Univerza v Mariboru

Fakulteta za varnostne vede

Teo Nuhanovič

UPORABA INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJ ZA INFORMACIJSKE OPERACIJE

Diplomsko delo

visokošolskega študijskega programa Informacijska varnost

Ljubljana, december 2023

Univerza v Mariboru

Fakulteta za varnostne vede

UPORABA INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJ ZA INFORMACIJSKE OPERACIJE

Diplomsko delo

Študent: Teo Nuhanovič

Študijski program: Visokošolski študijski program Informacijska varnost

Mentor: prof. dr. Igor Bernik

ZAHVALA

Ta zahvala gre vsem posameznikom, ki so mi stali ob strani, me spodbujali in mi dali nasvete. Brez Vas mi ne bi uspelo.

Posebno se zahvaljujem svoji družini, očetu Munibu, mami Emini in sestri Enni, ki so verjeli vame.

Hvala tudi mentorju prof. dr. Igorju Berniku za potrpežljivost, strokovne nasvete in spodbudo v času pisanja zaključnega dela.

UPORABA INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJ ZA INFORMACIJSKE OPERACIJE

Ključne besede: informacija, vpliv, politika, mediji, lažne informacije

UDK: 004.056(043.2)

Povzetek

Svet se je v zadnjih letih močno spremenil in eden od razlogov je sektor informacijsko-komunikacijskih tehnologij, ki je eden od najhitreje rastočih in spreminjajočih se sektorjev v današnjem svetu. Hkrati pa so se vzporedno razvijale tudi informacijske operacije, ki se zdaj za dosego svojih ciljev močno zanašajo na informacijsko-komunikacijske tehnologije. Tako je nastala nova vrsta vojskovanja, informacijsko vojskovanje. To novo obliko vojskovanja uporabljajo številne države po svetu z različnimi cilji. Nekatere države ga uporabljajo v vojaške namene, druge pa v politične. Posledice so pogosto uničujoče, saj lahko vodijo do manipulacije in celo pranja možganov med ljudmi, ki so jim vsakodnevno izpostavljeni. Uporaba informacijskih operacij ni omejena zgolj na vojaške organizacije. Uporabljajo jih tudi nedržavni akterji, politične stranke in korporacije. Zato je za vsako državo pomembno, da razume in razvije strategijo informacijskih operacij, ki bi ji zagotovila prednost pred nasprotniki. Informacijske operacije se lahko uporabijo za vplivanje na nasprotnikov proces odločanja tako, da spremenijo njegovo dojemanje realnosti z lažnimi podatki ali z ustvarjanjem napačne slike v njegovem umu o tem, kaj se dogaja na bojišču.

Zaključno delo se osredotoča na informacijske operacije v dveh primerih, ki sta se zgodila v zadnjem desetletju, to sta rusko vmešavanje v ameriške volitve leta 2016 in ruske informacijske operacije v ukrajinski vojni. Oba primera sta podvržena informacijskim operacijam istega akterja. Zato skušamo skozi analizo in primerjavo ugotoviti, kje pretijo nevarnosti, orodja, ki jih akterji uporabljajo, in pa seveda kako implementirati varnostne mehanizme proti pretečim nevarnostim.

USING INFORMATION COMMUNICATION TECHNOLOGIES FOR INFORMATION OPERATIONS

Keywords: information, influence, politics, media, disinformation

UDC: 004.056(043.2)

Abstract

The world has changed a lot in recent years and one of the reasons is the ICT sector, which is one of the fastest growing and changing sectors in the world today. At the same time, Information Operations, which now rely heavily on ICT to achieve their goals, have also developed in parallel. Thus, a new type of warfare was born, information warfare. This new form of warfare is used by many countries around the world with different goals. Some countries use it for military purposes, while others use it for political purposes. The consequences are often devastating, as they can lead to manipulation and even brainwashing among people who are exposed to them on a daily basis. The use of information operations is not limited to military organizations only. They are also used by non-state actors, political parties and corporations. Therefore, it is important for any country to understand and develop an information operations strategy that would give it an advantage over its adversaries. Information operations can be used to influence an adversary's decision-making process by altering his perception of reality through false information or by creating a false picture in his mind of what is happening on the battlefield.

The thesis before you focuses on information operations in two cases that occurred in the last decade. Russian interference in the 2016 US election and Russian information operations in the Ukrainian war. Both cases are subject to the information operations of the same actor. Therefore, through analysis and comparison, we try to find out

where the threats are, the tools that the actors use and, of course, how to implement security mechanisms against threats.

KAZALO VSEBINE

KAZALO SLIK

UPORABLJENI SIMBOLI IN KRATICE

DDoS – distributed denial of service (porazdeljena ohromitev storitve)

GRU – ruska obveščevalna služba

IKT – informacijsko-komunikacijska tehnologija

IRA – Internet research agency (Agencija za internetna raziskovanja)

JCS – Joint chief of staff (Urad združenega vojaškega štaba ZDA)

OK – Odnoklassniki, ruska različica družbenega omrežja Twitter

RICU – The Research, Information and Communications Unit (Enota za raziskave, informacije in komunikacije)

VK – VKontakte, ruska različica družbenega omrežja Facebook

ZDA – Združene države Amerike

1 UVOD

Informacije so ključen dejavnik pri naših odločitvah. To lahko opazimo že pri nakupovanju osnovnih potrebščin in dražjih stvari, kot je avto ali hiša. Več informacij ko imamo o posamezni stvari s pozitivnim predznakom, lažje se bomo odločili za nakup te stvari, saj s tem lažje argumentiramo naš nakup. Podoben učinek imajo informacije z negativnim predznakom, vendar v tem primeru nam informacije povedo, da ta stvar ni v redu, zato se izognemo nakupu in tako mogoče privarčujemo kakšen evro. Najslabši primer je, ko nimamo zadostnih informacij in so te pomešane. Takrat bi lahko rekli, da tavamo v temi in nismo prepričani v našo odločitev. V tem primeru je v naši naravi, da poslušamo nekoga, ki ima več izkušenj v dani situaciji in nas usmeri k pravi odločitvi. To nas spravi v ranljiv položaj, saj smo s tem prepuščeni v nemilost osebe, ki ima lahko dobre ali slabe namene. In prav v tej dani situaciji, ko smo najbolj ranljivi in tavamo v temi, je z nami mogoče najbolje manipulirati, kar po navadi opazimo občutno pozneje.

Tega so se zavedali tudi politiki in vojskovodje skozi zgodovino. Tukaj je moč opaziti tudi konstanto v naši zgodovini. Kdor je imel nadzor nad informacijami, je imel tudi oblast ali pa neposreden vpliv na oblast. Lee (2014) je lepo zapisal, da je informiranje moč, dezinformiranje pa zloraba moči (angl. Information is power. Disinformation is abuse of power).

Tisti, ki poseduje informacije večje pomembnosti, ima veliko moč, z njimi lahko vpliva na mišljenje civilne populacije. To še posebej vidimo v političnih krogih, kjer z informacijami kakor tudi z dezinformacijami politiki skušajo očrniti svoje politične nasprotnike ter tako dobiti na svoji popularnosti, medtem ko nasprotnik izgublja na svoji. Ni nam treba pogledati daleč v zgodovino, da bi opazili tako ravnanje. V začetku tridesetih let prejšnjega stoletja je tako Adolf Hitler prišel na oblast in si nato s spretnim manipuliranjem informacij podredil celotno prebivalstvo.

Vsako manipuliranje informacij, s katerim skušamo vplivati na mnenje ali izbiro sovražnika, imenujemo informacijske operacije. Informacijske operacije so v vojaškem

repertoarju že od začetka vojskovanja in običajno je bil to jeziček na tehtnici, ki je prevesil situacijo v našo prid. To je tudi vzrok, da države namenjajo veliko časa in denarja proučevanju domačega in tujega okolja ter vplivanja na psihološko stanje oziroma miselnost ljudi na ciljanem območju (Bernik in Prislan, 2012).

Z razvojem informacijsko-komunikacijske tehnologije (v nadaljevanju IKT) pa so informacijske operacije doživele nov razcvet. Z novo tehnologijo in aplikacijami, med katerimi so najbolj ranljiva družbena omrežja, imajo informacijske operacije še večji vpliv in doseg. Poleg vsiljevanja mnenja širši populaciji se informacijske operacije na družbenih omrežjih koristijo tudi kot orodje za politično diskreditacijo in oviranje demokratskih procesov. Zelo odmeven je primer iz leta 2018, ko so ruski »boti« pričeli s celovito in sistematsko kampanjo okoli pomanjkljivih dokumentov, ki so implicirali, da Obamova administracija stoji za vrsto zlorab v zvezi z nadzorom Trumpove kampanje. Čeprav operacija ni dosegla želenega cilja republikanske stranke, je ustvarila politično afero, znano kot #releasethememo, in vplivala na mnenje mnogih gorečih privržencev republikanske stranke, da državne institucije FBI in ministrstvo za obrambo stojijo za poskusom delegitimizacije Trumpove uprave (Desouza idr., 2020).

Informacijske operacije so zelo močno orodje, ki je uporabljeno s strani države, organizacij, posameznikov. Uporabljene so v politične namene, vojaške namene, pa tudi v marketingu. Velikokrat jih ljudje niti ne opazimo, čeprav so vsepovsod okoli nas. Lažne novice, namerno dezinformiranje, tako imenovano bombardiranje z novicami, ali namerno zadrževanje informacij so vse del informacijskih operacij, s katerimi nam akterji vsiljujejo svojo direktivo, s čimer dosežejo, da se prebivalstvo mnogokrat razdeli na dva pola in se tako obrnejo eni proti drugim.

1.1 Namen in cilji diplomskega dela

Namen diplomskega dela je skozi teoretični del opisati in predstaviti informacijske operacije in skozi primerjavo ter analizo dveh primerov, ki sta se zgodila v zadnjem

desetletju, pokazati, kako so IKT postale ključen element v izvajanju informacijskih operacij. Prav tako je namen predstaviti različne akterje, posledice in odziv.

Cilji diplomskega dela je z analizo in primerjavo dveh donedavnih primerov, konkretno ameriških volitev iz leta 2016 in ukrajinske vojne, prikazati pomembnost rabe IKT v informacijskih operacijah.

1.2 Teze

V diplomskim delom želimo potrditi oziroma ovreči naslednje teze:

- Napadene države, organizacije ali posamezni akterji nimajo pripravljenega scenarija v primeru informacijskih operacij, usmerjenih proti njim.
- Reakcija »žrtev« na informacijske operacije je prepoznana in povzročena škoda je nepopravljiva.
- Države v vlogi agresorja z uporabo informacijskih operacij prepričujejo lastno prebivalstvo v dobrobit svojih dejanj.

Z zastavljenimi tezami in analizo dveh primerov bomo skušali ugotoviti, ali imajo države, čeprav se zavedajo, kakšno grožnjo informacijske operacije predstavljajo, že dalj časa, kljub raznim ustanovljenim centrom in delovnim skupinam, posvečenim informacijskim operacijam, pravi odgovor, kako se obraniti pred informacijskimi operacijami. Ravno tako bomo skušali ugotoviti, ali države masovno uporabljajo informacijske operacije v namene manipuliranja prebivalstva že dalj časa in kaj se je skozi zgodovino menjavalo ter ali so glavna platforma za izvajanje informacijskih operacij novo nastala družbena omrežja.

1.3 Metode

Za predstavitev vidikov drugih avtorjev in del bomo uporabili metodo deskripcije in kompilacije. Za predstavitev temeljnih pojmov in teorije bomo uporabili analizo virov. V nadaljevanju bomo analizirali in primerjali ameriške volitve 2016 in ukrajinsko vojno

2022, dva primera, kjer so bile informacijske operacije uporabljene za dva različna namena s strani istega akterja. Za ta del bomo uporabili metodo analize in primerjave.

Gradivo, potrebno za izdelavo diplomskega dela, bomo pridobili iz spletnih podatkovnih zbirk, kot sta Scopus in Web of science, strokovnih knjig, časopisnih člankov in novic, najdenih na informativnih portalih. Tako bo diplomsko delo sestavljeno iz prvega teoretičnega dela in drugega, ki bo študija primerov.

