе суперионости кроз утицај на непријатељске информације, информационо засноване процесе, информационе системе, рачунарско засноване мреже истовремено дефинишући сопствене информације, информационо засноване процесе, информационе системе и рачунарски засноване мреже[12].

Листа начина за злоупотребу информација на друштвеним мрежама које се могу сматрати лажним вестима у постојећој литератури се дефинишу (Tandoc, 2018):

Мамац за кликове: брзи наслови који лако привлаче пажњу корисника без испуњавања очекивања корисника јер су често слабо повезани са стварном причом. Њихов главни циљ је повећање прихода повећањем броја посетилаца на веб локацији.

Пропаганда: Намерно пристрасне информације осмишљене да обману публику. У последње време примећује се повећано интересовање за пропаганду због њеног значаја за политичке догађаје

Сатира или пародија: Лажне информације које објављује неколико веб локација за забаву корисника Ова врста лажних вести обично користи претеривање или хумор да би публици представила ажуриране вести.

Траљаво новинарство: Непоуздане и непроверене информације које деле новинари и које могу да доведу читаоца у заблуду

Обмањујући наслови: Приче које нису потпуно лажне, али садрже сензационалистичке или обмањујуће наслове.

Искривљене или пристрасне вести: Информације које описују једну страну приче потискујући доказе који подржавају другу страну или аргумент.

Дељењем лажних информација представља механизам манипулације корисницима односно грађанима који долазе у додир са таквим садржајем. Нарочито је ризично када се деле дезинформације у погледу јавног здравља, маргинализованих група, изборног процеса, међудржавних тензија, а не ретко дезинформације прати говор мржње и дискриминације. Што је случај агресије Русије на Украјину, где се неретко пласирају садржаји који негирају право

12 Joint Publication 1-02, Department of Defense Dictionary of Military Associated Terms, 1996.

Украјинаца на живот, језик, културу и државност описујући их као „нацистичку хорду“.

Проблем употребе дезинформација заокупио је пажњу и Светског економског форума[13] који указује на четири начина путем којих се врши експлоатација на друштвеним мрежама:

Друштвени инжењеринг: Пружање оквира за погрешну карактеризацију и манипулацију догађаја, инцидената, питања и јавног дискурса. Друштвени инжењеринг често има за циљ да помери јавно мњење у корист одређене агенде.

Неаутентично појачавање: Коришћење тролова, спам робота, лажних налога идентитета, плаћених налога и сензационалних утицајних особа за повећање обима злонамерног садржаја.

Микроциљање: Искоришћавање алата за циљање дизајнираних за пласман огласа и ангажовање корисника на платформама друштвених медија како би се идентификовала и ангажовала највероватнија публика која ће делити и појачавати дезинформације.

Узнемиравање и злостављање: Коришћење мобилисане публике, лажних налога и тролова за замагљивање, маргинализацију и избацивање новинара, супротних ставова и транспарентног садржаја.

Набројане манифестације уколико су координиране и подржане државним ресурсима могу постати безбедносни облик угрожавања са несагледивим последицама. Из разлога што дуготрајна примена ових активности, у односу на слабу националну отпорност, може довести до хронично „отрованог” обрасца мишљења код цивилног становништва. Обрасци мишљења и модели уверења су јако тешко променљиве категорије. Нарочито уколико су поткрепљене личним истинама и порукама државних носиоца власти. Познати социолог и сенатор државе Њујорк Данијел Патрик Мојнихан је у 20. веку изјавио „Свако има право на своје мишљење, али не и на своје чињенице”. Овај цитат нам може послужити као илустрација шта се заправо догађа као исход пласирања дезинформација. Људи формирају своје мишљење у односу на „чињенице” које су им пласиране и доступне. Важна је карактеристика да се дезинформације и теорије завере у већини случајева ослањају на недостатке у знању по питању сложених друштвених, историјских и научних чињеница, и те недостатке испуњавају лако разумљивим игнорантским информацијама које су разумљиве широким слојевиа друштва. Они појединци који се вероватно могу пронаћи у теоријама завере имају алтернативни поглед на свет који има смисла за њихове ситуације и означава недвосмислен узрок друштвених неправди у које верују (с правом или погрешно) и чије могу бити жртве (Landau and Rothschild, 2010)

13 https://www.weforum.org/agenda/2022/08/four-ways-disinformation-campaigns-are-propagated-online/

Примера у историји је бесконачно. Можемо кренути од најбруталнијих, а који се тичу дезинформација о Јеврејима у нацистичкој Немачкој, или о Јерменима у отоманском Истанбулу. И једна и друга активност је резултовала геноцидом који је био широко прихваћен у јавности која је била заведена једностраном пропагандом која је код цивилног становништва створила утисак да су злодела према њиховим сугрђанима оправдана.