2 INFORMACIJSKE OPERACIJE

Opredelitve informacijskih operacij se je lotilo kar nekaj strokovnjakov na tem področju in vsi imajo različne poglede na tematiko. Na ministrstvu za obrambo Združenih držav Amerike so svoj pogled na tematiko pojasnili v dokumentu *Information Operations Roadmap*. Informacijske operacije so ovrednotili kot pomembno sredstvo za dosego zmage v prihajajočih vojnah in jih definirali kot uporabo petih med seboj povezanih elementov vojskovanja. Ti elementi so: elektronsko vojskovanje, operacije računalniških omrežij, psihološke operacije, vojaške prevare in varnostne operacije. Namen teh operacij je vplivati, kvariti in motiti nasprotnikov bodisi človeški bodisi avtomatiziran proces odločanja. Hkrati pa je pomembno obvarovati svoje procese pred sovražnikovim napadom (Department of Defense, 2003). Definicija ameriškega ministrstva za obrambo informacijske operacije opredeli z vojaškega vidika, kar je povsem legitimno, vendar iz te definicije ne moremo točno razbrati, na katero raven odločanja z informacijskimi operacijami ciljajo in ali so namenjene za vplivanje nad procesom odločanja samo vojaških ciljev ali tudi civilnih. Lin in Kerr (2019) v svojem članku definirata informacijske operacije kot sovražne nekinetične aktivnosti, ki z informacijami ustvarijo zmedo, zavedejo in vplivajo na odločitve in izbiro sovražnika. Informacijske operacije ne okarakterizirata kot vojskovanje, saj naj ne bi imelo znakov vojskovanja po Clausewitzu, temveč kot sovražno psihološko manipulacijo nasprotnika. Informacijske operacije imajo konotacijo mehke moči: propaganda, prepričevanje, kultura, družbene sile, zmeda in prevara. Avtorja razširita ameriško definicijo in ji dodata, da so poleg vplivanja na odločitve namenjene tudi ustvarjanju zmede in zavajanju. Čeprav avtorja ne priznavata informacijskih operacij kot vojskovanje, smo drugačnega mnenja. Informacijske operacije aktivno sodelujejo pri vojaških operacijah kot podporna ali pa samostojna operacija in velikokrat je uspeh odvisen prav od učinkovitosti njih, zato smo mnenja, da bi morale biti priznane kot del vojskovanja. Prav tako pa vidiki Clausewitza izhajajo 19. stoletja in v nekaterih pogledih zaostajajo. Cohen in Bar'el (2017) pa predlagata definicijo informacijskih operacij kot operacije med dvema ali več akterjema, kjer ena stran povzroči motnje ali okvaro v delovanju računalniškega in elektromagnetnega

informacijskega okolja, na katerega se zanaša nasprotna stran in katero je sestavljeno iz tehnoloških in človeških virov. S tem dejanjem pobudnik onemogoči nasprotnikovo možnost posredovanja objektivnih vsebin ciljnemu občinstvu, onemogoči, da bi pravilno razumeli dogajanje oziroma realnost, in onemogoči vzpostavitev učinkovite zaščite. Na ta način si pobudnik zagotovi prednost v celotni kampanji in nevtralizira ali onemogoči nasprotnikovo možnost odgovora. Ta definicija poleg namena in načina opredeli tudi prizorišče vsega dogajanja kot informacijsko okolje in opiše učinke informacijskih operacij.

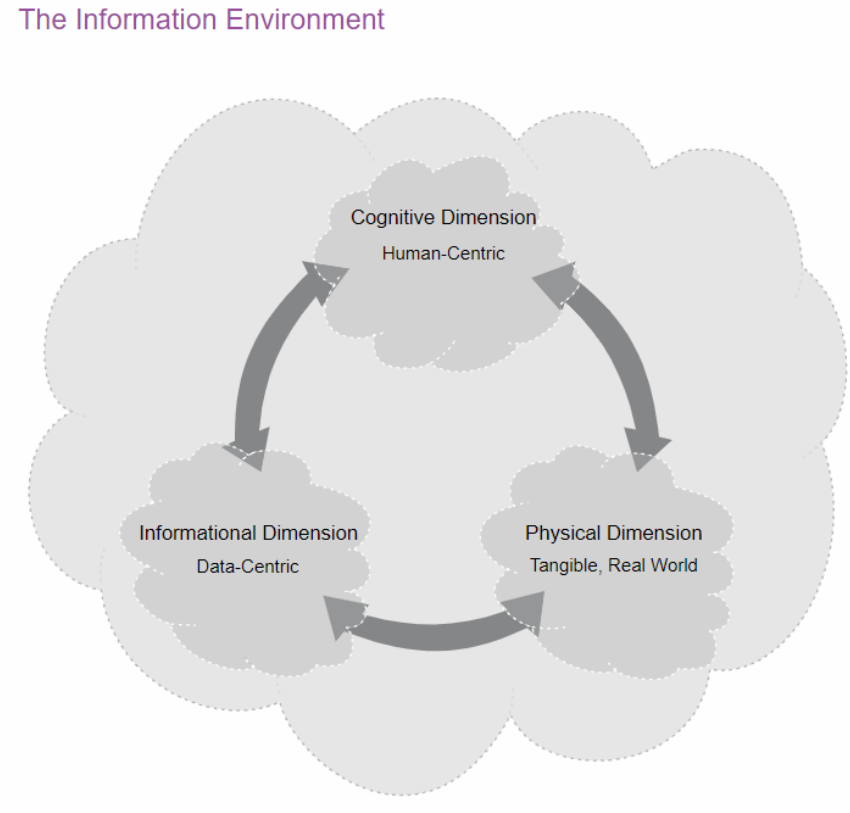
V vseh podanih definicijah opazimo veliko skupnega. Če strnemo bistvo teh definicij informacijskih operacij, lahko povzamemo, da so informacijske operacije dejavnosti, ki so nekinetične narave v informacijskem okolju, katerih glavni namen je ustvarjanje kaosa in zmede, vlivanje dvoma v civilno prebivalstvo in vplivanje na proces odločitve sovražnika na politični, vojaški in civilni ravni.

Na podlagi prebranega in napisanega lahko informacijske operacije strnemo v naslednjo definicijo: Informacijske operacije so vojaške in politične nekinetične aktivnosti v informacijskem okolju, ki s kibernetskimi in psihološkimi operacijami skušajo vplivati na mnenje in odločitve ciljne skupine, ki je bodisi lastno ali tuje prebivalstvo.

2.1 Informacijsko okolje

Informacijsko okolje je navidezni prostor, kjer potekajo informacijske operacije. Informacijsko okolje je sestavljeno iz posameznikov, organizacij in sistemov, ki zbirajo, procesirajo, širijo in ukrepajo na pridobljene informacije. V okolju so prepletene tri dimenzije oziroma sfere, in sicer informacijska sfera, fizična sfera in kognitivna oziroma emotivna sfera, skozi katere posamezniki in organizacije ter različni sistemi nenehno sodelujejo. Fizična dimenzija je sestavljena iz komandnih in nadzornih sistemov, programskega orodja, ključnih odločevalcev in podporne infrastrukture. Ti elementi omogočajo posameznikom in organizacijam želeni učinek. Informacijska sfera opredeljuje način in vir pridobljenih informacij ter njihovo procesiranje, širjenje,

hranjenje in varovanje. Kognitivna ali emotivna sfera informacijskega okolja predstavlja umske procese in čustva ljudi, ki pridobljene informacije sprejmejo ali posredujejo, ter ljudi, ki se na te informacije odzovejo oziroma sprejmejo odločitev na podlagi novo pridobljenih informacij.



Slika 2.1: Shematski prikaz informacijskega okolja (Joint Chiefs of Staff [JCS], 2012, str. I–2)

Slika 2.1 prikazuje informacijsko okolje in povezavo njegovih sfer, ki so med seboj prepletene. Brez informacijskega okolja informacijske operacije ne morejo delovati. Na primer, če izvzamemo kognitivno sfero iz informacijskega okolja, potem ostanemo brez sposobnosti razumevanja pridobljene informacije in sposobnosti odzivanja na pridobljeno informacijo. V informacijski sferi pravzaprav določimo vrednost te informacije in na podlagi tega se odločimo, kakšen bo naš naslednji korak, in recimo, da vplivamo na pomembnost informacije tako, da jo predstavimo sovražniku kot nepomembno, ko je ta v resnici pomembna, ima to lahko hude posledice za sovražnika. Brez fizične sfere pa ne bi bilo mogoče vplivati na informacije, saj to predstavlja vse načine, s katerimi lahko operiramo.

Poleg komponent morajo akterji poznati družbeno delovanje oziroma kaj je tisto, zaradi česar se ciljna skupina ali posameznik vede na določen način. Pri JCS (angl. Joint chief of staff, Urad združenega vojaškega štaba ZDA) so ugotovili, da na vedenje posameznikov in družbe vplivajo pravila, prepričanja in norme, medtem ko vedenje sistemov v fizični in informacijski sferi urejajo izključno pravila (JCS, 2012).

Razlog za poznavanje konstruktov pravil, norm in prepričanj vidimo v tem, da smo si ljudje različni. V različnih skupinah so se zaradi drugačnih načinov življenja norme, prepričanja in pravila razvijala drugače kot pri drugih skupinah ljudi. Ker drugače delujemo kot posameznik, skupina ali pa prebivalci države, je pomembno poznati te konstrukte, da bi lahko natančno vedeli, na katerega od teh konstruktov moramo vplivati, da bi dosegli želeni učinek.

2.1.1 Teoretična izvedba informacijskih operacij

JCS (2012) je predstavil korake, ki so pomembni za izvedbo informacijskih operacij. Le-ti se izvedejo kot predpriprava pred operacijo in na njih sloni uspeh operacije:

- Prepoznava in analiza ciljne skupine: S prvim korakom moramo pridobiti znanje o informacijskem okolju ciljne skupine, kakor tudi razumevanje pravil, norm in prepričanj. S tem postavimo temelje operacije, saj na podlagi te analize prilagodimo naslednje korake.
- Izbira sredstev: Na podlagi prejšnje analize izberemo sredstvo za dosego našega cilja. Sredstva so lahko diplomatske, vojaške, ekonomske, akademske, komercialne, verske ali etnične narave in so med seboj povezljiva.
- Načrtovanje učinka: Učinek je pogojen s sredstvi, ki smo jih izbrali v koraku pred tem. Če hočemo, da je učinek informacijskih operacij sprememba pravil, norm ali prepričanj, morajo izbrana sredstva to zagotavljati.
- Izbira orodja, tehnike ali aktivnosti: Zadnji korak, ki je odvisen od tega, ali hočemo ciljno skupino prepričati ali prisiliti v dejanje. Zato na podlagi te odločitve izberemo primerna orodja, tehnike ali aktivnosti.

Opazimo, da so tudi ti koraki med seboj tesno povezani. Vsak korak je strogo premišljen, vnaprej pa je tudi predviden njegov vpliv na naslednji korak in operacijo. Zaradi tega se pripravi nekaj scenarijev pred operacijo, na katere se akterji lahko obrnejo. V načrtovanju informacijskih operacij noben korak ni prepuščen naključju.

2.2 Pomembni akterji na področju informacijskih operacij

Na področju informacijskih operacij deluje veliko več entitet, kot jih bomo predstavili, vendar te so najpomembnejše. Predstavljene entitete vlagajo veliko denarja za prilagajanje na taktične in strateške izzive, ki jih ponuja večno razvijajoč se kibernetski svet. Prav tako predstavljeni akterji vlagajo veliko napora za ohranitev operativnih aktivnosti na področjih konfliktov, kjer so vpleteni.

2.2.1 NATO

Natova enota za strateško komunikacijo se nahaja v Latviji in je del Natovega centra odličnosti za strateško komunikacijo. Cilj enote je izboljšanje procesa razvoja, učenja in implementacije strateških komunikacij v operacije Natovih institucij in držav članic. Nato nima stalne enote za izvrševanje informacijskega bojevanja, temveč le ad hoc enoto, ki se formira v času konflikta, v katerega je Nato vpleten. Čeprav je sestava enote odvisna od razpoložljivega osebja, še zmeraj zajame vse pomembne aspekte informacijskega bojevanja (The NATO Strategic Communications Centre of Excellence, n. d.).

2.2.2 Združeno kraljestvo

Leta 2015 so v Združenem kraljestvu ustvarili 77. brigado. Cilj brigade je izvajati psihološke operacije skozi različne vrste medijskih kanalov, tudi družbenih omrežij. Sodeluje z britanskimi oboroženimi silami na terenu in jim je v pomoč z različnimi vedenjskimi analizami. Na obveščevalnem področju deluje skupina za odkrivanje groženj. Prav tako sodeluje in podpira 77. brigado pri njenem delovanju. Hkrati pa deluje še na kibernetskem, psihološkem in obveščevalnem področju. Skupina podpira vojaške

misije po vsem svetu z obrambnimi in obveščevalnimi operacijami znotraj in zunaj Britanije. Skupina izvaja ofenzivno kibernetsko vojskovanje kot del svoje protiteroristične kampanje (napadi DDoS, angl. distributed denial of service, ponarejanje strani) in uporablja taktična orodja na konfliktnih območjih, kjer deluje britanska vojska (Sengupta, 2015).

Medtem na področju strateške komunikacije deluje vladni oddelek za raziskovanje, informacije in komunikacijo (v nadaljevanju RICU). Naloga oddelka je koordinacija vladnih naporov v borbi proti ideologiji, ki podpira terorizem. Na področju razumevanja ekstremističnih sporočil svetujejo policiji in ostalim silam pregona.

2.2.3 Evropska unija

Evropska unija je po terorističnih napadih v Franciji v začetku leta 2015 ustanovila skupino po vzoru britanske enote RICU. Sprva je bila namenjena za boj proti širjenju sporočil na družbenih omrežjih, ki novačijo Evropejce muslimanske vere v boj v Sirijo (European Parliament, 2016). Rezultati so bili uspešni in kmalu se je enota prelevila v evropski center strateških komunikacij (ESCP), ki skuša dobiti vpogled v komunikacijske prakse in tako pomagati v boju proti radikalizaciji in terorizmu (Council of the European Union, 2016). Konec leta 2015 je po ilegalni priključitvi Krima in vse večji prisotnosti ruskih botov, ki so širili rusko propagando, Evropska unija vzpostavila posebno enoto za boj proti ruskim dezinformacijami. Enota je mreža več kot 400 novinarjev različnih civilnih organizacij in akademskih institucij, lociranih v več kot 30 evropskih državah. Z dokumentiranjem ruskih poskusov in boja le-teh dobimo boljši vpogled v ruske informacijske operacije in v trend, v katerega se razvijajo (European External Action Service, n. d.). Prav tako pa je bil na Finskem ustanovljen Evropski center odličnosti za preprečevanje hibridnih groženj. Center naj bi služil kot osnova za stalno sodelovanje med državami članicami Evropske unije in Natom, za oblikovanje doktrine ter izvajanje programov usposabljanja in certificiranja, namenjenih krepitvi individualnih zmogljivosti udeležencev v boju proti hibridnim grožnjam, kamor sodijo tudi informacijske operacije (The European Centre of Excellence for Countering Hybrid Threats, n. d.).

2.2.4 Izrael

V izraelski vojski na področju informacijskih operacij delujejo tri enote. Center za psihološke operacije, ki deluje pod izraelskim vojnim obveščevalnim direktoratom, se s svojimi operacijami osredotoča predvsem na pristaše Hamasa in civilno prebivalstvo v Gazi, operacije zajemajo propagando in širjenje lažnih novic. Bataljon Psagot deluje na področju elektronskega bojevanja in skuša držati prevlado v tej sferi informacijskih operacij. Tretja enota skrbi za odnose z javnostjo. Odnosi z javnostjo upravljajo z operacijami, namenjenimi mednarodni javnosti. So pobudniki in organizatorji obiskov tujih visokih predstavnikov. Namen je ustvariti proizraelsko klimo in prepričati tuje predstavnike o bolj prijateljskem pristopu do države.

Na politični ravni so za informacijske operacije zadolženi oddelki pod okriljem ministrstva na zunanje zadeve in ministrstva za medije in odnose z javnostjo. Njihove naloge so, da identificirajo organizacije in posameznike, ki bojkotirajo Izrael v medijih in družbenih omrežjih. Ena izmed nalog je tudi usposabljanje ambasadorjev o načinih distribuiranja proizraelskih sporočil na različnih družbenih omrežjih (Cohen in Bar'el, 2017).

2.2.5 Združene države Amerike

Pod budnim očesom urada načelnika združenega štaba v Združenih državah Amerike od leta 1999 deluje središče za bojevanje z informacijskimi operacijami. Deluje na dveh ravneh, strateški in taktični. Na taktični ravni deluje ekipa strokovnjakov za informacijsko bojevanje in sodeluje z ekipo na misijah. Na podlagi socialno-kulturnih analiz ciljnega prebivalstva jim svetujejo vrsto informacijskih operacij. Na strateški ravni je center zadolžen za vse agencije, ki so pod okriljem ministrstva za obrambo. Center je zadolžen za posredovanje informacij med agencijami. Tri divizije, ki načrtujejo in izvajajo psihološke operacije, pa delujejo v kopenskih silah ameriške vojske. V večini primerov ciljajo na civilno prebivalstvo na konfliktnih področjih. S psihološkimi operacijami

skušajo prebivalstvo odvrniti, da bi pomagali gverilskim borcem in da pomagajo njim (Cohen in Bar'el, 2017).

Na področju informacijskih operacij delujejo tudi v centralnem komandnem centru ameriške vojske (CENTCOM), ki je zadolžen za uničevanje nasprotnikove propagande in širjenje primerov sovražnikove hinavščine in kriminala. Prav tako je zadolžen za ekipo 11 ljudi, ki tekoče govorijo arabsko, rusko, urdujsko in perzijsko, ter je namenjena za nadzor komunikacij na družbenih omrežjih (Parrish, 2016).

Ameriške volitve 2016

Na tej točki bomo predstavili primer vmešavanja ruskih akterjev v ameriške volitve. Američani so se sredi jeseni 2016 odpravljali na volišča. Izbirali so novega predsednika države, že 45. po vrsti v svoji zgodovini. Po vseh političnih kampanjah in zborih sta na koncu ostala dva kandidata. Čeprav so v ZDA tudi ostale politične stranke, se zaradi svoje majhnosti težko vključijo v predsedniško dirko in, kot je to bilo že od nastanka države, sta se za mesto potegovala kandidata demokratske in republikanske stranke. Tistega leta sta se za mesto predsednika potegovala članica demokratske stranke Hillary Clinton, žena nekdanjega predsednika ZDA Billa Clintona, in republikanec Donald J. Trump. Volitve tistega leta so požele več mednarodnega zanimanja kot katere koli prej. Po spletu so se širili sovražni govori Donalda Trumpa in bučni aplavzi, ki jih je dobival s strani svojih privržencev, kar so demokrati ostro obsojali. Vendar so afere prihajale tudi z njihove s strani, med njimi je recimo objava ukradene e-pošte, kjer so se posmehovali drugemu demokratskemu kandidatu Bernieju Sandersu. Na koncu, čeprav je bilo število glasovnic, ki so bile naklonjene demokratski kandidatinji, večje od tistih, kjer je bil obkrožen Donald J. Trump, je zaradi elektorskega glasu zmagal prav on (Gambino in Pankhania, 2016).

Ameriške predsedniške volitve so dogodek, ki nima le vpliva v ZDA, vendar tudi drugod po svetu. S svojim statusom, ki ga ima kot država, in po mnenju mnogih najmočnejšo vojsko ima vpliv po celem svetu. Prav zaradi tega postane izvoljeni predsednik ali

predsednica eden izmed ključnih voditeljev na svetu. To je odličen razlog za poskus vplivanja na izhodišče volitev, saj bi s tem lahko pridobili predsednika, ki bi favoriziral akterjeve interese. To se je tudi zgodilo. Po predsedniških volitvah so postajale govorice o vmešavanju Kremlja v volitve vse glasnejše. Začele so se preiskave in ameriške oblasti so potrdile njihov sum. Ruske oblasti so se vmešavale v demokratski proces volitev. Zanimivo, da to ni bil prvi poskus takega podviga, saj so poskušali že davnega leta 1964 in nato še 20 let pozneje, vendar, sodeč po ameriških odzivih, nista bila tako uspešna, kot je bil ta leta 2016 (Gioe, 2018). Podvig take ravni si lahko privoščita samo Rusija in Kitajska, oboji imajo kibernetske sposobnosti na zelo visoki ravni, hkrati pa tudi vojsko, s katero lahko podpreta svoja dejanja in finance. Poleg tega pa imajo samo ti dve državi in Severna Koreja razlog za vmešavanje v ameriške volitve.

Operacija se je začela s krajo zasebne e-pošte tesnega sodelavca Hillary Clinton in vdorom na strežnik nacionalnega demokratskega komiteja. Na začetku sta sodelovali hekerski skupini Fancy Bear in Cozy Bear, ki sta v hekerskih krogih znani kot skupini, ki sta podprti s strani Kremlja, ter po svoji uspešnosti in učinkovitosti (Department of Homeland Security, 2016). Zaradi tajnosti operacije ruski operaterji niso smeli objaviti informacij kot oni, kar bi bilo absurdno in ne bi imelo smisla, saj bi s tem uničili vse delo. Zato so se obrnili na Juliana Assangea. Julian Assange, znani žvižgač, je delil pridobljene informacije na svoji spletni strani Wikileaks.com. Poleg Juliana Assangea so prav tako ustvarili svojo spletno stran DCLeaks.com, kjer je spletna persona oziroma računalniški bot z imenom Guciffer 2.0 delil ukradene informacije (Gioe, 2018).

Nato je prišla druga faza načrta. Sedaj so ukradene informacije morali približati širši množici. To jim je uspelo s tako imenovano farmo računalniških botov in skupino internetnih trolov. Tukaj je operacijo prevzela IRA, kjer je s svojo vojsko trolov in botov, nastanjenih v ruskem mestu Sankt Petersburgu, povzročila kaos na družbenih omrežjih (Office of the Director of National Inteligence [DNI], 2017). Z manipuliranjem informacij na družbenih omrežjih so dosegli željeno. Najprej je sledil razdor na družbenih omrežjih, ki je kmalu prerasel v nasilje v resničnem svetu. Uspeli so zmanjšati zaupanje v demokratske procese, izvoljeno vlado in njene predstavnike (Desouza idr., 2020).

Ali je vmešavanje res vplivalo na volitve, bomo težko kadar koli raziskali. Je pa zagotovo pustilo posledice, ki so, če malo pomislimo, kar strašljive. Rusi so z malo denarja in uporabo družbenih omrežij povzročili kaos v državi, ki je njihova največja tekmica v vseh aspektih, in če bi delovali bolj previdno, s tem mislimo na sledi, ki so jih pustili za sabo, najverjetneje ne bi bili nikoli odkriti. Po drugi strani pa je možno, da je bilo odkritje načrtovano in je bila celotna operacija mišljena kot »power play« oziroma kazanje svojih vojaških sposobnosti in kot opozorilo.

2.2.6 Ruska federacija

Za razliko od ostalih držav so informacijske operacije v Ruski federaciji napadalno usmerjene aktivnosti. Tehniko informacijskih operacij so začeli piliti že v času Sovjetske zveze in jo sčasoma dograjevali. Njihov general Valery Gerasimov je v začetku prejšnjega desetletja v svoji vojaški doktrini postavil informacijske operacije v sam vrh pomembnosti ruske vojaške strategije. Informacijske operacije Rusije vključujejo sistematične napade na digitalna omrežja, psihološko vojskovanje, goljufije, preusmerjanje pozornosti in dezinformacije. S temi sredstvi dobesedno bombardirajo opozicijsko stran s poplavo informacij, ki vključujejo digitalne, elektronske in zaznavne elemente. Primarna orodja ruskih informacijskih operacij so računalniški boti, internetni troli in hekerji. Ruski troli se na svetovnem spletu vključujejo v različne debate in z dezinformacijami širijo prorusko propagando. Njihove komentarje najdemo tudi na zahodnih medijskih portalih, posebej tistih, ki so kritični do Rusije. Čeprav so zelo neprepričljivi v širjenju svojih pogledov, to ni njihova glavna naloga. S svojo navzočnostjo kontrolirajo tok informacij in tako ustvarjajo občutek strahu in negotovosti ter spodkopavajo kredibilnost vira informacij. Prav tako s širjenjem novic, ki so bile objavljene v ruskih medijih, dosežejo, da algoritem na družbenih omrežjih zazna te novice kot najnovejši trend, kar poveča možnost poročanja istih novic v zahodnih medijih (Adamsky, 2015).