Један од разлог за забринутост због успеха ових теорија завера је тај што постоји веза између прихватања неких од њих и склоност ка политичком и/или верском насиљу (Bronner, 2013, 2015).

Пандемија корона вируса је добар и свеж пример како се теорије завера могу користити у циљу остварења геополитичких интераса у конфронтацији великих сила. НР Кина[14] која се нашла пред изазовом сопственог глобалног лидерства услед неконтролисане пандемије, прибегла је званичној употреби постојећих теорија завера у циљу конфронтације са САД и либерланим државама и уједно са задатком одбране сопственог међународног положаја. Недостатак транспарентности у кинеској политици учинио је да се завере усредсређене на институције транзиције моћи, борбе за моћ, сукобе и политичке завере преовлађују у кинеском политичком дискурсу. Оставља простран простор за спекулације и теорије завере када се догоде несвакидашњи догађаји(Cheng, Zhang, W. J. & Zhang, Q, 2022).

Теорије завере некада маргиналне идеје из алтернативних извора и појединаца, нашироко су промовисане и дато им је поверење власти и институција у пандемији Ковид-19 (Kinetz, 2021). Као кључна ствар због чега су такви маргинални наративи постали предмет доминатног друштвеног дискурса разазнаје се путем саопштења америчког Стејт Дипартмента који упозорава[15] да постоји механизам кроз који

> ***„Медији НР Кине и КП Кине представљају непроверене информације и тврдње које потичу од руских државних медија и званичника. У повратној спрези, руски државни медији затим цитирају медије НР Кине и КП Кине како би приказали позицију Русије као широко подржану".***

Увидели смо да информације и те како могу бити оружје које без кинетичке силе постиже резултате, оставља дуготрајне ефекте по нападнуто друштво, а елиминацијом дезинформација не елиминише се и њихово штетно дејство. Зашто? Зато што дезинформације путем операција утицаја индоктринирају део цивилног становништва на такав начин који трајно успоставља образац мишљења који је тешко променити. А из психологије је познато да ставови

14 https://www.czsa.org/single-publicaiton/5

15 https://www.state.gov/disarming-disinformation/prc-efforts-to-amplify-the-kremlins-voice-on-ukraine/

и чињенице које су у супротности са обрасцима мишљења изазивају гнев, мржњу и отклон у односу на онога ко нарушава устаљени образац мишљења. Из свега произилази да подлога дугорочне друштвене конфронтације може настати за неколико месеци, а трајати деценијама.

Методи и технике операција утицаја

Не доживљавају сви међународни субјекти меку моћ и слободу говора на исти начин. Док је за либералне демократија карактеристична јавна дебата, слобода говора, покретање јавне иницијативе па и окупљање, за ауторитарне режиме све набројано представља безбедносну претњу по националну безбедност. Ауторитарни режими могу да прибегну низу различитих актера који служе као заступници или мултипликатори њихових порука, отимајући дебату (нпр. тролови и ботови)[16]. Метод отимања дебате је постао нарочито актуелан током америчких избора 2016. године и скандала са фабрикама тролова који су истовремено симулирали да су припадници различитих друштвених група и покрета[17]. Циклус операција утицаја полази од фазе одређивања циљева, избора метода и техника, до успешног инфилтрирања одређених дезинформација до тренутка док оне не постану део јавног дискурса. Зависно од временских оквира који су на располагању операције могу користити постојеће теорије завере и дезинформације. Или могу креирати потпуно нове теорије завере које ће се касније разрађивати и аутономно мултипликовати.

Пример за то је операција „Инфекција".