Ukrajinska vojna

Rusko strategijo lahko predstavimo tudi na primeru ukrajinske vojne. Zametki vojne v Ukrajini segajo že v leto 2014 po Majdanskem gibanju in uporih proti takratnemu ukrajinskemu predsedniku Viktorju Janukoviču in njegovi proruski politiki. Razmere so se zaostrovale in predsednik je pobegnil v Rusijo, ti pa so v vsem tem kaosu videli priložnost in ilegalno priključili polotok Krim. Prav tako so oborožili separatistična gibanja v pokrajinah Donbas in Lugansk, ki so se preteklih osem let konstantno spopadala z ukrajinskimi varnostnimi organi. V letih po priključitvi Krima so se spopadi umirili, vendar so še vedno bili prisotni in čeprav je bilo stanje med državama napeto, ni prišlo do nobenih mednarodnih incidentov vse do konca leta 2021, ko je ruski predsednik Vladimir Putin zelo jasno povedal, da se morata Evropska unija in organizacija Nato umakniti in se nehati vmešavati v politiko nekdanje sovjetske države. Podal jima je tudi rok za izpolnitev svojih pogojev in če ne bo upoštevan, bo ukazal napad vojaških sil. Del mednarodne skupnosti je menil, da je to »blef«, medtem ko je drugi del menil, da so to resnične grožnje, kar se je na koncu izkazalo za resnično. Dne 24. februarja 2022 so ruske sile vkorakale v Ukrajino s treh strani in začela se je ukrajinska vojna (Council on Foreign Relations, 2023).

Vloga informacijskih operacij je bila tudi v tej misiji velika. S strani Rusije so bile uporabljene na mednarodni ravni, kakor tudi na ruskem in ukrajinskem prebivalstvu. Po ilegalni priključitvi so sprožili masovno operacijo, s katero so opravičevali in argumentirali svoja dejanja mednarodni skupnosti in svojim prebivalcem. Z uničenjem radijskih in televizijskih oddajnikov so onesposobili možnost komunikacije ukrajinskih voditeljev s svojimi prebivalci in preostankom sveta. K širjenju lažnih informacij in propagande so pripomogle ruske različice Facebooka in Twitterja, VKontakte in Odnoklassniki, kakor tudi lažne spletne strani, ki so se pretvarjale za proukrajinske in podkupljene medijske hiše (Treyger idr., 2022).

V opisanih centrih opazimo, da v njih sodelujejo ljudje z različnih področij, kot so obramboslovje, psihologija, kibernetska varnost, novinarstvo. S tem povečajo

učinkovitost delovanja takih centrov. Če izvzamemo ZDA in Rusko federacijo, vidimo, da so ostale države oziroma agencije dokaj pozno začele ustanavljati podobne centre. Evropa je zaznala potrebo po takih centrih v zadnjem desetletju, ko so v Evropo masovno migrirali ljudje z Bližnjega vzhoda in ob porastu terorističnih napadov. Opazimo tudi, da znotraj teh centrov deluje več agencij, ki spadajo pod okrilje države, od državnih obveščevalnih agencij, vojaškega štaba do raznih ministrstev. V principu je delovanje teh centrov dokaj podobno, ena velika razlika pa se vidi med ruskim centrom in ostalimi. Medtem ko so ostali centri bolj defenzivno naravnani, s tem mislimo na spremljanje dogodkov in ukrepanje le takrat, ko je zaznana nevarnost, so ruski centri edini med navedenimi, ki so aktivno ofenzivno naravnani.

3 ANALIZA IN PRIMERJAVA PRIMEROV

V naslednjem sklopu zaključnega dela bomo analizirali in primerjali obravnavana primera. Navedena primera smo si izbrali zaradi skupnega imenovalca, ki v obeh primerih izvaja informacijske operacije v dobrobit sebe oziroma za izpolnitev svojih ciljev ne glede na posledice v ciljni državi. Za primerjavo smo si izbrali nekaj opornih točk, ki se nam zdijo smiselne za primerjavo informacijskih operacij v obeh primerih.

3.1 Obvladovanje medijev

Mediji v demokratičnih državah predstavljajo orodje, s katerim prebivalstvo dobi vpogled v dogodke na domačih in tujih tleh. Z njimi lahko novinarji izvajajo tako imenovano četrto vejo oblasti in nam predstavijo dejanja našega političnega vrha. Objektivnost medijev je zelo pomembna, saj je pomembno, da si bralec ali gledalec postavi svoje lastno mnenje na podlagi resničnih dejstev o dogodku ali dogodkih in ne na podlagi subjektivnega mišljenja avtorja članka oziroma prispevka. To objektivnost medijev dosežemo samo z neodvisnostjo le-teh od političnega vrha, kar pomeni, da mediji ne smejo biti v lasti nobene politične stranke ali osebe na politični funkciji.

V primeru informacijskih operacij so mediji uporabljeni kot orožje, s katerim manipulirajo z informacijami tako, da predstavijo določene dogodke v drugačni luči, kot so v resnici. Krojenje resnice po željah svojih voditeljev in subjektivno poročanje so znaki medijev, ki delujejo v korist države in ne v korist ljudstva. Tako obvladovanje medijev lahko opazimo v vseh nedemokratičnih državah na svetu, kjer so običajno mediji v lasti politikov. Z obvladovanjem medijev imajo voditelji moč manipulirati na mnenje in odločitve svojega ljudstva, do neke mere pa tudi na mnenje tujih prebivalcev.

Če primerjamo obvladovanje medijev v obeh primerih, opazimo, da so se Rusi v primeru ukrajinske vojne osredotočili povsem na tradicionalne medije, kot so televizija, radio in časopisi. Treyger idr. (2022) na področju separatističnih regij poročajo o omejitvi internetnega dostopa, uničevanju radijskih in televizijskih oddajnikov in vse večjem

objavljanju dezinformacij in propagande v časopisih in televizijskih novicah. Prav tako naj bi z vplivom nad zaposlovanjem v večjih televizijskih hišah poskrbeli, da se ruska propaganda predvaja tudi v ostalih predelih Ukrajine. Z obvladovanjem medijev so prav tako omejili informacije svojim lastnim prebivalcem. Po ocenah spletne strani freedomhouse.org (Freedom House, n. d.) o svobodi medijev je Ruska federacija že pred vojno imela oceno 20 od 100, po vojni se je ta spustila na 18. To nam pove, da so Rusi informirani samo s strani svojih medijev, ki pa si resnico prilagajajo po svojih željah. Nytimes.com (Smart, 2022) je objavil zanimiv graf (slika 3.1), ki prikazuje porast člankov, ki označujejo Ukrajince za naciste. Članki, kjer Ukrajince dehumanizirajo, jih prikažejo kot barbare in necivilizirane, so bili namenoma objavljeni. Ko so ruski prebivalci brali o takih osebah, se ti niso mogli počutiti krive zaradi dejanj svoje vlade in vojske, prav nasprotno, v njih je narasel še večji bes, kar je razlog za veliko podporo vojne v Rusiji.

Slika 3.1: Porast števila člankov o povezavi med nacizmom in Ukrajino (Smart, 2022)

Smart (2022) v svojem članku omeni, da je to privedlo do manka kognitivne disonance. Kar pomeni, da prebivalci Rusije, četudi so postavljeni pred resnična dejstva o dejanjih svoje vojske, to zanikajo in verjamejo le svojim informacijskim virom.

Medtem v primeru vpletanja v ameriške volitve leta 2016 ruski akterji niso skušali obvladovati tradicionalnih medijev. Preprosto bi bilo pretežko vplivati na kakršne koli tradicionalne medije v ZDA s strani ruskih akterjev. Zgodovina teh dveh držav od hladne vojne dalje je pripeljala do tega, da se tudi prebivalci med seboj sovražijo. Kar pomeni, da kakršnega koli morebitnega omenjanja Rusije na televiziji in radiu Američani ne bi dobro sprejeli oziroma bi hitro zaznali, da nekaj ni v redu. Seveda so se tega ruski akterji zavedali in so se odločili za drugačen pristop. Izkoristili so moč družbenih omrežij.

3.2 Družbena omrežja

Čeprav tudi družbena omrežja sodijo v medije in bi lahko bila omenjena v prejšnji točki, smo se odločili, da jih bomo na podlagi pomembnosti v obeh primerih obravnavali posebej. Družbena omrežja so v današnjem hitrem načinu življenju za mnoge ljudi postala glavna informativna točka. Prek njih izvemo o pomembnih dogodkih, ki so se zgodili prek dneva. Interaktivnost družbenih omrežij nam omogoča komunikacijo z ostalimi uporabniki, s katerimi lahko delimo svoja mnenja in nam pomembne informacije. Ta interaktivnost je glavni atribut družbenih omrežij in prav zaradi tega so tudi nastale, a ruski akterji so prepoznali možnost spremembe družbenih omrežij iz orodja v orožje za spreminjanje mnenj in manipulacije sovražnega naroda. Prav tako zaradi takrat slabih obrambnih mehanizmov na omrežjih, kot sta Twitter in Facebook, je IRA z lahkoto delila svojo propagando in dezinformacije.

Pravzaprav so bila družbena omrežja v obeh primerih uporabljena na skoraj enak način za deljenje dezinformacij, propagande in profiliranje ter socialni inženiring. V primeru ameriških volitev 2016 so se družbena omrežja izkazala za odlično platformo za deljenje ukradene e-pošte nacionalnega demokratskega komiteja, ki je pokazala nespoštovanje in posmehovanje do njihovega kolega, prav tako predsedniškega kandidata Berniea Sandersa. Mnogi menijo, da je prav ta incident prevesil tehtnico na stran Donalda Trumpa (Gioe, 2018).

Na drugi strani tudi Treyger idr. (2022) ugotavljajo, da so bila v ukrajinski vojni družbena omrežja uporabljena za deljenje ruskih laži in dezinformacij, vendar najprej na ruskih omrežjih OK in VK, saj so ti dve omrežji Ukrajinci uporabljali v večini. Ker je večina ukrajinskih prebivalcev uporabljala ti dve omrežji in ne ameriških različic, so bili ti izpostavljeni še bolj agresivni ruski kampanji z informacijskimi operacijami, ki je vsebovala cenzuro, propagando, lažne novice in ostala orodja informacijskih operacij. Po priključitvi polotoka Krima je sledila prepoved omrežij OK in VK v Ukrajini. Zaradi tega se je ukrajinsko prebivalstvo preselilo na ameriške različice omrežja, vendar tudi tam niso bili varni pred informacijskimi operacijami s strani ruskih akterjev, a vseeno bolj kot prej.

Gioe in Treyger prav tako navajata, da sta bili za deljenje informacijskih operacij na družbenih omrežjih ključni dve stvari, internetni troli in računalniški boti. Internetni troli so ljudje, ki na družbenih omrežjih večinoma z deljenjem in objavljanjem lažnih informacij ter komentiranjem objav delajo kaos. Tako rečeno, prilivajo olje na ogenj s komentiranjem na občutljive teme in deljenjem le-teh. S tem so velikokrat na družbenih omrežjih naredili dva pola, ki sta oba zagovarjala svoje favorite, in tako se je vnel hud besedni boj, ki je le povečeval razdrtost v skupnosti. Enako velja za računalniške bote, le da so ti računalniški program in predstavljajo lažnega človeka oziroma lažni profil na družbenih omrežjih, ki je upravljan večinoma s strani internetnih trolov. V ta namen je IRA v mestu Sankt Petersburg zgradila poslovno poslopje, ki služi kot baza za informacijske operacije na družbenih omrežjih. Prav tako iz Ukrajine prihajajo poročila o odkritjih tako imenovanih farmah botov, ena izmed večjih je bila odkrita v začetku poletja, z njo so upravljali več kot milijon računalniških botov na različnih omrežjih (Petkauskas, 2023). Kot smo omenili, so družbena omrežja idealna platforma za deljenje informacijskih operacij. Vendar niso bili vsi enakega mnenja. Direktor Facebooka Mark Zuckerberg je dejal, da ne verjame, da bi lahko lažne novice na Facebooku kakor koli vplivale na izid volitev (Larson, 2016). A prav to se je zgodilo. Zaradi možnosti anonimnosti in prikritega delovanja mnogokrat institucije niso zaznale kakršnega koli delovanja, iz katerega bi bilo razvidno, da gre za informacijske operacije na družbenih omrežjih, dokler ni bilo prepozno. V zadnjih letih se je to spremenilo, saj so na sedežih

družbenih omrežij sprejeli protiukrepe in zaščite proti informacijskim operacijam, prav tako pa brišejo veliko lažnih profilov na dnevni bazi. Kljub temu menimo, da to ni dovolj in da je potrebno še veliko dela na področju zaščite pred informacijskimi operacijami na družbenih omrežjih. Težava je, da kompletno zaščito, ki jo iščemo, lahko dosežemo le z nadziranjem vsake objave in preverjanjem dejstev, kar bi verjetno vodilo v cenzuro, kar pa bi bilo kontradiktorno namenu družbenih omrežij, ki je izražanje in deljenje svojih mnenj, kakor tudi pravici svobodnega izražanja. Zato popolne zaščite na družbenih omrežjih ne bo nikoli in bi morali našo pozornost usmeriti v izobraževanje ljudi, kako lahko prepoznajo informacijske operacije na družbenih omrežjih.

3.3 Lažne informacije

V obeh primerih smo priča popolnoma različnima pristopoma ruskih akterjev. Za dosego svojih ciljev so morali podrobno analizirati, kateri pristop bi bil najbolj primeren. Za dosego ciljev pri vmešavanju v ameriške volitve leta 2016 so ubrali prepričevalni pristop. Informacije, ukradene s strežnika demokratskega narodnega komiteja, so bile dovolj škodljivega značaja, zato ni bilo potrebe po nikakršnih posegih na družbenih omrežjih z lažnimi novicami, le spretno objavljanje in komentiranje radikalnih mnenj, ki je razklalo ameriško družbo. Eden od načinov širjenja radikalnih mnenj je bilo objavljanje teh v obliki memeov (gre za viralno širjenje šal, idej in podobnega, ki so v formatu slike). Med drugim so objavljeni memei prikazovali borbo Jezusa in Hillary Clinton (upodobljeno kot hudič), na vrhu slike pa je bilo sporočilo »všečkajte in delite, če hočete, da Jezus zmaga«. Cilj takega objavljanja je bila interakcija z ostalimi uporabniki na Facebooku. V tem primeru z Američani, ki se identificirajo kot republikanci. Ker je znano, da večino republikancev predstavljajo kristjani, so s takimi objavami dosegli, da so Hillary Clinton v tem primeru dojemali kot zlobno osebo, neprimerno za vodenje države. To so izkazali s komentiranjem in deljenjem podobnih objav, kar je rezultiralo, da je algoritem na družbenih omrežjih razumel objavo kot popularno in jo prikazal tudi ostalim. Preiskava po volitvah je ocenila, da je vsebina ruskih akterjev, ki je bila deljena na tak način, dosegla okoli 126 milijonov ameriških Facebook uporabnikov (Mayer, 2018).

Ruski akterji so v primeru ameriških volitev zaznali ponujeno priložnost in jo maksimalno izkoristili. Zaradi ukradenih informacij, ki so bile dovolj obremenilne, ni bilo potrebe po generiranju lažnih informacij. Treba jih je bilo le predstaviti na način, ki bo v ciljanih osebah vzbudil čustva jeze ali sovraštva. Ta čustva so nato delili z ostalimi in tako so generirali promet na družbenih omrežjih, kar je velikokrat rezultiralo v besedne spopade med privrženci dveh političnih strank. K temu je pripomogla tudi zgodovina teh dveh strank, saj se že od nekdaj ne marata. Zaradi dobre analize ni bilo potrebno veliko dela ruskih akterjev, treba je bilo le prilivati olje na ogenj.

Če lažne informacije niso predstavljale tako pomembne vloge v vmešavanju v ameriške volitve 2016, tega ne moremo reči za primer ukrajinske vojne. Lažne informacije ali dezinformacije so bile glavno orožje ruskih akterjev. Z lažnimi informacijami so obstreljevali tri ciljne skupine, ukrajinsko in rusko prebivalstvo in pa mednarodno skupnost. Mednarodna skupnost je bila deležna trditev, kot so, da se Nato širi in tako krši dogovor iz devetdesetih let, da se izvaja genocid v regijah Lugansk in Donbas ter da morajo zaščititi tamkajšnje rusko prebivalstvo, da ni odgovorna za konflikt, saj le brani svoje interese pred agresivno Ukrajino. To je le nekaj trditev, ki jih je evropski projekt Evropska unija proti dezinformacijam naštel in ovrgel (European External Action Service, 2022). Mednarodna skupnost je hitro spregledala skozi te trditve in se postavila na stran Ukrajine. Medtem so ruski akterji širili tudi rusko propagando med vojake in prebivalce Ukrajine ter jim z lažnimi informacijami o domnevnih prepirih med predsednikom in generalom o kritičnem stanju predsednika skušali načeti bojno moralo (Lapienytė, 2023). To jim zaenkrat ni uspelo, saj se ukrajinska vojska uspešno brani. Tretja žrtev lažnih informacij pa je rusko prebivalstvo, ki je izpostavljeno člankom, ki navajajo porast nacizma v Ukrajini in jih je treba ustaviti. Poleg tega so izpostavljeni popolni cenzuri, mediji ne smejo pisati o resničnem stanju na bojišču, saj bi jih doletela popolna zaporna kazen.

3.4 Odziv

V tem delu bomo primerjali odziva obeh držav na informacijske operacije, usmerjene proti njim. Odziv države na informacije operacije je zelo pomemben, saj s pravim odzivom lahko pomirijo svoje prebivalce in s tem nekako preprečijo nadaljnje vplivanje na svoje prebivalce. V obeh primerih bomo videli, da je bil začetni odziv zelo slab ali pa ga sploh ni bilo. To je tudi tlakovalo nadaljnji potek informacijskih operacij v obeh primerih.

Zaradi poznega odkritja informacijskih operacij je bil ameriški odgovor zelo šibek. Na ruske informacijske operacije so se odzvali z izgonom 35 ruskih diplomatov, za katere je obstajal sum, da so bili agentje pod krinko. Prav tako so ruskemu osebju prepovedali dostop do dveh oporišč, za katera se verjame, da sta bili uporabljeni kot baza za rusko obveščevalno dejavnost. Eden od ukrepov je bila tudi prepoved uporabe antivirusnega programa Kaspersky, ki je narejen s strani ruskega programerja. Takrat še predsednik Barack Obama, ki je počasi zapuščal ovalno pisarno (volitve so ponavadi konec oktobra, začetek novembra, vendar novo izvoljeni predsednik priseže šele v sredini januarja), je izdal še enega izmed zadnjih ukazov, ki je povečal predsednikovo moč. Kar je pomenilo, da lahko predsednik uvede sankcije ne samo proti izvajalcem kibernetskega napada, temveč tudi proti vsakomur, ki je spoznan za vmešavanje, spreminjanje ali povzročanje zlorabe informacij z namenom vmešavanja ali spodkopavanja volilnih postopkov ali institucij (Greenberg, 2016). Odziv ZDA je bil po našem mnenju kar malo smešen, vendar po drugi strani tudi razumljiv, saj zaradi poznega odkritja niso več imeli veliko opcij. Rusija se je tako rekoč vmešala v najbolj pomemben demokratičen proces na svetu, a ti so lahko le nemočno gledali, kako so ruski akterji odkorakali brez posledic. V ta namen tudi niso mogli sprožiti vojne, saj ni bilo uporabljeno nobeno kinetično orožje, je pa tu tudi vprašanje nadaljnjega odgovora Rusije, ki bi lahko imel katastrofalne posledice ne samo za ti dve državi, ampak za celoten svet. Menimo, da če bi vir informacijskih operacij izhajal od drugod, bi odziv vseboval tudi vojaško ukrepanje.

Na drugi strani je bil ukrajinski odgovor po ilegalni priključitvi prav tako šibak. Neenotno poročanje stanja s strani politikov je povzročilo dodatni kaos med prebivalci, kar je bil razlog za ustanovitev novega ministrskega resorja, ki je bil zadolžen za informacijsko politiko. Skrbijo za koordinacijo izjav ministrstev in vladnih agencij ter diseminacijo komunikacij in informacij ter preprečevanje ruske informacijske agresije. Prav tako so vzpostavili boljše obrambne mehanizme v vojski, tam so zaposlili strokovnjake na področjih sociologije, novinarstva, psihologije, ki jim pomagajo pri nadzorovanju informacijskega okolja. Drugi ukrep vojske je bila tudi prepoved nošnje telefona na bojišče. Z ukrepom upajo, da bodo preprečili kakršen koli vpliv na svoje vojake. Ukrajina je v boj proti informacijskim operacijam poslala tudi nevladne organizacije, ki so pomagale in še vedno pomagajo pri izobraževanju ljudi o nevarnostih lažnih informacij in propagandi ter pri boju proti ruskim informacijskim operacijam (Treyger idr., 2022). Pomoč pri boju proti vplivom informacijskih operacij so poiskali tudi pri domači filmski produkciji. Namreč v obdobju po ilegalni priključitvi polotoka Krim in pred začetkom vojne februarja 2022 je ukrajinska filmska produkcija posnela kar nekaj filmov. Filmi so bili financirani s strani države in njihov namen je bil okrepiti narodno zavest ukrajinske družbe (Ladygina, 2022). Ukrajinski odgovor je bil konkreten in odločen. Ukrepi niso bili videti kot obupan zadnji poskus odgovora samo zato, da bi odgovorili, kot je bilo to recimo videti pri ZDA, vendar so bili premišljeni in vsak je imel svoj namen. Tak odziv je pomiril in združil ukrajinsko družbo. Ukrajinski odziv bi si lahko vzeli za vzor, kako ravnati v primeru informacijskih operacij, in bi lahko služil kot osnutek ukrepov vsaki državi, ki se znajde v tej situaciji.

3.5 Analiza in primerjava

Informacijske operacije so postale ključno orodje v sodobnih geopolitičnih konfliktih, saj državam omogočajo vplivati na javno mnenje, širiti propagando in doseči svoje politične cilje. V tej nalogi smo se osredotočili na primerjavo ruskega vmešavanja v ameriške volitve leta 2016 in ruske invazije na Ukrajino, zlasti z vidika uporabe informacijskih operacij. Obe situaciji sta razkrili močno vlogo, ki jo imajo informacijske tehnologije in mediji pri oblikovanju javnega mnenja in vplivanju na politične procese v drugih državah.

Pri primerjavi ruskega vmešavanja v ameriške volitve leta 2016 in ruske invazije na Ukrajino obstaja več razlik kot podobnosti. Kljub temu da obe situaciji vključujeta uporabo informacijskih operacij in ciljata na vplivanje na javno mnenje ter podporo političnim ciljem Rusije, so njihovi konteksti, obsegi in posledice precej različni.