Током те кампање, КГБ је, уз помоћ СССР-ове Агенције за штампу и савезничких обавештајних служби совјетског блока, настојао да широм света прошири тезу да је вирус људске имунодефицијенције (*HIV*) који изазива синдром стечене имунодефицијенције (*AIDS*) генетски модификован. или је на други начин измислио Пентагон као део свог наводног истраживања биолошког оружја на Институту за медицинска истраживања за инфективне болести америчке војске (USAMRIID) у Форт Детрику, Мериленд[18]. Једна веома сложена операција за чију пуну реализацију је био неопходан вишегодишњи пропагандни циклус, данас у доба потпуне експанзије друштвених мрежа своди се на питање неколико сати или дана. Пример дезинформација о Ковиду-19 такође је покрио различите теме. Покривајући различите теме – од његовог порекла до потенцијалних излечења, или његовог утицаја на западна друштва – стварање и ширење дезинформација о Ковид-19 на мрежи постало је широко распрострањено (Bradshaw, 2020). Актери који изводе операције утицаја то чине са циљем да

16 https://www.voanews.com/a/silicon-valley-technology_cyborgs-trolls-and-bots-guide-online-misinformation/6183912.html

17 https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house

18 https://www.sciencedirect.com/science/article/pii/S1084804521001326#bib158

би утицали на жељено понашање у одређеној држави. Са разним тактикама и техникама се извршавају ове операције, али метод пласмана дезинформација и обмањујућег садржаја је нешто што представља карактеристику за овакве операције.

Америчка агенција за безбедност инфраструктуре и сајбер безбедност[19] даје преглед тактика за дезинформисање:

а) култивисање лажних и обмањујућих личности и вебсајтова- ово подразумева креирање мреже лажних извора који промовишу поруке које су лажне или омбањујуће циљаној пулбици. Агенција наводи да су то често неаутентични акредитиви. На овом месту желимо да прокоментаришемо да то могу бити вебсајтови који својим садржајем и визуелним идентитетом могу подсећати на угледне и поштоване јавне или приватне организације. У њих спадају онлајн лажни идентитети, а неретко и стварне индивидуе које се оглашавају са позиције „експерта“ који нису познати релевантној стручној јавности.

б) Осмишљавање или појачавање теорија завера.

в) Оркестрирана кампања и „затрпавање” информационог окружења. Кампање дезинформација ће често објављивати огромне количине садржаја са истим или сличним порукама са неколико неаутентичних налога.

г) Злоупотреба алтернативних платформи. У ово, примера ради, спада Телеграм апликација.

д) Искоришћавање празнине у информацијама. Актери дезинформација могу да искористе ове празнине генеришући њихове сопствене утицаје на садржај и постављање термина за претрагу на друштвеним медијима како би подстакли људе да га потраже.

ђ) Манипулисање путем „корисних идиота”. Актери дезинформација циљају на истакнуте појединце и организације који им помажу да се појачају њихове приче. Мете често нису свесне да понављају дезинформишући наратив или да је наратив намењен да манипулише.

е) Ширење циљаног садржаја. Ови актери добијају статус инсајдера и развијају се кроз ппраћење на мрежи које може учинити будуће напоре манипулације успешнијим. Ова тактика је приступ „дуге игре” ширења циљаног садржаја током времена како би се изградило поверење и кредибилитет код циља публике.

Друштвене мреже поседују компаративне предности које погодују операцијама утицаја. То су алгоритам, аутоматизација и анонимност. Платформе примењују алгоритме – или аутоматизоване скупове правила или инструкција – да трансформишу податке у жељени излаз. Користећи математичке формуле, ал-

19 https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

горитми оцењују, рангирају, наручују и испоручују садржај на основу фактора као што су подаци појединачног корисника и личне преференције (Bennett, 2012). Платформе омогућавају аутоматизацију – где налози могу аутоматски да објављују, деле или се ангажују са садржајем или корисницима на мрежи. За разлику од људског корисника, аутоматизовани налози – који се понекад називају „политички ботови" или „налози појачавача" – могу објављивати много чешће и доследније од било ког људског корисника (McKelvey and Dubois, 2017).

Институт за стратешка истраживања оружаних снага Француске када пише о операцијама утицаја у иностранству наводе два главна, али не међусобно искључива циља: први, завести и заробити страну публику и други инфлитрација и награизање (Charon,Vilmer, 2021).

За разумевање метода и техника подесно је искористити својетски концепт „активних мера". „Активне мере", које укључују дезинформације, фалсификовање, саботажу, операције дискредитације, дестабилизацију страних влада, провокације, операције лажне заставе и манипулације усмерене на слабљење друштвене кохезије, регрутовање „корисних идиота" и стварање фронт организација.