Vmešavanje v ameriške volitve je imelo globalni vpliv, saj je ciljalo na eno od najmočnejših držav na svetu. Na drugi strani pa je invazija na Ukrajino pomenila vojaški poseg in kršitev suverenosti države, kar je imelo regionalne in mednarodne posledice. Vmešavanje v ameriške volitve je bilo namenjeno podpiranju političnih interesov Rusije v ZDA. Ruske informacijske operacije so ciljale poglobiti delitve v ameriški družbi in ustvariti politično nestabilnost. S širjenjem dezinformacij in manipulacijo so se osredotočili na krepitev določenih političnih struj, ki so bile bolj naklonjene ruski politiki, in na zmanjšanje zaupanja v demokratične institucije. V primeru ruske invazije na Ukrajino pa je Rusija želela doseči svoje geostrateške interese v regiji, zlasti glede nadzora nad Črnim morjem in ohranjanja vpliva v nekdanjih sovjetskih republikah. Aneksija Krima je predstavljala poskus krepitve ozemeljskih interesov Rusije na račun suverenosti Ukrajine. Podpiranje separatizma na vzhodu Ukrajine pa je prav tako služilo cilju oslabitve ukrajinske vlade in preprečitve približevanja Ukrajine Evropski uniji in Natu.

Rusko vmešavanje v ameriške volitve leta 2016 je temeljilo predvsem na uporabi družbenih omrežij in spletnih platform za širjenje dezinformacij in propagande. Ruski akterji so se posluževali avtomatiziranih botov, lažnih računov in ciljanega oglaševanja za dosego določenih skupin volivcev. IKT so uporabljali predvsem za ciljanje na širšo ameriško javnost in širjenje sporočil, ki bi podprla njihove politične interese. Na drugi strani pa je bila uporaba IKT v informacijskih operacijah v primeru ruske invazije na Ukrajino bolj usmerjena v vohunjenje, kibernetske napade in nadzor nad državnimi komunikacijskimi omrežji. Kibernetski napadi so bili usmerjeni na državne ustanove in infrastrukturo, vključno z ukrajinskimi vladnimi organizacijami, mediji in elektronsko komunikacijo. Ruska vojaška in obveščevalna enota GRU je bila obtožena kibernetskih napadov na različne cilje v Ukrajini, kar je pokazalo bolj vojaško naravo uporabe IKT.

V primeru ruskega vmešavanja v ameriške volitve je bila uporaba IKT usmerjena v manipulacijo z javnim mnenjem in širjenje dezinformacij za podporo določenim političnim strujam v ZDA. Cilji so bili predvsem politični in informacijski, saj je Rusija želela vplivati na volilni proces in izid volitev ter širiti svoje politične narative. V primeru ruske invazije na Ukrajino pa je bila uporaba IKT bolj vojaško usmerjena. Kibernetski napadi so bili del vojaških operacij za dosego ciljev v vojnem konfliktu. To je vključevalo onemogočanje komunikacijskih omrežij, prisluškovanje na tajne komunikacije, krajo občutljivih informacij in podobno. Cilji so bili predvsem vojaški, saj je Rusija uporabljala IKT za pomoč pri dosegu vojaških operativnih ciljev.

Vmešavanje v ameriške volitve je povzročilo široko mednarodno obsodbo in uvedbo sankcij proti Rusiji s strani številnih držav. Vpliv operacije je bil globalen, saj je prizadel eno od vodilnih svetovnih sil. Odkritje uporabe IKT za manipulacijo volitev je privedlo do uvedbe mednarodnih sankcij proti Rusiji in krepitve kibernetske varnosti v mnogih državah. Nasprotno pa je bila reakcija na rusko invazijo na Ukrajino bolj usmerjena regionalno, z uvedbo sankcij proti Rusiji in podporo ukrajinski suverenosti. Kibernetski napadi in vohunjenje so povzročili napetosti med državami in resne posledice v odnosih med Rusijo in Ukrajino ter med Rusijo in drugimi državami.

Rusko vmešavanje v ameriške volitve leta 2016 je bilo večinoma usmerjeno v določeno obdobje pred volitvami in med volilnim procesom. Aktivnosti so bile bolj kratkotrajne in osredotočene na ključne dogodke volilnega cikla. Ruska invazija na Ukrajino in uporaba informacijskih operacij v tem kontekstu sta bili bolj dolgotrajni in trajali v več fazah. Kibernetski napadi, vohunjenje in manipulacija so potekali tako med pripravami na invazijo kot tudi med dejanskimi vojaškimi operacijami.

Ruska invazija na Ukrajino je bila vojaška operacija z oboroženimi konflikti in ozemeljsko spremembo (aneksija Krima), kar je imelo neposreden vpliv na življenje in stabilnost ljudi v regiji. Nasprotno pa je bilo vmešavanje v ameriške volitve bolj nevidno z usmerjanjem informacijskih kampanj in kibernetskih napadov. Kljub tem razlikam je pomembno razumeti, da obe situaciji odražata širšo uporabo informacijskih operacij kot orodje za

doseganje političnih ciljev, pa naj bo to destabilizacija družbe, vplivanje na politično dogajanje ali krepitev geostrateških interesov. Čeprav so razlike pomembne, so informacijske operacije postale vse bolj pomemben element sodobnih geopolitičnih in vojaških konfliktov.

Na drugi strani pa je bilo prisotnih kar nekaj podobnosti. Čeprav smo v prejšnjih odstavkih razlikovali uporabo IKT v obeh primerih, je tukaj ena velika podobnost. V obeh primerih je IKT omogočila hitro in široko širjenje sporočil in manipulacijo z javnim mnenjem, kar je vplivalo na dogodke in politično ozračje.

Te podobnosti se vidijo tudi v uporabi tehnologije »deep fake«, ki je igrala ključno vlogo tako pri ruskem vmešavanju v ameriške volitve kot tudi v ukrajinski vojni. V obeh primerih je bila uporaba tehnologije »deep fake« usmerjena v oblikovanje lažnih vsebin, ki bi vplivale na javno mnenje in politične procese. V primeru ruskega vmešavanja v ameriške volitve so ruski akterji ustvarili realistične videoposnetke in avdio posnetke, ki so prikazovali politične kandidate in druge vplivne osebe, kako izjavljajo neresnične izjave ali se vedejo neprimerno. Te lažne posnetke so nato širili prek družbenih medijev in spletnih platform, kar je ustvarilo zmedo med volivci in podkopalo zaupanje v politične procese v ZDA. V vojni v Ukrajini pa so vpleteni uporabili tehnologijo »deep fake« za ustvarjanje propagandnih vsebin, s katerimi so poskušali utemeljiti svoje stališče in pridobiti mednarodno podporo. Te vsebine so bile usmerjene tako na domače prebivalstvo kot tudi na mednarodno občinstvo, kar je prispevalo k naraščajoči napetosti med stranmi v konfliktu. V obeh primerih so posnetki »deep fake« ustvarili dvom o resničnosti dogodkov in otežili pridobivanje jasnega vpogleda v dogajanje na terenu. To poudarja pomen razvoja tehnologij za odkrivanje vsebin »deep fake«, okrepitev kritičnega razmišljanja in medijske pismenosti med prebivalci ter potrebo po regulaciji teh tehnologij na mednarodni ravni.

Cilj informacijskih operacij je bil poglobiti delitve v ameriški družbi, saj se je ruska vlada zavedala, da so razdeljene družbe bolj ranljive za vplivanje in dezinformacije. Spodbujanje političnih ekstremov in poudarjanje kontroverznih tem so prispevali k

razdeljenosti ameriške družbe in kreiranju politične nestabilnosti. Ruska vlada je s svojo propagandno kampanjo ciljala na oblikovanje negativnega dojemanja ukrajinske vlade in spodbujanje separatističnih nastrojenosti v vzhodnih regijah. S tem je Rusija poskušala oslabiti enotnost Ukrajine in ustvariti notranjo nestabilnost v državi. Obema operacijama je skupna strategija ciljanja na ranljivost in razdor v ciljnih državah, kar je pripomoglo k dosegi njihovih političnih ciljev.

V obeh primerih je bila izvedba informacijskih operacij dobro organizirana in koordinirana, saj je zahtevala sodelovanje različnih akterjev in entitet. Informacijske operacije so vključevale sodelovanje različnih akterjev, vključno z obveščevalnimi agencijami, medijskimi organizacijami in plačanimi provokatorji. Skupno delovanje med različnimi entitetami je zagotovilo dosledno širjenje sporočil na različnih platformah. Pri ruski invaziji pa je poleg tega mogoče še opaziti koordinacijo med vojaškimi operacijami na terenu in informacijskimi kampanjami, ki so podpirale ruski pogled na konflikt. Koordinacija med različnimi akterji je bila ključnega pomena za učinkovito izvajanje informacijskih operacij v obeh primerih.

Oba primera informacijskih operacij sta imela jasne politične cilje, ki so služili interesom Rusije. Cilj vmešavanja v proces volitev je bil podpreti politične kandidate in struje, ki so bili bolj naklonjeni ruski politiki, ter oslabiti položaj kandidatov, ki so zagovarjali protirusko politiko. Tako bi Rusija lahko bolj vplivala na politično dogajanje v ZDA in zaščitila svoje interese. Cilj invazije pa je bil doseči geostrateške interese v regiji, kot so pridobitev nadzora nad strateškimi ozemlji, ohranjanje vpliva v nekdanjih sovjetskih republikah in omejevanje približevanja Ukrajine evropskim in zahodnim organizacijam. Informacijske operacije so bile izvedene z jasnim namenom podpore političnim ciljem Rusije v obeh primerih.

Rusko vmešavanje v ameriške volitve leta 2016 in ruska invazija na Ukrajino sta odraz kompleksnih informacijskih operacij, ki jih je Rusija izvajala za dosego svojih političnih ciljev. Obe situaciji sta imeli podobnosti v uporabi informacijskih tehnologij, ciljanju razdora in destabilizacije, organizaciji in podpori političnim ciljem. Razumevanje teh

podobnosti je ključnega pomena za obravnavanje izzivov, ki jih prinašajo informacijske operacije v sodobnem svetu, in za razvoj učinkovitih mehanizmov za preprečevanje zlorabe informacijskih tehnologij v politične namene.

4 DISKUSIJA

Rusko vmešavanje v ameriške volitve in vojna v Ukrajini sta dva izrazita primera informacijskih operacij, ki sta se odvijala v različnih kontekstih, vendar imata nekaj skupnih točk, in sicer oba poudarjata kompleksnost in nevarnost informacijskih operacij v sodobnem svetu.

V obeh primerih je bila uporabljena dezinformacija kot ključno orodje. Rusko vmešavanje v ameriške volitve je vključevalo širjenje lažnih informacij in ustvarjanje zmede med ameriškimi volivci. Podobno je bila v vojni v Ukrajini uporabljena dezinformacija za opravičevanje ruskih dejanj in prikaz Ukrajincev v negativni luči.

Psihološka vojna je bila prisotna v obeh primerih. Rusija je poskušala v ameriškem primeru polarizirati družbo in poglobiti razkole, medtem ko je v vojni v Ukrajini uporabila psihološko manipulacijo za dehumanizacijo nasprotnika.

Kibernetska varnost je bila ogrožena v obeh primerih. Rusko vmešavanje v ameriške volitve je vključevalo kibernetske napade na politične organizacije, medtem ko so v vojni v Ukrajini kibernetski napadi vplivali na infrastrukturo.

Poleg tega sta obe situaciji poudarili pomen komunikacijskega vpliva. Rusija je izkoriščala družbena omrežja in medijsko pokrajino za širjenje svojega vpliva ter oblikovala sporočila, ki so ciljala na določene demografske skupine.

Oba primera nas opominjata, kako informacijske operacije postajajo vse bolj sofisticirane in kako lahko države in organizacije uporabljajo informacijsko manipulacijo za dosego svojih političnih ciljev. Hkrati pa obe situaciji poudarjata tudi pomen ozaveščenosti o dezinformacijah in kibernetski varnosti v današnjem digitalnem svetu.

Na začetku zaključnega dela smo si postavili tri teze, in sicer:

- Napadene države, organizacije ali posamezni akterji nimajo pripravljenega scenarija v primeru informacijskih operacij, usmerjenih proti njim.
- Reakcija »žrtev« na informacijske operacije je prepozna in povzročena škoda je nepopravljiva.
- Države v vlogi agresorja z uporabo informacijskih operacij prepričujejo lastno prebivalstvo v dobrobit svojih dejanj.

Prvo tezo smo z analizo in primerjavo primerov potrdili. Obe državi, ki sta bili žrtvi napada, nista imeli pripravljenega nobenega scenarija v primeru napada. Ameriške oblasti niso mogle niti odgovoriti na grožnjo, saj je bila zaznava nevarnosti prepozna. Medtem so ukrepi ukrajinskih oblasti proti informacijskim operacijam Ruske federacije, ki so bili improvizirani, prav tako pokazali nepripravljenost Ukrajine na nevarnost.

Druga teza ne drži v celoti. V obeh primerih lahko potrdimo prvi del hipoteze. Žrtvi informacijskih operacij sta na nevarnost reagirali po napadu in ni bilo nobenih varnostnih mehanizmov, ki bi zaznali morebitno nevarnost, če pa so bili, le-ti niso pravilno delovali. Medtem ko drugi del hipoteze o nepopravljivi škodi ne drži. Tukaj ni mišljena materialna škoda, temveč predvsem zaupanje prebivalstva v politični vrh države. Informacijske operacije lahko s svojim delovanjem uničijo zaupanje, ki pa ni nepopravljivo. Le s časom, trdim in transparentnim delom lahko izničijo učinke informacijskih operacij.

Tretjo tezo prav tako potrdimo. Rusija je povsem skrila realno situacijo pred svojim prebivalstvom. S pošiljanjem dezinformacij in lažnih novic ter medijsko propagando so prebivalcem onemogočili dostop do resničnih dejstev. Zaradi vsebine člankov, ki povezuje Ukrajince in nacizem, ter lažnih novic o genocidu, ki naj bi ga Ukrajinci izvršili sami nad sabo v mestu Bucha, in genocidu ruske populacije v regijah Donbas in Luhansk, so dehumanizirali Ukrajince in s tem opravičili svoja dejanja ter tako prepričali svoje Ruse, da so oni tisti, ki delajo dobro.

Teze so pokazale, da informacijske operacije postajajo čedalje večja nevarnost, ki preti državam in njihovim prebivalcem. Nevarnost preti s strani drugih držav kakor tudi s strani lastne države, kot je to potrdila tretja teza. Države pa ne glede na ustanovitev mnogih centrov, ki naj bi se borili proti informacijskim operacijam, niso najbolj pripravljene, saj je dobro pripravljene informacijske operacije težko zaznati. Da niso najbolje pripravljeni, se vidi tudi v reakcijah napadenih držav. Reakcije so pozne in narejena škoda je že kar velika.

Z diplomskim delom nismo hoteli samo potrditi ali ovreči navedenih tez. Želeli smo raziskati tematiko, ki je v današnjem svetu vse bolj prisotna, na žalost pa malokrat opažena. Z raziskavo smo pridobili razumevanje o nevarnosti informacijskih operacij. Čeprav so orodje iz preteklosti, so sedaj z napredkom IKT postale glavno orožje vsake države. S svojim delovanjem predstavljajo grožnjo nacionalni in tudi mednarodni varnosti, načinu poslovanja in sposobnosti medsebojnega komuniciranja. S svojimi orodji, kot so dezinformacije, propaganda, psihološke operacije, in kibernetskimi operacijami je njihov glavni namen spremeniti oziroma vplivati na mnenje in vedenje ciljne publike, tako da bo rezultat po godu akterja. Zaradi svoje kompleksnosti so zelo težko izsledljive, zato so kot nalašč za skrivne vojaške in obveščevalne akcije. Zaradi svoje uporabnosti pa niso več uporabljene samo v te namene. Informacijske operacije lahko prepoznamo tudi v marketingu in politiki, saj so vsestransko orodje.

Če si na podlagi primerov postavimo enostavno vprašanje, kaj sploh so informacijske operacije, bi po prebranem hitro zaključili, da so informacijske operacije orožje, ki za dosego svojih ciljev uporablja dezinformacije in propagando. Na podlagi napisanega in opisanega smo mnenja, da so informacijske operacije zahrbtnega značaja, so posredno orožje, ki za dosego svojih ciljev potrebuje veliko potrpežljivosti. Mnogokrat so v tako imenovani sivi coni in jih posameznik niti ne prepozna. Lahko so v obliki marketinške kampanje, filmov, glasbe ali pa v drugačni obliki, ki je zmožna deliti sporočilo.

Menimo, da so informacijske operacije orožje, ki je bolj učinkovito v demokratičnih državah kakor pa v državah s totalitarnim režimom vladanja. V demokratičnih državah

ima vsak pravico do govora, do izražanja svojega mnenja in mediji imajo svobodo glede poročanja. Če pogledamo z vidika akterja, ki je sprožil informacijske operacije, ima v demokratičnih državah zaradi odprtosti sistema veliko več možnosti za implementiranje informacijskih operacij. Kot smo videli na primeru ameriških volitev leta 2016, so za ta namen izkoristili družbena omrežja. Prav tako bi lahko v ta namen izkoristili medijske in časopisne hiše, kjer je možnost podkupiti uslužbence. K temu je pripomogla še vsa novonastala IKT. Edina ovira pri informacijskih operacijah je kreativnost akterja, ki jih implementira v sistem demokratične države. Medtem pa je implementirati informacijske operacije v totalitarno državo praktično nemogoče. Če pogledamo Rusko federacijo, opazimo, da Kremelj že sam izvaja informacijske operacije nad svojim lastnim prebivalstvom, zato bi bilo ostati anonimen neizvedljivo. Prav tako sta internet in televizija omejena oziroma zaprta do zunanjega sveta. Tako prebivalci lahko prebirajo in gledajo samo dogodke, ki so po volji voditeljev, oziroma je realno stanje predstavljeno tako, da je večina stvari vzeta iz konteksta in tako predstavi nekatere dogodke, posameznike ali pa organizacije v slabi luči. Zato je povsem razumljivo, da so tudi prebivalci nagnjeni k mnenju, ki jim je bilo dobesedno vsajeno s strani države.

Čeprav smo podvrženi vse večji nevarnosti informacijskih operacij, menimo, da njihova efektivnost ni večja kakor v državah s totalitarnim režimom. Zaradi vse večjega ozaveščanja s strani državnih organov, pa tudi evropskih, se prebivalci vse bolje zavedamo nevarnosti lažnih novic in propagande, prav tako pa jih lažje prepoznamo. Tudi družbena omrežja so stopila skupaj in začela bolje spremljati vse novice, ki so objavljene na njihovih portalih. Če se spomnimo, v času koronavirusa so kakršne koli novice v zvezi s cepljenjem označili kot mogočo dezinformacijo in da smo ob branju le-teh bolj previdni. Tako je bilo tudi v času pred parlamentarnimi volitvami meseca aprila, ki so bile ene najbolj pričakovanih volitev pri nas, kar potrjuje tudi visoka volilna udeležba. V obdobju pred volitvami so potekala soočenja, ki so bila ena najbolj »umazanih«, obtožbe in žaljivke so letele na vse strani. Kandidati, ki so se borili za mesto predsednika vlade, so kakršno koli umazano skrivnost ali pa slabo dejanje nasprotnika izkoristili za rušenje njegovega imidža, čeprav je bilo veliko stvari izvzetih iz konteksta in ni podajalo celotne slike in razlage. V ta namen je bila na portalu 24ur.com ekipa, ki je

preverjala vsa navedena dejstva, ki so jih izustili kandidati, in podobno kakor na družbenih omrežjih so nekatere trditve označili za pravilne, lažne ali pa, da so izvzete iz konteksta. Tako so kampanje postale bolj transparentne in verodostojne, saj si kandidati niso mogli privoščiti kakršnih koli laži ali drugačnega zavajanja prebivalstva, ker bi to povzročilo več škode njihovemu ugledu in končnemu cilju kakor pa nasprotnikovemu.

Preverjanje dejstev je v bistvu tudi najboljši način za boj proti lažnim informacijam. Kar pa zahteva veliko človeške moči za preverjanje, saj umetna inteligenca, čeprav je zelo napredovala in lahko zazna lažne novice, še vedno nima razvitega kritičnega razmišljanja, ki bi pri taki nalogi zelo prav prišlo. Zato še vedno veliko lažnih novic in propagande zaide na internet, še posebej na družbena omrežja, ki so postala leglo informacijskih operacij. Zato je veliko breme na posamezniku, ki se mora naučiti, kako prepoznati znake informacijskih operacij. Evropska unija je za ta namen vzpostavila spletno stran EUvsdisinfo.eu, kjer predstavi znake lažnih novic, prav tako pa ponujajo različne kvize, kjer lahko uporabnik testira svoje znanje. Najbolj pomembna stvar pa so članki o dogodkih, ki so v celoti analizirani in predstavljeni bralcem v objektivni luči.

Informacijske operacije pa niso prisotne samo na političnem in vojaškem parketu. Vse več jih opazimo tudi v zabavni industriji, kot so filmi, pa tudi v marketingu. To je bil tudi eden od protiukrepov ukrajinske vlade proti informacijskim operacijam s strani Rusije. Profesor Bernik (2014) pojasni, da je bil to tudi eden izmed ukrepov ameriške oblasti, ki je v letih med 2000 in 2010 s filmskimi produkcijami podpisala pogodbo o snemanju filmov na tematiko vojne v Afganistanu. Njihov namen je bil izrecno, da vpliva na mnenje ljudi in s tem pridobijo odobravanje obsežne vojaške akcije. Mogoče so nam bližje filmi, ki so bili posneti v neposredni bližini, in sicer film Quo Vadis, Aida?, ki prikazuje genocid v Bosni in Hercegovini. Malo zatem je izšel tudi film iz Srbije, naslovljen Dara iz Jasenovca, ki prikazuje življenje deklice v koncentracijskem kampu. Oba filma sta požela veliko zanimanja, pa tudi kritike, da je veliko informacij lažnih in vzetih iz kontekstov z namenom manipuliranja javnega mnenja. Seveda je treba ohranjati zgodovino in si zapomniti tudi slaba dejanja, ki smo jih storili, vendar manipuliranje zgodovinskih dejstev prinaša samo še več sovraštva in razkola v družbi.

V marketingu so informacijske operacije eno najpomembnejših orodij, ki jih imajo tržniki v svojem arzenalu. Pomaga jim prepoznati, kaj si njihova ciljna publika želi, kako to želi in kdaj to želi. Prav tako jim pomaga doseči tiste ljudi s ciljno usmerjenimi sporočili, ki so ustrezna in pravočasna. Podjetja uspešno uporabljajo informacijske operacije tako, da izkoriščajo svojo široko mrežo stikov po vsem svetu. Uspelo jim je izslediti ljudi, ki bi jih zanimala njihova ponudba, in jih nato usmeriti s posebnimi sporočili, ki bodo pritegnila prav njih. To podjetju omogoča, da doseže čim več potencialnih strank, hkrati pa na splošno porabi manj denarja za marketinška prizadevanja, ker ne plača za vsako posamezno sporočilo, ki doseže ciljno občinstvo.

Zanimivo je predvidevati, kam bo IKT popeljala informacijske operacije v prihodnosti. Že zdaj imamo umetno inteligenco, imenovano »deep fake«. V prevodu bi bil globok ponaredek, kar je malo smešno, mogoče bi bil boljši izraz sofisticirani ponaredek. Gre pa za lažne videe, ki lahko predstavljajo pomembne osebe, kot so predsedniki ali visoki funkcionarji ali slavne osebe. Umetna inteligenca je tako dobra, da ponaredi celo govorico telesa osebe, ki jo predstavlja, kakor tudi glas. Pred videi so obstajali samo glasovni posnetki, sedaj pa so se razvili v prave videoposnetke, ki jih težko razlikujemo od originala. Samo zamislimo si lahko, kakšne posledice bi imeli te vrste posnetki, če bi recimo ponaredili morebitni vojaški ukaz za napad in tako sprožili vojno. Zato morajo biti implementirani ukrepi, kot je dvofaktorska avtentikacija, s katero bi se izognili takim primerom, vendar pa še vedno ne bi ponujali celovite zaščite.