Разлог зашто је употреба друштвених мрежа делотворна код пласмана дезинформација је у томе што наше сајбер окружење је уједно и медијум за пренос лажног и обмањујућег садржаја. Више се не налазимо у позицији да једнострано конзумирамо садржај, већ се такав садржај „препоручује" од стране наших конатаката. Постоје два разлога за стратегију стварања дезинформација која постаје омбањујућа је тако моћна. Прво, људи верују својим пријатељима и другима које они доживљавају да су слични њима. У одлучивању у шта од делова информација да верују, људи узимају уочену веродостојност делиоца као веома важну (O'Connor, Weatherall, 2019).

Методе и технике еволуирају са доступним техничким могућностима. Некадашња борба за илегалне радио сигнале, претворила се у контролу лажних налога на друштвеним мрежама, креирање мреже за обману кроз интернет презентације и пласман дезинформација које су унапред припремљене и координирано пласиране и подржане.

Закључак

Широка заступљеност коришћења друштвених мрежа ставила их је у незаобилазан центар савремених комуникација. Могућност да се манипулише јавним мнењем је додатно повећана самом природом човека и техничким могућностима друштвених мрежа. Заинтересовани актери користе друштвене мреже за дестабилизацију својих супарника и противника. Потенцијал за продубљивање друштвених подела и изазивање сукоба додатно се повећава процесом

нагризања демократија. Слобода говора и протока информација користи се као оружје за напад управо на ту слободу. Технике експлоатације информација се мењају само са техничког становишта. Као изазов се поставља начин јасног и недвосмисленог приписивања одговорности за такве акције. Одговорност и довођење у везу актера и налогодаваца често обухвата врло сложену анализу која се састоји од анализе садржаја, техничке форензике, законског оквира. Законски оквир представља све већи изазов, јер се директно поставља изазов приватности у односу на надзор над комуникацијом оних који нису низашта оптужени. А једном када се таква граница пређе имамо довољно модела из историје да будемо сигурни куда то води. Изазов унапређења јавно-приватног партнерства чини се као добар модел. Како би државе надоместиле неопходне ресурсе и знање кроз партнерство са власницима друштвених мрежа, сајбер компанијама и научно-истраживачком заједницом стављају се претпоставке за успостављање консензуса када је реч о изградњи националне отпорности на операције утицаја. Анализа садржаја може послужити као индикатор и рани знак упозорења да се на друштвеним мрежама шири садржај који је опасан, али нам не може дати прецизне податке о налогодавцу таквог садржаја.

Хибридне претње свој пун замах доживљавају у одсуству конвенционалног сукоба. Њихова примена више није теоријско разматрање већ реална претња по националну безбедност.

ЛИТЕРАТУРА

1. Aslam, S. (2018): *Twitter by the Numbers: Stats, Demographics & Fun Facts*; San Francisco, CA, USA: Omnicore.
2. Bennett, L. (2006): Communicating Global Activism: Strength and Vulnerabilities of Networked Politics, in *Cyberprotest: New Media, Citizens and Social Movements*, eds. W. van de Donk, B. D.Loader, P. G. Nixon, and D. Rucht; London: Routledge.
3. Bennett, W. Lance and Steven Livingston(2018): The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions, *European Journal of Communication*.
4. Borgesius, F. and Zuiderveen J. (2016): Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, *Computer Law & Security Review*.
5. Borgesius Zuiderveen, Frederik and Trilling, Damian and Moeller, Judith and Bodó, Balázs and de Vreese, Claes H. and Helberger, Natali (2005): Should We Worry About Filter Bubbles? *Internet Policy Review* Journal on Internet Regulation, Volume 5, Issue 1.
6. Bimber, B. A. and Flanagin J. and Stohl C. (2005): Reconceptualizing Collective Action in the Contemporary Media Environment, *Communication Theory*.
7. Bilgin, P. & Eliş, B. (2008): Hard power, Soft power: Toward a more realistic power analysis, *Insight Turkey*, 10 (2), pp. 5-20.
8. Cheng, C. Y; Zhang, W. J. & Zhang, Q. (2022): Authority-led conspiracy theories in China during the COVID-19 pandemic – Exploring the thematic features and rhetoric strategies, *Convergence*, 28(4), pp. 1172–1197.
9. Ventre, Daniel (2016): *Information Warfare*; John Wiley & Sons.
10. Kaplan M. Andreas (2015): Social Media, the Digital Revolution, and the Business of Media, *International Journal on Media Management*, 17:4.
11. Kagan, Kimberly (2022): *Military Learning and the Future of War*; Institute for the Study of War.
12. Khan, Tanveer; Michalas, Antonis & Akhunzada Adnan (2021): Fake news outbreake 2021: Can we stop the viral spread?, *Journal of Network and Computer Application*, Volume 190.
13. Laurent, Cordonier; Florian Cafiero & Gérald Bronner (2021): Why are conspiracy theories more successful in some countries than in others? An exploratory study on Internet users from 22 Western and non-Western countries, *Social Science Information*, SAGE Publications.
14. Nye, J.S. (2000): *Understanding international conflicts: An introduction to theory and history*; New York: Longman.
15. Nye, Joseph S. (2004): Soft Power and American Foreign Policy, *The Annals of the American Academy of Political and Social Science*, Volume 119, Issue 2.
16. Nye, Joseph S. (2008): Public diplomacy and soft power, *The Annals of the American Academy of Political and Social Science*, Vol. 616, No. 1.
17. Hoffman, Frank G. (2007): Complex Irregular Warfare: The Next Revolution in Military Affairs, *Orbis*, 50.3, pp 395-411.

18. Singer P.W. & Brooking, E.(2018): *Like War the Weaponization of social media*; Boston, New York: Mariner Books.
19. Stegnel, Richard (2020): *Information Wars*; New York: Grove Press.

ВЕБОГРАФИЈА:

1. Cunningham, Daniel; Sean F. Everton, and Robert Schroeder (2022): Social Media and the ISIS Narrative, *White Paper*; Monterey, CA: Defense Analysis Department, Naval Postgraduate School. http://hdl.handle.net/10945/53059 (приступљено 20.03.2022.)
2. Miracola, S. (2018). Chinese Hybrid Warfare. Available at: https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853
3. https://www.armyupress.army.mil/portals/7/military review/archives/english/militaryreview_20160228_art008.pdf
4. https://www.benning.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/tc7_100.pdf
5. https://www.oii.ox.ac.uk/news-events/reports/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/
6. https://datareportal.com/reports/digital-2022-favourite-social-platforms
7. https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/
8. www.euvsdisinfo.eu
9. www.nato.int
10. https://mediaengagement.org/wp-content/uploads/2016/03/ENP-News-Commenters-and-Comment-Readers1.pdf
11. https://www.sciencedirect.com/science/article/pii/S1084804521001326#bib53
12. https://www.sciencedirect.com/science/article/pii/S1084804521001326
13. https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/
14. https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
15. https://issues.org/wp-content/uploads/2019/11/OConnor-Weatherall-The-Social-Media-Propaganda-Problem-Fall-2019.pdf

Darko OBRADOVIĆ
Center for Strategic Analysis
Belgrade, Serbia

OPERATIONS OF INFLUENCE ON SOCIAL NETWORKS AS A HYBRID THREAT

Abstract: Social networks as a phenomenon create their impact on real life every day. Certain social phenomena and processes started on social networks have their consequences on life outside cyberspace. Many social movements had their beginnings precisely on social networks, many initiatives and political demands were first initiated on social networks. This is evidenced by online petitions, calls for protests and demonstrations, pointing to existing and "existing" social contradictions.

What we discuss in this paper is how certain discourses and opinions are spontaneous on social networks, and how much they are the result of coordinated actions that have clearly defined short-term and long-term goals. Are individuals, interest groups and state institutions behind such activities? What is particularly important for our analysis is what the activities with states behind them look like. What methods can be used in time to detect such a source of danger as an occurrence and a process. What techniques are available to us that can unequivocally establish that a certain state is behind a certain activity. In this context, the so-called "attribution", i.e. making accusations that carry political responsibility, is of special importance. Due to all of the above, it is very profitable to perform such operations at the present time. The literature recognizes such actions as "influence operations". However, in order to understand this security phenomenon, it is important to use competent tools that allow us to understand the very training ground where the action takes place - social networks, but also to understand the wider context that makes a certain action more or less successful. In this paper, we are going to look at the new reality of human society and why influence operations are more successful, dynamic and economical today than they were 50 years ago.

The paper tries to analyze hybrid threats, i.e. influence operations, in a "narrow" domain of social networks. The possibilities of performing influence operations are very challenging. However, not every disinformation or social media campaign is an influence operation.

We are going to focus on influence operations as informational and psychological operations that pose a security threat to modern states.

Keywords: HYBRID WAR, SOCIAL NETWORKS, PROPAGANDA, FAKE NEWS, DISINFORMATION, SECURITY.