Informacijske operacije bodo zagotovo stremele k neki stopnji avtomatizacije, če ne celo popolni avtomatizaciji. Tako bodo recimo informacijske operacije na družbenem omrežju bile v bistvu kompleksen program, ki je popolnoma samostojen in ni potrebe, da ga upravlja oseba. Medtem pa bodo razni kibernetski napadi še vedno plod človeške domišljije in človekove vztrajnosti, da najde napake v sistemu in jih izkoristi. Prav tako pa navadne operacije, ki bi potrebovale fizično prisotnost človeka, ne bodo kar izumrle. Tukaj so mišljeni razni agenti v obveščevalnih službah, ki pridobivajo informacije na ta način. Zagotovo pa jim bo delo še bolj olajšano z napredkom IKT.

Prihodnost informacijskih operacij je nejasna, vendar lahko pričakujemo več stvari, in sicer da jih bodo še naprej uporabljale vlade in druge organizacije ter posamezniki. Postale bodo bolj sofisticirane, še naprej se bodo uporabljale v javni sferi – tako v dobro kot v slabo. Informacijske operacije so bile uporabljene za dobre namene, kot je razkrivanje korupcije ali nesposobnosti, in za slabe, kot je širjenje propagande na platformah družbenih medijev. Ne bo manjkalo tarč, ko gre za tiste, ki želijo manipulirati z ljudmi z informacijskimi operacijami. Ljudje so vedno lačni informacij o svojih voditeljih in institucijah, zaradi česar so lahek plen za vse, ki želijo to znanje uporabiti proti njim.

5 ZAKLJUČEK

V zaključnem delu smo se dotaknili tematike informacijskih operacij in kako je uporaba informacijsko-komunikacijskih tehnologij pripomogla k razvoju informacijskih operacij. Dela smo se lotili z analizo dveh primerov. Rusko vmešavanje v ameriške volitve leta 2016 in vojna v Ukrajini sta služila kot ključna študija primera za razumevanje informacijskih operacij v sodobnem svetu. Skozi to raziskavo smo razkrili številne vidike, ki jih je treba upoštevati v tej naraščajoči obliki vplivanja na družbo, politiko in mednarodne odnose.

Obe študiji primera sta nam pokazali, kako so informacijske operacije postale nepogrešljiv instrument zunanjepolitičnih strategij držav. S pomočjo manipulacije z informacijami, kibernetskimi napadi in propagando so države lahko dosegle svoje cilje, ne da bi se morale zatekati k tradicionalnim vojaškim sredstvom. To je jasno pokazalo, kako se je narava konfliktov v digitalni dobi premaknila na splet in v virtualni prostor.

Obe študiji primera sta izpostavili resne posledice, ki jih imajo informacijske operacije za družbo in politiko. Rusko vmešavanje v ameriške volitve je razkrilo, kako lahko informacijske operacije vplivajo na politično polarizacijo, zmanjšanje zaupanja v informacijsko okolje in demokratične procese. Ta zmeda in dezinformacije še vedno vplivajo na našo družbo, kar poudarja dolgoročno naravo teh groženj.

Obe študiji primera sta nas spodbudili k razmišljanju o etičnih in pravnih vprašanjih, povezanih z informacijskimi operacijami. Potrebujemo ravnovesje med svobodo izražanja in zaščito pred manipulacijo. Regulacija in normiranje informacijskih operacij na mednarodni ravni postajata neizogibna, vendar se moramo hkrati zavedati, da se tehnologije hitro razvijajo in izzivajo obstoječe norme.

Na podlagi teh dveh primerov pozivamo k nadaljnjim raziskavam, ki bi vključevale proučevanje uporabe umetne inteligence, kot je tehnologija »deep fake«, v informacijske operacije. Analiza regionalnih primerov, ki vključujejo različne države in

konflikte, lahko razkrije raznolikost teh groženj in pristopov k njihovi obravnavi. Poleg tega moramo nenehno razvijati boljše strategije za kibernetsko varnost, ki lahko zaščitijo naše digitalne infrastrukture pred napadi.

Naše zaključno delo nas je opomnilo na nevarnosti in priložnosti, ki jih prinašajo informacijske operacije v današnjem svetu. Ozaveščenost, izobraževanje in sodelovanje vseh deležnikov so ključni za ohranjanje demokracije, varnosti in integritete informacijskega okolja. Vsak posameznik, politik, novinar in raziskovalec ima vlogo pri razkrivanju manipulacij in spodbujanju transparentnosti.

Kot zaključek tega zaključnega dela se zavezujemo, da bomo nenehno proučevali, raziskovali in ukrepali na tem področju, da bomo lahko varovali naše družbe pred meglo informacijskih operacij in ohranjali integriteto naše digitalne dobe. Pridobljeno znanje nas usmerja k boljšemu razumevanju, preprečevanju in obvladovanju informacijskih operacij ter k učinkovitemu varovanju naših demokracij in digitalnih prostorov.

VIRI IN LITERATURA

Adamsky, D. (2015). *Cross-domain coercion: The current Russian art of strategy.* IFRI Security Studies Center. https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

Bernik, I. (2014). *Cybercrime and cyber warfare.* John Wiley & Sons

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem.* Fakulteta za varnostne vede.

Cohen, D. in Bar'el, O. (2017). *The use of cyberwarfare in influence operations.* Tel-Aviv University. https://en-cyber.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf

Council of the European Union. (20. 12. 2016). *Implementation of the counter-terrorism agenda set by the European Council.* https://data.consilium.europa.eu/doc/document/ST-14260-2016-ADD-1-EXT-1/en/pdf

Council on Foreign Relations. (17. 10. 2023). *War in Ukraine*. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

Department of defense. (2003). *Information operations roadmap.* https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Information_Operations_Roadmap_30_October_2003.pdf

Department of Homeland Security. (29. 12. 2016). *Russian Malicious cyber activity.* https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Desouza, K. C., Ahmad, A., Naseer, H. in Sharma, M. (2020). Weaponizing information systems for political disruption: The actor, lever, effects, and response taxonomy (ALERT). *Computers and Security*, *88*, 101606. https://doi.org/10.1016/j.cose.2019.101606

European External Action Service. (24. 1. 2022). *Disinformation about the current Russia-Ukraine conflict – seven myths debunked.* https://euvsdisinfo.eu/

disinformation-about-the-current-russia-ukraine-conflict-seven-myths-debunked/

European External Action Service. (n. d.). *About.* https://euvsdisinfo.eu/about/

European Parliament. (12. 5. 2016). *Answer given by Mr Avramopoulos on behalf of the Commission.* https://www.europarl.europa.eu/doceo/document/E-8-2016-000505-ASW_EN.html?redirect

Freedom House. (n. d.). *Democracy status.* https://freedomhouse.org/explore-the-map?type=nit&year=2023

Gambino, L. in Pankhania, M. (8. 11. 2016). How we got here: a complete timeline of 2016's historic US election. *The Guardian.* https://www.theguardian.com/us-news/2016/nov/07/us-election-2016-complete-timeline-clinton-trump-president

Gioe, D. V. (2018). Cyber operations and useful fools: The approach of Russian hybrid intelligence. *Intelligence and National Security*, *33*(7), 954–973. https://doi.org/10.1080/02684527.2018.1479345

Greenberg, A. (29. 12. 2016). *Obama's Russian hacking retaliation is biggest »Since the Cold war«.* Wired. https://www.wired.com/2016/12/obama-russia-hacking-sanctions-diplomats/

Joint Chiefs of Staff. (27. 11. 2012). *Information operations.* https://irp.fas.org/doddir/dod/jp3_13.pdf

Ladygina, Y. V. (2022). Cyborgs vs. Vatniks: Hybridity, weaponized information, and mediatized reality in recent Ukrainian war films. E*ast/West: Journal of Ukrainian Studies, 9*(1), 105–138. https://doi.org/10.21226/ewjus588

Lapienytė, J. (15. 11. 2023). *Ukranian radio stations hacked to spread lies about Zelensky's health.* Cybernews.com. https://cybernews.com/cyber-war/ukrainian-radio-stations-hacked-to-spread-lies-about-zelenskys-health/

Larson, S. (10. 11. 2016). *Mark Zuckerberg: The idea that fake news influenced the election is »crazy«.* Cnn.com. https://money.cnn.com/2016/11/10/technology/facebook-mark-zuckerberg-fake-news/

Lee, N. (2014). *Facebook nation: Total information awareness.* Springer.

Lin, H. in Kerr, J. (2019). On cyber-enabled information warfare and information operations forthcoming. V P. Cornish (ur.), *Oxford handbook of cybersecurity* (str. 251). Oxford University Press. https://ssrn.com/abstract=3015680

Mayer, J. (24. 9. 2018). How Russia helped swing the election for Trump. *The New Yorker.* https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump

Office of the Director of National Inteligence. (6. 1. 2017). *Background to "Assessing Russian activities and intentions in recent US elections": The analytic process and cyber incident attribution.* https://www.dni.gov/files/documents/ICA_2017_01.pdf

Parrish K. (6. 7. 2016). *Centcom counter ISIL propaganda.* DOD news. https://www.defense.gov/News/News-Stories/Article/Article/827761/centcom-counters-isil-propaganda/

Petkauskas, V. (15. 11. 2023). *Ukraine dismantled million-strong disinformation bot farm.* Cybernews.com. https://cybernews.com/cyber-war/ukraine-dismantled-million-strong-disinformation-bot-farm/

Sengupta, K. (31. 1. 2015). *New British army unit Brigade 77 to use Facebook and Twitter in psychological warfare.* Independent.com. https://www.independent.co.uk/news/uk/home-news/return-of-the-chindits-mod-reveals-cunning-defence-plan-10014608.html

Smart, C. (2. 7. 2022). How the Russian media spread false claims about Ukrainian nazis. *The New York Times.* https://www.nytimes.com/interactive/2022/07/02/world/europe/ukraine-nazis-russia-media.html

The European Centre of Excellence for Countering Hybrid Threats. (n. d.). *About us.* https://www.hybridcoe.fi/about-us

The NATO Strategic Communications Centre of Excellence.(n. d.). *About NATO StratCom COE.* https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5

Treyger, E., Cheravitch, J. in Cohen, R. S. (2022). *Russian disinformation efforts on social media.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR4373z2.html

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE ZAKLJUČNEGA DELA

ZD-2

Univerza v Mariboru

Fakulteta za varnostne vede

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE ZAKLJUČNEGA DELA

Ime in priimek študent-a/-ke: Teo Nuhanovič

Študijski program:

Informacijska varnost

Naslov zaključnega dela:

Uporaba informacijsko-komunikacijskih tehnologij za informacijske operacije

Mentor: prof. dr. Igor Bernik

Somentor: _____

Podpisan-i/-a študent/-ka Teo Nuhanovič

- izjavljam, da je zaključno delo rezultat mojega samostojnega dela, ki sem ga izdelal/-a ob pomoči mentor-ja/-ice oz. somentor-ja/-ice;
- izjavljam, da sem pridobil/-a vsa potrebna soglasja za uporabo podatkov in avtorskih del v zaključnem delu in jih v zaključnem delu jasno in ustrezno označil/-a;
- na Univerzo v Mariboru neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve avtorskega dela v elektronski obliki, pravico reproduciranja ter pravico ponuditi zaključno delo javnosti na svetovnem spletu preko DKUM; sem seznanjen/-a, da bodo dela deponirana/objavljena v DKUM dostopna široki javnosti pod pogoji licence Creative Commons BY-NC-ND, kar vključuje tudi avtomatizirano indeksiranje preko spleta in obdelavo besedil za potrebe tekstovnega in podatkovnega rudarjenja in ekstrakcije znanja iz vsebin; uporabnikom se dovoli reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo;
- dovoljujem objavo svojih osebnih podatkov, ki so navedeni v zaključnem delu in tej izjavi, skupaj z objavo zaključnega dela;
- izjavljam, da je tiskana oblika zaključnega dela istovetna elektronski obliki zaključnega dela, ki sem jo oddal/-a za objavo v DKUM.

Uveljavljam permisivnejšo obliko licence Creative Commons: CC BY-NC SA 4.0 (navedite obliko)

Kraj in datum: Grosuplje, 15.12.2023

Podpis študent-a/-ke: