Društvene mreže kao alati utjecaja u hibridnim sukobima

Mlinac, Nikola

Doctoral thesis / Disertacija

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

https://doi.org/10.17234/diss.2022.8745

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:988657

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-11-04**

Sveučilište u Zagrebu
Filozofski fakultet
University of Zagreb
Faculty of Humanities
and Social Sciences

Repository / Repozitorij:

ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Sveučilište u Zagrebu

Filozofski fakultet

Nikola Mlinac

DRUŠTVENE MREŽE KAO ALATI UTJECAJA U HIBRIDNIM SUKOBIMA

DOKTORSKI RAD

Zagreb, 2022.

Sveučilište u Zagrebu

Filozofski fakultet

Nikola Mlinac

DRUŠTVENE MREŽE KAO ALATI UTJECAJA U HIBRIDNIM SUKOBIMA

DOKTORSKI RAD

Mentor:
prof. dr. sc. Jadranka Lasić Lazić

Zagreb, 2022.

University of Zagreb

FACULTY OF HUMANITIES AND SOCIAL SCINCES

Nikola Mlinac

SOCIAL NETWORKS AS MEANS OF INFLUENCE IN HYBRID CONFLICTS

DOCTORAL THESIS

Supervisor:
Prof. dr. sc. Jadranka Lasić Lazić

Zagreb, 2022.

ŽIVOTOPIS MENTORA

Prof emerita Jadranka Lasić Lazić (Požega, 1949.) pohađala je i završila gimnaziju u Požegi. Na Filozofskome fakultetu Sveučilišta u Zagrebu diplomirala je filozofiju i jugoslavenske jezike i književnosti 1975. godine. Magisterij znanosti stječe nakon završenog Poslijediplomskog studija informacijskih znanosti Sveučilišta u Zagrebu magistriravši na temi „Pedagoško-animatorski rad s djecom u dječjim odjelima narodnih knjižnica“. Doktorat znanosti stječe iz područja informacijskih znanosti 1991. godine na Sveučilištu u Sarajevu obranom doktorske disertacije „Razvoj bibliotečno informacijskih sustava“. U Zavodu za informacijske znanosti obnašala je dužnost urednice, uredivši tri zbornika i dvije knjige. Autorica je ili koautorica četiriju knjiga, te preko 120 znanstvenih i stručnih članaka u domaćim i stranim časopisima. Dr. Jadranka Lasić Lazić dobitnica je (2008.) godišnje nagrade Filozofskog fakulteta za rezultate postignute u teorijskom i praktičnom radu u razvoju i afirmaciji informacijskih znanosti i za izniman doprinos u promicanju e-učenja i načina usvajanja znanja i vještina koje nudi informacijska znanost.

DRUŠTVENE MREŽE
KAO ALATI UTJECAJA U HIBRIDNIM SUKOBIMA

Sažetak

Rezultat istraživanja prikazan je u šest glavnih dijelova: „Informacijski prostor i novi obrasci organiziranja podataka i informacija“, „Informacijske strategije, društvene mreže i operacije utjecaja u kiber prostoru“, „ Hibridni sukobi i novi instrumenti moći u kiber prostoru“, „Novi instrumenti moći: hibridne prijetnje i hibridne operacije“, „Hibridne operacije u hibridnim sukobima i hibridnom ratovanju“ te „Novi obrasci prevencije i obrane od hibridnih prijetnji“.

U prvom dijelu društvene mreže promatraju se kao snažni i učinkoviti komunikacijski i medijski alati za globalnu, masovnu, umreženu, neposrednu i anonimnu komunikaciju, koji se u kiber prostoru koriste i za učinkovito nametanje ideja, ideologija te za stvaranje i širenje dezinformacija.

U drugom dijelu opisana je izvršena prilagodba informacijskih strategija i informacijskih operacija te su opisani novi obrasci planiranja, provođenja i djelovanja psiholoških i medijskih operacija u kojima različiti akteri (državni, nedržavni i korporativni) tehnologije umjetne inteligencije na društvenim mrežama zloupotrebljavaju za vlastite potrebe i interese.

U trećem dijelu disertacije prikazani su uzroci i nastanak hibridnih sukoba, definicije i glavna obilježja.

Potom su prikazane hibridne prijetnje i hibridne operacije utjecaja kao novi instrumenti moći u kiber prostoru koji su nastali kao posljedica zloupotrebe kiber prostora i tehnologija umjetne inteligencije na društvenim mrežama. Društvene mreže u ovom dijelu istraživanja promatraju se kao alati kojima se planiraju i provode hibridne operacije utjecaja koje se pak promatraju kao glavni informacijski instrument hibridne moći koji najsnažnije učinke ostvaruje kroz kiber prostor i služi za stvaranje snažnih i učinkovitih dezinformacija te ostalih vrsta hibridnih prijetnji.

U petom dijelu disertacije prikazani su rezultati istraživanja povezani s reprezentativnim uzorkom poznatih i priznatih primjera zloupotreba tehnologija umjetne inteligencije na društvenim mrežama za planiranje i izvođenje hibridnih operacija utjecaja. Primarno se istražuju hibridne operacije utjecaja koje su izvodile Sjedinjene Američke Države i Ruska Federacija na različitim geografskim područjima i u različitim kontekstima.

U šestom dijelu disertacije predloženi su novi obrasci prevencije i obrane od hibridnih prijetnji i operacija, izrada nove informacijske strategije te su predloženi mehanizmi i modeli obrane. Na kraju ovog dijela ukazano je na važnost i ulogu izgradnje digitalne i podatkovne suverenosti.

Istraživanjem je potvrđena glavna hipoteza. Tehnologije umjetne inteligencije i društvene mreže u hibridnim sukobima koriste se kao snažni i učinkoviti taktički alati s potencijalnim strateškim posljedicama nad korpusom javnog znanja ciljanih publika u svrhu njegovog (pre)oblikovanja prema potrebama informacijskog napadača.

Prikazano je da se radi o psihološkim operacijama strateškog karaktera u kojima se tehnologije umjetne inteligencije i sve društvene mreže, u prostorno i vremenski neograničenom opsegu, koriste kao dominantni i učinkoviti taktički alati, za stvaranje dezinformacija, različitih vrsta hibridnih prijetnji te konstantnih (24/7) informacijsko-psiholoških pritisaka usmjerenih prema ciljanim publikama (pojedinačno, grupno ili masovno), ovisno o potrebama i ciljevima informacijskog napadača.

Ključne riječi: kiber prostor, algoritmi, umjetna inteligencija, društvene mreže, informacijske strategije, psihološke operacije, hibidni sukobi, hibridne operacije utjecaja, hibridna inteligencija, dezinformacije, dezinformacijske kampanje, hibridna obrana.

SOCIAL NETWORKS AS MEANS OF INFLUENCE IN HYBRID CONFLICTS

Summary

The results of the research are presented in six main parts, as follows: “Information space and new patterns of data and information organization”, “Information strategies, social networks and influence in cyberspace”, “Hybrid conflicts and new instruments of power in cyberspace”, “New instruments of power: hybrid threats and hybrid operations”, “Hybrid operations in hybrid conflicts and hybrid warfare” and “New patterns of prevention and defence against hybrid threats”.

In the first part, social networks are considered as powerful and effective means of communication and media for global, mass, networked, direct and anonymous communication, which are used in cyberspace to effectively impose ideas, ideologies and create and spread disinformation.

The second part describes the adjustment of information strategies and information operations, and describes new patterns of planning, implementation and operation of psychological and media operations in which various actors (state, non-state and corporate) use artificial intelligence technologies on social networks for their own needs and interests.

The third part of the dissertation presents the causes and occurrence of hybrid conflicts, their definitions and main features. Then, hybrid threats and hybrid operations of influence are presented, as new instruments of power in cyberspace that have emerged as a result of cyberspace misuse and artificial intelligence technologies on social networks.

In this part of the research, we observe social networks as means of planning and conducting hybrid influence operations, which we consider here as the main information instrument of hybrid power, that achieves the strongest effects through cyberspace and serves to create strong and effective disinformation and other types of hybrid threats.

The fifth part of the dissertation presents the results of research related to a representative sample of known and recognized examples of misuse of artificial intelligence technologies on social networks for planning and conducting hybrid impact operations. The primary scope of research relates to the hybrid influence operations carried out by

the United States and the Russian Federation in different geographical areas and in different contexts.

The sixth part of the dissertation proposes new patterns of prevention and defence against hybrid threats and operations, the creation of a new information strategy, and defence mechanisms and models. The end of this section points out the importance and the role of building digital and data sovereignty.

The research confirmed the main hypothesis. Artificial intelligence and social networking technologies in hybrid conflicts are used as powerful and efficient tactical tools, with potential strategic consequences for the body of public knowledge of target audiences, in order to (re)shape it according to the needs of the information *attacker*.

We have demonstrated that these are psychological operations of a strategic nature, in which artificial intelligence technologies and all social networks are used as dominant and effective tactical means, in a spatially and temporally unlimited range, to create disinformation and other various types of hybrid threats and constant (24/7) information-psychological pressures directed at target audiences (individually, in groups or *en masse*) depending on the needs and goals of the information *attacker*.

Keywords: cyberspace, algorithms, artificial intelligence, social networks, information strategies, psychological operations, hybrid conflicts, hybrid impact operations, hybrid intelligence, disinformation, disinformation campaigns, hybrid defence.

Sadržaj:

1. UVOD

1.1. Predmet istraživanja

Informacijsko-komunikacijski sustavi, računalne tehnologije i primjena umjetne inteligencije na društvenim mrežama otvorili su novi prostor i nove mogućnosti za ostvarivanje programa globalnih informacijskih dominacija. Novonastali kiber prostor bezgraničan je i legislativnim pravilima nedovoljno reguliran prostor. U nereguliranom kiber prostoru nastali su novi alati utjecaja poznati kao društvene mreže na kojima je (kao novom medijskom i komunikacijskom kanalu) omogućena zloupotreba tehnologija umjetne inteligencije a legislativnim, etičkim i moralnim pravilima nisu dovoljno regulirane norme ponašanja. Pojavom kiber prostora i društvenih mreža došlo je do dramatičnog obrata u ljudskoj komunikaciji. Nastali su novi uvjeti i nova pravila kojima su preko kiber prostora pomoću društvenih mreža različitim akterima omogućeni novi načini rješavanja međunarodnih sukoba, stvaranja informacijske nadmoći i preoblikovanja korpusa javnog znanja ciljanih publika. Ciljane publike mogu biti države, društvo, organizacije, zajednice, grupe i pojedinci. Kiber prostor nastao na osnovi umrežavanja informacijsko-komunikacijskih sustava, računalnih mreža i tehnologija umjetne inteligencije postao je primarni prostor u kojem se pomoću društvenih mreža međunarodni akteri bore za nametanje vlastitih ideja i ideologija. Široka dostupnost i sveprisutnost društvenih mreža transformirala je načine pristupanja, dijeljenja i prezentiranja obavijesti bez obzira na njihovu točnost i objektivnost. Komunikacija je prestala biti ograničena prostorom a podaci, obavijesti i informacije (bez obzira na točnost i objektivnost) distribuiraju se ciljanim publikama u realnom vremenu i u neograničenom dosegu. Nastala je nova digitalna stvarnost u kojoj društvene mreže kao digitalni i automatizirani posrednici u komunikaciji i distribuciji znanja, ograničavaju, filtriraju i usmjeravaju pozornost korisnika samo na određeni skup podataka, obavijesti i informacija koje ne moraju biti točne i pouzdane. Posljedično je došlo do urušavanja stvarnosti i do urušavanja objektivnog znanja. Društvene mreže su komercijalizirale tehnologije umjetne inteligencije, a u kiber prostoru nastali su novi oblici prikazivanja stvarnosti. Problem je što su društvene mreže, preko kiber prostora, u korpusu javnog znanja pojednostavile masovno stvaranje i širenje dezinformacija koje, ukoliko je to nekome u interesu, mogu biti prilagođene uvjerenjima, načelima i vrijednostima korisnika koji na temelju takvih dezinformacija organiziraju život, donose odluke i određuju vlastita ponašanja. Na ovaj način društvene mreže preko kiber prostora imaju snažan negativan učinak i na oblikovanje korpusa javnog znanja. Budući da se javno znanje sa stajališta novih tehnologija definira kao „znanje

koje je dostupno svakome“, javno znanje koje je oblikovano u kiber prostoru proizvod je i informacijskog rata.[1]

Na području informacijskog ratovanja razvojem informacijsko-komunikacijskih sustava, računalnih tehnologija i umjetne inteligencije nastala je nova bojišnica za dominaciju informacija, ideja i ideologija. Razvoj kiber prostora na osnovi ovakvih sustava i tehnologija odredio je nastanak društvenih mreža koje unutar kiber prostora omogućavaju globalno, masovno i umreženo povezivanje, komuniciranje i razmjenu ideja. Tehnologije umjetne inteligencije na društvenim mrežama upravljaju komunikacijskim procesima i razmjenom podataka, informacija i ideja. Međutim, pri tome se vlasnici ovih tehnologija i društvenih mreža ne vode kriterijima istine i objektivnosti niti kriterijima temeljem kojih možemo prosuditi istinitost i valjanost tvrdnji, odnosno informacija, već se vode kriterijima koji uopće ne moraju odgovarati stvarnom i činjeničnom stanju. Tehnologije umjetne inteligencije na društvenim mrežama postale su *nadzornici i upravitelji komunikacija* i razmjene ideja. Pri komunikaciji i razmjeni ideja vlasnici društvenih mreža određuju kriterije kojima se oblikuje i osigurava dominacija samo određenih informacija prema ciljanim publikama, sukladno njihovim sklonostima i interesima.

Pojavom društvenih mreža uvelike su se obistinila predviđanja vojnih stratega s početka 1990-ih. U nastanku kiber prostora vojni stratezi vidjeli su novi borbeni prostor, a u informacijsko-komunikacijskim i računalnim tehnologijama umjetne inteligencije vidjeli su nove alate za učinkovitije upravljanje informacijama u cilju (pre)oblikovanja ljudskog razmišljanja i donošenja odluka u korist vlastitih ideja i ideologija. Društvene mreže jesu povezale ljude, obitelji, prijatelje i omogućile su razmjenu ideja. Međutim, na štetu temeljnih ljudskih i društvenih normi transparentnosti i zaštite ljudskih prava; sprječavanja monopola, cenzure i širenja dezinformacija, odgovornosti za nešto što je napisano, objavljeno i podijeljeno te na štetu temeljnih načela koja vrijede za prostor javnog znanja a to su transparentnost i pravo na pouzdanu i točnu informaciju. Rješenja koja nude tehnologije umjetne inteligencije na društvenim mrežama u procesima s podacima i informacijama su anonimnost, brzina, filtriranje podataka, obavijesti i informacija te ciljano usmjeravanje objektivno netočnih i nepouzdanih podataka, obavijesti i informacija, kada je to nekome u interesu. Zbog neadekvatne reguliranosti ponašanja u kiber prostoru i mogućnosti zloupotrebe tehnologija umjetne inteligencije koje

1 Tuđman Miroslav, Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb, 2008, str. 134.

koriste društvene mreže, neupitna je činjenica da su društvene mreže postale snažni alati borbe za nametanje ideja i ideologija, nametanje volje i borbe za informacijsku nadmoć različitih aktera (državnih, nedržavnih i korporacija). Mogućnost anonimnog komuniciranja u kiber prostoru pomoću društvenih mreža, zloupotrebe tehnologija umjetne inteligencije i nepostojanje odgovarajućih mehanizama penalizacije prema kriterijima koji se ne vode istinom i objektivnošću otvorilo je prostor za stvaranje učinkovitih dezinformacija. Na osnovi dezinformacija koje je moguće stvarati na društvenim mrežama iz kiber prostora moguće je stvarati druge različite vrste prijetnji i na taj način (pre)oblikovati razmišljanja ciljanih publika na nove načine. Navedena mogućnost u kiber prostoru svestrano se koristi u metodama planiranja i izvođenja napadnih informacijskih operacija (psiholoških operacija). Ova vrsta operacija u kiber prostoru, između ostalog, omogućena je načinom na koji su osmišljavane društvene mreže odnosno kriterijima prema kojima su vlasnici umjetne inteligencije odredili njezine funkcije i svrhu na društvenim mrežama, kroz povezivanje, komuniciranje i razmjenu ideja. Društvene mreže su informacijske operacije učinile komercijalnim proizvodom i globalno dostupnom uslugom.

Visokotehnološke korporacije (Facebook Inc., Twitter i Alphabet Inc. vlasnik Googla i YouTubea) koriste društvene mreže radi stvaranja profita u poslovima digitalnog marketinga i oglašavanja. Međutim, zbog nedovoljnog interesa da otklone negativne posljedice koje proizvode društvenoj zbilji, različiti akteri pomoću društvenih mreža na učinkovitiji način zloupotrebljavaju kiber prostor i društvene mreže za dekonstrukcije postojećih i na objektivnoj istini utemeljenih društvenih i političkih konstrukata, odnosno koriste ih za nametanje vlastitih ideja, ideologija i s njima povezanih vrijednosti, uvjerenja i načela. Posljedično je došlo do dramatičnih promjena u dometu, neposrednosti i u razmjerima utjecaja u svijetu politike i načinima planiranja i provedbe psiholoških operacija. Politika, ratovanje, informacije, moć i utjecaj oduvijek su bili međusobno isprepleteni i povezani. Društvene mreže dodatno su ubrzale ove procese, povećale su njihovu povezanost te u kiber prostoru diktiraju dinamiku politike, ratovanja i informacija.

Vodeći svjetski politički i gospodarski subjekti (države i tvrtke) prema novim kriterijima i uvjetima koje diktiraju društvene mreže, usvojili su sve prednosti i nedostatke kiber prostora i društvenih mreža te su, sukladno njima, prilagodili vlastite informacijske doktrine i strategije. Temeljem prednosti i nedostataka kiber prostora i društvenih mreža preko kiber prostora pomoću društvenih mreža provode informacijske, psihološke i medijske operacije prema protivničkim korpusima javnog znanja. Države i tvrtke pomoću društvenih mreža i

primijenjenih tehnologija umjetne inteligencije stvaraju učinkovite dezinformacije i pseudodogađaje kojima upravljaju i vode ih u pravcima koji odgovaraju njihovim težnjama.

Napadačke informacijske operacije (psihološke operacije) koje se u kiber prostoru izvode pomoću društvenih mreža postale su učinkovitije jer su anonimne, jer se odvijaju u realnom vremenu, one su masovne, neposredne i prilagođene društvenim slabostima ciljanih publika. Novost u ovoj međuzavisnoj interakciji politike i informacijskih operacija je u zloupotrebama osobnih i/ili grupnih uvjerenja, načela i vrijednosti i u zloupotrebama umjetne inteligencije koja ih obrađuje i u njima prepoznaje slabosti ciljanih publika koje mogu biti pojedinci i grupe koje se broje na stotine tisuća i milijune korisnika, s različitim vrijednostima, uvjerenjima i načelima. Njihova strukturirana uvjerenja, načela i vrijednosti na društvenim mrežama postala su izloženija interesima da se njima manipulira i da ih se oblikuje prema volji drugih.

Komercijalizacijom umjetne inteligencije koju koriste društvene mreže na globalnoj razini osobni podaci i obavijesti koje se stvaraju, kojima se strojno upravlja, ubrzava ih se i automatizirano usmjerava umrežavaju se s proizvodima i uslugama koje nude društvene mreže. Tako je došlo i do transformacije organiziranja korpusa javnog znanja te do društvenih, ekonomskih i kulturnih promjena. Problem je jer u tržišno i tehnološki diktiranom okruženju umjesto pouzdanosti, točnosti i integriteta obavijesti prioritete imaju komercijalni imperativi. U digitaliziranom prostoru javnog znanja vidljivo izostaje element odgovornosti društvenih mreža prema društvu i stvaranju objektivnog znanja i točnih informacija. Društvene mreže trebale su povezati društvo i prostor digitaliziranog javnog znanja na transparentan način u svrhu stvaranja objektivnog znanja i u svrhu razmjene točnih i objektivnih informacija. Međutim „tvorničke postavke“ umjetne inteligencije koju koriste društvene mreže dovele su do dramatičnog obrata temeljne funkcije koju su društvene mreže trebale predstavljati društvu.

Na osnovi zloupotreba informacijsko-komunikacijskih tehnologija i globaliziranih, umreženih medija i kiber prostora, kojima se na učinkovit način umanjuje protivnička volja i borbena spremnost a povećavaju izgledi za učinkovito nametanje vlastitih ideja i ideologija, nastale su nove forme međunarodnih sukoba i u njima primjena novih instrumenata moći. Nove forme sukoba zahvaljujući novim instrumentima moći ne moraju prerasti u rat, zadržavaju se primarno u kiber prostoru u kojem se vodi glavna borba za um ciljanih publika, njihovo razmišljanje i donošenje odluka. Tek iznimno, ukoliko se to smatra potrebnim, informacijski sukobi iz kiber prostora koji su konstantni (24/7) mogu se prenijeti u stvarni fizički prostor i u njemu mogu prerasti u rat kao krajnje rješenje međunarodnih sporova. Globalne informacijske i medijske

operacije planiraju se i izvode pomoću globalno dostupnih društvenih mreža i tehnologija umjetne inteligencije. One čine osnovu sukoba u 21. stoljeću. Društvene mreže i umjetna inteligencija postali su novi instrumenti moći u kiber prostoru i kao takvi postali su nositelji novih formi informacijskih i medijskih operacija i na njima utemeljenih novih načina stvaranja prijetnji iz kiber prostora prema demokratskom poretku i korpusu javnog znanja ciljanih publika.

Hibridni sukobi predmet su istraživanja jer je njihov nastanak rezultat razvoja informacijskih i komunikacijskih sustava i tehnologija umjetne inteligencije koje su na društvenim mrežama primijenjene za globalno i umreženo povezivanje pojedinaca, grupa, ideja i komercijalnih usluga. Društvene mreže osmišljene su da upravljaju informacijskim procesima u kojima umjetna inteligencija ima presudnu ulogu. Međutim, ujedno su omogućile stvaranje anonimnih, masovnih i automatiziranih dezinformacija (protuobavijesti) kojima su dale brzinu, neposrednost i bezgraničnost u prostoru i vremenu.

Istraživanjem nastanka dezinformacija na društvenim mrežama i definiranjem uloge društvenih mreža u njihovom stvaranju u korpusu javnog znanja, prepoznaju se nove sigurnosne prijetnje te novi obrasci napada na korpuse javnog znanja kroz nove oblike i nove mogućnosti manipuliranja podacima i obavijestima s društvenih mreža za stvaranje, oblikovanje i distribuciju dezinformacija. Tehnologije umjetne inteligencije koje koriste društvene mreže u radu se promatra kroz sposobnost različitih aktera da ih u međunarodnim sukobima zloupotrebljavaju i koriste za stvaranje informacijske nadmoći kroz prikriveno uvjeravanje ciljanih publika pomoću anonimnih dezinformacija koje su prilagođene sklonostima i interesima ciljanih publika. Stvaranje dezinformacija zloupotrebom umjetne inteligencije u sinergiji s ljudskom inteligencijom promatra se kroz hibridnu inteligenciju. Hibridna inteligencija za rješavanje zadaća koristi sve najbolje što nudi umjetna i ljudska inteligencija, a razni akteri koriste je na društvenim mrežama za stvaranje učinkovitih dezinformacija kojima pospješuju ostale prijetnje. Prijetnje koje dolaze iz kiber prostora a u svojim učincima potpomognete su umjetnom inteligencijom koju koriste društvene mreže naziva se hibridnim prijetnjama, a psihološke operacije u kojima se zloupotrebljava hibridna inteligencija na društvenim mrežama za stvaranje hibridnih prijetnji naziva se hibridnim operacijama.

Istraživanje i raščlambu pojavnih oblika, primijenjenih metoda i sredstava zloupotrebe tehnologija umjetne inteligencije na društvenim mrežama prikazat će se na relevantnim primjerima hibridnih operacija, s glavnim naglaskom na psihološkim operacijama i

dezinformacijama koje se promatraju kao ključan „proizvod“ i izvor prijetnji u kiber prostoru pomoću kojih je moguće stvarati niz hibridnih prijetnji. Kombiniranje hibridne inteligencije, dezinformacija, psiholoških operacija, hibridnih prijetnji i društvenih mreža kroz planiranje i izvođenje hibridnih operacija promatraju se kao glavne prijetnje demokratskim procesima i organizaciji korpusa javnog znanja.

Psihološke operacije u kiber prostoru kao napadačka odrednica informacijskih operacija i društvene mreže predmet su istraživanja jer su društvene mreže ključan novi informacijski instrument moći kojim se, zahvaljujući umjetnoj inteligenciji koju koriste, kroz kiber prostor na učinkovitiji način multiplicira moć ostalih nekinetičkih i kinetičkih instrumenata moći te se na taj način pospješuje ostvarivanje informacijske nadmoći u korpusu javnog znanja ciljanih publika. Moć utjecaja koja proizlazi iz sposobnosti da se kroz kreativnost, višeznačnost i nelinearnost kiber prostora svi instrumenti hibridne moći (politički, diplomatski, vojni, gospodarski i informacijski) istovremeno sinkroniziraju s kognitivnim elementima hibridnih operacija naziva se hibridna moć.

Osnovni motiv i polazište znanstveno-istraživačkog rada je bolje razumijevanje nastanka i uloge učinkovitih dezinformacija na društvenim mrežama, što su hibridne operacije, što su hibridni sukobi, što hibridne sukobe razlikuje od hibridnih ratova kao i davanje odgovora na pitanje na koji način hibridni (državni i nedržavni) akteri kroz kiber prostor pomoću društvenih mreža i umjetne inteligencije oblikuju i sinkroniziraju kognitivne elemente psiholoških operacija kako bi utjecali na razmišljanje i donošenje odluka ciljanih publika u vlastitu korist. Motiv je prikazati metodologiju stvaranja učinkovitih dezinformacija, prepoznati prijetnje i dati odgovore na prijetnje koje proizlaze iz psiholoških (hibridnih) operacija kojima se planiraju i izvode dezinformacijske kampanje pomoću društvenih mreža. Za potrebe ovog rada hibridni sukobi promatraju se isključivo kroz informacijsku komponentu, odnosno kroz hibridne operacije u kojima psihološke operacije promatramo kao nositelje dezinformacijskih kampanja i hibridnih prijetnji. Predmet istraživanja nisu drugi nekinetički instrumenti hibridne moći (diplomatski, politički, ekonomski itd.) niti su predmet dubljeg istraživanja kinetički (vojni) instrumenti moći.

Zbog mogućnosti lažnog predstavljanja, (pre)usmjeravanja pozornosti ciljanih publika na dezinformacije, automatiziranog ubrzavanja dometa dezinformacija, anonimnog širenja, ograničavanja pristupa određenim informacijama te izvršenih podjela korisnika, društvene mreže omogućavaju učinkovito manipuliranje načelima, uvjerenjima i vrijednostima ciljanih

publika kad je to nekome u interesu. Posljedično omogućavaju utjecanje na njihovo ponašanje i donošenje odluka, što i jest osnova i svrha psiholoških operacija. Daljnjim istraživanjem prikazat će se da se umjetna inteligencija koju koriste društvene mreže u hibridnim sukobima koristi kao snažan i učinkovit informacijski instrument moći pomoću kojeg se planiraju i izvode hibridne operacije i stvaraju različite prijetnje prema ciljanim publikama. Potom će se utvrđene obrasce, metode i tehnike hibridnih operacija primijeniti na niz događaja koji se vežu za pojmove hibridnih prijetnji u primjerima hibridnih sukoba i hibridnog ratovanja. Time se želi pokazati da se tehnologije umjetne inteligencije koje koriste društvene mreže kroz primjenu hibridne inteligencije, osim za komercijalne interese, zloupotrebljavaju za stvaranje učinkovitih dezinformacija i hibridnih prijetnji. Primjerice, za produbljivanje podjela unutar protivničkih vrijednosti, uvjerenja i načela što i predstavlja ispunjenje širih strateških ciljeva iz grupe hibridnih operacija. Važno je napomenuti da se pri tome postavlja jasna distinkcija između hibridnog sukoba i rata.

Hibridno ratovanje ima brojne definicije koje su kroz brojna dosadašnja znanstvena istraživanja dovoljno puta obrađene, tako da same definicije i obilježja hibridnog ratovanja nisu predmet detaljnijeg istraživanja. Hibridni rat promatra se isključivo kao vojni neizravni pristup ratovanju pod specifičnim okolnostima. Fokus istraživanja je na hibridnim sukobima. Hibridne sukobe promatra se isključivo kroz upotrebu hibridnih operacija u razdobljima mira (političkih napetosti i izbornih procesa u drugim državama), kad su ciljane publike najviše podijeljene i kad ih se pomoću društvenih mreža može dodatno dijeliti i stvarati učinkovite hibridne prijetnje (destabilizirati društvene i političke procese ili pogoršavati sigurnosno stanje u drugim državama ili na nekom širem geografskom području). Može se reći da hibridni sukobi, hibridne operacije i hibridne prijetnje prethode hibridnom ratu. Ovakvi sukobi su konstantni, odvijaju se primarno u kiber prostoru i vode se primarno psihološkim operacijama prema svim kategorijama ciljanih publika na pojedinačnoj, lokalnoj, globalnoj ili masovnoj razini. Kad se hibridnim psihološkim operacijama pridoda kinetički element, dakle vojni instrument hibridne moći, tada hibridni sukob prelazi u kategoriju hibridnog rata. Hibridne (psihološke) operacije utjecaja u takvim okolnostima također jesu glavna metoda kojom se stvaraju hibridne prijetnje, ali u kontekstu ostvarivanja ciljeva hibridnog rata. Hibridnim operacijama primjenom hibridne inteligencije na društvenim mrežama vrlo jednostavno se napada čitav „informacijski sustav“ nekog društva i njegov sustav vrijednosti, odnosno njegovo opće znanje koje je glavna meta informacijskih napada iz grupe hibridnih operacija, bez obzira radi li se o ratu ili miru, ovisno o potrebama napadača.

Povezivanjem utvrđenih obrazaca, metoda i tehnika planiranja i provođenja hibridnih (psiholoških) operacija s nizom događaja koji se vežu za hibridne ratove i sukobe dokazat će se postavljena hipoteza rada: da se društvene mreže, kroz ovu novu kategoriju operacija utjecaja, koriste kao snažni i učinkoviti alati utjecaja za stvaranje hibridnih prijetnji i postizanje specifičnih ciljeva u hibridnim ratovima i sukobima: za organiziranje i upravljanje posredničkih oblika sukoba, za izazivanje političke, identitetske ili društvene nestabilnosti iza kojih se kriju prikriveni interesi informacijskog napadača kako bi ostvario vlastite politike, društvene, strateške i geopolitičke ciljeve te kako bi onemogućio učinkovite protuodgovore. Ovim će se (dodatno) potvrditi glavna hipoteza rada da informacijski napadač, u cilju postizanja vlastite informacijske nadmoći u hibridnim sukobima, umjetnu inteligenciju koju koriste društvene mreže zloupotrebljava kao alat snažnog utjecaja za oblikovanje korpusa javnog znanja ciljanih publika za vlastitu korist.

U psihološkim operacijama koje se planiraju i izvode pomoću društvenih mreža osobni podaci građana (njihova uvjerenja, njihove vrijednosti i njihova načela) uz primjenu hibridne inteligencije zloupotrebljavaju se za stvaranje dezinformacija i na osnovi njih stvaraju se i pojačavaju hibridne prijetnje. Sasvim sigurno, ove mogućnosti još uvijek nisu jasno prepoznate kao dio informacijskih i medijskih operacija nametanja volje ciljanoj publici i promjeni korpusa javnog znanja (koji je pak legitiman predmet istraživanja informacijskih znanosti).[2] Oblikovanjem korpusa javnog znanja ciljane publike na osnovi zloupotrebe osobnih podataka i umjetne inteligencije koju koriste društvene mreže postiže se stanje informacijske nadmoći za napadača, a nametnute prijetnje iz kiber prostora stvaraju dodatne preduvjete za konačno ispunjavanje ciljeva i zadaća informacijskih stratega.

Stoga će se u ovom radu dati poseban naglasak na istraživanje sinergije, metoda i tehnika, odnosno utvrđivanje obrazaca zloupotrebe društvenih mreža i umjetne inteligencije u kiber prostoru kroz hibridne operacije koje su različiti akteri izvodili na geografskim područjima Baltika, Crnog mora, SAD-a, pojedinih država članica EU-a i istočnog Mediterana za stvaranje dezinformacija, hibridnih prijetnji i postizanje informacijske nadmoći, odnosno za oblikovanje korpusa znanja ciljanih publika prema vlastitim potrebama.

2 Usp. Akrap Gordan, Informacijske strategije i operacije u oblikovanju javnog znanja, Filozofski fakultet, Zagreb, 2011., str. 2.

Istraživanje hibridnih operacija kroz proces i metodologiju stvaranja dezinformacija i hibridnih prijetnji u svrhu oblikovanja korpusa javnog znanja ciljanih publika i stjecanja stanja informacijske nadmoći podijeljeno je na sedam glavnih dijelova.

U dijelu pod nazivom „Informacijski prostor i novi obrasci organiziranja podataka i informacija“ definiran je kiber prostor, definirane su društvene mreže i umjetna inteligencija, njihov nastanak, glavna obilježja i definicije. Kiber prostor je u sinergiji s društvenim mrežama otvorio čitav spektar mogućnosti iskorištavanja nekinetičkih sredstava (operacija utjecaja) borbe radi postizanja maksimalnog strateškog učinka. Komercijalizacijom tehnologija umjetne inteligencije i njihovom sinergijom s kiber prostorom i društvenim mrežama, novim medijskim kanalom koji omogućava globalan i neposredan doseg ciljanih publika, kroz organizaciju podataka, informacija i javnog znanja, unesena je dramatična novost u planiranju i izvođenju psiholoških operacija. Definirane su tehnologije i vrste umjetne inteligencije koje održavaju osnovne funkcije društvenih mreža, negativni učinci društvenih mreža na organizaciju znanja u javnom prostoru te hibridna inteligencija. Hibridna inteligencija prikazana je kao nova mogućnost za stvaranje učinkovitih dezinformacija i različitih hibridnih prijetnji iz kiber prostora.

Nakon toga prikazana je i dodatno objašnjena manipulativna moć umjetne inteligencije u obradi osobnih podataka korisnika društvenih mreža te kako takva moć ima negativne manifestacije na različite društvene pojave. Ovdje su prikazane i objašnjene različite tehnike uvjeravanja koje su vlasnici društvenih mreža nametnuli kroz komercijalizaciju vlastitih usluga kako bi učinkovitije nametali vlastitu volju na tržištu digitalnog marketinga. Različite tehnike uvjeravanja kada se koriste u marketingu predstavljaju određenu prijetnju društvu. No, daleko veću prijetnju predstavljaju kad se zloupotrebljavaju za stvaranje dezinformacija, hibridnih prijetnji, poticanje političkih ili društvenih sukoba i kriza. Tada imaju katastrofalne posljedice po društvo u cjelini.

Dezinformacije su definirane kao glavna negativna posljedica u organizaciji znanja na društvenim mrežama. Dezinformacijske kampanje definirane su glavnim metodama kojima se u kiber prostoru pomoću društvenih mreža na osnovi primijenjenih tehnologija umjetne inteligencije planski i na organiziran način stvaraju i šire dezinformacije. Potom je dodatno objašnjena metodologija kojom se planiraju i izvode dezinformacijske kampanje pomoću društvenih mreža, kroz sve prednosti koje nude lažni profili, umjetna inteligencija i različite tehnike uvjeravanja te su podijeljene na nekoliko faza. Pojašnjeno je kako je cjelokupan proces

anoniman i na osnovi sinergije sustava povratne sprege i umjetne inteligencije automatiziran i optimiziran prema slabostima i preferencijama ciljanih publika.

Definirani su sigurnosni i društveni paradoksi do kojih je dovela zloupotreba društvenih mreža, a potom je napravljen prikaz snažnog i negativnog utjecaja društvenih mreža. U tom kontekstu napravljen je prikaz zloupotrebe društvenih mreža koje, kao komunikacijski alati i medijski kanal, pogoduju stvaranju i diseminaciji dezinformacija, pogoduju njihovoj većoj učinkovitosti, doprinose učinkovitoj mobilizaciji ili demobilizaciji ciljanih publika ovisno o potrebama onog tko ih koristi, da pogoduju produbljivanju postojećih podjela te suptilnim oblicima utjecaja na vrijednosti, uvjerenja i načela ciljanih publika.

U dijelu pod nazivom „Informacijske strategije, društvene mreže i operacije utjecaja u kiber prostoru“ definirane su informacijske strategije, njihovi ciljevi te prilagodbe koje su državni akteri nužno trebali izvršiti u informacijskim strategijama prema prednostima koje nude kiber prostor, društvene mreže i umjetna inteligencija. Definirane su operacije utjecaja u kiber prostoru i njihove osnovne prednosti u odnosu na operacije utjecaja koje se vode pomoću tradicionalnih medijskih kanala (TV-a, radija, tiska). Definirane su osnovne sastavnice operacija utjecaja s fokusom na informacijske operacije, psihološke operacije i medijske operacije te na razloge i prednosti koje ove operacije postižu u kiber prostoru pomoću društvenih mreža. Posebno su definirane razlike između psiholoških operacija i strateškog komuniciranja, s obzirom na međusobne kontradikcije kad se provode izvan razdoblja rata za nametanje napadačeve volje.

U dijelu pod nazivom „Hibridni sukobi i novi instrumenti moći u kiber prostoru“ definirani su hibridni sukobi, otklonjene su konceptualne nejasnoće oko razlika s hibridnim ratom te su definirana glavna obilježja prema kojima se prepoznaje da hibridni sukobi predstavljaju širi pojam od hibridnog rata. Ujedno su prikazani i objašnjeni uzroci njihovog nastanka.

Prikazano je da su u hibridnim sukobima težišta informacijske borbe prebačena na um ciljanih publika, na njihove vrijednosti, uvjerenja i načela s ciljem njihovog kratkoročnog ili dugoročnog preoblikovanja. Hibridni sukobi prikazani su kao sukobi u kojima su glavna nekinetička težišta borbe kultura, jezik i identitet ciljanih publika te da se, u tu svrhu, društvene mreže, tehnologije umjetne inteligencije i osobni podaci korisnika društvenih mreža zloupotrebljavaju za pripremanje i izvođenje psiholoških operacija u kojima se utvrđene

društvene slabosti na osnovi uvjerenja ciljanih publika koriste kao glavne uporišne točke za planiranje i stvaranje dezinformacija i hibridnih prijetnji iz kiber prostora.

Identificiranje društvenih slabosti ciljanih publika pomoću društvenih mreža ključan je dio uspjeha cjelokupne strategije. Prikazano je da su društvene mreže unijele važan paradigmatski pomak u planiranju i izvođenju psiholoških operacija. Društvene mreže olakšavaju identifikaciju društvenih slabosti prema kojima hibridna inteligencija olakšava uobličavanje dezinformacija. Cijeli ovaj proces, sustavom povratne sprege kojim upravlja umjetna inteligencija, društvene mreže su automatizirale te pomoću lažnih računa učinile anonimnim. Anonimnost psihološkog djelovanja u kiber prostoru pomoću društvenih mreža jedan je od glavnih razloga zbog kojih se hibridne sukobe teško predviđa u njihovom nastanku.

U dijelu pod nazivom „ Novi instrumenti hibridne moći: hibridne prijetnje i hibridne operacije“ definirane su hibridne prijetnje kao nova paradigma prijetnji koje se planiraju i stvaraju psihološkim operacijama u kiber prostoru a pomoću društvenih mreža se usmjeravaju na um ciljanih publika, njihove vrijednosti, uvjerenja i načela. Društvene mreže i umjetna inteligencija u ovom kontekstu dovele su do nastalih promjena paradigme sukoba i ratova. Definirane su vrste hibridnih prijetnji, njihova strateška logika i ciljevi. Prikazano je kako je glavna ideja hibridnih prijetnji na slabljenju obrane, na ciljanju društva njegovim vlastitim društvenim slabostima, njegovoj destabilizaciji, poticanju da ciljane publike donose odluke od volje napadača i (pre)oblikovanju protivničkog korpusa javnog znanja. Objašnjeno je da se radi o skupu suptilnih aktivnosti koje su pomoću društvenih mreža u kiber prostoru neprimjetne i da postaju veliki sigurnosni izazov za demokratske procese. Njihovoj neprimjetnosti dodatno pridonosi činjenica da se provode pomoću lažnih računa, a u pravilu ih planiraju i izvode sigurnosno-obavještajne strukture. U ovom kontekstu, kiber prostor prikazan je kao prostor u kojem se dezinformacije i hibridne prijetnje stvaraju novom paradigmom napadačkih akcija hibridnim operacijama u kojima zloupotreba hibridne inteligencije na društvenim mrežama igra ključnu ulogu.

Potom su definirane hibridne operacije te je prikazano da su primjenom umjetne inteligencije društvene mreže postale glavni informacijski instrument hibridne moći pomoću kojih se u kiber prostoru upravlja informacijskim sukobom i svim sastavnicama iz kategorije operacija utjecaja. Također prikazana je manipulativna moć umjetne inteligencije koju je razvio Facebook koji ima veliki utjecaj na pojave i procese koji se koriste za postizanje ciljeva iz definicije psiholoških i hibridnih operacija. Pokazano je da su ove vrste operacija utjecaja preko kiber

prostora, zbog niza prednosti koje nude društvene mreže i hibridna inteligencija, glavno izvorište prijetnji društvu iz kiber prostora, odnosno da je zloupotreba društvenih mreža i hibridne inteligencije osnova stvaranja dezinformacija i hibridnih prijetnji. Prikazano je da se društvenim mrežama može provoditi cijeli niz aktivnosti usmjerenih prema postizanju stanja informacijske nadmoći i oblikovanju napadnutog cilja u skladu s napadačevim potrebama.

Nakon toga definirane su dvije glavne kategorije hibridnih operacija kojima se stvaraju konstantni (24/7) informacijsko-psihološki pritisci, njihove međusobne razlike i zajedničke poveznice s ciljem stvaranja strateških posljedica: stvaranje informacijske nadmoći, odnosno preoblikovanje korpusa javnog znanja ciljanih publika.

Potom su hibridne operacije prikazane kao oblik političke borbe u kiber prostoru za postizanje informacijske nadmoći. Prikazane su kao glavni informacijski instrument hibridne moći pomoću kojeg napadač u hibridnim sukobima pojačava ostale instrumente hibridne moći (diplomatske, vojne i ekonomske) kako bi korpus javnog znanja protivnika oblikovao prema vlastitim potrebama, odnosno kako bi njegovo pamćenje kratkoročno ili dugoročno sveo na dezinformacije te na skup podataka i informacija koje sustavno i planski projektira i memorira u njegov informacijski prostor. Ovim se dodatno htjelo pokazati da su hibridne operacije strateške prirode u svojim ciljevima i glavna metoda kojom se stvaraju hibridne prijetnje i provode nacionalne informacijske strategije.

U dijelu pod nazivom „Hibridne operacije u hibridnim sukobima i hibridnom ratovanju“ prikazane su osnovne sličnosti i razlike u zapadnom i ruskom pogledu na hibridne sukobe i hibridne ratove i njihova tumačenja hibridnih sukoba i hibridnih ratova. SAD i Rusija izabrani su s metodološkog stajališta iz nekoloko razloga. Ove dvije zemlje u većini literature opisane su kao ključni međunarodni čimbenici koji za rješavanje međunarodnih sukoba koriste kiber prostor i društvene mreže za ispunjavanje ciljeva nacionalnih informacijskih strategija. Oružane snage SAD-a jedan su od ključnih kreatora kiber prostora koji je nastao za vojne potrebe te su predvodnici razvoja tehnologija umjetne inteligencije koja danas ima ključnu ulogu u održavanju osnovnih funkcija i zadaća društvenih mreža. Također, ove dvije zemlje imaju najbolje razvijene doktrine informacijskog ratovanja, metodologije planiranja i izvođenja psiholoških operacija te razvijene informacijske, gospodarske, diplomatske, financijske i vojne instrumente hibridne moći. One su ključni kreatori hibridnih sukoba i hibridnih ratova u zemljama i na geografskim područjima od vlastitih interesa te imaju sposobnosti hibridnim operacijama nad korpusima javnog znanja ciljanih publika stvarati učinkovite hibridne prijetnje

i ostvarivati informacijsku nadmoć. Ovim se hoće pokazati i dokazati da su za oba aktera društvene mreže označile važan paradigmatski pomak u njihovim informacijskim strategijama i taktikama planiranja i izvođenja operacija utjecaja u kiber prostoru. Primjerima hibridnih operacija čiji su nositelji Rusija i SAD objašnjeno je da oba aktera sveobuhvatno zloupotrebljavaju sve mogućnosti koje im nude kiber prostor, društvene mreže i umjetna inteligencija, ovisno radi li se o ciljevima i potrebama hibridnog sukoba ili hibridnog rata.

Pored obrađenih primjera postoji i znatan broj drugih, manje ili više sličnih primjera koji ovdje nisu navođeni, jer se smatra da su ovi primjeri dovoljni za potrebe ovog istraživanja.

U dijelu pod nazivom „Novi obrasci prevencije i obrane od hibridnih prijetnji“ predložen je teorijski model obrane od dezinformacija i hibridnih prijetnji iz kiber prostora. Pokazano je da se kao posljedica hibridnih operacija i hibridnih prijetnji neupitno javlja potreba za stvaranjem nove nacionalne informacijske strategije. Glavni doprinos nove informacijske strategije je u pravovremenom prepoznavanju dezinformacija i hibridnih prijetnji i njihovih nositelja, ublažavanje te otklanjanje takvih prijetnji. Također, zadaća nacionalne informacijske strategije je budućim generacijama u korpusu javnog znanja osigurati ravnopravnost u razmjeni znanja na osnovi objektivnih i točnih informacija kao temeljnom ljudskom pravu.

U zaključnom razmatranju ukazano je na potrebu podizanja percepcije donositelja političkih odluka o nužnosti otklanjanja novih oblika prijetnji iz kiber prostora te na potrebu jačanja svjesnosti i politika koje zagovaraju stvaranje novih pravila kako bi se nacionalni informacijski i digitalni prostor adekvatno štitio od dezinformacija, hibridnih prijetnji i štetnih utjecaja vanjskih aktera na nacionalni korpus javnog znanja.

1.2. Cilj rada i polazna pretpostavka

Cilj ove disertacije je utvrditi uzroke i načine na osnovi kojih informacijski napadač u hibridnim sukobima, s ciljem postizanja informacijske nadmoći, zloupotrebljava društvene mreže i umjetnu inteligenciju kao snažne i učinkovite alate utjecaja za oblikovanje prostora javnog znanja ciljane publike za vlastitu korist te na taj način testirati polaznu pretpostavku i istraživačka pitanja. Polazna pretpostavka ove doktorske disertacije jest da informacijski napadač u hibridnim sukobima koristi društvene mreže za stvaranje učinkovitih dezinformacija i hibridnih prijetnji pomoću kojih preko kiber prostora želi ostvariti informacijsku nadmoć i realizirati političke interese. Polaznom pretpostavkom želi se potvrditi da su društvene mreže postale snažni, učinkoviti i dominantni alati za stvaranje dezinformacija i taktički alati utjecaja pomoću kojih je u kiber prostoru moguće planirati i izvoditi strateške i u pravilu prikrivene psihološke operacije s mogućim strateškim posljedicama. Pod strateškim posljedicama podrazumijeva se (pre)oblikovanje korpusa javnog znanja, utjecanje na temeljna načela, uvjerenja i vrijednosti i ostvarivanje informacijske nadmoći.

Radom se želi ukazati na ulogu i mogućnosti zlouporabe umjetne inteligencije koju koriste društvene mreže za stvaranje učinkovitih dezinformacija i hibridnih prijetnji. Također se želi ukazati da su dezinformacije koje se stvaraju uz pomoć umjetne inteligencije koje koriste društvene mreže primarna prijetnja koja proizlazi iz kiber prostora na osnovu kojih se na učinkovit način mogu stvarati hibridne prijetnje. Želi se ukazati da su zbog toga društvene mreže postale ključan element u psihološkim operacijama napada na korpuse javnog znanja i da društvene mreže jesu jedan od ključnih informacijskih instrumenta hibridne moći. Želi se ukazati da pomoću dezinformacija i hibridnih prijetnji koje se stvaraju pomoću društvenih mreža svi instrumenti hibridne moći postaju učinkovitiji, da se u kiber prostoru multipliciraju u moći i da su međusobno ovisni u stvaranju željenih učinaka.

Stoga će se u ovom radu poseban naglasak dati na istraživanje metoda i tehnika, odnosno na utvrđivanje obrazaca prema kojima su društvene mreže dovele do učinkovitih dezinformacija i s njima povezanih negativnih implikacija na organizaciju javnog znanja. Ujedno, naglasak je na istraživanju kako se dezinformacije koje se stvaraju uz pomoć tehnologija umjetne inteligencije koje koriste društvene mreže iskorištavaju za postizanje krajnjeg cilja nacionalnih informacijskih strategija: stvaranje informacijske nadmoći.

Facebook (Meta) predmet je istraživanja jer se radi o društvenoj mreži koja trenutno dominira na globalnom tržištu digitalnog marketinga, najpopularnija je društvena mreža po broju korisnika zahvaljujući globalnoj dostupnosti vlastitih aplikacija WhatsAppa, Facebook Messengera te Instagrama za dopisivanje na mobilnim uređajima, jer posjeduje najveću bazu osobnih podataka korisnika te razvija nove tehnologije umjetne inteligencije kako bi na adekvatan način za vlastite potrebe upravljala takvim bazama podataka. You Tube je predmet istraživanja jer se, nakon Facebooka, radi o najpopularnijoj društvenoj mreži po broju aktivnih korisnika koja je trenutno vodeća globalna internetska platforma za stvaranje i diseminaciju video sadržaja i pružanje usluga izravnog prenošenja video i audio sadržaja u realnom vremenu. Twitter (engl. cvrkut) predmet je istraživanja jer se trenutno radi o najpopularnijoj društvenoj mreži na temelju aktivnih korisnika koju se u političkoj komunikaciji koristi za širenje ideja i ideologija. Facebook, YouTube i Twitter predmet su istraživanja jer se ove društvene mreže u brojnim sukobima koriste kao alati utjecaja u (pre)oblikovanju i organiziranju protivničkog korpusa javnog znanja prema potrebama informacijskog napadača.

Želi se potvrditi da se u kiber prostoru trenutno najpopularnije društvene mreže (Facebook, YouTube i Twitter) koriste kao snažni i učinkoviti taktički alati za stvaranje anonimnih, automatiziranih, masovnih i optimiziranih dezinformacija sa strateškim posljedicama i da državni i nedržavni akteri tehnologije umjetne inteligencije koje održavaju osnovne funkcije ovih društvenih mreža kao i osobne podatke korisnika njihovih usluga, zloupotrebljavaju u psihološkim operacijama kako bi, u hibridnim sukobima, postigli određene i specifične ciljeve na (lokalnim, regionalnim i globalnim) geografskim područjima prema svim kategorijama ciljanih publika (pojedinačnim, grupnim ili masovnim). Pod specifičnim ciljevima podrazumijeva se stvaranje učinkovitih dezinformacija i hibridnih prijetnji prema potrebama napadača. Kao glavnu hibridnu prijetnju koja proizlazi iz kiber prostora u kontekstu opisane zloupotrebe promatra se stvaranje i diseminacija učinkovitih dezinformacija koje pogoduju stvaranju hibridnih prijetnji (produbljivanju postojećih društvenih i političkih podjela i društvenih slabosti, izazivanju društvenih, političkih i sigurnosnih destabilizacija, uplitanju u izborne procese u drugim državama) koje informacijski napadač usmjerava prema ciljanim publikama kako bi ostvario informacijsku nadmoć.

Istraživanjem se želi pokazati, ali i dokazati da su Twitter, YouTube i Facebook proširili raspone i mogućnosti za stvaranje učinkovitih dezinformacija te da je zakonodavni vakuum, u otklanjanju štetnih posljedica i u uvođenju adekvatne zakonodavne regulative za otklanjanje zloupotrebe umjetne inteligencije na ovim društvenim mrežama, doveo do toga da sve veći broj

aktera za rješavanje međunarodnih sukoba društvene mreže koriste za ostvarivanje političke moći. Također, želi se pokazati da je Facebook kroz komercijalni interes integrirao sfere unutarnje i vanjske politike s informacijskim ratovanjem, osnovnim elementima vojnih psiholoških operacija i vojne obmane te da je ova činjenica dovela do negativnih društvenih i sigurnosnih posljedica.

Radom se također želi otkloniti nejasnoće i ukazati na razlike između hibridnih sukoba i hibridnog rata te dati bolje razumijevanje korijena njihovog nastanka. Ujedno, želi se dati odgovor kako hibridni akteri u hibridnim sukobima, dakle izvan konteksta oružanih sukoba, pomoću društvenih mreža u kiber prostoru oblikuju i sinkroniziraju kognitivne elemente psiholoških operacija kako bi učinkovitije nametali vlastitu volju.

Cilj istraživanja je pokazati i dokazati[3] da su društvene mreže kao medijski kanal, zbog mogućnosti zloupotrebe tehnologija umjetne inteligencije koje u svijetu digitalnog marketinga održavaju osnovne funkcije društvenih mreža, u hibridnim sukobima postale moćni i učinkoviti alati utjecaja u kiber prostoru za (pre)oblikovanje vrijednosti, uvjerenja i načela ciljnih publika s mogućim strateškim posljedicama.

Želi se pokazati da su računalne tehnologije umjetne inteligencije koje koriste društvene mreže informacijama na društvenim mrežama dale moć za stvaranje učinkovitih dezinformacija i hibridnih prijetnji, da pomoću njih napadač ciljanim publikama učinkovitije nameće vlastitu volju i nad korpusom javnog znanja učinkovitije postiže informacijsku nadmoć. Želi se pokazati da moć dezinformacija na društvenim mrežama proizlazi iz mogućnosti zloupotreba umjetne inteligencije i osobnih podataka korisnika društvenih mreža (načela, uvjerenja i vrijednosti) na osnovu čega se može anonimno, automatizirano i optimizirano stvarati i oblikovati dezinformacije.

Želi se pokazati da su hibridne operacije nova forma napadnih informacijskih operacija (psiholoških operacija) iz kategorije operacija utjecaja u kiber prostoru, u kojima se za stvaranje i diseminaciju dezinformacija zloupotrebljava moć umjetne inteligencije i hibridne inteligencije koje su na taj način postale glavni nositelji napada na sustav vrijednosti, uvjerenja i načela ciljanih publika, odnosno da se njihovom zloupotrebom na društvenim mrežama ostvaruje

3 Hipoteza: Informacijski napadač u hibridnim sukobima u cilju postizanja vlastite informacijske nadmoći koristi društvene mreže i umjetnu inteligenciju kao alate utjecaja za oblikovanje prostora javnog znanja ciljane publike za vlastitu korist.

strateška logika hibridnih prijetnji: postizanje stanja informacijske nadmoći i oblikovanja napadnutog cilja u skladu s napadačevim potrebama. Napadačeve potrebe promatraju se kroz njegov interes da dezinformacijama i hibridnim prijetnjama napada sustav vrijednosti, uvjerenja i načela ciljnih publika, da produbljuje podjele unutar društvenih i političkih konstrukata ciljanih publika i/ili da potencira destabilizaciju u političkom, društvenom ili sigurnosnom kontekstu za vlastite potrebe.[4]

Cilj znanstvenog rada je prepoznati i dati odgovore na sigurnosne prijetnje koje proizlaze za društvo iz komercijalnih postavki koje su na društvenim mrežama odredili njihovi vlasnici.

Metodologija testiranja polazne pretpostavke opisana je u poglavlju koje slijedi.

4 Drugo istraživačko pitanje je: Na koji način se društvene mreže i umjetna inteligencija koriste kao sredstva za provođenje utjecaja za ostvarivanje vlastitih politika, za izazivanje društvenih nemira i oružanih sukoba te vlastitih ciljeva u izbornim kampanjama ciljanih publika.

1.3. Metodologija

Zlouporaba tehnologija umjetne inteligencije i osobnih podataka korisnika društvenih mreža (načela, uvjerenja i vrijednosti) za stvaranje dezinformacija i ostalih prijetnji iz kiber prostora predstavlja relativno novi fenomen na problemskom području provođenja operacija utjecaja. Teorijski okviri još nisu dovoljno izgrađeni. Kako je izgradnju teorijskih okvira moguće utemeljiti na induktivnom pristupu proučavanja empirijskih slučajeva ili objekata[5] u istraživanju se koristila kvalitativna metodologija. Znanstvena istraživačka metoda na kojoj se temelji ova doktorska disertacija je metoda instrumentalne studije slučaja i komparativna analiza, budući da je predmet istraživanja fenomen provođenja operacija utjecaja pomoću društvenih mreža, u tu svrhu istražit će se empirijske slučajeve te će se komparativnom analizom njihove primjene na geografskim područjima SAD-a, EU-a, Baltika, Crnog mora i istočnog Mediterana utvrditi obrasci sličnosti i razlika u zloupotrebama društvenih mreža ovisno o potrebama i kontekstima planiranja i izvođenja napadačkih informacijskih operacija (psiholoških operacija) iz grupe hibridnih operacija u hibridnim sukobima i hibridnom ratovanju. Studija slučaja učestalo se koristi za analizu nekog zbivanja ili zemlje "u sklopu komparativne perspektive koja zahtijeva da opis posebnog uključuje široke analitičke konstrukte".[6] „Studija jedne zemlje može se smatrati komparativnom ako se služi pojmovima koji se mogu primijeniti i na druge zemlje, razvija pojmove koji se mogu primijeniti i na druge zemlje ili teži nekim općenitijim zaključcima"[7], što je također obuhvaćeno u metodologiji izrade ove doktorske disertacije. „Općenito, u studijama slučaja nastoji se dati nove uvide u procese koji su unutar znanstvene discipline prihvaćeni kao važni."[8] U praksi su studije slučaja u pravilu višemetodske i koriste iščitavanje stručne literature, pregled sekundarnih dokumenata i traženje primarnih materijala.[9]

Koristit će se analiza sadržaja u sklopu koje će se napraviti analitička matrica pojavnih oblika mogućih koncepata i modaliteta zloupotrebe tehnologija umjetne inteligencije na društvenim mrežama, njihova učestalost i pojavnost u psihološkim operacijama, a potom će se iz

---

5 Kohlbacher Florian, The Use of Qualitative Content Analysis in Case Study Research, Volume 7, No. 1, Art. 21., 2006., dostupno na http://www.qualitative-research.net/index.php/fqs/article/view/75/153#g332 ( )

6 Brzica Nikola, Hibridni ratovi i suvremeni sukobi, Fakultet političkih znanosti, Zagreb, 2018., str. 20.; prema: Scarow H. (1969). Comparative political analysis, Harper and Row, New York.

7 Ibid.; prema: Landman, Todd. Issues and methods in Comparative Politics. Routledge, 2008.

8 Brzica, 2018., str. 20.

9 Ibid.

analiziranih strateških dokumenata, analitičkom matricom potvrditi ili proširiti novi koncepti obrane, prevencije i odvraćanja od dezinformacija, psiholoških operacija i prijetnji koje proizlaze iz kiber prostora.

Kao temelj instrumentalne studije slučaja i komparativne analize poslužila su dosadašnja istraživanja iz ovog područja dostupna u literaturi, studijama i drugim relevantnim izvorima. Izvori koj i će se koristiti kako bi se izvršile navedene analize, a relevantni su za ovo istraživačko područje, javno su dostupni. Literaturu se može podijeliti u nekoliko cjelina:

- službeni dokumenti, publikacije i izvještaji i izvori koji su javno dostupni; većina dokumenata potiče iz javnih službenih izvora Europske komisije, Europskog parlamenta, Europskog centra za borbu protiv hibridnih prijetnji (European Centre of Excellence for Countering Hybrid Threats), NATO saveza, njegovih specijaliziranih centara za energetsku sigurnost (Energy Security Centar of Exellence) i strateško komuniciranje (Strategic Communications Centre of Excellence) te za kiber obranu (NATO Cooperative Cyber Defence Centre of Excellence), javni službeni izvori SAD-a, Rusije, pojedinih država članica EU-a i NATO saveza;
- stručne analize nastale kao posljedica promatranja učinaka djelovanja hibridnih (psiholoških) operacija na pojedine ciljane publike (kao što su one u SAD-u, državama članicama EU-a i NATO-a, Rusije te na kriznim žarištima);
- vojne, političke i znanstveno-istraživačke institucije SAD-a i NATO saveza i Izraela na engleski jezik prevele su stručne analize publikacije i izvještaje bitne za shvaćanje integracije informacijsko-komunikacijskih i računalnih tehnologija s američkim i ruskim konceptom informacijskog ratovanja koje su primijenjene u američkim i ruskim hibridnim operacijama. Političke i znanstveno-istraživačke institucije Rusije objavile su na engleskom jeziku stručne analize, publikacije i izvještaje bitne za shvaćanje modernizacije, usvajanja i prilagodbe američkog koncepta informacijskog ratovanja u skladu s razvojem informacijsko-komunikacijskih i računalnih tehnologija koje koriste društvene mreže;
- dio dokumenata dostupan je iz sudskih procesa vođenih pred američkim pravosudnim i istražnim tijelima koji opisuju rusku metodologiju kojom su ruski hakeri zloupotrebljavali društvene mreže za planiranje i izvođenje hibridnih (psiholoških) operacija na teritoriju SAD-a i pojedinih država članica EU-a;

Dostupna literatura omogućava kvalitetnu i učinkovitu raščlambu informacijskih doktrina SAD-a i Rusije te bolje razumijevanje razlika između hibridnih sukoba i ratova, otklanjanje

međusobnih konceptualnih nejasnoća, korijena nastanka hibridnih sukoba, kiber prostora, algoritama, umjetne inteligencije i društvenih mreža. Dostupna literatura također omogućava kvalitetnu i učinkovitu raščlambu načina na koji planeri hibridnih (psiholoških) operacija za napade dezinformacijama, stvaranje konstantnih (24/7) informacijsko-psiholoških pritisaka kroz kiber prostor zloupotrebljavaju algoritme i druge tehnologije umjetne inteligencije koje koriste društvene mreže te kako su pomoću njih sinkronizirali nelinearnost kiber prostora i kognitivne elemente informacijskog ratovanja za planiranje i izvođenje napadnih informacijskih operacija (psiholoških) operacija s krajnjim ciljem: oblikovati korpus javnog znanja ciljanih publika, postići informacijsku nadmoć i ostvariti ciljeve nacionalnih informacijskih strategija.

1.4. Znanstveni doprinos

Znanstveni doprinos je u generiranju interpretativnog teorijskog okvira zlouporabe osobnih podataka korisnika društvenih mreža i tehnologija umjetne inteligencije koje koriste društvene mreže za stvaranje učinkovitih dezinformacija i štetnih utjecaja na korpuse javnog znanja, čime će se proširiti znanje iz interdisciplinarnog područja računalnih znanosti, informacijsko-komunikacijskih znanosti i obrambeno-sigurnosnih znanosti te će se predložiti novi koncepti zaštite informacijskog sadržaja i korpusa javnog znanja koje jest glavna meta dezinformacija i psiholoških operacija iz grupe hibridnih operacija.

Konkretan znanstveni doprinos je u istraživanju uloge tehnologija umjetne inteligencije koje koriste društvene mreže kao snažnih taktičkih sredstava za stvaranje učinkovitijih dezinformacija i učinkovitijih načina planiranja i izvođenja psiholoških operacija iz kiber prostora sa strateškim posljedicama na organizaciju javnog znanja i stjecanje informacijske nadmoći. Doprinos je u istraživanju metodologije kojom se zloupotrebljavaju osobni podaci korisnika društvenih mreža (njihova uvjerenja, načela i vrijednosti) i tehnologije umjetne inteligencije koje koriste društvene mreže u svrhu stvaranja učinkovitih dezinformacija koje se iskorištavaju u planiranju i izvođenju psiholoških operacija u kiber prostoru s ciljem produbljivanja postojećih društvenih, političkih i sigurnosnih kriza.

Dodatni doprinos je u definiranju potrebe za povećavanjem svijesti o spomenutim zloupotrebama i mogućnostima. Također, doprinos je u definiranju potrebe za uvođenjem nove nacionalne informacijske strategije s odgovarajućim preporukama, koracima i modelima kojima bi se obuhvatila odgovarajuća paradigma u cilju uspostave adekvatnih mehanizama u

odvraćanju i obrani od dezinformacija, hibridnih prijetnji i psiholoških operacija iz kiber prostora.

Doprinos je u raščišćavanju terminologije i izrada konceptualne analize pojmova koji određuju problemski prostor hibridnog sukoba poput pojmova hybrid intelligence, hybrid security, hybrid defence i drugih pojmova koji se vežu uz hibridne oblike sukobljavanja.

1.5. Ograničenja rada i smjernice za buduća istraživanja

Ograničenja rada odnose se uglavnom na dostupnost literature koju ova doktorska disertacija obrađuje. Naime, disertacija se najvećim dijelom oslanja na primarne izvore – istraživačke radove, doktrinarne publikacije, javno dostupne podatke, znanstvene i stručne radove teoretičara i publikacije zapadnih zemalja. Također, treba imati na umu i činjenicu da značajan dio izvora nije javno dostupan, budući da planiranje i izvođenje napadačkih informacijskih operacija utjecaja iz grupe hibridnih operacija (psiholoških operacija) u hibridnim sukobima i hibridnom ratovanju izvode obavještajne državne strukture, službe i agencije.

Ovo ograničenje naročito dolazi do izražaja u dijelu disertacije koji se odnosi na istraživanje američkih i ruskih pristupa u planiranju i izvođenju hibridnih (psiholoških) operacija iz kiber prostora, odnosno načina i razmjera iskorištavanja tehnologija umjetne inteligencije koje koriste društvene mreže za stvaranje dezinformacija u hibridnim sukobima tj. razdobljima društvenih i političkih kriza, izvan konteksta rata. Naime, predmet istraživanja su hibridne (psihološke) operacije u hibridnim sukobima kad su ove operacije uglavnom tajne te je, razumljivo, literatura uglavnom ograničena. Dodatno ograničenje je da javno dostupna zapadna literatura opisuje i stavlja naglasak na ruske hibridne (psihološke) operacije izvan konteksta oružanih sukoba, a hibridne (psihološke) operacije SAD-a opisuju isključivo u legitimnom kontekstu tj. u kontekstu hibridnog rata[10] kad se smatraju legitimnom metodom informacijske borbe. Nadalje, potrebno je istaknuti da je većina literature korištene u ovom radu izvorno na engleskom jeziku te zastupa zapadna stajališta koja naginju SAD-u i NATO savezu. Istinitost i točnost zapadnih izvora dijelom su ograničene te stoga na njihovu objektivnost, zbog određene doze pristranosti, treba gledati s potrebnom dozom rezerviranosti. Međutim, to nije u velikoj mjeri ograničavajuće za ovaj rad jer je cilj rada utvrditi pojavnost čimbenika koji neupitno

10 Primjer su vojne psihološke operacije koje su SAD-a izvodile protiv terorističke organizacije ISIL tijekom rata u Siriji i Iraku.

ukazuju na evidentan trend porasta zloupotreba društvenih mreža za stvaranje dezinformacija i hibridnih prijetnji i ostvarivanje prikrivenih političkih ciljeva, bez obzira radilo se o stanjima rata ili mira, kriza ili poraća.

Zbog toga znanstvena i akademska zajednica o fenomenu stvaranja dezinformacija na društvenim mrežama treba pružiti dodatne znanstvene dokaze te je nužno provoditi dodatna istraživanja o štetnim posljedicama zloupotrebe osobnih podataka građana, tehnologija umjetne inteligencije koja ih obrađuje i uloge lažnih profila na društvenim mrežama za stvaranje dezinformacija i hibridnih prijetnji.

Doktorska disertacija može dati doprinos za izradu i institucionaliziranje proaktivnog i učinkovitog pristupa s iscrtanim procedurama za identifikaciju novih oblika prijetnji iz kiber prostora koje proizlaze iz automatiziranih, anonimnih i masovnih dezinformacija prilagođenih društvenim slabostima i iz negativnih manifestacija dezinformacija na organizaciju javnog znanja te na različite društvene i političke procese i krize. Ovakve krize nastaju kao posljedica neadekvatne zaštite osobnih podataka na društvenim mrežama i zloupotrebe tehnologija umjetne inteligencije koje obavljaju temeljne zadaće društvenih mreža. Istraživanje se može koristiti za stvaranje nacionalne obrambene i informacijske politike, posebice obavještajnih procedura koje bi mogle biti osnova za donošenje pravovremenih i učinkovitih protuodgovora i informacija o namjerama, sposobnostima i društvenim slabostima državnih i nedržavnih aktera koji planiraju i izvode dezinformacijske kampanje pomoću društvenih mreža.

Ključne riječi: kiber prostor, nacionalne informacijske strategije, društvene mreže, umjetna inteligencija, dezinformacije, hibridna inteligencija, psihološke operacije, hibridne operacije, hibridni sukobi, hibridno ratovanje, hibridne prijetnje, hibridna obrana.

2. INFORMACIJSKI PROSTOR I NOVI OBRASCI ORGANIZIRANJA PODATAKA I INFORMACIJA

2.1. Nastanak informacijskog prostora

Ideje i vizije o nastanku globalne informacijske infrastrukture i globalnog informacijskog prostora iz sredine 1990-ih predstavljene su interesom za stvaranje nove digitalne kulture i civilizacije u kojoj će sve znanje u digitalnoj formi biti dostupno svima. Jedno od temeljnih ljudskih prava, pravo na informaciju i pravo na slobodan pristup informacijama, trebalo je postati glavna osnova za stvaranje globalnog informacijskog društva, pretpostavka održivog razvoja te pokretačka sila novog svjetskog poretka. [11]

Ove ideje razvijale su se s dva gledišta. Jedno gledište je civilno s društveno-političkog, a drugo vojno s obrambeno-napadačkog gledišta. Prema društveno-političkom gledištu razvoj globalne informacijske infrastrukture i novog globalnog informacijskog prostora trebao je osigurati slobodan pristup informacijama, stvaranje znanja kojim bi se rješavala većina problema suvremenog društva i unaprjeđivala demokracija. Prema vojnom obrambeno-napadačkom gledištu nastanak novog informacijskog prostora predstavljao je priliku za razvoj novog borbenog prostora i korištenje informacijsko-komunikacijskih sustava i računalnih tehnologija za upravljanje informacijama u cilju (pre)oblikovanja ljudskog razmišljanja i donošenja odluka.

Globalna informacijska infrastruktura i globalni informacijski prostor nastali su na razvoju informacijsko-komunikacijskih sustava i računalnih tehnologija umjetne inteligencije, temeljem kojih su nastale društvene mreže - alati koji omogućavaju globalnu, masovnu i umreženu komunikaciju te razmjenu podataka, obavijesti, informacija i ideja. U informacijskom prostoru javnog znanja i na društvenim mrežama umjetna inteligencija dobila je presudnu ulogu u obavljanju ključnih funkcija i temeljnih zadaća: organiziranje ogromne količine podataka, obavijesti i informacija kroz prikupljanje, pohranu i obradu u digitaliziranim formama a u svrhu njihovog korištenja, prikazivanja i dostavljanja na nove digitalizirane načine. Došlo je do nove forme organiziranja podataka i informacija te znanja u javnom informacijskom prostoru.

Unutar javnog informacijskog prostora postoji korpus javnog znanja „koji je određen sadržajem koji postoji u javnome informacijskom prostoru koji u njemu ima dominantni položaj

11 Usp. Tuđman, 2008, str. 45-46.

i status.“[12] Korpus (prostor) javnog znanja „uglavnom, oblikuje se utjecajem različitih javnih medija.“[13] Različita društva i zajednice određuju korpuse javnog znanja koji mogu biti bitno različitog sadržaja. Postoje i druge odrednice organizacije znanja. Međutim oni nisu predmet dubljeg istraživanja.[14] Informacijska i komunikacijska tehnologija, djelatnost i oprema koja čini tehničku osnovu za sustavno prikupljanje, pohranjivanje, obradbu, širenje i razmjenu informacija različita oblika, tj. znakova, teksta, zvuka i slike, donijela je takve promjene u suvremenome društvu razvijenih zemalja da se ono s pravom naziva informacijskim društvom.[15]

Znanje informacijskog društva postalo je digitalizirano. Digitalizirane forme i načini organizacije podataka, obavijesti i informacija razvojem informacijskih tehnologija doveli su do radikalnih promjena u stvaranju i prenošenju predmeta obavijesti i činjenica, ali i predmeta javnoga znanja.

„Podaci imaju numeričku vrijednost, predstavljaju informacije i mogu biti zapisani u obliku signala. Da bi ostvarili interakciju s fizičkim svijetom, podaci se prevode u signale i obrnuto. U općem smislu, signal predstavlja funkciju koja nosi informaciju o ponašanju ili atributima nekog fenomena. U teoriji informacija signal predstavlja kodificiranu poruku.“ Tradicionalno, signal predstavlja „fizičku manifestaciju informacije koja se mijenja kroz prostor i/ili vrijeme“[16], ali isto tako i apstraktnu informaciju koja postoji u informacijskom ili biološkom području (na primjer molekula DNK sagrađena od gena).“[17] „Pri tome je obrada signala tehnologija koja omogućava obuhvaćanje fundamentalne teorije, aplikacija, algoritama i primjene obrade ili prijenosa informacija koje postoje u mnogim različitim fizičkim, simboličkim ili apstraktnim oblicima generalno označenim kao signali i koja koristi

12 Akrap Gordan, Informacijske strategije i oblikovanje javnog znanja, National Security and Future, Svezak 10, br. 2., 2009., dostupno na: https://hrcak.srce.hr/80639

13 Ibid.

14 O organizaciji i vrstama znanja vidi više Tuđman M., Informacijsko ratište i informacijska znanost, Zagreb 2008. str. 48.-86., Tuđman M., Programiranje istine, Rasprava o preraspodjelama društvenih zaliha znanja, Zagreb, 2013. i Akrap G., Informacijske strategije i operacije u oblikovanju javnog znanja, Doktorska disertacija, Filozofski fakultet, Zagreb, 2011. str. 8.-11.

15 Informacijska i komunikacijska tehnologija. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Pristupljeno 17. 2. 2022. http://www.enciklopedija.hr/Natuknica.aspx?ID=27406

16 Mladenović, 2016., str. 85., prema: Jose M.F. Moura, „What Is Signal Processing?“, IEEE Signal Processing Magazine, 26, no. 6 (2009), 6, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5230869 (preuzeto 18. avgusta 2015).

17 Mladenović, str. 85.

matematičke, statističke, računarske, heurističke i/ili lingvističke reprezentacije, formalizme i tehnike za predstavljanje, modeliranje, analizu, sintezu, otkrivanje, oporavljanje, očitavanje, dobavljanje, izdvajanje, učenje, sigurnost ili forenziku“.[18] Osnove svih informacijskih tehnologija ogledaju se u mogućnostima njihove međusobne interakcije na nivou podataka, a te osnove nalaze se u samom načinu matematičko-logičke interpretacije i obrade podataka. Primjena tehnologija omogućila je matematičko-logičke interpretacije i obradu podataka, koji u suvremenoj praksi mogu biti neograničeni broj puta konvertirani u nekom od elektromagnetnih oblika zapisa: elektronskom, magnetnom, svjetlosnom ili kvantnom.[19]

„Informacija ili obavijest (lat. informatio: nacrtak, predodžba, pojam, tumačenje) skup je podataka s pripisanim značenjem, osnovni element komunikacije koji, primljeni u određenoj situaciji, povećavaju čovjekovo znanje. Čovjek stječe znanje iskustvom, učenjem i informiranjem (obavješćivanjem). Preko svojih osjetila čovjek prima informacije u obliku skupova podataka. Može ih primati izravno, prirodnim kanalima ili posredno, umjetnim kanalima uz pomoć informacijske i komunikacijske tehnologije.“[20] „Uobičajena je postavka da su obavijesti prikaz pojava, podataka i događaja.“[21] Pojave su pak sve što nas okružuje, sve što se događa oko nas. „Podaci sami za sebe nemaju značenje, oni su signali koji prikazuju pojave pa njihovo puko gomilanje ne pridonosi razumijevanju pojave na koju se odnose. Podaci se sastoje od skupa kvantitativnih parametara koji opisuju neku činjenicu ili zbivanje. Podaci su, međutim, osnova za oblikovanje informacije. Informacija nastaje pripisivanjem značenja primljenim podacima.“[22] Percepcija je pak čin koji obuhvaća i prijam i poimanje signala, a tu novu cjelinu percipiranih signala predstavlja podatak.[23] Obavijesti ne predstavljaju činjenice i one nisu isto. Obavijesti prenose poruke o događajima i pojavama te iz njih doznajemo o tim pojavama i događajima. Činjenice su produkt prosudbe koje se temelje na dokazima, da bi prosudba o pojedinim događajima bila istinita.[24] „Ključnu ulogu u pretvorbi podataka u

18 Ibid.

19 Usp. Ibid. str. 84.

20 Informacija. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Pristupljeno 17. 2. 2022. http://www.enciklopedija.hr/Natuknica.aspx?ID=27405

21 Tuđman, 2008., str. 119.

22 Ibid.

23 Ibid.

24 Ibid., str. 158.

informaciju ima dakle znanje kojim čovjek raspolaže.“[25] „Ono mu omogućuje razumijevanje informacije, odnosno prepoznavanje podataka, jezika kojim su ti podatci povezani u informaciju i konteksta na koji se odnose.“[26] „Znanje kojim čovjek raspolaže čini okruženje za tumačenje (interpretaciju) i vrednovanje novih informacija, a time i stvaranje novoga znanja. U tome je procesu značajna i mogućnost pamćenja informacija (unutarnje pamćenje) i njihova zapisivanja (vanjsko pamćenje). Uz informacije koje oblikuje na temelju primljenih podataka, pojedinac može izravno oblikovati informaciju na temelju znanja kojim raspolaže. Oblikovane informacije mogu se drugim pojedincima prenositi u obliku poruka. Zahvaljujući informacijskoj i komunikacijskoj tehnologiji u današnje su doba raznovrsni oblici informacija postali dostupnima velikomu broju ljudi. Razmjenom informacija među pojedincima stvara se zajednički korpus znanja.“[27]

Digitalizacija javnog znanja, podataka, obavijesti i globalizacija društva, osim pozitivnih strana, pokazala je i svoje tamne strane. Obavijesti (informacije) nisu samo čimbenici razvoja i blagostanja, nego su dobile i niz novih neželjenih i zlonamjernih atributa i primjena. Informacija je postala oružje, globalni prostor javnog znanja postao je bojište, a informacijsko-komunikacijski sustavi i računalne tehnologije umjetne inteligencije koje koriste društvene mreže preuzele su glavnu ulogu u organiziranju podataka, njihovoj pretvorbi u obavijesti (informacije) te znanja. Društvene mreže kao novi netradicionalni medijski kanal preuzele su ulogu posrednika u prenošenju informacija koju su imali tradicionalni mediji (tisak, tv, radio). Postale su digitalni posrednici te su omogućile izravne mogućnosti utjecaja na percepciju, prosudbe, realnost i na organizaciju znanja bez prostornog i vremenskog ograničenja. Znanje je postalo umreženo i automatizirano u stvaranju i raspodjeli, globalno dostupno svima u realnom vremenu. Došlo je do transformacije dotadašnje forme stvaranja, pristupanja, dijeljenja i prezentiranja podataka, obavijesti (informacija), činjenica i te znanja. Korisnici prostora javnog znanja i društvenih mreža postali su stvaraoci obavijesti (informacija), različitih informacijskih sadržaja u različitim digitalnim oblicima te znanja a ne više samo njihovi pasivni konzumenti.[28] Međutim, bez obzira na njihovu točnost i objektivnost, nova tehnološka paradigma - trenutačna komunikacija i neprekinuti protok informacija „mnoštvo na mnoštvo“

25 Informacija. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Pristupljeno 17. 2. 2022. http://www.enciklopedija.hr/Natuknica.aspx?ID=27405

26 Ibid.

27 Ibid.

28 Usp. Akrap, 2011., str 88.

koja je konstantna (24/7) – izravnala je geografske udaljenosti, političke granice i potrebno vrijeme i napor da ih informacije pređu. Društvene mreže „u prostoru javnog znanja ne služe samo za prijenos obavijesti i informacija s ciljem obavještavanja djela javnosti, već služe kao snažni i učinkoviti alati utjecaja pomoću kojih se prostor javnog znanja oblikuje, uzrokuju i vode procesi promjene tog znanja ili se pomoću njih djeluje sukladno interesima koji ih pokreću.“[29]

Primjena umjetne inteligencije u obavljanju osnovnih funkcija i temeljnih zadaća na društvenim mrežama u prikupljanju, pohrani, obradi i preoblikovanju podataka u obavijesti (informacije) bitno je utjecala i na oblikovanje prostora javnog znanja: Temeljna obilježja ovakvih preoblika su da je znanje ostalo bez subjekta spoznaje tj. došlo je do proizvodnje znanja neovisno od subjekta spoznaje, da su informacije postale supstrat znanja te da je došlo do institucionalizacije informacijskog poretka.[30] Informacijska tehnologija oduzela je čovjeku primat autorstva nad znanjem: znanje je zadobilo autonomiju i funkcionira bez subjekta spoznaje.“[31] „Nastao je rez između forme obavijesti i sadržaja obavijesti.“[32] „Obavijesti više ne prikazuju sadržaj nekog objekta u realnom svijetu.“ „Drugim riječima, informacijsko-komunikacijska funkcija ima dominaciju nad spoznajom. Posljedice su očite: prikaz događaja prestigao je razumijevanje zbilje pa su informacije zamijenile znanja. Odnosno, informacije su se razdvojile, otrgle od znanja, a budući da je pitanje istine temeljna odrednica znanja, i informacije su se odmakle od istine.“[33] „Došlo je do urušavanja stvarnosti u hiperrealizam, u brižno podvostručavanje stvarnosti“,[34] na osnovi koje korisnici javnog znanja organiziraju svoj život, odluke i ponašanja. „Ovakvi prikazi realnosti postali su njihova realnost koju doživljavaju kao točniju i pouzdaniju od same realnosti.“[35]

U novom informacijskom poretku „globalna informacijska infrastruktura i planetarne mreže generiraju podatke nad kojima ni jedan pojedinac više nema kontrole, često ni spoznaje kako

---

29 Ibid.

30 Tuđman Miroslav, Programiranje istine, Rasprava o preraspodjelama društvenih zaliha znanja, Hrvatska Sveučilišna zaklada, Zagreb, 2013., str.181.

31Tuđman, 2013., str. 180.

32 Tuđman, 2008, str. 20.

33 Tuđman, 2013., str. 180.

34 Tuđman, 2008., str. 154.; prema J. Baudrillard, 2001., str. 101.

35 Ibid., str. 40.

su nastali ni gdje su sve nastali, niti tko ih je sve generirao. A vjerojatno ni tko ih sve posjeduje.“[36] U ovako mrežnom generiranju i distribuciji podataka posljedično „Čovjek više nema drugačijeg pristupa ni stvarima ni drugim ljudima, nego posredstvom podataka i informacija. Nemati izbora, znači biti osuđen na podatke i informacije, te biti u vlasti informacijskih mreža i sustava“.[37] „Drugim riječima, nije uputno poistovjetiti informacije i znanje. Informacija u najboljem slučaju nudi odgovor na pitanje što, a znanje na pitanje kako i zašto. Davanje prednosti informacijama nije defekt kognitivne kompetencije, nego nezainteresiranost za razumijevanje zbilje, odnosno nehtijenja da se razumiju uzroci i razlozi pojava i događaja. Za razliku od nacionalnih, regionalnih i lokalnih informacijskih prostora, globalni informacijski prostor umrežena je, decentralizirana ali globalno nedjeljiva „tvorevina“, odnosno infrastruktura suvremene civilizacije. Zato filozofiju razvoja globalnog informacijskog prostora nije netočno povezivati i s politikom globalizacije, preciznije s politikama informacijske dominacije na globalnoj razini. Jer globalna informacijsko-komunikacijska infrastruktura pretpostavka je uspostave globalne dominacije u informacijskom prostoru.“[38]

U digitaliziranom prostoru (korpusu) javnog znanja više nije moguće napraviti razliku između prikaza objekta i samog objekta. Globalna informacijska transformacija i primjena umjetne inteligencije u informacijskim i komunikacijskim mrežama i sustavima planetarnih mreža, sa svojom svrhom i zadaćom koja joj je određena ljudskim čimbenikom, urušila je tradicionalnu predodžbu o prostoru i vremenu. Nastala je digitalna stvarnost koja je postala stvarnost koja nije fikcija niti je „virtualna“[39] kao što ni znanje koje se u njoj stvara nije virtualno. Ono je virtualno samo po prostoru u kojem nastaje, ali ne i po učincima: ono ima realne psihološke i socijalne, političke i gospodarske učinke.“ „Virtualna stvarnost“ proizvodi korpus realnog javnog znanja, samo što taj korpus nije valoriziran prema kriteriju istine jer je u oblikovanju korpusa javnog znanja komunikacijska funkcija postala važnija od spoznajne funkcije.“[40] „Podaci sad nastaju generiranjem iz različitih automatiziranih izvora ili umrežavanjem većeg broja baza podataka. Informacije ne ovise više o čovjeku, pojedincu, nego o preciznosti i

36 Ibid.

37 Ibid.

38 Ibid.

39 Ibid., str. 22.

40 Ibid., str. 154.

učinkovitosti sustava koji generiraju te podatke“.[41] Društvene mreže s primijenjenim algoritmima i rješenjima umjetne inteligencije u prikupljanju i obradi podataka i njihovih preoblika u prikazivanju obavijesti (informacija) glavni su kreatori i upravitelji nove digitalne „virtualne stvarnosti“. Na društvenim mrežama „više nema čvrstog kriterija za novo određenje istine, obavijesti na njima izgubile su značenje a njihova zadaća nije na razmjeni istinitih, nego korisnih (relevantnih) obavijesti. S pravom se može postaviti pitanje: Ako ne znamo što je istina, kako možemo znati što je dobro i što je pravedno u tom novom digitalnom svijetu.“ [42]

U novom globaliziranom informacijskom prostoru i informacijskom poretku prepletenom planetarnim mrežama „svjedoci smo dekonstrukcije temeljnih postavki i paradigme informacijske znanosti i njezina predmeta: informacije su sve manje istinite i objektivne, sve češće su pogrešne, neistinite i lažne, šire se s namjerom da se njima dezinformira i manipulira te ih se ciljano usmjerava prema korisnicima prostora javnog znanja. Korisnici na ovaj način stvorenog znanja „prema toj činjenici ostali su ravnodušni jer su informacije izgubile značenje, a njezini korisnici traže prvenstveno njihov smisao.“[43] Posljedično došlo je do dekonstrukcije objektivnog znanja. Uloga, način i pravila koja diktiraju društvene mreže predstavljaju novu referencu informacijske znanosti u kojoj je došlo „do poremećaja u postulatu objektivnosti, kognitivnoj hijerarhiji (od podatka, obavijesti do znanja) te prikaza sadržaja obavijesti da bi se one mogle koristiti kao istinit podatak i objektivnu činjenicu“.[44] Korisnicima ovakvog znanja „na raspolaganju su im ogromne količine informacija, ali do znanja teško mogu doći“ jer je u nastaloj dominaciji digitalne stvarnosti i digitalnih posrednika došlo do „odvajanja riječi od realnosti“[45]. Novi digitalni posrednici, društvene mreže, time ujedno odlučuju o stvaranju znanja koje se ne temelji na osnovnim postavkama i paradigmama informacijske znanosti, već prema interesima i pravilima koje sami nameću. Prema njihovim interesima i pravilima „znanje postoji ako je isplativo, a proizvodi se ako je unosno“.[46]

Primjena umjetne inteligencije na društvenim mrežama omogućila je matematičko-logičke interpretacije i obradu podataka koji sada mogu biti neograničeni broj puta konvertirani u

41 Ibid.

42 Ibid., str. 24.

43 Ibid., str. 17.-18.

44 Ibid., str. 19.

45 Ibid., str. 21; prema J. Lotman, 1998., str.155.

46 Ibid., str. 17.-18.

digitalni oblik zapisa. Time je donijela ključnu paradigmu u obradi podataka: podatke korisnika moguće je preoblikovati u obavijesti i informacije prema sklonostima i interesima, odnosno korisničkim preferencijama. Na osnovi ove mogućnosti, za komercijalne potrebe moguće je mijenjati i stvarnost. Osobni podaci korisnika društvenih mreža, njihova uvjerenja, načela i vrijednosti, postali su „imovina“ njezinih vlasnika koja ima svoju tržišnu vrijednost.

Novim obrascem u organiziranju podataka i informacija te stvaranju znanja, društvene mreže dovele su do urušavanja monopola moći u kontroli nad procesima stvaranja i dijeljenja obavijesti, informacija i znanja. Globalna distribucija znanja prema novim pravilima nije razgradila tradicionalna središta moći koju su imale države i tradicionalni mediji, nego je s ovih središta moć pomaknuta prema društvenim mrežama. S ulogom digitalnih nadzornika pristupima podacima i obavijestima, društvene mreže postale su najmoćniji alati utjecaja u informacijskom dobu. Moć u njemu ostvaruje onaj koji nove tehnologije bolje iskorištava za vlastite potrebe.[47] Društvene mreže u ulozi digitalnih nadzornika podataka, informacija i znanja u javnom prostoru donijele su novu dimenziju u odnosima „gospodar-sluga“. Društvene mreže postale su kontrolori podataka i informacija u informacijskom društvu i prostoru te pristupa obavijestima. One su „postali gospodari, a korisnici njihovih usluga su jedva svjesni da su „sluge“ jer imaju pristup mnoštvu informacija, ali bez uvida u strategije njihove distribucije.“ „Običan“ korisnik obično ne zna da je njegov pristup informacijama kontroliran od malog broja ljudi, iz središta moći, koji odlučuju o pristupu određenim prijenosnicima, ali i o načinu prezentiranja informacija.“[48] Društvene mreže, dakle, imaju moć nadziranja i upravljanja znanjem. Njihova zadaća nije organizirati i prenositi istinite podatke, obavijesti i informacije. Njihova zadaća je oblikovati i osigurati dominaciju samo određenih informacija prema sklonostima i interesima, odnosno korisničkim preferencijama. Time su postale glavna prepreka u raspodjeli objektivnog znanja. Glavni uzroci mogu se sagledati kroz nekoliko činjenica. Društvene mreže nastale su u digitaliziranom prostoru javnog znanja u kojem još uvijek ne postoje adekvatni mehanizmi kontrole javnog znanja prema kriteriju istine i objektivnosti. Osim toga, nema adekvatnih pravila i normi, kao ni volje vlasnika društvenih mreža da se one uvedu, kojima bi se na adekvatan način regulirala, odnosno spriječila zloupotreba umjetne inteligencije u upravljanju podacima, obavijestima i informacijama na društvenim mrežama, odnosno nema adekvatne volje da se umjetna inteligencija koristi prema

47 Usp. Tuđman, 2008., str 154.

48 Tuđman, 2008., str 43.

temeljnim načelima koja vrijede za prostor javnog znanja, a to su transparentnost i pravo na pouzdanu i točnu informaciju.

Društvene mreže aktivno koristi 58,4% ukupne svjetske populacije.[49] Svim korisnicima omogućeno je da na njima stvaraju i organiziraju znanje, ali i da se sukobljavaju i bespoštedno bore za svoje interese, da se obavijesti i informacije uobličavaju prema korisničkim preferencijama, bez stvarnog i adekvatnog preuzimanja odgovornosti za napisanu i podijeljenu riječ.

Zbog nepostojanja adekvatnih mehanizama nadzora, adekvatnih zakonodavnih normi ponašanja i penalizacije globalnog dosega, porasle su mogućnosti njihove zloupotrebe u napadačkim aktivnostima sa svrhom (pre)oblikovanja protivničkog prostora (korpusa) javnog znanja prema potrebama napadača. Društvene mreže postale su ključni čimbenici planiranja i izvođenja digitaliziranih formi napadačkih informacijskih operacija – psiholoških operacija koje se, zahvaljujući tehnologijama umjetne inteligencije primijenjenim na društvenim mrežama, mogu provoditi na daleko učinkovitije načine. Za vlastite potrebe i interese društvene mreže iskorištava sve veći broj državnih i nedržavnih aktera, korporacija, organizacija i sl. Primijenjene tehnologije postale su time i problem obrane od dezinformacija i različitih vrsta prijetnji. Obrana od dezinformacija postala je ključno pitanje i daleko složenija nego u vrijeme kad su se stvarali informacijsko-komunikacijski sustavi i tehnologije umjetne inteligencije na osnovi kojih su nekoliko desetljeća kasnije nastale društvene mreže.

2.2. Nastanak kiber prostora i društvenih mreža

Procesi koji su odredili nastanak kiber prostora su digitalizacija informacijskog prostora javnog znanja i daljnji razvoj informacijsko-komunikacijskih tehnologija, uključujući računala i računalne mreže te umrežavanje ovih tehnologija. Terminom kiber prostor opisuje se prostor koji je dio informacijskog prostora i u kojem se odvija glavnina suvremenih informacijskih i psiholoških operacija kojima se vodi borba za razmišljanje i donošenje odluka. Glavni alati borbe postale su tehnologije na kojima počiva i sam nastanak kiber prostora i koje odražavaju njegove osnovne karakteristike, a to su informacijsko-komunikacijski sustavi i višedimenzionalne računalne tehnologije umjetne inteligencije. Informacijsko-komunikacijski

49 We are Social, Digital 2022., We are Social, DIGITAL 2022: GLOBAL OVERVIEW REPORT, dostupno na https://datareportal.com/reports/digital-2022-global-overview-report , (26.01.2022.).

sustavi i umjetna inteligencija predstavljaju tehnološki aspekt kiber prostora, odnosno njihova pojava i razvoj odredila je njegov nastanak i razvoj. Kiber prostor predstavlja tehnološku osnovu digitalizacije informacijskog prostora (korpusa) javnog znanja.

Međutim, tvorci kiber prostora nisu uspjeli izgraditi i uspostaviti adekvatna pravila prema kojima bi se unutar njega reguliralo ponašanje niti pravila koja bi se primijenila na umjetnu inteligenciju u prikupljanju i obradi podataka, obavijesti i informacija. Posljedično, kiber prostor pretvorio se u bojište, a umjetna inteligencija postala je alat za nametanje volje i stjecanje informacijske nadmoći različitih aktera (državnih, nedržavnih i korporacija) nad korpusom znanja ciljanih publika. „Informacijska nadmoć predstavlja stanje pri kojem je jedna od strana u informacijskom sukobu preuzela kontrolu i nadzor nad protivničkim informacijsko-komunikacijskim sustavom, informacijskim sadržajem ili ključnim osobama uz istovremenu zaštitu vlastitih potencijala, čime su stvoreni uvjeti za utjecaj na ciljane publike na strateškoj razini odlučivanja i djelovanja.“[50] Predviđanja vojnih stratega s početka 1990-ih time su se obistinila na štetu temeljnih ljudskih i društvenih normi transparentnosti i zaštite ljudskih prava; sprječavanja monopola, cenzure i širenja dezinformacija, normi odgovornosti za nešto što je napisano, objavljeno i podijeljeno te na štetu temeljnih načela koja vrijede za prostor javnog znanja transparentnosti i prava na pouzdanu i točnu informaciju.

Termin kiber prostor nastao je i razvijao se paralelno s razvojem i primjenom računalne znanosti, informacijsko-komunikacijskih sustava i tehnologija za potrebe obrambene industrije u SAD-u i Velikoj Britaniji. Njegov razvoj odvijao se u sklopu programa Strategijske računarske inicijative. U sklopu obrambene industrije SAD-a paralelno su se razvijali i istraživački projekti i tehnologije u području računarstva i umrežavanja čiji rezultati predstavljaju osnovu računarstva, informacijsko-komunikacijskih tehnologija koje su danas u širokoj upotrebi postale tehnološka osnova kiber prostora, umjetne inteligencije i društvenih mreža. Primarni i strateški dugoročni cilj Strategijske računarske inicijative bilo je ostvarivanje umjetne inteligencije, odnosno „započinjanje integriranog plana promocije razvoja dizajna i proizvodnje računalnog procesora, računalne arhitekture i programa umjetne inteligencije“.[51] Temelji umjetnoj inteligenciji postavljeni su davno prije, „kroz filozofski pristup u opisivanju procesa ljudskog razmišljanja kao mehaničke manipulacije simbolima. Alan Turing 1936.

50 Akrap, 2011., str 310.

51 Mladenović Dragan, Multidisciplinarni aspekti kiber ratovanja, Fakultet organizacijskih znanosti Sveučilišta u Beogradu, 2016., str. 51.-54.

razvio je informatičko računalo, tzv. Turingov stroj, što je rezultiralo mogućnošću kojom se neživo može učiniti inteligentnim.“ „Time je pokazao kako je moguće izumiti stroj koji se može koristiti za izračunavanje bilo kojega kompjutacijskog procesa ili se njime može riješiti bilo koji algoritam.“[52] „Među pionirskim radovima umjetne inteligencije je i rad kojim je Claude Shannon opisao programiranje računala za igranje šaha. Razvijen je program koji samostalno izvodi logičke teoreme, odnosno osposobljen je za automatsko rasuđivanje. Nazvan Teoretičar logike bio je to program osmišljen kako bi oponašao čovjekove vještine rješavanja problema, a financirala ga je američka Korporacija za istraživanje i razvoj (RAND). Mnogi ga smatraju prvim programom umjetne inteligencije, a predstavljen je na Ljetnom istraživačkom projektu umjetne inteligencije u Dartmouthu, koji su 1956. ugostili John McCarthy i Marvin Minsky.“[53] Na ovoj povijesnoj konferenciji, McCarthy je, zajedno sa znanstvenicima iz raznih područja, osmislio pojam “Umjetna inteligencija” a konferencija je odredila sljedećih dvadeset godina istraživanja umjetne inteligencije. „Ubrzo je razvijen prvi jezik umjetne inteligencije LISP (List Processing) 1958. Predstavljen je iAdvice Taker – prvi cjelovit sustav umjetne inteligencije i cjelovita kognitivna teorija uma. Prvi uspješan model ljudskoga mišljenja, nazvan General Problem Solver – GPS, 1961. razvili su Newell i Simon. Formu neuralne mreže PERCEPTRON 1962. razvio je Rosenblatt. Ova mreža se i danas koristi, a njome je pokazano kako algoritam za učenje može prilagoditi snagu veza perceptrona da se usklade s bilo kojim ulazom.“[54] Od 1957. do 1974. umjetna inteligencija postala je vrlo zastupljena. „Računala su mogla pohraniti više informacija i postala su brža, jeftinija i pristupačnija. Algoritmi strojnog učenja također su se poboljšali i ljudi su postajali bolji u znanju koji algoritam primijeniti na svoj problem. Sredinom dvadesetoga stoljeća počela se razvijati i kibernetika kao interdisciplinarna znanost koja se bavi kontrolnim sustavima. Usmjerena je na proučavanje upravljanja u živim bićima, strojevima i njihovim kombinacijama. Napravljena su računala za inteligentno komuniciranje s ljudima.“[55] „Prva tri desetljeća razvoja umjetne inteligencije u različitim istraživanjima rezultirala su zajedničkom paradigmom, nazvanom simbolička umjetna inteligencija jer joj je središnji princip glasio kako je inteligencija manipulacija simbolima. Razvoj je započela s ciljem izgradnje inteligentnih računalnih sustava kako bi se stvorio sustav koji posjeduje

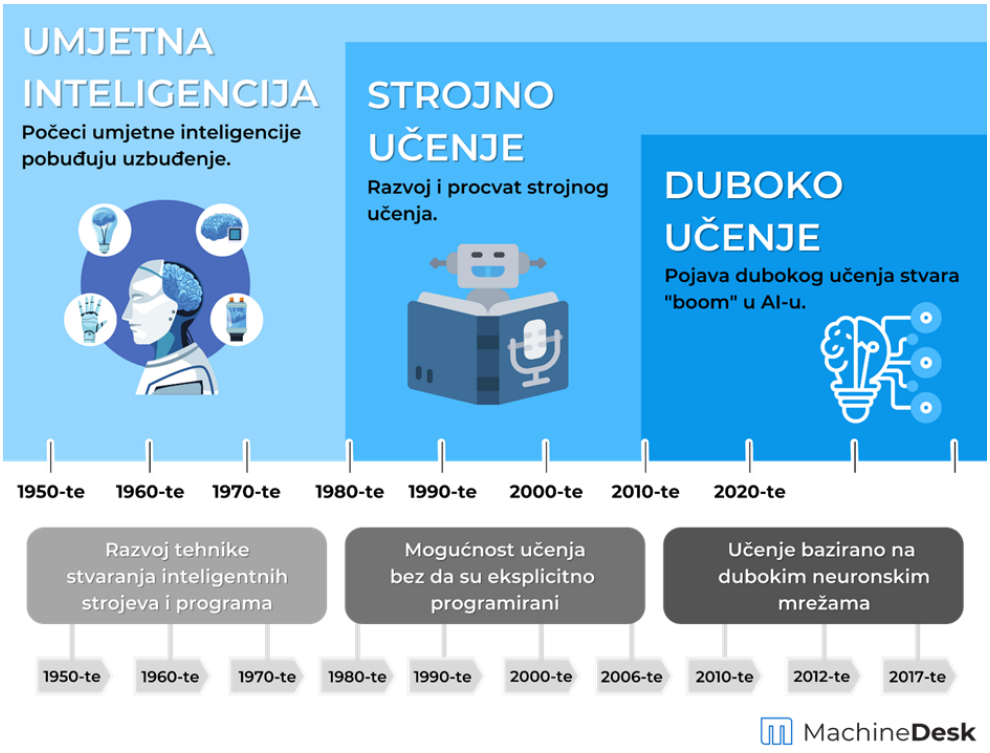
52 Putica Marija, Umjetna inteligencija: Dvojbe suvremenog razvoja, Filozofski fakultet Sveučilišta u Mostaru, 2018, str. 202.-204.

53 Ibid.

54 Ibid.

55 Ibid.

univerzalnu inteligenciju. Takav bi sustav posjedovao univerzalnu sposobnost razmišljanja, rješavanja problema, razumijevanja jezika i obavljanja svih ostalih aktivnosti primjerenih odraslim inteligentnim ljudima.“[56] Prije 1949. „računala nisu imala ključni preduvjet za inteligenciju: nisu mogla pohranjivati naredbe, već ih samo izvršavati. Drugim riječima, računalima se moglo reći što trebaju raditi, ali se nisu mogla sjetiti što su učinila. Drugo, računarstvo je bilo izuzetno skupo tako da su samo prestižna sveučilišta i velike tehnološke tvrtke mogle priuštiti rad na računalima. Sedamdesetih godina 20 st. nastali su i prvi programi za razumijevanje prirodnoga jezika. Tijekom 1980-ih uslijedila je izgradnja ekspertnih sustava za specifične potrebe, došlo je do razvoja robotike te je obnovljen interes za razvoj umjetnih neuronskih mreža. Robotika, strojni vid, strojno učenje umjetnih neuronskih mreža danas su snažno prisutni u umjetnoj inteligenciji“[57] koja se sveobuhvatno primjenjuje u obnašanju osnovnih zadaća i funkcija društvenih mreža: u prikupljanju, pohrani, preoblikama te isporučivanju informacija uobličenih prema korisničkim načelima, uvjerenjima i vrijednostima.



Izvor: Markotić, Umjetna inteligencija - Sve što trebate znati.

Slika 1. Prikaz razvoja tehnologija umjetne inteligencije od 1950-ih do 2017-e.

56 Ibid., str. 205.

57 Ibid.

Slika 1. prikazuje razvoj i napredak u primjeni tehnologija umjetne inteligencije u razdoblju od 1950-ih do 2020-ih u kojem je od 1950-ih do 1970-ih bio označen snažnim interesom za razvoj tehnika stvaranja inteligentnih strojeva i programa, zatim razdoblje od 1980. do 2010., u kojem je razvijeno strojno učenje te razdoblje od 2010-ih do 2020-ih u kojem je razvijeno duboko učenje na bazi dubokih neuronskih mreža. Važno je naglasiti da je primjena nastalih programa i umjetne inteligencije, ponajprije strojnog učenja, sredinom 2000-tih rezultirala pojavom društvenih mreža novog komercijalnog proizvoda visoko tehnoloških korporacija. Kiber prostor i društvene mreže kakve poznajemo rezultat su razvoja i unaprjeđivanja računalnih tehnologija umjetne inteligencije koja se inicijalno razvijala za vojne potrebe. „Internet, početna osnova i najveća globalna mreža u konceptu koji se danas naziva kiber prostor, tehnički je razvijan i kreiran u periodu od kraja šezdesetih do početka devedesetih godina 20. st. u više projekata kojima je u osnovi bio projekt ARPANET Ministarstva obrane SAD-a. Cilj projekta ARPANET, pokrenutog 1969., bilo je kreiranje nacionalne vojne komunikacijske mreže sposobne da preživi razaranja mrežne infrastrukture u potencijalnom nuklearnom ratu. Zbog toga je osnova programa bila izgradnja mreže između udaljenih vojnih centara i komandi s distribuiranim i decentraliziranim čvorištima, sposobnih da dinamično mijenjaju mrežnu topologiju. Ovaj vojni projekt doživio je nagli razvoj kada su u njega, pored Ministarstva obrane SAD-a, uključeni predstavnici civilne akademske zajednice, sveučilišni centri, znanstveno-istraživačka zajednica vodećih američkih sveučilišta u području računalnih znanosti i informacijsko-komunikacijskih tehnologija te znanstveno-istraživačka Agencija za napredne istraživačke projekte (engl. Advanced Research Projects Agency – ARPA).[58] „ARPA je preteča današnje agencije DARPA (United States Defense Advanced Research Project Agency). Osnovana je 1958., s ciljem rukovođenja znanstveno-istraživačkim projektima radi ostvarivanja proboja u postojećim znanjima u području tehnologije i znanosti koji su od značaja za obrambene potrebe. Promijenila je ime u Defense Advanced Research Projects Agency (DARPA) 1972. Osnovala ju je Vlada SAD-a zbog obrambeno-političkih razloga, kao odgovor na prethodne uspjehe Sovjetskog Saveza u razvoju i primjeni svemirske tehnologije, poput uspješnog lansiranja prvog umjetnog satelita Sputnjik u Zemljinu orbitu 1957. DARPA projekte ne izvodi neposredno, već ih planira, organizira, vodi i financira.“[59] Tako je „DARPA financirala te je dala značajan doprinos u istraživanju umjetne inteligencije za potrebe Vlade

58 Usp. Mladenović, 2016, str. 51-54.

59 Ibid.

SAD-a koja je bila zainteresirana za razvijanje stroja koji može transkribirati i prevesti govorni jezik te obrađivati podatke velike propusnosti.“[60] Osamdesetih godina 20. stoljeća razvoj umjetne inteligencije obilježila je popularizacija tehnike "dubokog učenja" koja je omogućila računalima da uče koristeći iskustvo. „Od 1983., Ministarstvo obrane SAD-a je u odvojenom projektu počelo razvijati novu, sigurnosnu mrežu MILNET, a ARPANET je nastavio život u obliku nove mreže NSFNET od koje je nastao suvremeni Internet početkom devedesetih godina 20. st.“[61] Prve godine interneta u SAD-u bile su obilježene slobodarskim optimizmom o promociji slobode u pristupu informacijama. Razvoj globalne informacijske infrastrukture te prostora poznatog kao internet i novih sustava za komuniciranje unutar takvog prostora, doveo je do novih mogućnosti za ostvarivanje vanjskopolitičkih interesa. Nove komunikacijske tehnologije interneta trebale su pomoći SAD-u da u autoritarnim državama vladinim neistomišljenicima pomogne u međusobnoj komunikaciji. Komercijalizacija tehnologija umjetne inteligencije i njihova primjena u razvoju te nastanku društvenih mreža sredinom 2000-tih također se temeljila na optimističnoj premisi da će svijet biti bolji, time što će biti više i bolje povezan slobodnim protokom informacija. Međutim, zadnjeg desetljeća svjedočimo da se asimetrija preokrenula te da su drugi državni akteri (Rusija, Kina i Iran) koje zapadna literatura apostrofira autokracijama, u kontekstu korištenja kiber prostora kao bojišta, u međuvremenu izgradili obrambene mehanizme zaštite te su izgradili vlastite napadačke kapacitete u kiber prostoru uz pomoć umjetne inteligencije koja pokreće i održava osnovne funkcije društvenih mreža. Ironija je da je jedan od uzroka slabosti SAD-a bio u usponu tehnologija društvenih mreža i mobilnih uređaja u čijem su razvoju američke visokotehnološke tvrtke bile globalni lider.[62]

2.3. Kiber prostor - osnovna obilježja i definicije

Kiber prostor rezultat je primjene računalnih znanosti i upotrebe informacijsko-komunikacijskih tehnologija u kojem računalni informacijski sustavi „imaju sposobnost međusobne interakcije, odnosno stalnog ili povremenog umrežavanja te u kojem sve informacijsko-komunikacijske tehnologije funkcioniraju kroz operacije s podacima i

60 Ibid.

61 Ibid.

62 Nye Joseph, Protecting Democracy in an Era of Cyber Information War, Belfer Center for Science and International Affairs, Harvard Kennedy School, SAD, 2019.

Dostupno na: https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war

informacijama.“[63] U pogledu osnove kiber prostora, opći stav je da on predstavlja okruženje, prostor ili, najčešće, sredinu u kojoj postoje podaci elektromagnetne prirode i koji je nastao umjetnim putem ljudskom aktivnošću s primjenom informacijsko-komunikacijskih tehnologija“.[64] Radi se dakle o elektromagnetnom okruženju u kojem se podaci elektromagnetne prirode stvaraju, čuvaju, šalju, primaju, obrađuju i uništavaju, a podaci, sustavi, procesi i ljudi se umrežavaju ili mogu biti umreženi. [65] Kiber prostor definira se kao „četverodimenzionalni prostor u koji se ubraja zemljopisna rasprostranjenost, logičke mreže, ljudski čimbenik sa svojim stvarnim i virtualnim identitetima te umjetnu inteligenciju, u kojemu svaka od utvrđenih dimenzija ima svoju ulogu, važnost i odgovornost, ali i osjetljivost na različite podražaje.“[66] On je „složen po formi, strukturi i logički zasnovanim procesima. Po formi, nije ograničen vidljivim granicama poput geografskih prostora, kopna, mora, zraka ili svemira, već je amorfan i nestalan, uz tendenciju širenja, kako se povećava zastupljenost i domet informacijskih tehnologija“.[67]

U njemu „dimenzije prostora i vremena nemaju isto značenje kao u fizičkom prostoru.“[68] „Međutim, kiber prostor nije virtualan, apstraktni fenomen zasnovan na informacijama i idejama koji nema materijalnu komponentu, niti je neovisan od fizičkog okruženja.“[69] „Njegovu strukturu, sadržaj i formu neprekidno mijenjaju njegovi korisnici svojim aktivnostima, znanjem i umijećem, kao i mnogobrojni automatizirani tehnički sustavi (softverski i hardverski) vlastitim funkcioniranjem. Kiber prostor ima dinamičnu i rastuću strukturu.“[70] „Kiber prostor je umjetna tvorevina ljudi i tehničkih sustava pa se razvija u skladu sa voljom ljudi i unaprijed definiranim procesima, a ne po prirodnim zakonima.“[71] Njegovu dinamiku ostvaruju automatizirani procesi razmjene podataka koji mogu biti i anonimni. U osnovi kiber prostor ima nematerijalnu prirodu, odnosno dio je šireg informacijskog prostora.

---

63 Mladenović, 2016, str. 70.

64 Ibid.

65 Usp. Mladenović, 2016., str. 77.

66 Akrap, Gordan, Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura, Strategos, 2019, str. 37-49. Dostupno na: https://hrcak.srce.hr/231009 (Datum pristupa: 14.01.2022.).

67 Mladenović, 2016., str. 82.; prema Alexander Hellemans, „Two Steps Closer to a Quantum Internet,“ IEEE Spectrum, 2015, http://spectrum.ieee.org/telecom/security/two-steps-closer-to-a-quantum-internet

68 Ibid.

69 Mladenović, 2016., str. 82.

70 Ibid.

71 Ibid., str. 177.

Najčešće se opisuje kao „virtualni prostor“, odnosno djelomično se poklapa s pojmom „virtualna stvarnost“ koji se više odnosi na tehničke aspekte realizacije kiber prostora. Virtualna stvarnost ujedno predstavlja društveni prostor u kojem se ljudi i dalje susreću licem u lice, ali uz novo značenje riječi »susresti« i »lice«. Ti novi prostori primjer su brisanja granica između društvenog i tehnološkoga, biologije i stroja, prirodnog i umjetnoga. Pun opseg utjecaja tehnologija koje se koriste u virtualnom prostoru na društvene i psihološke značajke pojedinca i društva tek će se pokazati u budućnosti.[72]

Direktni kreatori kiber prostora su ljudi, stvarajući i utječući na njegovu strukturu, sadržaj i procese koji se u njemu odvijaju, i tehnologije koje utječu na različite procese unutar njega. Procese u kiber prostoru ljudi mogu realizirati i indirektno, preko tehnoloških sustava koji su stvoreni i napravljeni prema njihovoj namjeri i prema potrebama. Simboli te organizirane aktivnosti čiji je cilj ostvarivanje nekakvih zadataka ili koristi, su servisi koje izvršava softver, izvođenjem procesa i upotrebom podataka. Dakle, kiber prostor je skup sustava koji se konstantno ili povremeno povezuju ili međusobno komuniciraju razmjenom podataka na organizirani način.“[73]

Karakteristike kiber prostora su:[74]

- Kiber prostor je „umjetna tvorevina ljudi, zasnovana na primjeni tehnologije“;
- Dio je informacijskog prostora;
- „postoji na osnovi ili kao dio elektromagnetnog okruženja“;
- „u njemu se stvaraju, čuvaju, šalju, primaju, obrađuju i uništavaju podaci, odnosno informacije“;
- postoji i funkcionira na osnovi primjene računalnih informacijskih tehnologija;
- „njegovi elementi su podaci/informacije (u digitalnom obliku), informacijski sustavi i infrastruktura, procesi i ljudi kao kreatori, sudionici aktivnosti i procesa“;
- „karakterizira ga sposobnost ili mogućnost umreženosti i protoka podataka između dijelova sustava ili između odvojenih sustava“;
- povezanost između njegovih dijelova načelno se ostvaruje na razini podataka, a može biti ostvarena i na fizičkoj razini (fizičke infrastrukture i veze), razini procesa

72 Virtualna stvarnost. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Pristupljeno 22. 1. 2022. http://www.enciklopedija.hr/Natuknica.aspx?ID=64795

73 Mladenović, 2016., str.177.

74 Ibid., str. 77.

(uspostavljene veze), razini ljudi (kao kreatora kiber prostora, čimbenika koji omogućava njegovo postojanje, korisnika i obrađivača)";

- osnova, procesi, učinci i korisnici kiber prostora mogu postojati na fizičkoj, logičkoj i kognitivnoj razini.

Centralni dio kiber prostora čine „podaci i matematičko-logička pravila i instrukcije, koji se kroz obradu signala i značenje"[75] povezuju s fizičkim i informacijskim prostorom i njegovim korisnicima. Informacijsko-komunikacijske tehnologije imaju svoju logičku i materijalno-fizičku prirodu. Logičku prirodu čine računalni programi, a materijalno-fizičku infrastrukture koje podržavaju njihovu logičku primjenu. Obje kategorije koriste ljudi i drugi sustavi za manipuliranje informacijama u kiber prostoru. Kao dio šireg informacijskog prostora odnosno *svijeta današnjice* kiber prostor, sastoji se od tri osnovne domene: fizičke, informacijske, kognitivne: [76]

- Fizička domena kiber prostora, odnosno domena svijeta stvarnosti, jest područje preko kojeg se identificiraju pojedinci, organizacije i infrastrukture i informacije te koje uključuje činjenice, znanje i podatke. „Interakcija, odnosno sinergijsko djelovanje procesa koji se odvijaju u ovim domenama i kroz njih, omogućava stvaranje novijih korisnih i primjenjivih znanja te donošenje korisnih odluka". „Fizička domena predstavlja svijet stvarnosti, svakidašnjicu koja nas okružuje, našu prošlost te predviđenu, moguću i/ili očekivanu verziju bliže i/ili dalje budućnosti. To je domena u kojoj se događaju pojave, pojavljuju simboli, odnosno domena u kojoj se na fizičkoj razini postoji i djeluje."

- U informacijskoj domeni zahvaćaju se simboli iz svijeta stvarnosti, pretvara ih se u oblik koristan za daljnju uporabu te omogućava distribuciju različitim korisnicima u različitim, korisnicima prilagođenim, načinima i oblicima.

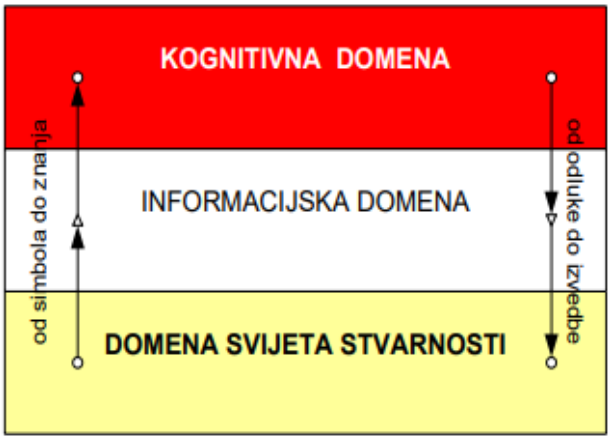
- Kognitivna domena jest područje iz kojeg se analizom sadržaja dolazi do spoznaje kako ljudi razmišljaju, razumiju i odlučuju; „kognitivna domena predstavlja svijet znanja, svijet svijesti i percepcije, svijet umnih sposobnosti i obučenosti pojedinca, grupe i/ili

75 Ibid.

76 Akrap, 2011., str. 11.-13.

zajednice, u njoj oblikujemo znanje, stvaramo izvjesnice i ona predstavlja domenu u kojoj se donose odluke.“

„Međusobni odnos i položaj različitih domena grafički se može prikazati na način prikazan“ *slikom 2*: [77]



Izvor: Akrap, 2009., Informacijske strategije i oblikovanje javnoga znanja.

Slika 2. Domene kiber prostora.

Na slici 2. dužine prikazane strelicama daju bitno pojednostavljen proces prijenosa simbola iz svijeta stvarnosti, njihove tvorbe u informacije i znanje te proces donošenja odluka koje imaju za posljedicu pokušaj promjene pojave i/ili događaja u svijetu stvarnosti.

Informacijska domena predstavlja logički sloj kiber prostora. Centralni dio logičkog sloja čine računalni programi, kao integralni dio svakog informacijskog sustava, te ga posredstvom sustava – hardvera, procesa i ljudi, povezuju s *domenom svijeta stvarnosti* odnosno fizičkom domenom te s značenjem, razumijevanjem informacija i znanjem odnosno s kognitivnom domenom kiber prostora.[78]

Svaka od navedenih domena kiber prostora ima određene funkcije. Funkcija informacijske domene kiber prostora čovjeku osigurava da djeluje u okruženju u kojem živi, da mijenja situacije u kojima se nalazi, da aktivno sudjeluje u događajima. Međutim, za samo poimanje situacije u kojoj se nalazi, za razumijevanje stvarnosti u kojoj djeluje, za stvaranje slike svijeta

77 Ibid., str. 12.

78 Usp. Mladenović, 2016.

u kojem obitava, presudna je kognitivna funkcija tj. mišljenja, koja se odvija u kognitivnoj domeni. Kognitivna funkcija omogućava čovjeku da objektivno analizira zbilju i razumije zbilju kao objektivnu stvarnost. Drugim riječima, kognitivna funkcija omogućava da se otkriju i ustanove činjenice, a činjenice su osnovni kriterij s pomoću kojeg možemo prosuditi istinitost i valjanost tvrdnji, odnosno informacija.[79]

Mišljenje je primarni proces i stvaralac znanja što ga strukturiraju informacije i kognitivna funkcija koje u tom procesu sudjeluju u društvenom i na individualnom planu. Znanje oblikuje nekoliko funkcija mišljenja: spoznajna, informacijska, komunikacijska funkcija i funkcija pamćenja. Kad informacijska i kognitivna funkcija ne djeluju sinkrono ili ako je kognitivna funkcija potisnuta, onda se otvara prostor za razumijevanje zbilje na pogrešnim informacijama i dezinformacijama.[80] Kognitivna funkcija osigurava uvid u činjenice i objektivni prikaz situacije. Primarna zadaća informacijske funkcije jest sudjelovanje u događajima, a cilj joj je mijenjanje situacije da bi se ostvarile namjere, htijenja i ciljevi.[81] „Usklađenost informacijske i kognitivne funkcije ne garantira učinkovitost poduzetih koraka i odluka. To ne može garantirati jednostavno zato što je pitanje koliko kognitivna funkcija može objektivno prikazati postojeće stanje stvari. Fragmentirano i necjelovito znanje može biti točno i istinito, ali to ne znači da je nužno i objektivno, jer ne daje cjelovit prikaz događaja ili razumijevanje zbilje.[82] Upravo fragmentirane i nepotpune obavijesti, s točnim ali necjelovitim sadržajem, osnova su na kojoj nastaju dezinformacije.“[83] Vezano za ovu činjenicu, potrebno je istaknuti da osnovu kiber prostora čine „logički odnosi koji omogućavaju procese i manipulaciju podacima“. Ti procesi i aktivnosti odvijaju se u logičkom području, ali unutar infrastrukture koja se prostire u fizičkom području. Oni imaju uzroke i ostvaruju učinke na fizički i informacijski prostor. U pogledu strukture i uzročno-posljedičnih odnosa, kiber prostor se ne može učinkovito promatrati kao fenomen u jednoj realnosti (ravni promatranja) u jednom trenutku vremena, već istovremeno u više njih, pri čemu su podaci ključan zajednički čimbenik na kojem počiva veza sve tri

79 Tuđman, 2013., str. 153.

80 Tuđman, 2013., str. 153.

81 Ibid., str. 153.-154.

82 Ibid.

83 Tuđman, 2008., str. 125.

domene.[84] Podaci su dakle poveznica između fizičke, informacijske i kognitivne domene kiber prostora. Oni omogućavaju „logičku, fizičku i kognitivnu vezu„ između njegovih domena.

Unutar njegovog elektromagnetnog područja primjenom računalnih informacijskih sustava i tehnologija podaci, elektromagnetne prirode, u kiber prostoru se stvaraju, čuvaju, saznavaju, primaju, preoblikuju, obrađuju i uništavaju. Njegovo postojanje u sklopu šireg informacijskog okruženja ne zasniva se na prirodi njegovog okruženja, sadržaja ili organizacije informacijskih sustava i njihovih mreža, već na sposobnosti da se vrše manipulacije podacima i obavijestima i uspostavljaju organizirane veze između njegovih domena (svijeta stvarnosti, informacijske i kognitivne) na razini podataka.[85] Čuvanje, obrada, preoblikovanje, slanje i primanje podataka obavlja se uz pomoć tehničkih sustava (hardvera tj. uređaja i infrastrukture), odnosno softvera (baza podataka, programa, odnosno bilo kojih logičkih pravila za izvršavanje programiranih naredbi) koji su dio fizičkog svijeta i logičkog okruženja te imaju sposobnost obrade podataka u digitalnoj formi.[86]

U kiber prostoru „prema načinu distribucije vrijednosti signalne funkcije u odnosu na vrijeme, signali mogu biti analogni, digitalni ili kvantni.“[87] „Analogni signali su kontinuirano promjenjive vrijednosti po intenzitetu (amplitudi) i frekvenciji u vremenu. Dok se ljudsko opažanje svijeta zasniva na analognim signalima (vid, zvuk, miris, okus, dodir), suvremene računalne informacijske tehnologije, zasnovane na tranzistorima u procesorima, zasnivaju se na obradi digitalnih podataka i signala.“[88] „Zbog navedene činjenice da se podaci mogu pretvarati u različite vrste signala, nije ispravno nazivati kiber prostor „digitalnim područjem“, pošto su digitalne tehnologije prevladavajuće u suvremenim tehničkim sustavima, ali ne i jedini mogući oblik predstavljanja i obrade podataka.[89]

„Vrsta zapisa podataka u signale zavisi od tehnologije i to nije suština kiber prostora, odnosno sukobljavanja u njemu. Njegova bit je manipulacija podacima i njihov transfer između fizičke,

---

84 Usp. Mladenović, 2016., str. 82.-83.

85 Usp. Mladenović, 2016., str. 78.

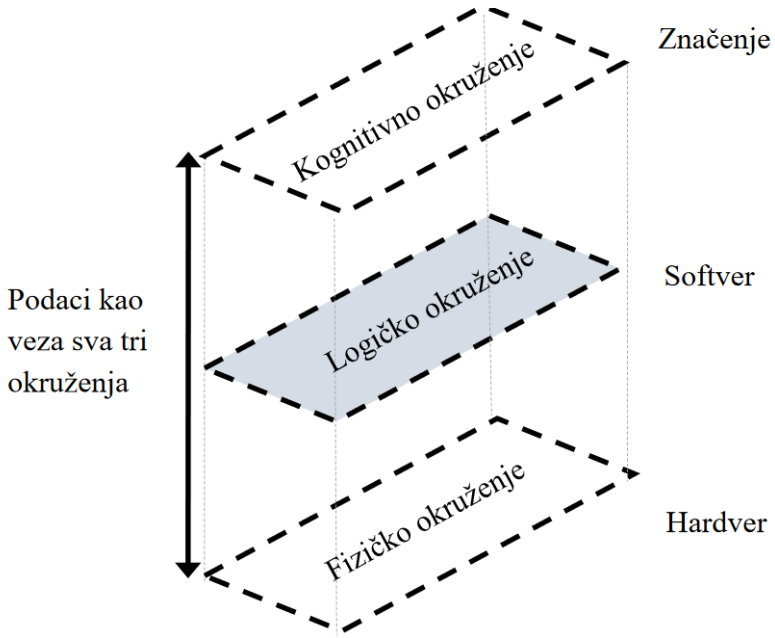
86 Usp. Mladenović, 2016., str. 84.

87 Mladenović, 2016., str. 85., prema: Yonina Chana Eldar, „Quantum Signal Processing,“ (PhD diss., Massachusetts Institute of Technology, Cambridge, 2002), https://dspace.mit.edu/bitstream/handle/1721.1/16805/50544999-MIT.pdf?sequence=2 (preuzeto 20. avgusta 2015)

88 Mladenović, 2016., str. 85.

89 Ibid.

logičke i kognitivne domene kiber prostora u cilju narušavanja informacijske sigurnosti sustava.“[90] Tehnološki sustavi uvijek obavljaju svoju funkciju manipuliranjem podataka. U informacijskoj domeni tj. na logičkoj razini kiber prostora to radi umjetna inteligencija. U fizičkoj domeni tj. na razini uređaja i infrastrukture to rade procesori.[91]



Izvor: Mladenović, Multidisciplinarni aspekti kiber ratovanja, 2016., str. 87.

Slika 3. Konceptualni prikaz okruženja kiber prostora.

Slika 3. prikazuje konceptualni prikaz okruženja odnosno opisanih domena kiber prostora kojim se grafički opisuje činjenica da su: „Podaci ključan čimbenik u računalnim informacijskim tehnologijama koji povezuju funkcioniranje tehnologija umjetne inteligencije koje su zadužene za logičku manipulaciju podacima i ostvarivanje međusobne interakcije informacijske domene (logičkog okruženja) i domene svijeta stvarnosti tj. fizičke domene: na logičkoj razini i na razini hardvera koji fizički obrađuje podatke i usmjerava tok signala prema kognitivnoj domeni u kojoj korisnici društvenih mreža koriste softver i hardver na višem nivou reprezentacije. Mikroprocesori vrše svoju funkciju sa podacima (u elektronskom obliku)

90 Ibid., str. 86.

91 Usp. Mladenović, 2016., str. 86.-87.

primjenjujući matematičke (aritmetičke ili logičke) operacije, definirane instrukcijama tehnologija umjetne inteligencije[92] koje su integrirane u njezin dizajn.“[93]

Tehnologije umjetne inteligencije „predstavljaju skup algoritama/instrukcija napisanih u nekom programskom jeziku s ciljem da usmjere procesore (iz fizičke domene) da izvode zadatke i aktivnosti s podacima.“ Podaci su dakle zajednička veza između različitih tehnologija umjetne inteligencije koja te „podatke obrađuje različitim programskim jezicima koji su zasnovani na istoj matematičkoj logici, uz različit način i razine predstavljanja naredbi.“[94] „Bez obzira na način obrade signala, u osnovi kiber prostora uvijek postoje podaci i matematičko-logičke instrukcije. Oni ujedno predstavljaju i vezu koju kiber prostor stvara između informacijske i fizičke domene.“[95] Veza podataka s kognitivnom domenom sadržana je u značenju vrijednosti koju podaci predstavljaju. Uvjerenja, načela i vrijednosti koje korisnici stvaraju i dijele na društvenim mrežama jesu podaci koji se u ovom istraživanju promatraju i predstavljaju vezu između informacijske domene i domene svijeta stvarnosti kojima manipulira umjetna inteligencija.

„U kontekstu računalnih znanosti, podaci i programi predstavljaju dvije opće kategorije umjetne inteligencije.“[96] Umjetna inteligencija koja djeluje unutar logičkog područja kiber prostora, odnosno unutar njegove informacijske domene, ključan je veznik koji povezuje fizički svijet s informacijskim područjem značenja i predstavlja osnovu prirode kiber prostora. Međutim, umjetna inteligencija se ne može promatrati kao samostalan čimbenik, već kao dio šireg sustava „u kojem postoji fizička infrastruktura i kognitivna sfera značenja“, pri čemu su ti slojevi povezani stanjima i procesima.[97]

„Iako je kiber prostor umjetna tvorevina ljudi, njegova funkcija ne zavisi nužno od ljudi.“[98] Potpuno je svejedno je li neki proces ili podatak stvorio čovjek ili tehnološki sustav. „Potpuno je svejedno da li ontološko značenje pojma ili značenje neke informacije razumije čovjek ili

92 Autor u tekstu navodi softver odnosno program. Kako program predstavlja oblik i dio je tehnologija umjetne inteligencije, umjesto termina softver koristi se termin tehnologije umjetne inteligencije.

93 Mladenović, 2016., str. 87.

94 Ibid., str. 89.

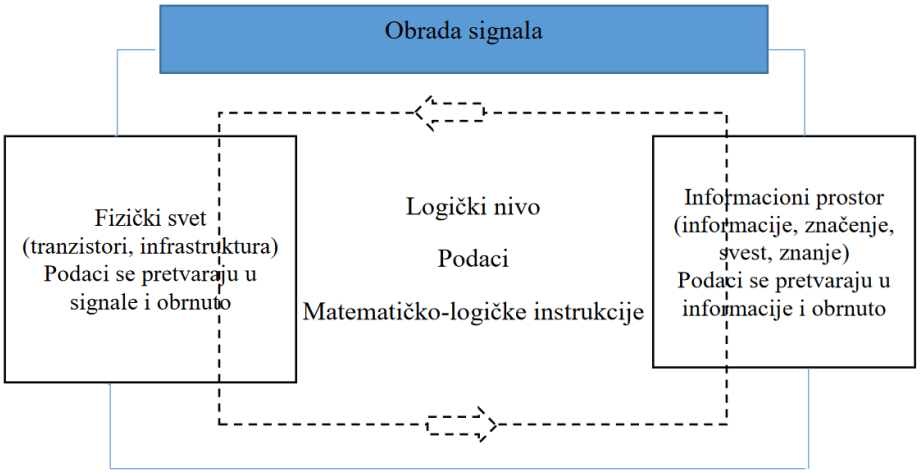
95 Ibid.

96 Ibid., str. 89-90.

97 Ibid.

98 Ibid., str. 90.

sustav umjetne inteligencije. Dakle, kiber prostor „ne zavisi primarno od sudionika, već od stanja i procesa.“[99]



Izvor: Mladenović, Multidisciplinarni aspekti kiber ratovanja, 2016., str. 90.

Slika 4. Reducirani model kiber prostora zasnovan na podacima o načelima, uvjerenjima, vrijednostima ciljanih publika i logičkim instrukcijama u informacijskoj (logičkoj) domeni.[100]

Slika 4. prikazuje reducirani model kiber prostora zasnovan na podacima i logičkim instrukcijama u njegovoj informacijskoj (logičkoj) domeni u kojem umjetna inteligencija obavlja matematiko-logičke instrukcije s podacima koje pretvara u signale a na osnovu kojih se povezuje fizički svijet i svijet svijesti. Navedenim prikazom želi se naglasiti kako umjetna inteligencija u ovoj domeni obavlja matematičko-logičke instrukcije s uvjerenjima, načelima i vrijednostima korisnika društvenih mreža. Također, želi se naglasiti da kiber prostor uvijek označava tehnološki stvoreno okruženje, u kojem se manipulacija uvjerenjima, načelima i vrijednostima ostvaruje na fizičkom, logičkom i informacijsko-kognitivnom (spoznajnom) nivou i u kojem, na osnovi manipulacija, postoji mogućnost umrežavanja na anonimne i automatizirane načine.

99 Ibid.

100 Usp. Ibid.

Radi se o sposobnostima obrade podataka koja je dio znanstvenog područja računalnih znanosti. Ono nije predmet dubljeg istraživanja. Međutim, fenomen obrade i preoblikovanja uvjerenja, načela i vrijednosti na društvenim mrežama bitan je za predmet istraživanja: na koje načine se na društvenim mrežama zloupotrebljavaju tehnologije umjetne inteligencije za manipuliranje uvjerenjima, načelima i vrijednostima u svrhu stvaranja učinkovitih dezinformacija. Prikazano usavršavanje informacijsko-komunikacijskih tehnologija i računalnih informacijskih sustava u znatnoj mjeri utjecali su na razvoj i današnju ulogu društvenih mreža u obavljanju osnovnih funkcija i temeljnih zadaća s uvjerenjima, načelima i vrijednostima koje stvaraju i dijele korisnici njihovih usluga. Ovaj dio istraživanja ujedno je bitan iz tri osnovna polazišta u radu: Prvo polazište je kako bi se naglasila činjenica da osnovnim funkcijama i zadaćama koje na društvenim mrežama obavlja umjetna inteligencija, primarno upravlja ljudski faktor, a ne umjetna inteligencija sama po sebi. Drugo je kako bi se u daljnjim dijelu istraživanja kroz opisane mogućnosti navedenih funkcija i zadaća umjetne inteligencije ukazalo na mogućnosti njezine zloupotrebe, i treće kako bi se na osnovi mogućnosti zloupotreba umjetne inteligencije koju koriste društvene mreže potvrdila ili odbacila hipoteza rada i odgovorilo na postavljena istraživačka pitanja.

S gledišta sigurnosti praksa je pokazala da zloupotreba umjetne inteligencije za (pre)oblikovanje korisničkih uvjerenja, načela i vrijednosti na društvenim mrežama „predstavlja najkritičniju točku cijelog kiber prostora“[101]. To je i razlog zašto se najviše pozornosti u planiranju i provođenju napadnih informacijskih operacija pridaje prikupljanju uvjerenja, načela i vrijednosti ciljanih publika. U međuvremenu, ovi podaci postali su od važnog značaja za izvještajno-sigurnosne strukture koje društvene mreže koriste za utvrđivanje društvenih slabosti ciljanih publika te kako bi se po toj osnovi zloupotrebom hibridne inteligencije prema njima prilagodile dezinformacije. Na osnovi prikupljenih uvjerenja, načela i vrijednosti i sposobnosti tehnologija umjetne inteligencije u mogućnostima njihovog (pre)oblikovanja u učinkovite dezinformacije, umjetna inteligencija koju koriste društvene mreže postala je snažan alat utjecaja i napadački alat prema potrebama napadača. Na osnovi snage tehnologija u prikupljanju, obradi i isporuci informacija kiber prostor postao je glavni prostor u kojem se planiraju i provode međudržavni i regionalni sukobi, političke i ekonomske tenzije te se međusobno odmjeravaju snage. U njemu se odvijaju „sukobi različitih intenziteta

101 Usp. Akrap, 2019., str. 37.-49. Preuzeto s: https://hrcak.srce.hr/231009 (Datum pristupa: 14.01.2022.).

(visokog i niskog) između različitih subjekata koji mogu, ali i ne moraju, biti svjesni takva stanja.“[102]

2.4. Umjetna inteligencija - osnovna obilježja i definicije

Pojmove koji povezuju “inteligenciju” i “učenje” nije lako ni jednostavno jasno definirati. “Učinak umjetne inteligencije”, uobičajeno poznat kao Teslerov teorem, kaže da je “umjetna inteligencija sve što još nije učinjeno” (zapravo, Larry Tesler je rekao: “Inteligencija je sve što strojevi još nisu učinili.”). Teslerov teorem pokazuje da su stvari koje su se prije smatrale umjetnom inteligencijom uklonjene iz njezine definicije kad one postanu standardne.[103]

Umjetna inteligencija (AI akronim od engl. Artificial Intelligence) „povezuje informatiku i robotiku, znanost i inženjerstvo.“[104] Predstavlja „dio računalne znanosti koja se bavi razvojem sposobnosti računala da obavljaju zadaće za koje je potreban neki oblik inteligencije za rješavanje različitih zadataka te davanja rješenja u novim okolnostima.“[105] „Kao grana računalnih znanosti (umjetna inteligencija, op.a.) bavi se razvojem pametnih strojeva koji mogu izvršavati ljudske zadatke bez ljudske inteligencije i intervencije.“[106] „Naziv se također rabi za označivanje svojstva svakoga neživog sustava koji pokazuje inteligenciju (inteligentni sustav); obično su to računalni sustavi, dok se izraz katkad neutemeljeno primjenjuje na robote koji nisu nužno inteligentni.“[107] „Inteligentnim sustavom smatra se svaki sustav koji pokazuje prilagodljivo ponašanje, uči na temelju iskustva, koristi velike količine podataka i znanja, pokazuje svojstva svjesnosti, komunicira s čovjekom prirodnim jezikom i govorom, dopušta pogreške i nejasnoće u komunikaciji ili dr.“[108] „Funkcije inteligentnoga sustava jesu: prikupljanje i obrada informacija, interakcija s radnom okolinom, komunikacija s čovjekom ili s drugim inteligentnim sustavima, prikupljanje i obrada znanja, zaključivanje te planiranje.“[109] „Dakle, jasno je, riječ „umjetno“ u terminu „umjetna inteligencija“ odnosi se na neživu prirodu

---

102 Ibid., str. 42.

103 Van der Aalst Wil, Hybrid Intelligence: to automate or not to automate, that is the question, International Journal of Information Systems and Project Management, 2021., str. 8. Dostupno na https://www.sciencesphere.org/ijispm/archive/ijispm-090201.pdf

104 Putica, 2018., Usp. Terrence J. Sejnowski, The Deep Learning Revolution, MIT Press, Cambridge, 2018.

105 Umjetna inteligencija. Vidi više: https://www.enciklopedija.hr/natuknica.aspx?ID=63150

106 Markotić, 2021., Uvid ostvaren 19.02.2022.

107 Umjetna inteligencija,Vidi više: https://www.enciklopedija.hr/natuknica.aspx?ID=63150

108 Ibid.

109 Ibid.

sustava.“[110] „Riječ je o sustavima koji su umjetno kreirani kako bi služili svojoj svrsi, makar ta svrha bila i puka demonstracija inteligencije.[111] Prema ocu umjetne inteligencije, Johnu McCarthyju, umjetna inteligencija je skraćenica za “Znanost i inženjering inteligentne proizvodnje strojeva, posebno inteligentnih računalnih programa”.[112]

Između uobičajenih računalnih programa i umjetne inteligencije postoje razlike. Uobičajeni računalni program slijedi samo ulazne podatke i upute, odnosno radi ono što mu je rečeno. Ovu radnju može neprestano ponavljati te postaje učinkovitiji kako ga ljudski programeri nadograđuju. Ova činjenica dobra je za automatizaciju cijelog procesa. Međutim, tipični računalni program je statičan, odnosno ne može se prilagoditi stvarnom vremenu ili promjenjivim uvjetima u podacima ili okruženju. To ga čini neprikladnim za brzo mijenjanje situacija i potreba. Umjetna inteligencija bitno je drugačija. Za razliku od tradicionalnog programa, umjetna inteligencija samostalno uči da postane pametnija. Može naučiti iz svojih uspjeha i neuspjeha na osnovi kojih poboljšava svoje učinke. Umjetna inteligencija omogućava da se strojevi nauče kako bi obavljali zadaće kao što ih obavljaju ljudi. Umjetnoj inteligenciji sposobnost daju ljudi da vidi, čuje, govori, miče i piše, čak i da razumije i predviđa na osnovi analize mnogih i različitih vrsta ulaznih podataka. U nekim slučajevima, pametni strojevi mogu se naučiti da se bolje snalaze od ljudi u obavljanju zadaća. To umjetnoj inteligenciji daje sposobnosti koje tipični računalni program nema.

Umjetna inteligencija ima sposobnost reagiranja, prilagođavanja situacijama i davanja preporuka odnosno rješenja u stvarnom vremenu – bez izričite upute čovjeka što da radi. Zbog toga je prikladna za širok spektar inteligentnih zadataka koji su obično bili rezervirani samo za ljude. Umjetna inteligencija postala je jedna od najvažnijih tehnologija u procesima donošenja odluka. „Kao dio računalnih i informacijskih sustava čini supstrat gotovo svih suvremenih tehnoloških i tehničkih sustava. Industrijske infrastrukture, objekti i okruženje sve više zavise od procesa kojima upravlja umjetna inteligencija kroz koju su ovi sustavi uvezani u kiber

110 Crnčić, Saša, Umjetna inteligencija u poslovanju, Diplomski rad, Sveučilište Sjever, 2020., dostupno na: https://urn.nsk.hr/urn:nbn:hr:122:847217, Datum preuzimanja: 2022-01-10.

111 Ibid.

112 Nada i Nadia Berchane, Artificial Intelligence, Machine Learning, and Deep Learning: Same context, Different concepts, 2018., Master Intelligence Economique et Stratégies Compétitives (17.2.2022.), dostupno na: https://master-iesc-angers.com/artificial-intelligence-machine-learning-and-deep-learning-same-context-different-concepts/

prostor.“[113] „Najčešća područja primjene umjetne inteligencije su razumijevanje i obrada prirodnih i umjetnih jezika, raspoznavanje uzoraka, automatsko pretraživanje, robotika, formalizmi i metode prikaza znanja.“[114] „Umjetna inteligencija najširu primjenu našla je kod ekspertnih sustava u kojima u usko ograničenom stručnom području računalni sustav zamjenjuje čovjeka.“[115] „B. Copeland[116] definira je kao sposobnost digitalnoga računala ili računalno kontrolirana robota u izvođenju zadaće obično povezane uz inteligentna bića.“[117] „Umjetna inteligencija koristi se u informacijskoj tehnologiji, korisničkim službama, oglašavanju, upravljanju operacijama i još mnogo toga. Simulacija je prirodne inteligencije u strojevima programiranim za učenje i oponašanje čovjekovih postupaka. Takvi su strojevi sposobni učiti na temelju iskustva i obavljati ljudske zadatke.“[118]

„U knjizi „The Society of Mind“[119] Marvin Minsky određuje je kao pluridisciplinarnu i interdisciplinarnu znanost koja surađuje s disciplinama kao što su filozofija duha i psihologija, koje pomažu u shvaćanju oblikovanja duha i manipuliranja simbolima. Ne postoji jasno određena definicija umjetne inteligencije. S. Russel i P. Norvig[120] ih svrstavaju u sljedeće kategorije:

- „sustavi koji misle kao čovjek;
- sustavi koji se ponašaju kao čovjek;
- sustavi koji misle razumski;
- sustavi koji se ponašaju razumski;
- sustavi kojima je cilj imati sve izglede inteligencije (razumske ili ljudske);
- sustavi čije unutarnje funkcioniranje pokušava biti u skladu s ljudskim bićem, odnosno razumskim bićem.“

---

113 Mladenović, 2016., str. 81.

114 Putica, 2018.; Usp. Thomas H. Davenport, The AI Advantage, MIT Press, Cambridge, 2018.

115 Ibid., Usp. John Mueller – Luca Massaron, Artificial Intelligence For Dummies, John Wiley&Sons, Inc, Haboken, 2018.

116 Ibid., Usp. Brian Jack Copeland, Artificial intelligence (AI), http://www.britannica.com/EBchecked/topic/37146/artificial-intelligence-AI (8. IV. 2018.)

117 Ibid., Usp. Sean Gerrish, How smart machines think, The MIT Press, Cambridge, 2018.

118 Putica, 2018.

119 Ibid., Usp. Marvin Lee Minsky, Society of Mind, Simon&Schuster. Inc., New York, 1988.

120 Ibid., Usp. Stuart Russell – Peter Norvig, Artificial Intelligence: A Modern Approach, Pretince Hall, Upper Saddle River NY, 2003.

Definicija umjetne inteligencije u udžbenicima temelji se na dvije dimenzije: procesu mišljenja i zaključivanja te ponašanju. Stoga, umjesto gledanja na opću definiciju umjetne inteligencije, možemo se ograničiti na definicije prema gore spomenutim kategorijama odnosno dimenzijama. Ove dimenzije daju mnoge definicije a klasificirane su kako je prethodno spomenuto na: sustave koji razmišljaju kao ljudi, sustave koji djeluju poput ljudi, sustave koji razmišljaju racionalno i sustave koji djeluju racionalno. Prve dvije kategorije dakle ocjenjuju umjetnu inteligenciju u odnosu na ljudsku izvedbu, dok je posljednje dvije kategorije mjere prema idealnom konceptu inteligencije a to je "racionalnost". Povijesno gledano, evolucija umjetne inteligencije slijedila je ova četiri pristupa. Međutim, postoji proturječnost između umjetne inteligencije koja je usredotočena na čovjeka i one koja se poziva na koncept racionalnosti. Prva je definirana kao empirijska znanost koja se temelji na hipotezama i eksperimentalnim dokazima. S druge strane, racionalistički pristup zainteresiran je za stvaranje sustava temeljenih na evoluciji matematike i inženjerstva.[121]

„Postoji nekoliko jednostavnih objašnjenja umjetne inteligencije:[122]

- Inteligentna cjelina koju su stvorili ljudi.
- Sposobnost inteligentnog izvršavanja zadatka bez izričitih uputa.
- Sposobnost racionalnog i humanog razmišljanja i djelovanja."

„Svrha umjetne inteligencije je pomoći ljudskim sposobnostima i pomoći u donošenju naprednih odluka s dalekosežnim posljedicama."[123] Područje umjetne inteligencije sastoji se od mnogih disciplina, tehnologija i podpolja. Istaknut će se one koje su najvažnije za predmet istraživanja.

2.5. Tehnologije umjetne inteligencije

Algoritam - Algoritam je niz koraka koji se koriste za rješavanje problema ili izvođenje neke radnje na računalu. Njih stvaraju i funkcije im određuju ljudski programeri, a strojevi ih slijede kako bi proizveli rezultat. Gotovo svaki računalni program sastoji se od stroja koji slijedi upute koje je napisao čovjek. To uključuje i umjetnu inteligenciju. Osim što umjetna inteligencija koristi različite algoritme na različite načine kako bi učinila stvari koje tipičan računalni

121 Berchane, 2018.

122 Markotić, 2021.

123 Ibid.

program ne može učiniti.[124] Algoritmi su davne 1973. opisivani kao „skup pravila koja precizno definiraju redoslijed neke operacije kojeg slijedi neko računalo kako bi riješilo neki problem. U tehničkom smislu, računala algoritme obično koriste kako bi obrađivala podatke brže i preciznije nego što zahtijeva ručno izvršavanje nekog zadatka.[125] Algoritmi su međusobno povezani računalni kodovi.“[126] Računalno gledano, algoritam podrazumijeva postupak kojim računalo rješava neki problem koji se učestalo ponavlja ili koji slijedi fiksno utvrđene korake kao što su primjerice problemi u otkrivanju neželjene e-pošte.[127]

Strojno učenje[128] - „grana je umjetne inteligencije koja se bavi oblikovanjem algoritama koji svoju učinkovitost poboljšavaju na temelju empirijskih podataka.“[129] „Strojno učenje jedno je od danas najaktivnijih i najuzbudljivijih područja računarske znanosti, ponajviše zbog brojnih mogućnosti primjene koje se protežu od raspoznavanja uzoraka i dubinske analize podataka do robotike, računalnog vida, bioinformatike i računalne lingvistike.“[130] „Strojno učenje metoda je analize podataka koja automatizira izradu analitičkih modela. To je grana umjetne inteligencije koja se temelji na ideji da sustavi mogu učiti iz podataka, prepoznavati uzorke i donositi odluke uz minimalnu ljudsku intervenciju. Iako je umjetna inteligencija široka znanost oponašanja ljudskih sposobnosti, strojno učenje je njezin specifični podskup koji trenira stroj kako učiti.“[131] „Strojno učenje jest programiranje računala na način da se optimiziraju neki kriteriji uspješnosti temeljem podatkovnih primjera ili prethodnog iskustva.“[132] „Strojno učenje

---

124 Kaput Mike, The AI Terms Cheat Sheet [Easy Explainer of AI Terminology], Marketing Artificial Intelligence Institute, 2021a., dostupno na: https://www.marketingaiinstitute.com/blog/the-marketers-guide-to-artificial-intelligence-terminology?_ga=2.91286621.636606009.1634325315-126872872.1634325315

125 Mlinac, Nikola & Akrap, Gordan & Lazić, Jadranka. Novi oblici manipuliranja u digitaliziranom prostoru javnog znanja i potreba za uspostavom digitalnog i podatkovnog suvereniteta. National security and the future, 2021., str. 27-63.

126 Neudert Maria Lisa i Nahema Marchal, Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service, Brussels, 2019. Dostupno na:

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf

127 Bergh Arild, Social network centric warfare – understanding influence operations in social media, Norwegian Defence Research Establishment, Izvješće 19/01194, 2019. Dostupno na: https://www.ffi.no/en/publications-archive/social-network-centric-warfare-understanding-influence-operations-in-social-media

128 Engl. Machine learning.

129 Fakultet elektrotehnike i računarstva, Zagreb, dostupno na https://www.fer.unizg.hr/predmet/su

130 Ibid.

131 Markotić, 2021.

132 Bašić Dalbelo Bojana i Šnajder Jan; prema Alpaydin 2009.

je okosnica umjetne inteligencije.“[133] Uključuje „razvoj računalnih pristupa za automatsko razumijevanje podataka – ova tehnologija potvrđuje da je učenje dinamičan proces, što je omogućeno kroz primjere i iskustvo, a ne samo unaprijed definiranim pravilima.[134] „Važno je napomenuti kako stroj kod strojnog učenja nije programiran za točno određeni ishod, već je programiran da uči iz primjera. Iako strojno učenje implicira učenje, ono pripada, barem za sada i u takvom obliku, u područje slabe umjetne inteligencije. To je iz razloga što stroj ne razumije što se govori, nego samo povezuje simbole i značenje te identificira uzorke.“[135] „Strojno učenje temelji se na velikim količinama podataka i za sada se najviše primjenjuje uz potporu čovjeka“ s ciljem da otkrije „korisne obrasce, odnose ili korelacije između različitih podataka“, na osnovi kojih „stvara zaključke o budućem ponašanju te, sukladno zaključcima, determinira daljnje ponašanje čovjeka“.[136]

Strojno učenje može se promatrati kao dio znanosti o podacima, tj. šireg interdisciplinarnog područja čiji je cilj „pretvoriti podatke u stvarnu vrijednost.“ [137] Podaci mogu biti strukturirani ili nestrukturirani, veliki ili mali, statični ili nestatični. Vrijednost se može pružiti u obliku predviđanja, automatiziranih odluka, modela naučenih iz podataka ili bilo koje vrste vizualizacije podataka koja daje uvide. Znanost o podacima uključuje ekstrakciju podataka, pripremu podataka, istraživanje podataka, transformaciju podataka, pohranu i dohvaćanje, računalne infrastrukture, razne vrste rudarenja i učenja, predstavljanje objašnjenja i predviđanja te iskorištavanje rezultata uzimajući u obzir etičke, društvene, pravne i poslovne aspekte.[138] Strojno učenje omogućuje veću preciznost i nadopunjava ljudske procjene i predviđanja. U principu, može znatno ubrzati procese donošenja odluka omogućavajući donositeljima odluka da razumiju i analiziraju situacije mnogo brže nego prije. Pronalaženje načina da se umanje ili otklone pristranosti ili analitičke pogreške jedno je od područja intenzivnog istraživanja mogućnosti strojnog učenja. Trenutno je još uvijek s vanjskog stajališta teško procijeniti koliko će doista procjena generirana umjetnom inteligencijom biti precizna ili pouzdana u drugačijim okruženjima ili situacijama. Shodno tome, umjetna inteligencija ne smije dobiti preveliku moć

133 Bašić i Šnajder, Izvor: https://www.fer.unizg.hr/_download/repository/SU-1-Uvod%5B1%5D.pdf

134 Crnčić, 2020., str. 28.

135 Ibid., 29.

136 Ibid.

137 van der Aalst, Process Mining: Data Science in Action, Springer-Verlag, Berlin, 2016.

138 Ibid.

odnosno autoritet u donošenju odluka, poglavito na političko-strateškoj razini.[139] Onaj tko ima pristup umjetnoj inteligenciji u poziciji je da kontekstualizira i interpretira njezine rezultate. Nadzor, kontrola, upravljanje i kontekstualiziranje ciljeva koji se žele postići njezinom primjenom stoga su od ključne važnosti.

Duboko učenje[140] - „Duboko učenje vrsta je strojnog učenja koje računalo osposobljava da izvršava zadatke slično čovjeku, poput prepoznavanja govora, prepoznavanja slika ili predviđanja. Umjesto da organizira podatke koji se provode kroz unaprijed definirane jednadžbe, dubinsko učenje postavlja osnovne parametre podataka i osposobljava računalo da samostalno uči prepoznavanjem obrazaca pomoću mnogih slojeva obrade.“[141] „Kroz klasično strojno učenje o kojem je prethodno bilo govora, računalo uči uglavnom kroz nadzirano iskustvo. To znači da čovjek pomaže stroju u učenju te mu daje na stotine, tisuće pa i više praktičnih primjera za učenje. Greške se u takvom načinu rada ispravljaju ručno. Duboko učenje temelji se na korištenju hijerarhijske obrade podataka i informacija, što mu omogućava višeslojna arhitektura. I ovdje je riječ o upravljanju velikim podacima, samo na drugačiji, složeniji način koji u obzir uzima različite i brojne čimbenike, pa i različito vrijeme i različite razine.“[142]

Duboko učenje je forma jednostavnijeg strojnog učenja uz korištenje neuronskih mreža[143] (ANN akronim od engl. Artificial Neural Networks). Umjetne neuronske mreže počele su se razvijati 1980-ih u sklopu razvoja ekspertnih sustava za specifične potrebe razvoja umjetne inteligencije. Razvoj umjetnih neuronskih mreža nadahnut je biološkim živčanim sustavom. „Umjetne neuronske mreže obrađuju informacije na sličan način kao što bi to činio mozak. Klasični pristup u umjetnoj inteligenciji, zasnovan na znanju, naziva se simbolizam, dok se pristup temeljen na neuronskim mrežama naziva konekcionizam.“[144] “Simbolizam se temelji

---

139 Fabien Merz, AI in Military Enabling Applications, Center for Security Studies, Eidgenössische Technische Hochschule - ETH Zuric, CSS Analyses in Security Policy, No. 251, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf.

140 Engl. Deep learning

141 Markotić, 2021.; https://www.machine-desk.com/industrija-4-0/umjetna-inteligencija-ai

142 Crnčić, 2020., str. 31.

143 Crnčić, 2020., prema: Smolčić, T. i dr. Primjena strojnog učenja u naprednom računarstvu, 2018. URL: https://dei.srce.hr/sites/default/files/2018-04/Smolcic-Srce-DEI-2018.pdf (12. veljače 2020.)

144 Putica, 2018., str. 204.

na postojanju baze eksplicitnog znanja. U sustav se uključuju i pravila za pretraživanje, donošenje zaključaka, pohranjivanje i dohvaćanje znanja te umetanje novih pojmova u bazu. Konekcionizam je pristup temeljen na paralelnoj i distribuiranoj zamjeni malih procesuirajućih jedinica, bliskih apstraktnu neuronu i povezanih u mrežu.“[145] „Ideja neuronskih mreža odavno je poznata, ali procesna moć ondašnjih računala nije omogućavala njihovu implementaciju. Ideju neuronskih mreža nedavno su aktualizirale velike IT korporacije. Riječ je o korporacijama kojima su društvene mreže u središtu interesa pa neuronske mreže na računalima raspoznaju osobe i predmete s fotografija koji su na njima objavljeni. S razvojem umjetnih neuronskih mreža javlja se neuronsko računalstvo kao alternativa računalima zasnovanim na Von Neumannovoj arhitekturi kako bi se, sukladno načinu obrade informacija koju obavlja mozak, simulirala paralelna obrada informacija. Umjetna neuronska mreža definira se kao model zaključivanja na temelju ljudskoga mozga jer on sadrži maksimum poznate inteligencije.“[146] „Ovaj sustav sastavljen je od velikog broja neurona (elemenata) koji su povezani i djeluju kao jedna cjelina. Njihova ključna značajka je sposobnost učenja na primjerima. Svaka bi neuronska mreža trebala biti posebno dizajnirana za rješavanje određenog problema. Načini veze između neurona napravljeni su uvijek za specifičan zadatak koji treba učiniti.“[147] Umjetne neuronske mreže „primjenjuju se kod modeliranja procesa za predviđanje budućeg vladanja procesa i u sklopu naprednog vođenja procesa te u dijagnostici stanja pri radu procesa i strojeva. U metodama strojnog učenja neuronske mreže se dosta primjenjuju za klasifikaciju: prepoznavanje slika, govora, prevođenje, analiza društvenih mreža, inteligentno internetsko pretraživanje, ciljani marketing i sl.“[148] Danas kad se koristi izraz umjetna inteligencija većinom se misli na strojno učenje koje se temelji na umjetnim neuronskim mrežama. Međutim, kroz svoju povijest pod umjetnom inteligencijom dominirala je simbolička umjetna inteligencija koja je također poznata kao "klasična umjetna inteligencija", "umjetna inteligencija koja je utemeljena na pravilima" i "dobra staromodna umjetna inteligencija" koja je povezana s ekspertnim sustavima i logičkim razmišljanjem. Posljednjih godina umjetna inteligencije se sve više povezuje sa strojnim učenjem.[149]

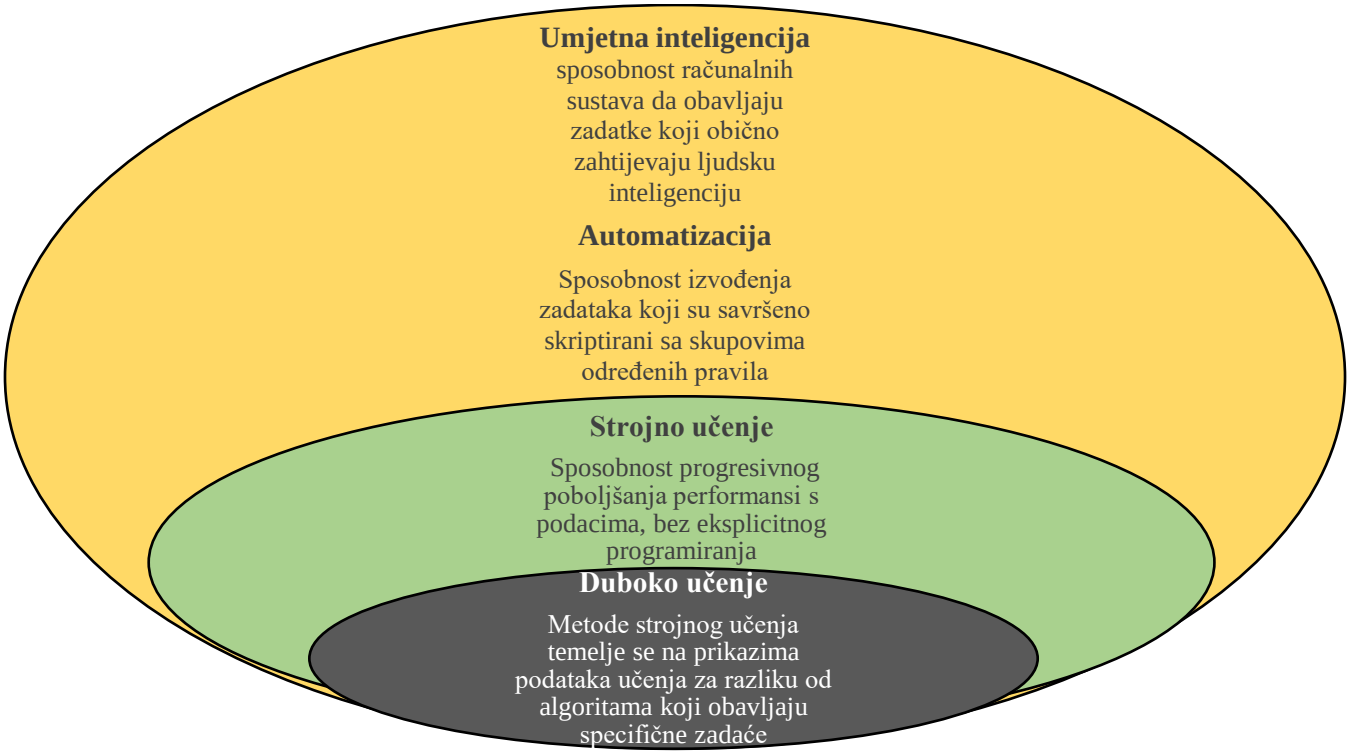
145 Ibid.

146 Ibid., str. 206.

147 Crnčić, 2020., str. 33., prema: Kovačević, R.; Cesar, I., Cafuta, D., Artificial Intelligence in Computer Games, Polytechnic and Design (2), 2019., str. 122.

148 Ibid., str. 36., prema: Ujević Andrijić, Ž., Umjetne neuronske mreže. Kemija u industriji, 2019. str. 220.

149 van der Aalst, 2021.



Izvor: Forrest, Boudreaux, Lohn, Ashby, Curriden, Klima i Grossman, Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World, Santa Monica, RAND Corporation, 2020., str.11.

Slika 5. Grafička taksonomija tehnologija prema definiciji umjetne inteligencije.

Budući da umjetna inteligencija obuhvaća toliko mnogo vrsta sustava i razina autonomije, bilo je potrebno i korisno klasificirati te tehnologije u grafičku taksonomiju koja ilustrira odnose među njima.

Kao što prikazuje slika 5., sustavi koji se općenito opisuju kao umjetna inteligencija obuhvaćaju širok raspon tehnologija s različitim stupnjevima složenosti i sofisticiranosti. Kao što je spomenuto, rani pristupi umjetnoj inteligenciji uključivali su razvoj automatiziranih sustava sa sposobnošću izvođenja skriptiranih zadataka prema skupovima specificiranih pravila. Takvi se pristupi još uvijek u određenoj mjeri koriste, ali tijekom posljednjih nekoliko desetljeća razvijeni su sofisticiraniji sustavi sposobni za strojno učenje. Ovi sustavi mogu progresivno poboljšati izvedbu prepoznavanjem uzoraka u velikim količinama podataka i poduzimanjem korektivnih radnji kako bi poboljšali sposobnosti za klasificiranje budućih obrazaca bez eksplicitnog programiranja za to.[150] Još sofisticiranija klasa sustava strojnog učenja predstavlja

150 Forrest M. i sur., 2020., str. 11.; prema Kaplan, 2016, str. 27.–28.

spomenuto duboko učenje. Ovi sustavi koriste višeslojne umjetne neuronske mreže za prepoznavanje uzoraka u prikazima podataka, kao što su označene slike, za razliku od upotrebe algoritama specifičnih za zadatak kao što se radi u osnovnijim sustavima strojnog učenja.[151] Kao što će se prikazati u nastavku rada, otkrića u dubokom učenju pomoću duboke neuronske mreže omogućila su značajan napredak u računalnom vidu i sustavima za prepoznavanje slika.

Obrada prirodnog jezika[152] - „Obrada prirodnog jezika grana je umjetne inteligencije koja pomaže računalima da razumiju, interpretiraju i manipuliraju ljudskim jezikom. Obrada prirodnog jezika pomaže računalima u komunikaciji s ljudima na njihovom jeziku, omogućujući računalima čitanje teksta, čuvanje govora, njegovo tumačenje, mjerenje osjećaja i određivanje važnih dijelova.“[153]

Računalni vid[154] - „Računalni vid je područje umjetne inteligencije koje osposobljava računala za tumačenje i razumijevanje vizualnog svijeta. Korištenjem digitalnih slika s fotoaparata i videozapisa i modela dubokog učenja, strojevi mogu točno identificirati i klasificirati predmete - a zatim reagirati na ono što "vide". Od prepoznavanja lica do obrade radnje uživo, računalni vid nadmašuje ljudske vizualne sposobnosti u mnogim područjima.“[155]

Robotska automatizacija procesa[156] – predstavlja sustav koji automatizira zadatke koji se ponavljaju putem računalnog programa.[157] Strojno učenje i robotska automatizacija procesa snizili su pragove automatizacije procesa u rješavanju zadaća koje su prije obavljali ljudi.[158] Procesi automatizacije podrazumijevaju automatizaciju zadataka i automatizaciju procesa. Automatizacija zadataka podrazumijeva aktivnosti koje su prije provodili ljudi, a sada ih obavljaju softverski/hardverski roboti. Automatizacija procesa podrazumijeva koordinaciju, kontrolu i poboljšanje cjelokupnog procesa koji podržavaju tehnologije vođene podacima s

151 Ibid., prema; Kaplan, 2016, str. 34.

152 Engl. Natural language processing (NLP).

153 Markotić, 2021.

154 Engl. Computer vision.

155 Markotić, 2021.

156 engl. Robotic Process Automation. Robotic Process Automation in Advertising, Social Media, Data Management, 2021. Dostupno na: https://www.robomotion.io/blog/rpa-in-advertising-social-media-data-management-seo/ (15.02.2022)

157 Ibid.

158 van der Aalst, 2021.

tendencijom smanjivanja ljudskog angažmana u njima.[159] Rezultati studije koju je proveo PricewaterhouseCoopers na temelju podataka Organizacije za ekonomsku suradnju i razvoj (OECD akronim od engl. Organization for Economic Cooperation and Development) prikupljenih u kontekstu Programa za međunarodnu ocjenu kompetencija odraslih (PIAAC akronim od engl. Program for the International Assessment of Adult Competencies) OECD-a predviđaju tri vala automatizacije podataka koji će uslijediti do sredine 2030.[160] Prvi val algoritamske automatizacije podataka već je započeo, drugi val njegovog povećanja dolazi krajem 2020-ih, a treći će se pojaviti sredinom 2030-ih. Prvi se val usredotočuje na automatizaciju jednostavnih računskih zadataka i analizu strukturiranih podataka, (…) između ostalih i u područjima informacije i komunikacije. Drugi val fokusira se na automatizaciju ponavljajućih zadataka (…) vezanih za komunikaciju i razmjenu informacija korištenjem tehnologija umjetne inteligencije kao što je robotska automatizacija procesa. Treći val će odrediti automatizaciju fizičkog rada i rješavanje različitih problema u različitim industrijskim granama, što će nesumnjivo utjecati i na smanjivanje fizičkog ljudskog angažmana u obavljanju brojnih poslova.[161]

Tehnike procesnog rudarenja[162] - „Rudarenje podataka“ podrazumijeva proces pronalaženja anomalija, uzoraka i korelacija unutar velikih skupova podataka radi predviđanja ishoda, odnosno metodologiju „kojom se otkrivaju vrijedni podaci u bazama podataka.“[163] Tehnike procesnog rudarenja koriste podatke o događajima kako bi pokazali što ljudi, strojevi, aplikacije i organizacije stvarno rade. Procesno rudarenje pruža nove uvide koji se mogu koristiti za prepoznavanje i rješavanje problema s performansama i usklađenošću. Baš kao što proračunske tablice mogu učiniti bilo što s brojevima, procesno rudarenje može učiniti sve s podacima o događajima, tj. to je generička tehnologija neovisna o domeni za poboljšanje procesa.[164] Primjenom širokog raspona tehnika podaci, obavijesti i informacije se, u širokom spektru industrija i različitih procesa, koriste za povećanje prihoda, smanjenje troškova, poboljšanje

159 Ibid., str. 6.-7.

160 van der Aalst, 2021., str. 6.; prema J. Hawksworth, R. Berriman, and S. Goel, “Will Robots Really Steal Our Jobs? An International Analysis of the Potential Long Term Impact of Automation,” Technical report, PriceWaterhouseCoopers, 2018.

161 Ibid.

162 engl. Big Data Mining.

163 Crnčić, 2020., str. 48.

164 van der Aalst, 2021., str. 14.

odnosa s kupcima, smanjenje rizika te niz drugih aktivnosti sa svrhom poboljšavanja poslovanja. „Metoda se naziva rudarenje podataka jer se u velikim količinama podataka traže informacije koje 'vrijede zlata'.“[165] „Rudarenje osobnih metapodataka mora se odviti sukladno ciljevima predviđanja.“[166] Definiraju se **„**pogodne publike i ciljevi, automatski se preporučuju strategije za postizanje željenih ciljeva.“[167] Jedan od načina uključuje „modeliranje sklonosti“[168]. Modeliranje sklonosti povezuje karakteristike ciljanih publika s predviđenim ponašanjima. Nakon toga nastaje prediktivni model koji potom ocjenjuju poslovni stručnjaci te se provjerava ostvarenje ciljeva i, po potrebi, odvija prilagodba cijelog procesa.[169] Prediktivni model tzv. prediktivna analitika „dio je podatkovne analitike uz deskriptivnu, dijagnostičku i preskriptivnu analitiku, a cilj joj je predvidjeti buduće vrijednosti nekih pojava, snagu i smjer veza, trendove, uzorke i izuzetke. Rezultat prediktivne analitike su modeli koji pomažu pri donošenju strateških odluka...“[170] Prediktivna analitika važna je značajka umjetne inteligencije koja informacije čini djelotvornim.[171] Ovaj dio istraživanja bitan je budući da će se na osnovu njega u daljnjem dijelu istraživanja nastojati potvrditi ili odbaciti hipoteza i odgovoriti na istraživačka pitanja.

2.6. Vrste umjetne inteligencije

“Danas se sustavi umjetne inteligencije grade dvosmjerno, kao autonomni programi za ostvarivanje vlastitih ciljeva, ali i za korelaciju s drugim sustavima. U područje umjetne inteligencije spadaju klasična umjetna inteligencija te umjetni život i evolucijsko računalstvo. Tako razlikujemo jaku i slabu umjetnu inteligenciju. Jaka umjetna inteligencija naziva se i svjesnom umjetnom inteligencijom, a podrazumijeva stroj sposoban ponašati se inteligentno, osjećati i razumijevati svoje rasuđivanje. Njome je moguće postići repliciranje ljudskih mentalnih svojstava kao što su emocije, kreativnost, motivacija i slično.“[172] „Prema tezi o slaboj

165 Crnčić, 2020., str. 48.; prema Pejić Bach, Rudarenje podataka u bankarstvu, Zbornik ekonomskog fakulteta u Zagrebu, 2005., str. 181.

166 Crnčić, 2020., str.48.

167 Ibid.

168 Ibid.

169 Usp. Crnčić, 2020., str. 48.

170 Crnčić, 2020. str. 47.; prema Zekić-Sušac M., Prediktivna analitika – alati i metode za izradu modela, 2017.

171 Millicent Abadicio, AI at the US Department of Homeland Security – Current Projects, Emerj Artificial Intelligence Research, April 16, 2019, https://emerj.com/ai-sector-overviews/artificial-intelligence-homeland-security/ (pristup ostvaren 22.02.2022.)

172 Putica, 2018., str. 204.

umjetnoj inteligenciji, glavna vrijednost koju računalo ima u istraživanju duha sastoji se u tome što istraživanju pruža djelotvorno pomoćno sredstvo tako što osnažuje, preciznije oblikuje ili provjerava hipoteze. Kod jake umjetne inteligencije računalo nije samo instrument za istraživanje duha. Dobro programirano računalo ima funkciju uma. Sukladno funkcionalističkoj teoriji, ako vrši radnje analogne ljudskim kognitivnim postupcima, računalo doslovno može razumijevati te mu se s pravom pripisuju mentalna, kognitivna stanja. Upravo se jaka umjetna inteligencija najčešće zove imenom umjetna inteligencija.“[173] „Slaba umjetna inteligencija naziva se i ograničenom, a podrazumijeva gradnju više autonomnih sustava ili algoritama sposobnih rješavati problemska područja. Kod ove vrste umjetne inteligencije stroj nije inteligentan, već simulira inteligenciju. Kod slabe umjetne inteligencije strojevi mogu oponašati određena mentalna stanja, ali ih ne posjeduju.“[174]

„Različiti subjekti umjetne inteligencije grade se za različite svrhe i na taj se način razlikuju.“[175] Na temelju funkcionalnosti umjetna inteligencija može se klasificirati na 3 tipa:

- Umjetna uska inteligencija

„Ovo je najčešći oblik umjetne inteligencije na tržištu, a sam naziv govori da mogu obavljati usko definirane zadatke na nadljudskim razinama. Ovakvi sustavi umjetne inteligencije dizajnirani su za rješavanje jednog jedinog problema i mogli bi zaista dobro izvršiti jedan zadatak. Po definiciji imaju uske mogućnosti, poput preporučivanja proizvoda korisniku e-trgovine ili predviđanja vremena, što znači da obavljaju samo usko definirane zadatke.“ Na primjer, sustav koji prepoznaje lica bolje i brže od ljudi ne može se okrenuti i naučiti voziti automobil. Bez obzira koliko moćna, ova vrsta umjetne inteligencije ograničena je opsegom onoga što može učiniti. „U stanju se približiti ljudskom funkcioniranju u vrlo specifičnim kontekstima pa čak ih i nadmašiti u mnogim slučajevima, ali samo u vrlo kontroliranim okruženjima s ograničenim skupom parametara.“ [176]

173 Putica, 2018., str 204.; usp. Darko Polšek, Zapisi iz treće kulture, Jesenski i Turk, Zagreb, 2003.

174 Ibid. str. 205.

175 Markotić, 2021.

176 Ibid.

- Umjetna opća inteligencija

„Ovo je još uvijek teorijski koncept. Definirana je kao umjetna inteligencija koja ima kognitivnu funkciju na ljudskoj razini u širokom spektru domena kao što su obrada jezika, obrada slika, računalno funkcioniranje i zaključivanje i tako dalje.“[177] Opća umjetna inteligencija ne postoji i nije ni blizu postojanju, ali opisuje sustav koji može naučiti i razumjeti bilo koji inteligentni zadatak. Ali to je ono na što mnogi ljudi prvo pomisle kada pomisle na umjetnu inteligenciju: superinteligentno računalo ili robot koji može učiniti sve što čovjek može. Neki stručnjaci su podijeljeni oko toga je li uopće moguće izgraditi takav oblik umjetne inteligencije ili ne. Ali kako tehnike poput dubokog učenja napreduju, možemo se približiti inteligentnim strojevima opće namjene. Potencijalno stvaranje umjetne opće inteligencije postavlja temeljna pitanja o prednostima i opasnostima tehnologije u oponašanju čovjeka što nosi pitanja o tome što znači biti čovjek. Srećom, danas to nisu pitanja na koja moramo odgovoriti, budući da je Umjetna opća inteligencija trenutno znanstvena fantastika.[178] Još smo daleko od izgradnje takvog sustava. Sustav bi trebao sadržavati tisuće sustava umjetne uske inteligencije koji rade u tandemu, međusobno komunicirajući oponašajući ljudsko rasuđivanje.[179]

- Umjetna super inteligencija

Umjetna super inteligencija smatra se logičnim napretkom umjetne opće inteligencije. Sustav umjetne superinteligencije mogao bi nadmašiti sve ljudske sposobnosti. To bi uključivalo donošenje odluka, donošenje racionalnih odluka pa čak i stvari poput stvaranja bolje umjetnosti i izgradnje emocionalnih odnosa.[180]

Jednom kada postignemo umjetnu opću inteligenciju, ovi sustavi brzo bi mogli poboljšati svoje sposobnosti i napredovati u područjima o kojima možda nismo ni sanjali. Iako bi razlika između opće i super umjetne inteligencije bila relativno mala (neki kažu tek u nanosekundi) super umjetna inteligencija predstavlja koncept koji bi se mogao ostvariti tek u dalekoj budućnosti.[181]

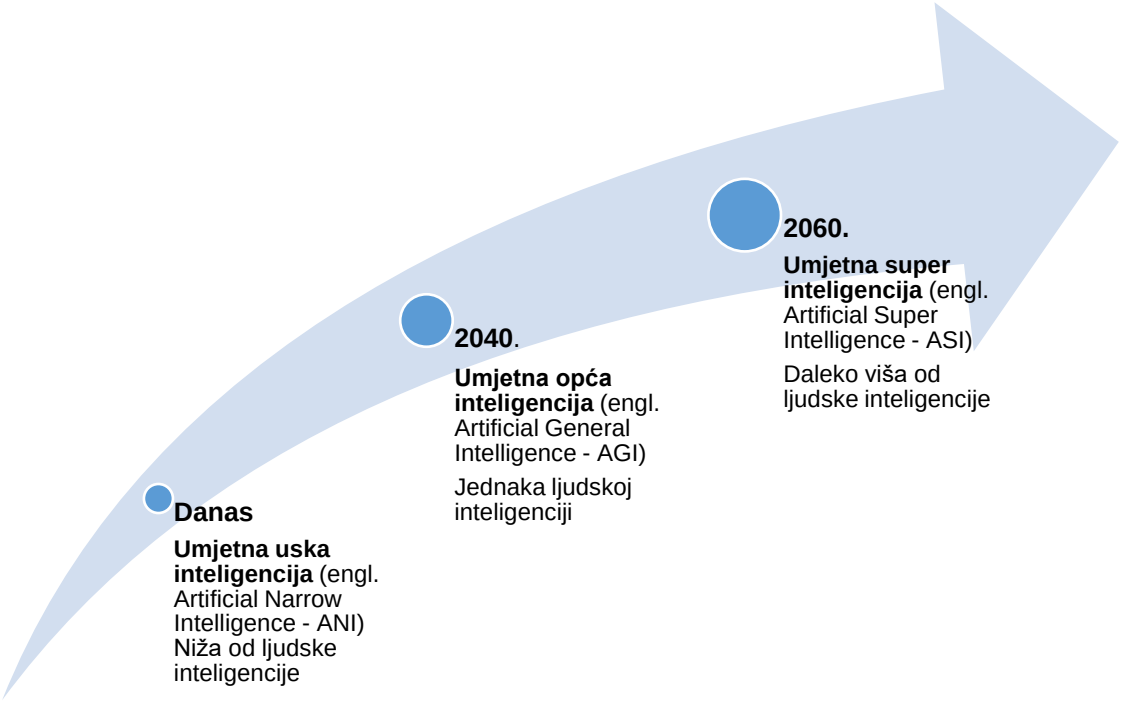
177 Ibid.

178 Kaput, 2021.

179 Usp. Markotić, 2021.

180 Ibid.

181 Ibid.



Izvor: Berchane, N.,N., Artificial Intelligence, Machine Learning, and Deep Learning: Same context, Different concepts, Master Intelligence Economique et Stratégies Compétitives, 2018.

Slika 6. Budući razvoj umjetne inteligencije.

Slika 6. prikazuje razvoj vrsta umjetne inteligencije iz koje je vidljiv trenutni doseg Umjetne uske inteligencije u odnosu na ljudsku (biološku) vrstu inteligencije s perspektivom razvoja Umjetne opće inteligencije i Umjetne super inteligencije. Razvoj tehnologija umjetne inteligencije pokretač je Četvrte industrijske revolucije. Četvrta industrijska revolucija predstavlja nastavak razvoja široko rasprostranjene dostupnosti digitalnih tehnologija koje su nastale kao rezultat Treće industrijske, ili digitalne, revolucije. Četvrta industrijska revolucija bit će uglavnom vođena konvergencijom digitalnih, bioloških i fizičkih inovacija,[182] odnosno može se sažeti kao "dolazak kiber-fizičkih sustava" i duboke integracije digitalnog, fizičkog i

182 Schwab, Klaus, The Fourth Industrial Revolution, Encyclopedia Britanica, 2021., dostupno na: https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734 (17.2.2022.).

biološkog svijeta.[183] Glavni pokretači ove revolucije su umjetna inteligencija, tehnologije virtualne stvarnosti (podrazumijeva simuliranje i računalno modeliranje na osnovi kojeg korisnici mogu stupiti u interakciju s trodimenzionalnim prostorom u stvarnom vremenu), robotika, Internet stvari i biotehnologije.[184] Nesporno je kako Četvrta industrijska revolucija već sad „redefinira i briše granice između digitalnog i fizičkog svijeta"[185] da rezultira „transformacijom društva na globalnoj razini"[186] (....) „mijenja načine na koji komuniciramo" (…) te „utječe na ljudske identitete, zajednice i političke strukture"[187]. Razvoj umjetne inteligencije u posljednjih nekoliko desetljeća omogućio je primjenu velikog raspona njezinog potencijala u informacijsko-komunikacijskim tehnologijama i biotehnologijama. Ove nove tehnologije uz pomoć umjetne inteligencije nastoje pronaći brže, učinkovitije, pametnije načine za izvršavanje različitih zadataka ili čak, u drugim slučajevima, za razvoj umjetne inteligencije nadmoćne ljudskoj inteligenciji.[188]

- Hibridna inteligencija

Strojno učenje i robotska automatizacija procesa snizili su pragove automatizacije procesa u rješavanju zadaća koje su prije obavljali ljudi. Tehnike procesnog rudarenja pomažu odlučiti što treba automatizirati, a što ne. Napredak u strojnom učenju i statističkim metodama učenja, dostupnost velikih podataka, mobilnih uređaja i društvenih mreža doveli su do eksplozije umjetne inteligencije i njezinih primjena u širokom rasponu komercijalnih, državnih i društvenih proizvoda i usluga. Postoje mnoge paralele između biološke i umjetne inteligencije. Neuroznanost i umjetna inteligencija mogu crpiti inspiraciju jedna iz druge i generirati nove teorije i hipoteze[189]. Međutim, dok umjetna inteligencija razvija zamah, također postaje očito da umjetnu inteligenciju i biološku inteligenciju karakteriziraju različiti mehanizmi koji se često ne preklapaju u potpunosti. U usporedbi s biološkom inteligencijom, umjetna inteligencija

183 Davis Nicholas, 5 ways of understanding the Fourth Industrial Revolution, World Economic Forum, 2015. Dostupno na: https://www.weforum.org/agenda/2015/11/5-ways-of-understanding-the-fourth-industrial-revolution/ (17.2.2022.).

184 Bouchrika Imed, What Is The Fourth Industrial Revolution: Risks, Benefits & Responses, Research.com, 2021. Dostupno na: https://research.com/careers/what-is-the-fourth-industrial-revolution (17.2.2022.)

185 Schwab, 2021.

186 Ibid.

187 Usp. Ibid.

188 Ibid.

189 Pescetelli Niccolo, A Brief Taxonomy of Hybrid Intelligence, Forecasting 3, no. 3, 2021, MDPI - Publisher of Open Access Journals,. https://doi.org/10.3390/forecast3030039. (17.2.2022.)

zahtijeva mnogo veće grupe treninga za prepoznavanje obrazaca, manje je otporna na male varijacije u unosu, ne uzima u obzir prethodno iskustvo, kulturne norme, situacijske ili kontekstualne informacije i manje je sposobna generalizirati nove probleme i okruženja.[190] Stoga, umjesto da koriste umjetnu inteligenciju za zamjenu ljudske inteligencije, istraživači su počeli istraživati kako integrirati ljudsku i umjetnu inteligenciju.[191] Praksa je pokazala da većina procesa najbolje funkcionira koristeći kombinaciju ljudske (biološke) i strojne inteligencije, na način da je upravljanje procesima s podacima i automatizacijom takvih procesa korištenjem robotske automatizacije i procesnog rudarenja dovelo do nastanka nove forme inteligencije, hibridne inteligencije.[192]

Hibridna inteligencija predstavlja jedan od ključnih elemenata nastale digitalne transformacije. Ona podrazumijeva usvajanje digitalne tehnologije za transformaciju usluga ili poslovanja zamjenom nedigitalnih ili ručnih procesa digitalnim procesima ili zamjenom starije digitalne tehnologije novijom digitalnom tehnologijom. Hibridna inteligencija oslanja se na automatizaciju procesa i tehnologija koje su vođene podacima. Međutim, hibridna inteligencija proteže se izvan tradicionalne automatizacije i može uključivati npr. nove poslovne modele, nove prodajne kanale, nove proizvode i nove usluge. Takve promjene obično zahtijevaju, ali i ubrzavaju, automatizaciju u obavljanju zadataka i procesa.[193] Pristupi koji se usvajaju mogu se razvrstati u nadzirano učenje (koristeći označene podatke, npr. za klasifikaciju), nenadzirano učenje (korištenje neoznačenih podataka, npr. za otkrivanje nepoznatih obrazaca) i učenje s pojačanjem (pronalaženje ravnoteže između istraživanja neistraženog područja i iskorištavanje trenutnog znanja). Jedan od primjera su mogućnosti i napredak dubokog učenja, u kojem umjetne neuronske mreže iz sirovih podataka progresivno mogu izdvajati nove značajke više razine.[194] Iako su neuronske mreže postojale desetljećima, ove tehnike počele su nadmašivati klasične pristupe u automatizaciji podataka oko 2012**.** Danas su evidentne nevjerojatne

190 Ibid.

191 Ibid.

192 van der Aalst, 2021., str. 8. upućuje na: LeCun Y., Bengio Y. i Hinton G., Deep learning, Nature, vol. 521, str. 436-444, 2015. i Rumelhart D.E., Hinton G. i Williams R.J., Learning Representations by Back-Propagating Errors, Nature, vol. 323, str. 533-536, 1986.

193 van der Aalst, 2021., str. 7.

194 van der Aalst, 2021., str. 8. upućuje na: LeCun i sur., 2015. i Rumelhart i sur. 1986.

mogućnosti dubokog učenja. Međutim, i ograničenja postaju sve vidljivija, posebno u organizacijskim postavkama i u situacijama s ograničenim podacima ili s mnogo promjena.[195]

Hibridna inteligencija, koja se ponekad naziva i proširena inteligencija, naglašava pomoćnu ulogu strojnog učenja, tj. dubokih neuronskih mreža i druge tehnike vođene podacima koje su tu da poboljšaju ljudsku inteligenciju, a ne da ju zamijene (baš kao što su teleskopi tu da poboljšaju ljudski vid).[196] Dellermann i sur. definiraju hibridnu inteligenciju kao „sposobnost postizanja složenih ciljeva kombiniranjem ljudske i umjetne inteligencije, čime se postižu superiorni rezultati u odnosu na one koje bi svaki od njih mogao postići zasebno te se kontinuirano poboljšavaju učeći jedni od drugih“.[197] Hibridna inteligencija je vjerojatno učinkovitiji i nijansiraniji pristup rješavanju složenih problema koje ljudi i strojevi nastoje riješiti sami. Prema jednoj definiciji, hibridna inteligencija je „...kombinacija ljudske i strojne inteligencije koja povećava ljudski intelekt i sposobnosti, umjesto da ih zamjenjuje i postiže ciljeve koji su bili nedostižni i ljudima i strojevima”. Na društvenim mrežama moguće je dakle kombinirati ljudsku inteligenciju i inteligenciju stroja radi postizanja boljih rezultata u (pre)oblikovanju uvjerenja, načela i vrijednosti korisnika i prilagođavanju informacijskih sadržaja prema utvrđenim obrascima razmišljanja i preferencijama.

Slika 7. ilustrira kako hibridna inteligencija kombinira upotrebu ova dva oblika inteligencije:[198]

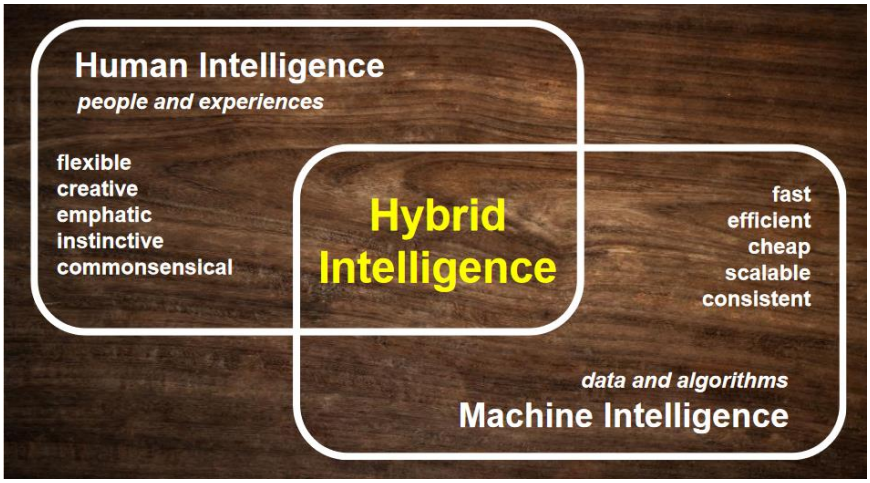
- Ljudsku inteligenciju, koja se odnosi na ljude i iskustva, može se okarakterizirati kao fleksibilnu, kreativnu, empatičnu, instinktivnu i zdravorazumsku.
- Strojnu inteligenciju, koja se odnosi na podatke i algoritme, može se okarakterizirati kao brzu, učinkovitu, jeftinu, skalabilnu i dosljednu.

195 van der Aalst, 2021., str. 8.

196 Ibid., str. 9.

197 Ibid.

198 Ibid., str. 10.



Izvor: Van der Aalst, W.M.P., Hybrid Intelligence: to automate or not to automate, that is the question, International Journal of Information Systems and Project Management, 2021., str.10.

Slika 7. Grafički prikaz hibridne inteligencije i kombiniranje učinaka koji se ostvaruju primjenom ljudske inteligencije i strojne inteligencije.

Slika 7. pokazuje prikaz hibridne inteligencije i kombinirane učinke koji se ostvaruju primjenom ljudske i strojne inteligencije. Slikom 7. želi se naglasiti kako hibridna inteligencija ima za cilj spojiti najbolje od oba svijeta, što se ostvaruje na dva načina. Tradicionalna uporaba umjetne inteligencije/strojnog učenja u organizaciji i automatizaciji podataka podrazumijeva da se umjetna inteligencija/strojno učenje koriste za pružanje podrške u odlučivanju ili kao pomoć u obavljanju zadataka koji se ponavljaju. Na primjer, predviđanje „prodaje“ informacijskog sadržaja u formi reklame i oglasa na društvenim mrežama temelji se na osobnim preferencijama njihovih korisnika i ono podržava donošenje odluka u logistici i proizvodnji novih sličnih informacijskih sadržaja, ili da algoritmi strojnog učenja pomažu ubrzati standardne rutine u odabiru ciljanih publika. U ovom procesu čovjek ima kontrolu, a umjetna inteligencija/strojno učenje koristi se kao učinkovit alat koji odabire ciljanu publiku. Drugi način je kad se strojna inteligencija koristi za automatsku obradu zadataka bez ljudske intervencije. Međutim, i tada, u iznimnim slučajevima stroj može pozvati čovjeka u pomoć kad je to potrebno.[199]

199 Ibid.

2.7. Društvene mreže, osnovna obilježja i definicije

Društvene mreže sastavni su dio društvenih medija i digitalnih platformi. Društveni mediji definiraju se kao internetski ili digitalni mediji koji pružaju, prikupljaju te koji omogućavaju dvosmjernu razmjenu informacija i razmjenu informacija između više strana. U društvene medije ubrajaju se web stranice za društveno umrežavanje i blogovi.[200] Digitalne platforme definiraju se kao skup tehnologija koje pomažu u razvijanju aplikacija i procesa koji potiču interakcije i stvaranje informacijskih sadržaja, dijeljenje veza do informacijskog sadržaja koji proizvodi treća strana, ažuriranje korisničkih profila, trenutačnih aktivnosti, sklonosti, razmjenu podataka, poveznica, fotografija, videozapisa te komentara.[201] U bezgraničnom globaliziranom informacijskom prostoru društvene mreže su novi informacijsko-komunikacijski i medijski kanal preko kojeg je moguće neposredno povezivati interese, ideje, vrijednosti, uvjerenja i načela koja stvaraju i dijele korisnici njihovih usluga (pojedinci, grupe, organizacije, korporacije, industrije, društva i države). Na društvenim mrežama informacijski sadržaji mogu biti u formi teksta, zvuka, slike i videa, a organiziraju se i rangiraju kako bi bili vidljiviji te kako bi ih se učinkovitije povezalo s krajnjim korisnicima.[202] „Funkcija društvenih mreža nije u pukom širenju informacija i informacijskih sadržaja, nego u određivanju uvjeta prema kojima će se neka informacija i/ili informacijski sadržaj širiti, dijeliti i objavljivati.“[203] Korisnici društvenih mreža pri registraciji nisu obvezni navoditi stvarne i objektivno točne osobne podatke. Činjenica je da su vlasnici društvenih mreža omogućili korisnicima njihovih usluga da, na temelju unesenih lažnih podataka, mogu komunicirati i razmjenjivati podatke i informacije u realnom vremenu. Također je činjenica da su postavkama odredili da umjetna inteligencija na osnovi određenih kriterija na društvenim mrežama određuje kojim će

200 Ministarstvo domovinske sigurnosti SAD-a, 2014.

201 Vilmer J.-B. Jeangène, Escorcia A., Guillaume M., Herrera J., Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, Paris, 2018. Dostupno na: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (uvid ostvaren 18.06. 2020.)

202 Usp. Vilmer i autori, 2018; prema definiciji društvenih platformi koju je dalo Francusko nacionalno digitalno vijeće (La Neutralité des plateformes), 2014.

203 Mlinac, Akrap, Lazić 2021.; prema Howard i Parks, 2012; Neudert Maria Lisa i Nahema Marchal, Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service, Brussels, 2019.

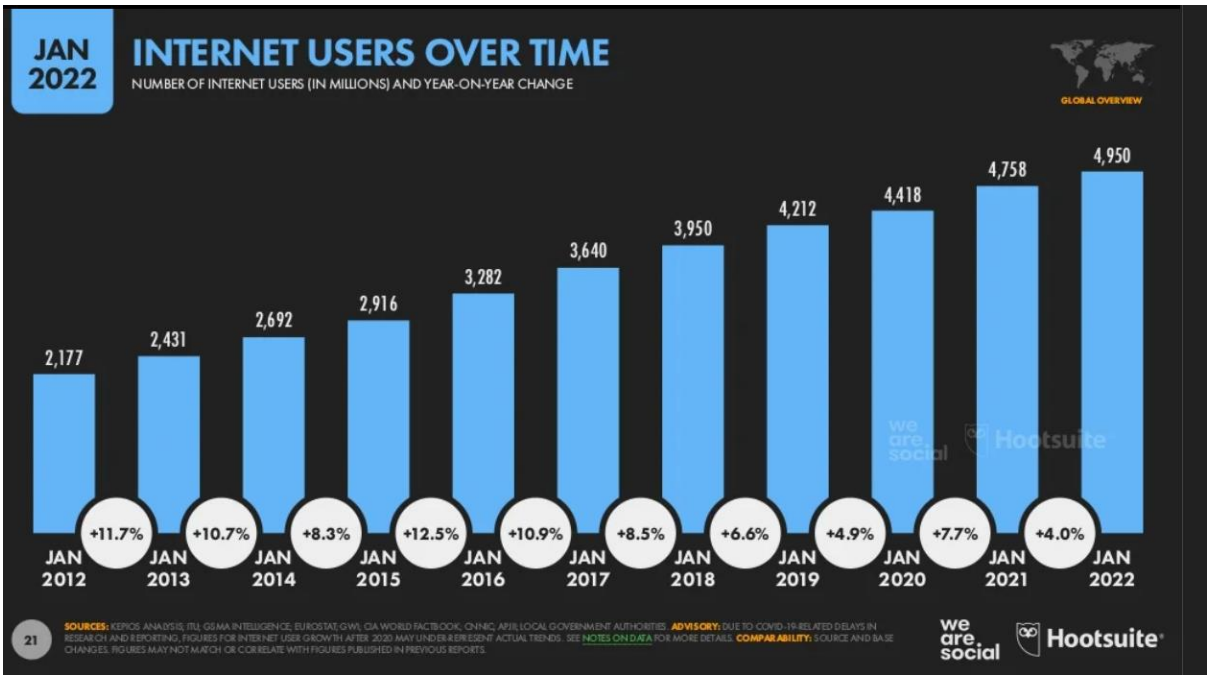
publikama biti vidljiviji samo određeni podaci i informacije. Merriam-Webster definira društvene medije kao oblik elektroničke komunikacije putem koje korisnici stvaraju vlastite zajednice za dijeljenje informacija, ideja, osobnih poruka i drugih sadržaja. Društvene mreže definira kao mogućnost stvaranja i održavanja osobnih i poslovnih odnosa. Društveni mediji su put koji omogućava prenošenje poruka ciljanim publikama u obliku videa, fotografija, grafika, blogova i još mnogo toga. Društvene mreže su alati pomoću kojih se koriste društveni mediji. Društvene mreže omogućavaju izgradnju kontinuiranih odnosa koji se baziraju na izgradnji povjerenja. Globalni informacijski prostor i globalno dostupne društvene mreže omogućili su globalnu digitalnu povezanost. Od ukupnog broja svjetske populacije 7,91 milijardi, 5,31 milijardi ili 67,1% koristi mobilne telefone, a 4,95 milijarde ili 62,5% koristi internet, 4,62 milijardi ili 58,4%, aktivno koristi društvene mreže.[204] Zanimljivo je usporediti da od ukupnog postotka svjetske populacije 57% živi u urbanim područjima a da je broj aktivnih korisnika društvenih mreža spomenutih 58,4%, što znači da je gotovo svaki „urbani“ stanovnik korisnik barem jedne društvene mreže. U odnosu na siječanj 2021., u siječnju 2022. broj svjetske populacije povećao se za 1% tj. za 80 milijuna stanovnika, broj korisnika mobilnih telefona povećao se za 1,8% tj. za 95 milijuna, broj korisnika interneta povećao se za 4% tj. za 192 milijuna korisnika. Najveći porast bilježi broj korisnika društvenih mreža za 10,1% ili 424 milijuna novih korisnika.[205] Od ukupnog broja svjetske populacije 96,2% koristi pametne mobilne telefone. Evidentno je da su eksponencijalnom rastu interneta i društvenih mreža pridonijele njihove mobilne aplikacije dostupne preko mobilnih uređaja. Time su promijenili i navike ljudi. Prosječan korisnik interneta dnevno na internetu provede 6 sati i 58 minuta, od čega prosječno 2 sata i 27 minuta na društvenim mrežama, a 2 sata u pregledavanju medija.[206] Najveći broj korisnika (92,1 %) internetu pristupa putem mobilnih telefona.[207] Preko mobilnih telefona na internetu prosječno dnevno provedu 3 sata i 37 minuta.

204 We are Social, DIGITAL 2022: GLOBAL OVERVIEW REPORT, (26.01.2022.) Dostupno na https://datareportal.com/reports/digital-2022-global-overview-report

205 Ibid.

206 Ibid.

207 Ibid.



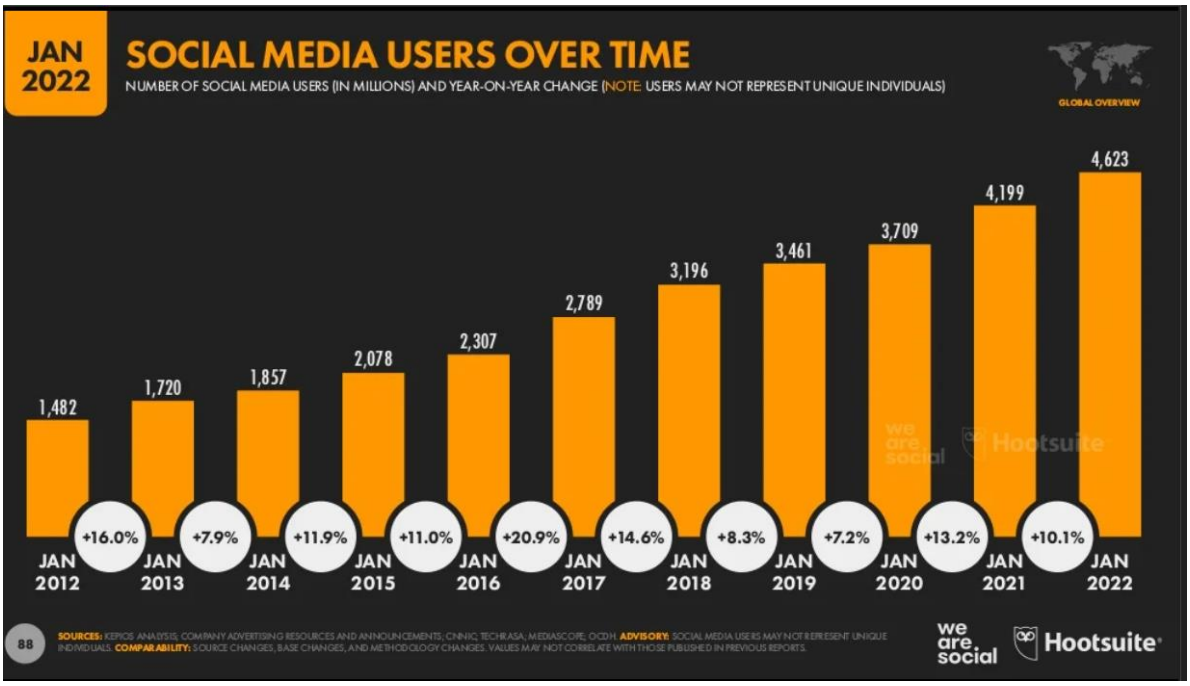
Izvor: We are Social, Digital 2022.

Slika 8. Grafički prikaz trenda eksponencijalnog rasta korisnika interneta.

Iz grafičkog prikaza na Slici 8. prepoznaje se trend eksponencijalnog rasta korisnika globalnog informacijskog prostora u razdoblju od 2012. do 2022. s prosječnim godišnjim rastom korisnika. Pronalaženje informacija glavni je razlog njegovog korištenja od čak 61%, na održavanje komunikacije s prijateljima i članovima obitelji otpada 55,2%, interes za vijestima i događajima iznosi 53,1%, a na pronalaženje ideja i inspiracija otpada 47,5%.[208] Od ukupnog broja na globalnoj razini svega 33,8% korisnika interneta zabrinuto je zbog moguće zloupotrebe osobnih podataka od strane tehnoloških tvrtki.[209]

208 Ibid.

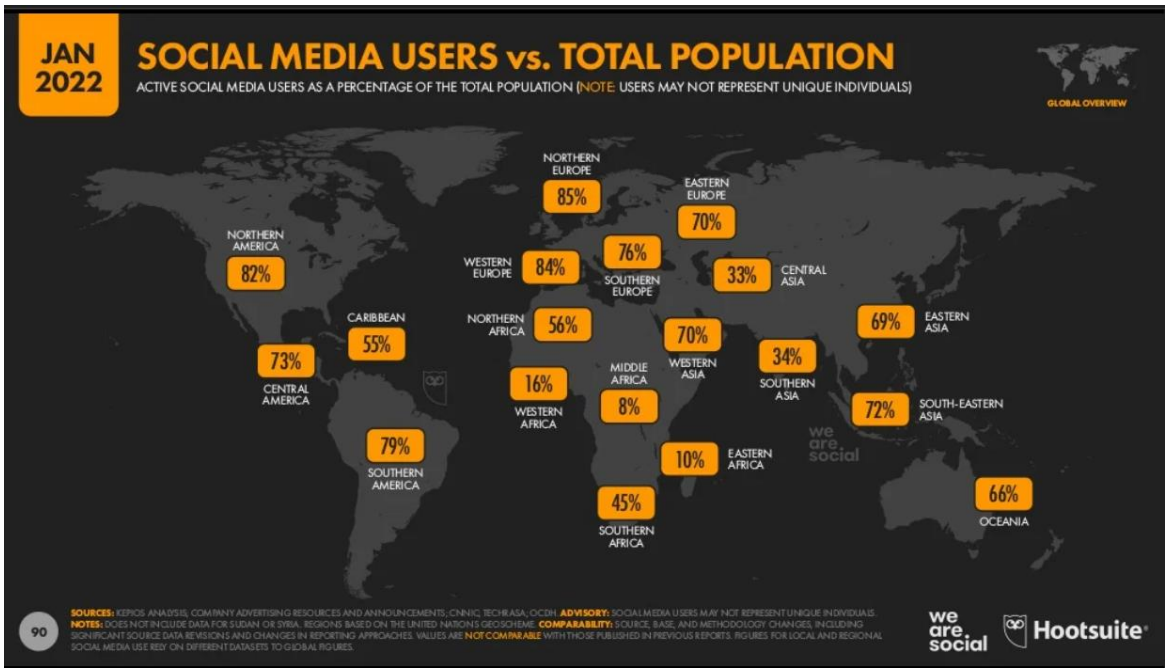
209 Ibid.



Izvor: We are Social, Digital 2022.

Slika 9. Grafički prikaz trenda eksponencijalnog rasta korisnika društvenih mreža od siječnja 2012. do siječnja 2022.

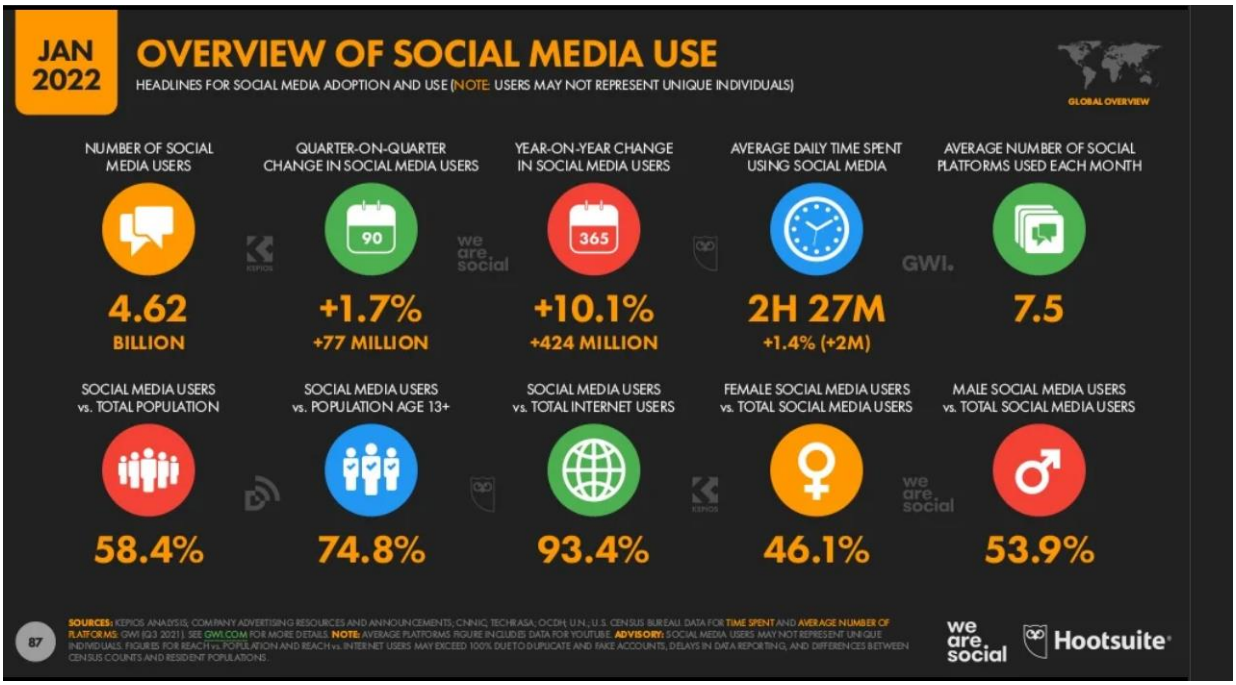
Iz grafičkog prikaza na Slici 9. vidljiv je trend eksponencijalnog porasta korisnika društvenih mreža za razdoblje od 2012. do 2022. U usporedbi s postotkom porasta korisnika interneta sa Slike 8. prepoznaje se kako je porast korisnika društvenih mreža u istom razdoblju veći u postotku na godišnjoj razini. Također, usporedbom Slike 9. sa Slikom.1. prepoznaje se kako je porast korisnika društvenih mreža koincidirao s razdobljem razvoja umjetne inteligencije u kojem je došlo do snažne primjene strojnog učenja koje se bazira na dubokim neuronskim mrežama.



Izvor: We are Social, Digital 2022.

Slika 10. Grafički prikaz globalne dostupnosti društvenih mreža prema kontinentima.

Slikom 10. želi se prikazati broj aktivnih korisnika društvenih mreža u ukupnom broju populacije na pojedinim kontinentima. Ovom slikom želi se prikazati kako se najveći udio aktivnih korisnika društvenih mreža, s preko 80%, nalazi unutar populacija na područjima Zapadne i Sjeverne Europe i sjeverne Amerike, zatim, s preko 70%, na područjima Južne Europe, Središnje i Južne Amerike te Jugo-istočne Azije, s 70% na područjima Zapadne Azije i Istočne Europe, s preko 60%, na područjima Istočne Azije i Oceanije, s ispod 50% na područjima afričkog kontinenta, Središnje i Južne Azije.



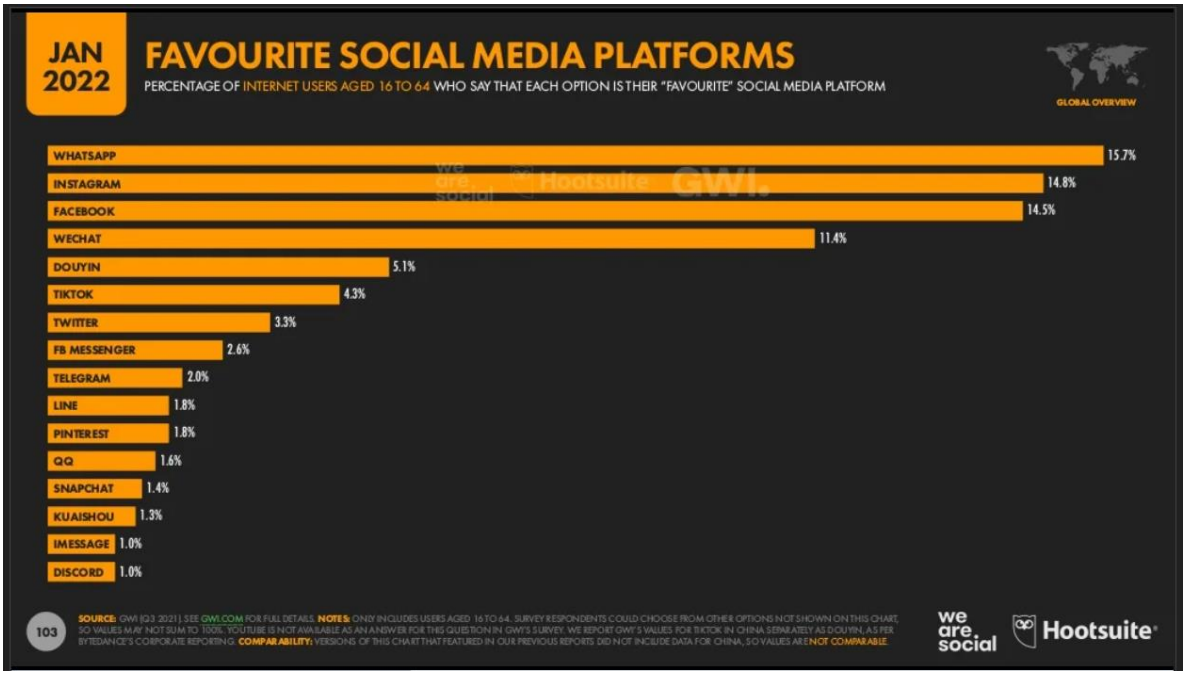
Izvor: We are Social, Digital 2022.

Slika 11. Grafički pregled korištenja društvenih mreža.

Iz prikaza na Slici 11. koji upućuju na omjere angažmana korisnika društvenih mreža prema pojedinim kategorijama upotrebe društvenih mreža, proizlazi da ukupan broj korisnika društvenih mreža trenutno broji 4,62 milijardi korisnika, da na kvartalnoj godišnjoj razini broj novih korisnika društvenih mreža raste za 1,7% ili za 77 milijuna, odnosno da je na godišnjoj razini u razdoblju od siječnja 2021. do siječnja 2022. porast novih korisnika društvenih mreža iznosio 10.1% ili 424 milijuna novih korisnika. Također, iz navedene slike proizlaze podaci da korisnici društvenih mreža u prosjeku dnevno na društvenim mrežama provedu 2 sata i 27 minuta, da svaki korisnik na mjesečnoj razini koristi 7,5 vrsta društvenih mreža, da je najveći postotak korisnika, 74,8% svjetske populacije, iznad 13 godina starosti, da društvene mreže koristi 58,4 % ukupne svjetske populacije, da društvene mreže koristi 93,4 % korisnika interneta od čega 46,1% žene a 53,9% muškarci.

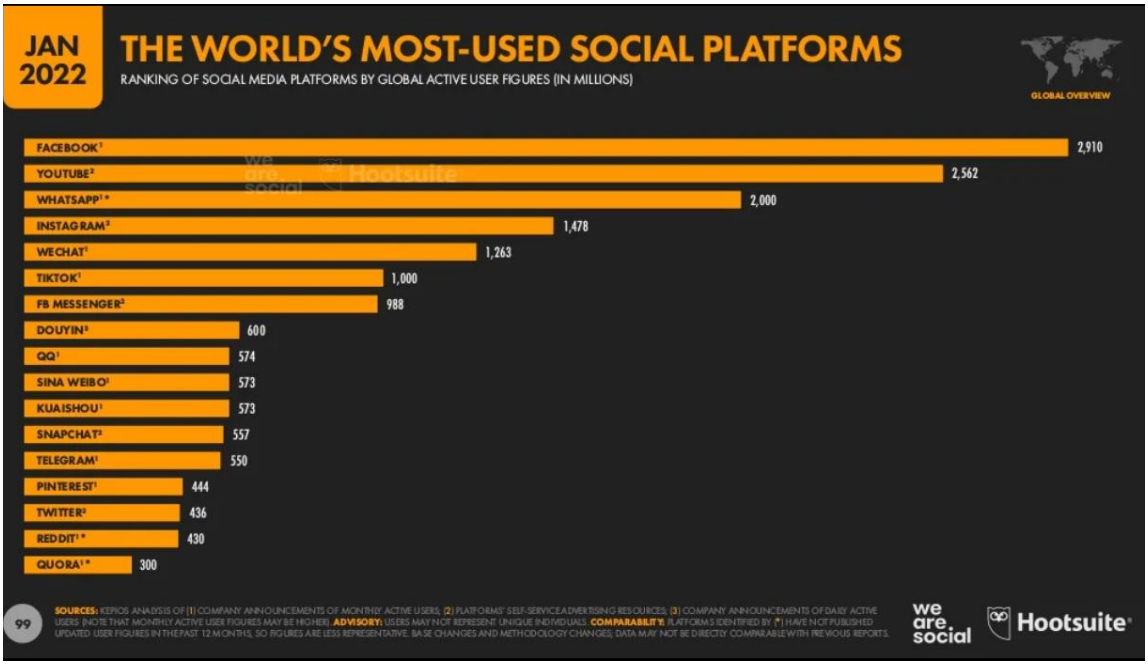
Niže navedenim slikama, 12. i 13., želi se prikazati da su Facebook (Meta) i njezine mobilne aplikacije WhatsApp, Instagram i Facebook Messenger za 45 % korisnika interneta, u starosnoj skupini od 16 do 64 godine, najpopularnije društvene mreže. Također želi se prikazati kako ukupan zbroj korisnika Facebooka (Mete) s navedenim mobilnim aplikacijama iznosi oko 7 milijardi i 376 milijuna korisnika, da je You Tube, koji broji 2 milijarde i 562 milijuna korisnika, nakon Facebooka (Mete) druga po redu najkorištenija društvena mreža, te da Twitter,

kao najpopularniju društvenu mrežu koju koriste političari, koristi svega 3,3% od ukupnih korisnika interneta s 436 milijuna aktivnih korisnika.



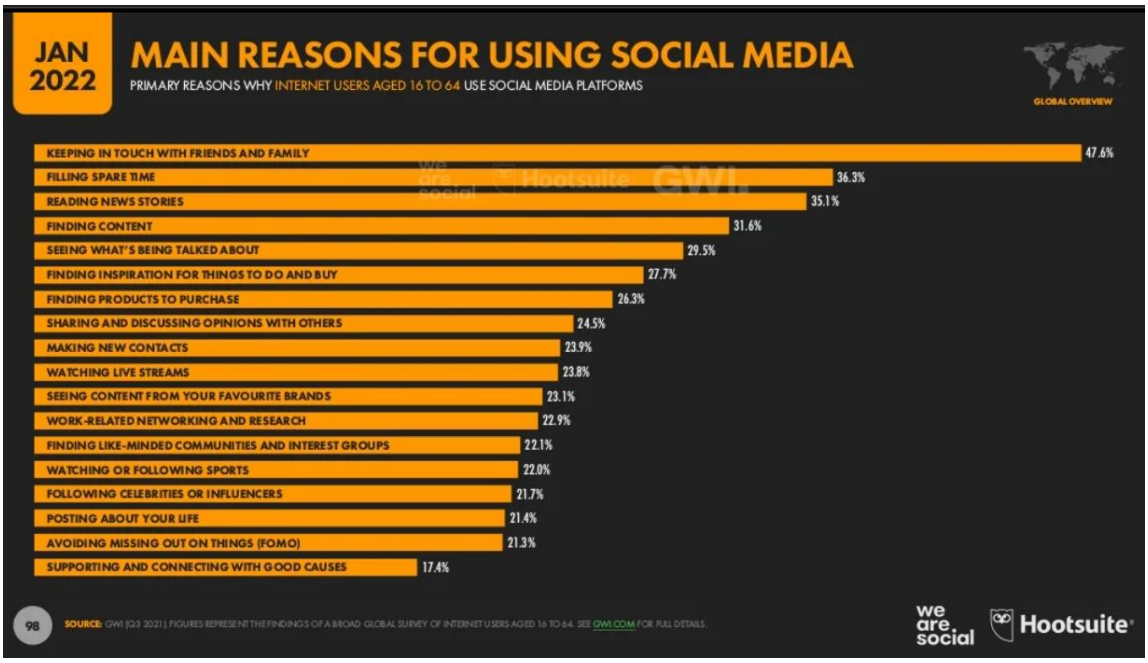
Izvor: We are Social, Digital 2022.

Slika 12. Grafički prikaz najpopularnijih društvenih mreža.



Izvor: We are Social, Digital 2022.

Slika 13. Grafički prikaz najkorištenijih društvenih mreža po broju korisnika.



Izvor: We are Social, Digital 2022.

Slika 14. Prikaz glavnih razloga upotrebe društvenih mreža.

Slikom 14. želi se prikazati da društvene mreže njihovi korisnici, najčešće, u postotku od 46,7% koriste za održavanje kontakata s obitelji i prijateljima, 36,4% ih koristi za popunjavanje slobodnog vremena, 35,1% za čitanje novih priča, 31,6% za pronalaženje novih sadržaja, 29,5% za uvide u aktualnosti o različitim kategorijama događaja i vijesti, 24,5% za razmjenu mišljenja i vođenje rasprava, 23,9% za stvaranje novih kontakata, 23,8% za gledanje direktnih prijenosa različitih događaja uživo i 22,1% za pronalaženje zajednica i grupa sa sličnim stavovima i mišljenjima. Ostali segmenti korištenja društvenih mreža su u manjem postotku te nisu predmet istraživanja.

Facebook (Meta) trenutno dominira na globalnom tržištu digitalnog marketinga. Dominantni položaj u njemu dodatno osigurava zahvaljujući globalnoj dostupnosti vlastitih aplikacija WhatsApp, Facebook Messenger te Instagram za dopisivanje na mobilnim uređajima. Na YouTubeu kao drugoj najpopularnijoj društvenoj mreži po broju aktivnih korisnika i trenutno vodećoj globalnoj internetskoj platformi za stvaranje i diseminaciju video sadržaja i pružanje usluga izravnog prenošenja video i audio sadržaja u realnom vremenu od početka 2021. velik dio prometa ostvaruje posredstvom drugih društvenih mreža. U prvom redu preko Facebookovog linka shim l.facebook.com koji u prosjeku generira 40 milijuna mjesečnih posjeta YouTubeu, dok je na drugom mjestu društvena mreža Reddit.com posredstvom koje

YouTube ostvaruje 26,6 milijuna pregleda mjesečno. Jedna od značajki YouTubea je da njegovi korisnici najčešće posjećuju samo jednu stranicu prije njezinog napuštanja. Primjerice u listopadu 2020. stopa napuštanja početne stranice YouTubea dosegla je 52%. Ovaj podatak znači da algoritmi preporuka i rangiranja sadržaja na YouTubeu u navedenom postotku uspijevaju zadržati pažnju korisnika na određene informacijske sadržaje čime u istom tom postotku mogu utjecati na (pre)oblikovanje načina razmišljanja o samim sadržajima koji se pregledavaju. Popularnosti YouTubea u značajnoj mjeri pridonosi mogućnost pristupanja posredstvom mobilnih uređaja, u prosjeku 4,63 stranice po sesiji u odnosu na 2,84 stranice koje korisnici YouTubea posjećuju posredstvom stolnih računala. Znakovito je istaknuti da su vodeće web stranice koje su posjećivali korisnici zahvaljujući poveznici na YouTube.com bile Google.com s više od 180 milijuna posjeta i Amazon.com s blizu 55 milijuna posjeta.[210] Ova činjenica upućuje na podatak da je u 2021. YouTube na globalnoj razini od oglašavanja ostvario više od 28,84 milijarde američkih dolara prihoda i da je time Googleu ostvario približno 11,2% ukupnog godišnjeg prihoda.[211] Za obraćanje ciljanim publikama društvenu mrežu Twitter, koji koristi svega 3,3% ukupnih korisnika interneta i koja broji 436 milijuna aktivnih korisnika, najčešće koriste političari, izabrani dužnosnici, vlade i ministarstva. Jedan od razloga je što je Twiter specijaliziran za stvaranje i diseminaciju kratkih poruka u obliku fotografija ili kratkih audio i videozapisa, mikroblogova i teksta do 280 znakova.[212] Ova društvena mreža broji konstantan rast mjesečno aktivnih korisnika na globalnoj razini koji se mogu unovčiti. U četvrtom tromjesečju 2020. Twitter imao 192 milijuna dnevno aktivnih korisnika, koji je u istom razdoblju 2021. porastao na 211 milijuna korisnika.[213] Prije nego što je tvrtka prestala izvještavati o metrici, posljednja objavljena brojka o mjesečnim aktivnim korisnicima iznosila je 330 milijuna.[214] Registrirani korisnici mogu čitati i objavljivati tweetove, kao i pratiti druge korisnike putem ažuriranja. Nakon što je tvrtka izašla na burzu u studenome 2013. bila je rangirana jednom od najvećih američkih internetskih tvrtki s tržišnom kapitalizacijom. U 2019. prihod tvrtke iznosio je 3,46 milijardi američkih dolara uz neto prihod od preko 1,47 milijardi

---

210 Statista.com, YouTube - Statistics & Facts, L. Ceci (20.03. 2022.) Dostupno na https://www.statista.com/topics/2019/youtube/#dossierKeyfigures

211 Ibid.

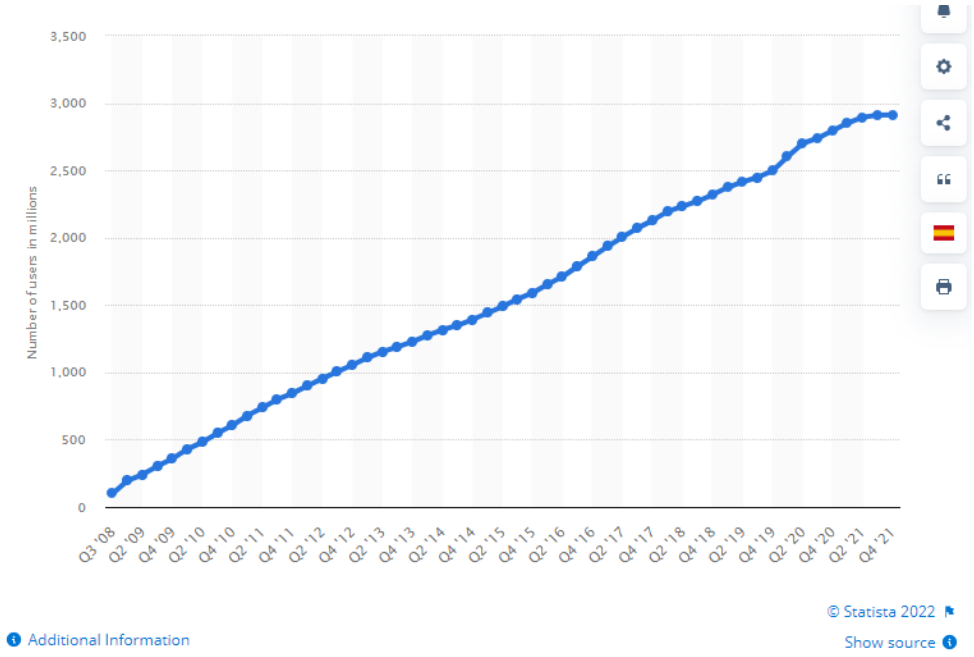
212 Statista.com, Twitter - Statistics & Facts, Statista Research Department (20.03.2022.). Dostupno na: https://www.statista.com/topics/737/twitter/#dossierSummary__chapter1

213 Statista.com, Number of monetizable daily active Twitter users (mDAU) worldwide from 1st quarter 2017 to 3rd quarter 2021 (20.03.2022.). Dostupno na: https://www.statista.com/statistics/970920/monetizable-daily-active-twitter-users-worldwide/

214 Ibid.

američkih dolara, od kojih je većinu ostvario oglašavanjem što ga je, uz Facebook i YouTube, odredilo jednom od tri vodeće tvrtke koje ostvaruju najveće prigode od objavljivanja i pružanja usluga reklama i oglašavanja. Važno je pri tome, u kontekstu negativnih posljedica na organizaciju korpusa javnog znanja, napomenuti podatak da se korisnici Twittera, kao i u slučaju Facebooka i YouTubea, u stvaranju i diseminaciji video sadržaja mogu koristiti lažnim profilima.

Stoga će se primjena Facebooka, YouTubea i Twittera u organizaciji korpusa javnog znanja u nastavku istraživanja prikazati na primjerima mogućnosti njihove zloupotrebe u napadačkim informacijskim operacijama (psihološkim operacijama) koje različiti akteri usmjeravaju na prostor javnog znanja ciljanih publika tijekom kriza i poraća. Ostale društvene mreže prikazane u gore navedenim grafikonima nisu predmet istraživanja.



Izvor: Statista.com, Facebook - statistics & facts, 2022.

Slika 15. Grafički prikaz eksponencijalnog trenda rasta mjesečno aktivnih korisnika[215] Facebooka u milijunima na globalnoj razini za razdoblje od 3. kvartala 2008. do 4. kvartala 2021.

215 Facebook mjeri mjesečno aktivne korisnike kao korisnike koji su se prijavili tijekom posljednjih 30 dana. Brojke ne uključuju korisnike Instagrama ili WhatsAppa, osim ako bi se kvalificirali kao takvi korisnici, odnosno na temelju svojih drugih aktivnosti na Facebooku.

Slikom 15. želi se pokazati eksponencijalni mjesečno aktivni rast korisnika Facebooka (Mete) za razdoblje od 3. kvartala 2008. do samog početka 2022. godine. 2021. godina za Facebook bila je značajna po tome što se promjenom imena u Meta Platforms Inc. tvrtka Facebook Inc. nastoji odmaknuti od negativnih konotacija s kojima se suočila pod nazivom Facebook zbog tužbi protiv monopola, pitanja privatnosti, niskih poreznih davanja, širenja dezinformacija i govora mržnje.[216] Kroz novo ime tvrtka je ponudila novu uslugu metaverzum.[217] Promjenom imena Facebook, Instagram, Facebook Messenger i WhatsApp postali su podružnicama Meta platforme te se javnosti predstavljaju kao Obitelj aplikacija Meta.[218] Promjena imena može se dovesti u korelaciju s korporativnim restrukturiranjem Googlea i osnivanjem matične i holding tvrtke Alphabet Inc. 2015. Promjena imena i daljnji razvoj u primjeni umjetne inteligencije u vlastitim uslugama Meti je 2021. donio porast prihoda od 31 milijardu američkih dolara u odnosu na prethodnu godinu. Ukupni prihod Obitelj aplikacija Meta za 2021. iznosio je 115,66 milijardi američkih dolara. Zahvaljujući dodatnom razvoju umjetne inteligencije radi pružanja novih usluga Meta's Reality Labs, odjel tvrtke za virtualnu stvarnost generirao je 2,27 milijardi dolara. Tako su primjerice izdaci za marketing Mete za 2021. iznosili nešto više od 14 milijardi američkih dolara, u odnosu na 11,6 milijardi američkih dolara u prethodnoj godini. Unatoč njegovoj popularnosti i uspjehu, značajan dio javnosti nema pozitivne stavove o novim uslugama metaverzuma i skeptičan je u tome da će promjena brenda promijeniti pristup njegovih vlasnika u primjeni umjetne inteligencije. Međutim, činjenica je da je Facebook često korišten kao izvor vijesti diljem svijeta i da ga različiti izdavači i oglašivači od siječnja 2022. koriste za poslovne interese preko kojeg ostvaruju najveću interakciju s vlastitim ciljanim publikama. U pretežnom dijelu radilo se o tradicionalnim medijskim kućama. Primjerice dailywire.com je bio rangiran kao vodeći izdavač kojeg su slijedili bbc.co.uk, dailymail.co.uk i cnn.com sa svojim web digitalnim verzijama. Zbog lake dostupnosti izvora vijesti i aktualnih događaja, platforma Mete suočava se s mnoštvom potencijalno obmanjujućih i štetnih sadržaja. Kako bi otklonila navedene sadržaje tijekom 2021. Meta je uklonila približno 6,5 milijardi lažnih računa, od čega su 34 milijuna primjeraka bili klasificirani kao uznemiravajući te su, kao takvi, uklonjeni.[219] Broj korisnika povećao se, unatoč problemima sigurnosti podataka i prošlim

216 Statista.com, Facebook - statistics & facts, 2022.

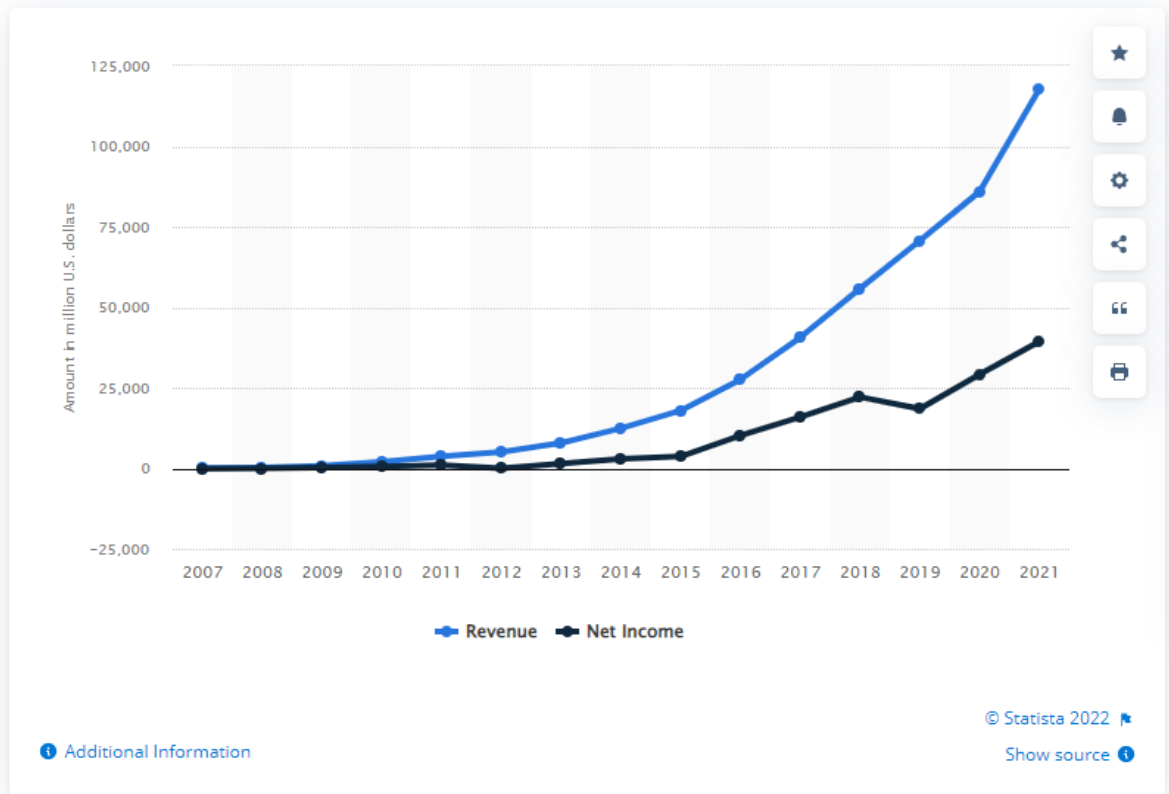
217 Statista.com, Facebook - statistics & facts (20.03.2022.) Dostupno na https://www.statista.com/topics/751/facebook/#topicHeader__wrapper

218 Engl. Meta's Family of Apps.

219 Ibid.

kontroverzama kao što je skandal Cambridge Analytica iz 2018. i unatoč negativnim posljedicama koje je izazvao u javnosti 2016. kad su ga ruski hakeri iskoristili za destabilizaciju izbornog procesa u SAD-u prilikom izbora novog američkog predsjednika. Facebook je u svijetu digitalnog marketinga u međuvremenu dodatno osnažio lidersku poziciju. Vlastite usluge i proizvode javnosti predstavlja misijom u izgradnji zajedništva i zbližavanju svijeta, aplikacije predstavlja alatima za povezivanje prijatelja, obitelji i pronalaženje zajednica i za omogućavanje rasta poslovanja drugim tvrtkama. No, Facebooku kao tehnološkoj korporaciji, prioritet nisu njezini korisnici, nego su to kupci njegovih proizvoda i stvaranje baza osobnih podataka korisnika pohranjenih na vlastitim serverima. Osobne podatke (uvjerenja, načela i vrijednosti) korisnici Facebooka daju besplatno kako bi zauzvrat besplatno koristili njegove usluge. Facebook ove podatke uz ostale identifikacijske podatke prikuplja, pohranjuje na serverima, obrađuje ih i prodaje na tržištu digitalnog marketinga kao robu koja ima svoju tržišnu vrijednost. Prikupljanje, pohrana, obrada i prodaja (pre)oblikovanih osobnih podataka nije transparentna, njegove usluge koriste se za širenje dezinformacija, a želja za profitom i nedostatak volje njegovih vlasnika u otklanjanju njegove zloupotrebe postali su prvorazredno političko i sigurnosno pitanje. S obzirom na dosadašnja iskustva o moći tehnologija umjetne inteligencije i mogućnosti njezine zlouporabe za širenje dezinformacija kao i skeptičnost javnosti oko pobuda vlasnika Facebooka za promjenom imena u Meta, ideje o metaverzumu koji Meta želi ponuditi kao komercijalnu uslugu izazivaju dodatnu zabrinutost javnosti i akademske zajednice o daljnjim mogućnostima zlouporabe novih tehnoloških dostignuća koja se primjenjuju u razvoju umjetne inteligencije za potrebe pružanja usluga multiverzuma svijeta nove virtualne stvarnosti.[220]

220 Usp. Ibid.



Izvor: Statista.com, Facebook - statistics & facts, 2022.

Slika 16. Grafički prikaz rasta prihoda i neto dohotka tvrtke Meta (bivši Facebook) za razdoblje od 2007. do 2021.

Slika 16. prikazuje omjer eksponencijalnog porasta prihoda i neto dohotka Facebooka od 2007. do 2021. U usporedbi sa slikom 1. proizlazi da je navedeni eksponencijalni porast koincidirao u razdobljima u kojem je najprije došlo do razvoja strojnog učenja, od. 2010., a nakon toga i do napretka strojnog učenja baziranog na primjeni dubokih neuronskih mreža.

Jedan od osnovnih razloga značajnog porasta korištenja društvenih medija i društvenih mreža rezultat je sve prisutnijeg emitiranja različitih sadržaja s tradicionalnih medija (TV-a) posredstvom aplikacija društvenih mreža na mobilnih uređajima. Korištenje TV-a kao tradicionalnog medija nadopunjeno je mogućnošću uključivanja ciljanih publika u različite oblike aktivnosti posredstvom pametnih telefona i mobilnih uređaja, od provjera informacija do interakcija s drugim korisnicima tijekom praćenja vijesti i događaja posredstvom TV-a. Ovaj fenomen višeznačnog korištenja tradicionalnih i netradicionalnih medija dodatno je osnažen društvenim mrežama pomoću kojih njihovi korisnici povećavaju vlastitu međusobnu interakciju čime postaju direktni akteri u različitim događajima, obavijestima, vijestima i informacijskim sadržajima koji se stvaraju i dijele putem tradicionalnih medija.

Jedan od osnovnih i najučinkovitijih načina za stvaranje interakcija na društvenim mrežama u vidu stvaranja vlastitih i pretraživanja željenih informacijskih sadržaja obavlja se putem hashtagova. Hashtag predstavlja bilo koju riječ koja ispred sebe ima oznaku # pomoću koje se pretražuje određeni pojam ili poruka s takvom oznakom. Može ga stvoriti svaki korisnik društvenih mreža i kao takav postoji dok je poruka aktivna. U ovom obliku osmislio ga je Twitter 2007. kao novi način grupiranja poruka. Značajan porast njegove upotrebe ostvaren je 2009. kada je Twitter dodao linkove na sve hashtagove čime je svojim korisnicima dodatno olakšao pretraživanje preferencija. Hashtag su, zbog odlične primjenjivosti, usvojile i druge društvene mreže. Hashtag se pokazao učinkovitim alatom informiranja tijekom kriznih situacija, protesta i sl. jer se poruke brzo šire, na jednostavan način ih može stvarati svatko te ih može pratiti svatko tko želi sudjelovati u određenim događajima. Primjeri su događanja, krize i prirodne katastrofe poput: #OccupyWallStreet, #HurricaneSandy, #Syria i dr.[221] Priroda platformi društvenih mreža otvorila je put novim vrstama interaktivne komunikacije u stvarnom vremenu. Političari i njihovi oponenti koriste ih kao alate kako bi ciljanim publikama promijenili poglede na različita politička ili društvena pitanja prema vlastitim interesima. [222]

Osnovne karakteristike društvenih mreža u nastavku istraživanja prikazat će se kroz primjenu umjetne inteligencije u procesuiranju, obradi, analizi i (pre)oblikovanju uvjerenja, načela i vrijednosti korisnika društvenih mreža u cilju kreiranja i isporučivanja informacijskih sadržaja prema istim ili sličnim uvjerenjima, načelima i vrijednostima.

2.8. Primjena umjetne inteligencije na društvenim mrežama

Primarna funkcija i zadaća umjetne inteligencije na društvenim mrežama jest prikupljanje, pohrana, obrada informacija i podataka. U obavljanju ovih zadaća glavnu ulogu imaju opisane tehnologije umjetne inteligencije čije su postavke određene komercijalnim interesima njihovih vlasnika.

Na društvenim mrežama umjetna inteligencija prikuplja, pohranjuje i (pre)oblikuje tri osnovne kategorije podataka. Prvu kategoriju čine metapodaci. Radi se o podacima podataka. Njihovo stvaranje, prikupljanje i obradu omogućila je primjena digitalnih tehnologija. „Metapodaci su (tehnički) podaci o podacima, koji ne sadrže informacije o sadržaju ili dijelovima sadržaja

221 GoDigital, Hrvatski Telekom, Što je hashtag i čemu služi, (12.01.2016.), dostupno na: https://godigital.hrvatskitelekom.hr/sto-je-hashtag-i-cemu-sluzi/ (30.03.2022.)

222 Statista.com., Social media and events - Statistics & Facts, Statista Research Department, (30.03. 2022). Dostupno na https://www.statista.com/topics/2040/social-media-and-events/#topicHeader__wrapper

primarne informacije, već podatke o mjestu i vremenu kada je neki skup podataka napravljen, sredstvu kojim je to urađeno, tko je ih je napravio, kome ih je poslao i tako dalje. Svaki skup ovakvih podataka smješten je u neku digitalnu datoteku koja, pored podataka o sadržaju, ima i metapodatke o informacijama o toj datoteci i podrijetlu podataka.“ [223]

Drugu kategoriju podataka čine osobni identifikacijski podaci (engl. Personal Identifiable Informations – PII). Ovi podaci nazivaju se demografskim podacima. Demografske podatke može se definirati kao statističke podatke koji su mjerljivi po broju i količini. Tipično se koriste za identificiranje kvantificiranih podskupina unutar određene ciljane publike. Neki od najčešćih demografskih podataka su osobni podaci kao ime, prezime, spol, dob, mobilnost, radni status, zaposlenje, e-mail, brojevi telefona, adrese, broj putnih isprava, etnička rasna, vjerska, politička pripadnost, zanimanje, interes, hobi, školovanje te drugi slični identifikacijski podaci.

Treću kategoriju podataka čine „ne-osobni podaci“ (engl. non-Personal Identifiable Informations – non PII Data), koji nisu jednostavno vidljivi kao što su vidljivi metapodaci i demografski podaci. „Ne-osobne“ kategorije podataka tehnologije umjetne inteligencije prikupljaju kako bi se nadziralo i bolje razumjelo ponašanje korisnika društvenih mreža na osnovu kojih umjetna inteligencija zauzvrat može poboljšavati njihov daljnji angažman. Na ovoj kategoriji podataka temelji se poslovna politika industrije digitalnog marketinga. U osnovi radi se o uvjerenjima, načelima i vrijednostima, odnosno korisničkim preferencijama korisnika društvenih mreža koje se u svijetu digitalnog marketinga naziva psihografskim podacima.

Psihografski podaci u industriji digitalnog marketinga „određuju stil života“.[224] Oni predstavljaju čimbenike koji obilježavaju nečiju osobnost, težnje i interese. „Varijable koje određuju način života su aktivnosti, interesi i mišljenja o sebi i svijetu, životne navike, o čemu se brinu potrošači, kako troše svoje vrijeme, na što će vjerojatno potrošiti novac i kako promatraju sebe. Ove individualne karakteristike neizbježno utječu na njihove odluke (…), a posebno na preferencije (…)“[225]… čime se između konzumenta i proizvođača „stvara put izgradnji dugog i lojalnog odnosa“.[226]

---

223 Mladenović, 2016, str. 107.

224 Čotić, Dominika, Uloga osobnih i demografskih čimbenika u namjeru online kupovine kod potrošača, Sveučilište u Splitu, Ekonomski fakultet, 2021., str. 22., (29.05.2022). Dostupno na: https://urn.nsk.hr/urn:nbn:hr:124:213833

225 Ibid.

226 Ibid; prema Jiangfeng i Nongbunnak, 2018.

2.9. Planiranje i izvođenje informacijskih operacija

Za potrebe industrije digitalnog marketinga i korisnika njihovih usluga umjetna inteligencija na društvenim mrežama na osnovi prikupljanja i obrade uvjerenja, načela i vrijednosti gradi odnos povjerenja između potrošača i društvenih mreža, ona informacije uobličava u formi marketinških oglasa i poruka na osnovu kojih planira i izvodi personalizirane informacijske operacije.

Ovakva vrsta informacijskih operacija temelji se na umjetnoj inteligenciji koja prikuplja, pohranjuje, analizira, obrađuje demografske i psihografske podatke na osnovu kojih za potrebe vlasnika i korisnika društvenih mreža donosi određene zaključke u predviđanju te nudi rješenja kako bi prikupljenim podacima ponudila dodatnu vrijednost. Skup ovih podataka čine baze Velikih podataka (engl. Big Data) korisnika društvenih mreža koje su u vlasništvu društvenih mreža i koje ovim podacima trguju. U baze Velikih podataka ulaze i podaci iz brojnih drugih i različitih izvora koje proizvode ljudi: s mobilnih aplikacija, interneta, iz komercijalnih transakcija i evidencija. Baze Velikih podataka „mogu generirati strojevi a prikupljati ih se može i uz pomoć objekata povezanih s internetom stvari“[227]. Veliki podaci i primjena umjetne inteligencije u njihovoj obradi jesu ključan element poslovanja tehnoloških korporacija koje upravljaju i razvijaju društvene mreže, oglašivača i drugih tvrtki koje se služe uslugama društvenih mreža u industriji digitalnog i političkog marketinga. „Ne-osobni podaci“ Facebooku predstavljaju ključnu imovinu za ostvarivanje zarade u industriji digitalnog marketinga.[228]

Jedan od boljih primjera kako umjetna inteligencija i baze Velikih podataka ostvaruju utjecaj na korisnike društvenih mreža vidljiv je na primjeni Analitike Velikih podataka (engl. Big Data Analytics)[229] u svrhu ciljanog izlaganja publika na društvenim mrežama personaliziranim informacijskim sadržajima. Ova forma izlaganja pojedinaca personaliziranim informacijama u svijetu digitalnog marketinga naziva se različitim nazivima tehnikom „mikrociljanja“,

---

227 Ibid.

228 Josá Gonzáles-Cabanás, Ángel Cuevas, Rubén Cuevas, Juan López-Fernández, David García, Unique on Facebook: Formulation and Evidence of (Nano)targeting Individual Users with non-PII Data, 2021., str. 1. Dostupno na: https://arxiv.org/abs/2110.06636

229 Usp. Kumar Ravi, Potential impact of Artificial Intelligence on future strategies, King's College London, 2021., dostupno na https://www.researchgate.net/publication/350022050_Potential_impact_of_Artificial_Intelligence_on_future_strategies

„personaliziranog ciljanja“ ili „nanotargetiranja“. Sve su to pojmovi koji u biti označavaju jedno te isto u svom konačnom cilju a to je utjecanje na donošenje odluka ciljane publike prema potrebi oglašivača. U industriji digitalnog marketinga ono se još naziva modeliranjem sklonosti. U osnovi radi se o automatizaciji svih dijelova isporuke informacijskog sadržaja[230] prema iskazanim preferencijama odnosno slabostima. Psihografski podaci korisnika društvenih mreža vlasnicima društvenih mreža i tvrtkama koje se služe njihovim uslugama omogućuju bolje razumijevanje ponašanja i angažmana ciljanih publika. Budući da su na društvenim mrežama njihovi korisnici strukturirani i grupirani putem algoritama strojnog učenja, društvene mreže omogućavaju personalizirano i izravno ciljanje pojedinca na temelju detaljnih specifikacija koje nadilaze rasu, dob, spol ili društveni položaj. Sinergija umjetne inteligencije, velikih podataka društvenih mreža i primjena Analitike Velikih podataka omogućuje izravno povezivanje planera i izvoditelja marketinških informacijskih operacija sa ciljanom publikom, povećavanje profita uz smanjenje troškova. U određenom smislu, što više ljudi koji su zainteresirani za određeni proizvod ili uslugu vidi oglas ili reklamu, to će tvrtka trošiti manje novca na oglašavanje pojedincima koje takav proizvod ili usluga ne zanima. Pristup brojnim podacima koje je umjetna inteligencija u stanju mjeriti, kao što su oznake sviđanja, nesviđanja, broj proslijeđenih poruka, reakcije na objave, odgovori na objave i još mnogo toga, tvrtkama omogućuje bolje razumijevanje same prirode komunikacije i interakcija između korisnika i informacijskih sadržaja koje razmjenjuju. Na ovaj način vlasnici društvenih mreža dobivaju uvid u „stil života“ korisnika usluga, sukladno kojem isporučuju preferirane informacijske sadržaje. Smještena u središtu rastuće digitalne marketinške scene, analitika podataka i personalizirano izlaganje prilagođenim informacijskim sadržajima prema korisničkim preferencijama tvrtkama na društvenim mrežama pruža priliku da usavrše što relevantnije i pravovremene marketinške poruke, oglase i informacije.

Jedna od zadaća umjetne inteligencije na društvenim mrežama prilikom planiranja i izvođenja informacijskih operacija u industriji digitalnog marketinga odnosi se na upravljanje *botovima*. Sam naziv bot predstavlja kraći pojam od riječi robot. To je automatizirani program koji održava osnovne funkcije i na društvenim mrežama je zadužen za pokretanje rutinskih zadataka: održava interakcije te upravlja stvarnim i lažnim računima. Ovaj program u stanju je

230 Crnčić, 2020. str. 47.

samostalno strojno i automatski širiti poruke ili vijesti.[231] Pomoću botova korisnici Facebooka izražavaju oznake sviđanja ili nesviđanja prema nekom informacijskom sadržaju. Na Twitteru omogućavaju ponovno objavljivanje, odnosno ponavljanje sadržaja u velikom broju. Ovaj automatizirani računalni program s nizom drugih različitih algoritama na društvenim mrežama izvršava ponavljajuće zadatke. Time ovaj program može pojačavati dojam da je neka obavijest i informacija jako bitna i važna, iako to ne mora odgovarati stvarnom činjeničnom stanju.

„Općenito, *botovi* se mogu podijeliti u tri osnovne kategorije:

1. *botovi* koji traže informacije,

2. *botovi* koji traže informacije kako bi odradili specifične zadatke,

3. *botovi* sa socijalnim sposobnostima i zadacima.“ [232]

Koriste se za automatsko komuniciranje, a pomoću rješenja umjetne inteligencije učinkovitije imitiraju ljudsko ponašanje. „Prikupljaju informacije o drugim korisnicima, prate navike i ponašanje. Oni su, stoga, samooptimirajući računalni programi“.[233] Na društvenim mrežama koristi ih se u zakonite i zlonamjerne svrhe.[234]

Osnovna i ključna primjena tehnologija umjetne inteligencije na društvenim mrežama vidljiva je kroz njihovu primjenu u automatiziranom sustavu povratne sprege u kojem imaju snažnu primjenu i učinkovitost kroz sustav prikupljanja, pohrane, obrade, analize, povratnog izvještavanja i isporuka obavijesti i informacija. Prema načelu funkcioniranja povratne sprege osmišljene su specifične tehnike pomoću kojih se ciljane publike pojedinačno, grupno i masovno mogu izlagati personaliziranim informacijskim sadržajima koji su prilagođeni korisničkim preferencijama. Sustav povratne sprege omogućava:[235]

---

231 Baezner Marie i Robin Patrice, Hotspot Analysis: Cyber and Information Warfare in elections in Europe, Center for Security Studies (CSS), ETH Zürich, December 2017, 2017, str. 17.; prema Chu et al., 2012. Hegelich, 2016.

232 Crnčić, 2020. str. 40., prema; Henry D. I. i sur.. Applied Artificial Intelligence: Where AI Can Be Used in Business, Rome, Springer, 2019.

233 Ibid. Teachtoday. Bot ili nije bot? URL: Teachtoday. Bot ili nije bot? URL: https://www.teachtoday.de/hr/Informirati/Stvaranje_mi_ljenja/2535_Bot_ili_nije_bot.htm (18. veljače 2020.)

234 Usp. Kaput, 2021. (10.01.2022.)

235 Akrap 2011., str. 38.

a) „praćenje procesa provođenja isplaniranih i pokrenutih djelovanja“;

b) „brzu i kvalitetnu reakciju s ciljem (re)modeliranja pojedinih aktivnosti na strateškoj i taktičkoj razini, sukladno prikupljenim podacima i informacijama“;

c) „izradu periodičnih i završenih izvješća s prijedlozima poboljšavanja u budućim djelovanjima.“

Kroz sustav povratne sprege umjetna inteligencija održava osnovne funkcije društvenih mreža. Prikupljanjem, obradom, zaključivanjem i planiranjem umjetna inteligencija kroz sustav povratne sprege pospješuje sposobnosti algoritama i drugih računalnih sustava i tehnologija. U poslovnom svijetu digitalnog marketinga umjetna inteligencija a naročito algoritmi i usluge strojnog učenja koristi se „kako bi se stvorili korisni uvidi i modeli predviđanja koji se temelje na ponašanju njihovih korisnika.“[236]

Općenito, može se reći da umjetna inteligencija kroz primjenu strojnog učenja, robotsku automatizaciju procesuiranja, rudarenjem podataka i algoritama u sustavu povratne sprege na društvenim održava tri ključne funkcije i zadaće s podacima, obavijestima i informacijama:

- Prikuplja i obrađuje ih, izvještava te donosi prijedloge i zaključke o korisničkim preferencijama;
- Grupira i vrši podjele korisnika;
- Poboljšava izlaganje ciljanih publika personaliziranim informacijskim sadržajima.

Umjetna inteligencija na osnovi prikupljenih psihografskih podataka korisnika utvrđuje njihove kognitivne slabosti, kako razmišljaju i donose odluke, njihove sklonosti, načela, interese, stavove, uvjerenja i vrijednosti te, temeljem takvih kriterija, pronalazi najpogodnije publike prema kojima će isporučiti informacijski sadržaj za koji su iskazale najveći interes. Facebook je ovo objasnio na sljedeći način. U kontekstu željenog marketinškog ishoda sustav oglašavanja i odlučivanja (koji se bazira na sustavu povratne sprege) prilagođava se onom što korisnici žele vidjeti, na osnovi čega se objave prilagođavaju i isporučuju u pravo vrijeme pravim korisnicima, dok na temelju povratne komunikacije od korisnika dobiva podatke o utiscima i daljnjim interesima (Facebook). Navedene tehnologije umjetne inteligencije s ovakvim

236 Crnčić, 2020. str. 37.; prema; Šestak, P.; Dobrinić, D., Primjena novih tehnologija u marketingu s osvrtom na marketing stvari. CroDiM: International Journal of Marketing Science 2, 2019., str. 244.

mogućnostima i sposobnostima u opisanom sustavu povratne sprege Facebook je nazvao tehnologijama prilagodljivog uvjeravanja. Tehnološku moć uvjeravanja i nametanja volje ciljanim publikama uz pomoć umjetne inteligencije Facebook je izgradio za vlastite potrebe. U njezinom razvoju primijenio je rezultate znanstvenih istraživanja s područja neuroznanosti, bihevioralnih znanosti, kognitivne psihologije i ekonomije ponašanja ljudi. Rezultati istraživanja pokazali su da korisnici globalnog informacijskog prostora (interneta), zbog ogromne količine podataka i informacija, pri donošenju određenih odluka pribjegavaju kognitivnim prečacima i neracionalnim odlukama. Odnosno da radije pribjegavaju navikama, mentalnim prečacima i signalima iz okoline[237], nego objektivnom sagledavanju točnosti i pouzdanosti obavijesti i informacija. Primjenom rezultata istraživanja umjetna inteligencija na društvenim mrežama u stanju je prepoznavati sklonosti i slabosti korisnika i na osnovi toga nuditi rješenja, poboljšavati usluge i predviđati njihova buduća ponašanja te na taj način učinkovito davati nove prijedloge kako bi se utjecalo na njihove odluke, primjerice prilikom kupnje nekog proizvoda. Sinergija umjetne inteligencije i analitike baza velikih podataka koje automatizirano evaluiraju ogromne količine osobnih podataka na bazi tehnologija prilagodljivog uvjeravanja: algoritama, strojnog učenja, robotske automatizacije cjelokupnog procesa omogućila je učinkovitiju procjenu i obradu svih relevantnih podataka i pravovremenu i učinkovitu primjenu takvih podataka.[238] Umjetna inteligencija u stanju je izazivati emocije, predviđati buduće odluke i aktivnosti,[239] otkrivati političke i religijske stavove[240] te stvarati

237 Usp. Nadler, Crain i Donovan, Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech, 2011., dostupno na: https://datasociety.net/library/weaponizing-the-digital-influence-machine/

238 Thiele Ralph, Artificial Intelligence –A key enabler of hybrid warfare, Hybrid CoE Working Paper 6, 2020., str. 9.

239 Usp. Berkovsky S., Kaptein M. i Zancanaro M., Adaptivity and personalization in persuasive technologies in Proceedings of the International Workshop on Personalization in Persuasive Technology co-located with the 11th International Conference on Persuasive Technology, Persuasive Technologies, CEUR Workshop Proceedings, str. 13-25, 2016., dostupno na http://ceur-ws.org/Vol-1582/17Kaptein.pdf,

Markopoulos P., Kaptein, M. C., Ruyter de, B. E. R. I Aarts, E. H. L., Personalizing persuasive technologies: explicit and implicit personalization using persuasion profiles. International Journal of Human Computer Studies, 77, 38-51., 2015., dostupno na: https://www.semanticscholar.org/paper/Personalizing-persuasive-technologies%3A-Explicit-and-Kaptein-Markopoulos/5f7351d1c71bac1f4bd0e18bb7eb94f817dc4908#citing-papers ,

Matz Sandra i Netzter Oded, Using Big Data as a Window into Consumers' Psychology, Current Opinion in Behavioral Sciences 18, str. 7-12, 2017., https://www.sciencedirect.com/science/article/pii/S2352154617300566

240 Kosinski Michal, Stillwell David, Graepel Thore, Digital records of behavior expose personal traits, Proceedings of the National Academy of Sciences, str. 5802-5805, 2013. Dostupno na: https://www.pnas.org/content/110/15/5802

psihološke učinke.[241] Na osnovi obrade uvjerenja, načela i vrijednosti koje generiraju korisnici društvenih mreža u zamjenu za „besplatne“ usluge: interakcije s okolinom i komunikaciju, te kroz prikupljanje i obradu znanja, zaključivanje i planiranje, umjetna inteligencija i algoritmi u stanju su pružiti preciznije procjene o ljudskim osobinama od procjena samih ljudi.[242]

Dodatna osnovna zadaća umjetne inteligencije na društvenim mrežama je grupiranje ɨ podjela korisnika društvenih mreža prema njihovim sklonostima, interesima, mišljenjima, stavovima, uvjerenjima, vrijednostima, načelima i idejama. Sama tehnika kojom je izvršena ovakva podjela poznata je kao psihometrijsko profiliranje (engl. psychometric profiling) ili psihografija.[243] Psihografiju se može definirati kao proučavanje „vrijednosti, osobnosti, načina života, mišljenja i interesa ljudi određene zajednice. Također se može smatrati ekvivalentom kulture kada se provodi na nacionalnoj razini. Psihografija je korisna u poljima kao što su demografija, marketing, istraživanje mišljenja i društvena istraživanja općenito, kao i strateška predviđanja“.[244]

Uvjerenja, načela i vrijednosti na društvenim mrežama umjetna inteligencija prikuplja, pohranjuje i obrađuje u formi digitalnih tragova koje korisnici ostavljaju kroz komentare, stvaranje i dijeljenje obavijesti i informacija. U digitalne tragove ubrajaju se i tzv. emotikoni – odgovarajući simboli koji u digitalnom obliku prikazuju različita psihološka stanja i emocionalne izričaje.[245] Na osnovi odgovarajućih simbola umjetna inteligencija kroz automatizirani sustav povratne sprege dobiva uvid u ono što korisnici društvenih mreža

241 Graves Christopher i Matz Sandra, What Marketers Should Know About Personality-Based Marketing, Harvard Business Review, 2018, dostupno na: https://hbr.org/2018/05/what-marketers-should-know-about-personality-based-marketing

242 Usp. Youyou Wu, Kosinski Michal i Stillwell David, Computer-Based Personality Judgments Are More Accurate Than Those Made By Humans, Proceedings of the National Academy of Sciences of the United States of America 112, no. 4, 2015. Dostupno na: https://www.pnas.org/content/112/4/1036 ,

Papakyriakopoulos Orestis, Hegelich Simon, Shahrezaye Morteza, Serrano Medina Juan Carlos, Social media and microtargeting: Political data processing and the consequences for Germany, Big Data & Society, Research Article, 2018, Dostupno na: https://journals.sagepub.com/doi/full/10.1177/2053951718811844#_i26

243 Psihografija prema Hrvatskom jezičnom portalu označava psihografsku biografiju osobe s prikazom psihološke uvjetovanosti razvoja i opisa njezinog nagonskog života. Dostupno na: https://hjp.znanje.hr/index.php?show=main

244 Ibid.

245 To su između ostalog simboli koji označavaju sviđanje kojim se izražava prihvaćanje, odnosno nesviđanje kojim se izražava neprihvaćanje. Umjetna inteligencija bilježi i druge vrste digitalnih tragova kao što su količine komentara ili učestalost ostvarenog prosljeđivanja određenih informacijskih sadržaja kojima korisnici izražavaju korisničke preferencije.

razumiju i kako percipiraju svijet oko sebe te na temelju toga predviđa i optimizira njihove daljnje aktivnosti, personalizira korisnička iskustva i na prilagodljive načine navodi ih na ciljane odluke. Široj javnosti algoritmi su poznatiji po tome što na temelju digitalnih tragova, prethodno pročitanih pravila, navika i redoslijeda ponašanja npr. navika i trajanja pregledavanja nekog informacijskog sadržaja, preporučuju sadržaje za koje su procijenili da je korisnik iskazao najveći interes. Algoritmi su programirani sa zadaćom da pobuđuju interes i da dugoročno fokusiraju pažnju na određeni preferencijski sadržaj. Algoritmi su zajednička poveznica svim aplikacijama i svim društvenim mrežama. Nove obavijesti, informacije i znanje koje na društvenim mrežama generiraju njihovi korisnici mogu se promatrati kao rezultat njihovih dosadašnjih aktivnosti, preferencija i izbora. Algoritmi poboljšani umjetnom inteligencijom na temelju određenog skupa pravila odlučuju koja će informacija biti najrelevantnija i najpogodnija u cilju dodatnog generiranja zainteresiranosti za iste ili slične informacije. Umjetna inteligencija poboljšava ovakav algoritamski sustav predviđanja. Na taj način upravlja podacima i informacijama, odnosno određuje u kojoj mjeri će informacija biti više ili manje vidljiva. Na opisani način nadzire, upravlja i organizira znanje. Važnu ulogu u ovakvom procesu „personaliziranja korisničkih iskustava“ imaju algoritamsko rangiranje i algoritamske preporuke informacija (kao što je predlaganje koji videozapis treba gledati dalje). Da bi personalizirano iskustvo bilo poboljšano, u mnogim slučajevima algoritmi rangiranja i preporuka rade u tandemu, na osnovi mnoštva parametara koji ih obavještavaju o implicitnom i eksplicitnom ponašanju korisnika.[246] Vlasnici društvenih mreža tvrde da na ovaj način korisnicima omogućavaju "relevantne" i "korisne" informacije, no očito je da se radi o povećavanju zainteresiranosti za iste ili slične sadržaje.

Ovakva praksa podrazumijeva identificiranje interesa ciljanih publika kroz opisane tehnologije prilagodljivog uvjeravanja odnosno pojmove personaliziranog ciljanja, nanotargetiranja ili personaliziranog izlaganja ciljanih publika preferiranim informacijskim sadržajima. Facebooku i svima koji se njime koriste u poslovima digitalnog marketinga sinergija umjetne inteligencije i analitike baze velikih podataka korisnika društvenih mreža osigurava učinkovito i relevantno usmjeravanje informacijskih operacija prema ciljanim publikama.[247]

246 Saslow Alec, Artificial Intelligence Plays a Critical Role Fueling Online Disinformation, 2021., dostupno na https://decode.org/news/artificial-intelligence-plays-a-critical-role-fueling-online-disinformation/ (10.01.2022.)

247 Usp. Gonzáles-Cabanás i autori., str. 2.-5., 2021.

U pravilu, algoritmi i umjetna inteligencija na društvenim mrežama rangiraju informacijske sadržaje na nekoliko načina: kroz rubriku Razmjena sadržaja interesnih grupa (engl. News Feed) ili sličnu rubriku koja se bazira na ponašanju i interesima korisnika; rangiranjem rezultata pretraživanja koje generira pretraživač koji prima izravan korisnički unos, kao što je primjer kod Google tražilica ili YouTube pretraživanja. Twitter, na primjer, koristi model koji "predviđa koji bi Tweet bio zanimljiviji i svrhovitiji u angažmanu korisnika" kako bi se utvrdilo na kojem će mjestu po rangu vidljivosti informacijski sadržaj biti objavljen. Slično tome, Facebook koristi sustav koji "određuje koje će se objave pojaviti u korisničkoj informativnoj traci za Razmjenu sadržaja interesnih grupa"[248] i u kojem redu vidljivosti, predviđajući za što će publike najvjerojatnije biti zainteresirane ili će se uključiti". YouTube algoritam preporuka koristi i algoritamske sustave koji se oslanjaju na klikove, vrijeme promatranja i istraživanja kako bi se smanjio ili prikazao sadržaj.

Algoritamski sustav preporuka temelji se na:[249]

- informacijama koje korisnika upućuju na informacije sličnog sadržaja za koje je korisnik prethodno pokazao interes;
- filtriranju informacija koje korisnika upućuju na informacije drugih sa sličnim interesima;
- znanju koje korisnika upućuje na informacijske sadržaje procjenom njegovih interesa i karakteristika koje su svojstvene za njegove predmete interesa.

Automatizirani sustav povratne sprege kroz primjenu umjetne inteligencije na društvenim mrežama u osnovi planira i upravlja informacijskim operacijama. U osnovi nadzire aktivnosti korisnika društvenih mreža, prikuplja i upravlja uvjerenjima, načelima i vrijednostima, osigurava povratne informacije o uočenim (ne)pravilnostima tj. slabostima ciljanih publika i time omogućava učinkovitije praćenje uspješnosti promidžbenih kampanja. Daje odgovore na pitanja zašto određene obavijesti i informacije koje se ciljano usmjeravaju dobivaju više oznaka sviđanja, nesviđanja i dijeljenja u odnosu na druge. Primjena tehnologija umjetne inteligencije: algoritama, strojnog učenja, dubokog učenja robotske automatizacije i rudarenje podataka u sustavu povratne sprege na društvenim mrežama značajno doprinosi analizi izvedbe informacijskih operacija. Prikuplja, obrađuje i analizira pojedinačna i grupna uvjerenja, načela

248 Ibid.

249 Ibid.

i vrijednosti te, sukladno unaprijed određenim ciljevima, definira pogodne publike i automatski preporučuje strategije za postizanje željenih ciljeva. Primjenom opisanih tehnologija umjetna inteligencija je kroz sustav povratne sprege na društvenim mrežama automatizirala modele prediktivne analitike koju je zahvaljujući tome moguće obavljati jednostavnije, uz uštedu vremena i uz veću učinkovitost.[250] Tehnološka moć prilagodljivog uvjeravanja odnosno modeliranje sklonosti u informacijskim operacijama koje se planiraju i izvode u industriji digitalnog marketinga vlasnicima društvenim mrežama podrazumijeva monetizaciju uvjerenja, načela i vrijednosti. Opisani proces monetizacije uvjerenja, načela i vrijednosti odvija se za potrebe vlasnika društvenih mreža i industrije digitalnog oglašavanja. Tehnološka moć uvjeravanja i modeliranja sklonosti koju posjeduje umjetna inteligencija stvara začarani krug između prikupljanja uvjerenja, načela, vrijednosti i poticanja daljnjeg angažmana korisnika društvenih mreža: što više osobnih podataka prikupljaju to će moći isporučiti više "relevantnih" oglasa, čime vlasnici društvenih mreža i tvrtke koje se služe njihovim uslugama oglašavanja, ostvaruju veće prihode.[251]

Izvršena podjela ciljanih publika prema osobnim ili grupnim uvjerenjima, načelima i vrijednostima koje stvaraju korisnici, robotska automatizacija, strojno učenje, rudarenje podataka, sve primijenjeno kroz sustav povratne sprege u značajnoj mjeri unaprijedili su planiranje i izvođenje informacijskih operacija. Točnost i istinitost informacijskih sadržaja koji pri tom nastaju na društvenim mrežama i posljedično se šire u korpusu javnog znanja nije važna. U informacijskim operacijama na društvenim mrežama podacima i informacijama upravlja umjetna inteligencija bez kriterija istine, već prema kriteriju stvaranja profita. Metodologija kojom se određuje je li informacijski sadržaj u obliku oglasa isporučen korisniku ili ne, ovisi o platformi te, u mnogim slučajevima, umjetna inteligencija i strojno učenje imaju ulogu u utvrđivanju ishoda. Na primjer, na Facebooku model strojnog učenja koristi se za predviđanje "kvalitete" informacijskog oglasa, što je jedan od čimbenika koji se razmatra tijekom postupka odabira ciljanih publika prema kojima će kvaliteta oglasa biti relevantnija. Kvaliteta oglasa

250 Na osnovi „podataka iz kolačića mobilnih aplikacija i web stranica koje posjećuje korisnik, umjetna inteligencija može ciljati određene kupce koje određuju oglašavači ili tvrtke. Kriteriji mogu biti, između ostalog, lokacija, starost, spol i vrijeme. Ako se podudaraju, sustav za kupnju oglasa automatski će licitirati pojavljivanje i prikazati sadržaj. Dobar primjer za to su Facebook oglasi koji trgovcima i oglašivačima omogućuju korištenje podataka u digitalnom marketingu za izradu prilagođenih profila za „ciljanje“ oglasima.“Usp. Crnčić, 2020. str. 47., prema: Grimms, K., AI Marketing: What, Why and How to use Artificial Intelligence Marketing, 2019. URL: https://www.mageplaza.com/blog/ai-marketing-what-why-how.html#sales-forecasting (20. veljače 2020.)

251 Saslow, 2021.

temelji se na brojnim točkama podataka, uključujući povratne informacije korisnika koji pregledavaju ili skrivaju oglase. Algoritmi koji se koriste za isporuke informacijskog sadržaja mogu generirati uvide koji dovode do toga da je oglas isporučen na određene kategorije ciljanih publika koje mogu biti različite od onih koje je odredio oglašivač. To je zato što automatizirani sustav povratne sprege predviđa da će informacijski sadržaj biti relevantniji za drugu određenu kategoriju ciljanih publika.[252]

Umjetna inteligencija kroz sustav povratne sprege na opisani način povećava doseg i brzinu širenja informacijskih sadržaja i time određuje koji će informacijski sadržaji biti ponuđeni za čitanje, koliko često i tko će ih pregledavati. Međutim, u prvom planu nije istinitost i objektivnost, već određivanje uvjeta prema kojima će se neka informacija i/ili informacijski sadržaj prodati odnosno širiti, dijeliti te će, na osnovi korisničkih preferencija, biti vidljiviji samo određenim kategorijama ciljanih publika. Problem je što su vlasnici društvenih mreža sposobnosti umjetne inteligencije proizveli za vlastiti poslovni interes, a ne za prenošenje točnih informacija i objektivnog znanja. U cilju ostvarivanja profita razvoj i primjena umjetne inteligencije podređena je interesima njezinih vlasnika. Rješenje koje nudi umjetna inteligencija primjenjuje se u povezivanju korisnika u zajednice i na osnovu njihovog udruživanja za globalno i umreženo komuniciranje na osnovu istih ili sličnih načela, uvjerenja i vrijednosti. U kontekstu ove kategorije osobnih podataka umjetna inteligencija može razumjeti riječi, a zatim odgovarati na pisani način ili govorom (primjer su botovi i chatbotovi, računalni programi koji imitiraju čovjeka). Umjetna inteligencija može prepoznavati ljude i predmete u slikama i videozapisima, a zatim poduzeti mjere na temelju onoga što vidi. Umjetna inteligencija na društvenim mrežama u stanju je koristiti prirodnu obradu jezika kako bi samostalno davala komentare, komunicirala s drugim korisnicima ili odgovorila na naredbe. Za dijeljenje sadržaja za koje procjenjuje da će pojačati angažman korisnika, za prepoznavanje uzoraka koristi opisane botove i algoritme preporuka te, na osnovi njih, daje preporuke za informacijske sadržaje, proizvode, web stranice i korisnike s istim ili sličnim načelima, uvjerenjima i vrijednostima.

Umjetna inteligencija omogućila je razvoj društvenih mreža, njihovim vlasnicima unaprijedila je mogućnosti ostvarivanja komercijalnih interesa te je na mnoge načine transformirala njihove

252 Ibid.

usluge. Međutim, s negativnim posljedicama na organiziranje podataka, obavijesti, informacija te znanja u korpusu javnog znanja.

2.10. Negativne posljedice primjene umjetne inteligencije na organizaciju podataka i informacija na društvenim mrežama

Vlasnici društvenih mreža predstavili su ih kao proizvode koji će pomoći u „povezivanju ideja“ ljudi i zajednica. Primjena umjetne inteligencije pri izvršavanju podjela korisnika prema osobnim ili grupnim uvjerenjima, načelima i vrijednostima, prikupljanje, pohrana i obrada ovakvih podataka u svrhu personaliziranog izlaganja ciljanim informacijskim sadržajima dovelo je do paradigmatske promjene u prikupljanju, obradi, uobličavanju i isporukama informacijskih sadržaja. U kiber prostoru tako su nastale nove mogućnosti i nove forme oblikovanja obavijesti, informacija te znanja. Tehnologije umjetne inteligencije nadziru i upravljaju osobnim i grupnim uvjerenjima, načelima i vrijednostima, na osnovi kojih se može stvarati nove informacije samostalno ili u suradnji s ljudskim čimbenikom. Umjetna inteligencija se u ovom kontekstu koristi za učinkovito planiranje i izvođenje informacijskih operacija za potrebe društvenih mreža. Posljedično je došlo do stvaranja ogromne količine informacija koje su, između ostalih informacija, oblikovane prema uvjerenjima, načelima i vrijednostima onih koji ih i stvaraju. Izvršenim grupiranjem, odnosno podjelom korisnika društvenih mreža prema istim i/ili sličnim korisničkim preferencijama u virtualnom prostoru, nastao je ogroman broj različitih homogenih zajednica kojima je ujedno ograničen pristup alternativnim informacijama i drugim vrstama znanja. Nastale podjele u prostoru „virtualne stvarnosti“ dovele su do vidljivih podjela znanja u korpusu javnog znanja, a u stvarnom svijetu produbljene su postojeće društvene i političke podjele. Automatizirani sustav povratne sprege na osnovi rješenja koja nude algoritmi i druge tehnologije umjetne inteligencije u ovom procesu ima ključnu ulogu: prikuplja, nadzire i filtrira obavijesti, informacije i znanje prema uvjerenjima, načelima i vrijednostima. Društvene mreže jesu povezale ljude i njihove ideje na osnovi istih interesa. Međutim, nastao je paradoks. Narušene su temeljne ljudske i društvene norme kao što su transparentnost i zaštita ljudskih prava; sprječavanje monopola, cenzure i širenja dezinformacija te norme odgovornosti za nešto što je napisano, objavljeno i podijeljeno.

Paradoks je da je pojavom brojnih podijeljenih zajednica na društvenim mrežama otvorena mogućnost učinkovite zloupotrebe njihovih stavova, uvjerenja, načela i vrijednosti koje dijele. Došlo je do brisanja granica između istine i laži na vrlo suptilan način po načelu anonimnosti i prešutnog pristanka. Paradoks je da se osobna i grupna uvjerenja, načela i vrijednosti mogu zloupotrebljavati za stvaranje utjecaja na njihovu percepciju o nečemu što se događa ili se ne

događa u stvarnom svijetu. Činjenica je da se primjenom hibridne inteligencije kroz kiber prostor na društvenim mrežama uvjerenja, načela i vrijednosti mogu (pre)oblikovati prema potrebama drugih, kada je to nekome u interese, da su prema tom načelu društvene mreže dobile ulogu „oružja“, a informacijske operacije koje se planiraju i izvode na društvenim mrežama dobile su jednaku snagu kao i vojne psihološke operacije. Facebook i druge društvene mreže koje nude usluge u svijetu digitalnog marketinga koriste metode koje su se prije nastanka kiber prostora koristile u psihološkim operacijama za vojne potrebe.[253]

Primijenjena praksa prilagođenog i ciljanog izlaganja pojedinaca informacijskim sadržajima potencijalno ima štetnu primjenu.[254] Naime, literature koje opisuju psihološko uvjeravanje (engl. psychological persuasion) pokazuju da je uvjeravanje pojedinaca učinkovitije ukoliko se informacijski sadržaji prilagode prema njegovim psihološkim karakteristikama, sklonostima i motivacijama.[255] U ovom kontekstu ističu da prilagođeno i ciljano izlaganje pojedinaca informacijskim sadržajima može biti vrlo moćan način izvođenja informacijskih napada koji za cilj imaju manipuliranje uvjerenjima, načelima i vrijednostima određenog pojedinca.[256] Ova tehnika koristi se za manipuliranje sklonostima i potrebama korisnika Facebooka kako bi ih se uvjerilo da kupe određeni proizvod ili da promijene mišljenje vezano za određeno pitanje. Također, ista tehnika koristi se za stvaranje lažne percepcije u kojoj će ciljani pojedinac biti izložen vlastitoj „realnosti“ drugačijoj od one kako je vide drugi. U konačnici koristi se i za druge štetne radnje kao što su ucjene.[257]

Facebook je algoritme javnosti predstavio kao alate kojima želi poboljšavati živote ljudi. Međutim, izložio ih je ideološki grupiranim različitim vijestima i mišljenjima.[258] Brojni primjeri, o kojima će detaljnije biti riječi u nastavku rada, ukazuju da je umjetna inteligencija

253 Usp. Langworthy Stacy, Power Dynamics in an Era of Big Data, London School of Economics and Political Science, 2019. Dostupno na: http://www.lse.ac.uk/ideas/publications/updates/big-data

254 Usp. Gonzáles-Cabanás i autori., 2021., str. 2.

255 Ibid. prema; S.C.Matz, M. Kosinksi, G. Nave and D.J. Stillwell. 2017. Psychological Targeting as an effective approach to digital masspersuasion. Proceedings of the National Academy of Science 114,48 (2017).

256 Usp. Gonzáles-Cabanás i autori., 2021., str. 2.

257 Usp. Ibid., str. 11.

258 Bakshy Eytan, Messing Solomon i Adamic, Lada, Political science, Exposure to ideologically diverse news and opinion on Facebook. Science, New York, 2015., str. 348. Dostupno na: https://www.researchgate.net/publication/276067921_Political_science_Exposure_to_ideologically_diverse_news_and_opinion_on_Facebook

pridonijela da algoritmi na temelju uočenih pravila, znanja, zaključivanja i planiranja, rudarenjem, odnosno analizom osobnih identifikacijskih podataka i podataka o uvjerenjima, vrijednostima i načelima, ističu različite pozitivne i negativne ljudske tendencije, da povećavaju vidljivost informacijskih sadržaja koji, ovisno o potrebama treće strane, produbljuju postojeće društvene i političke podjele.

Činjenica je da uvjerenja, načela i vrijednosti svojih korisnika društvene mreže obrađuju i uobličavaju za potrebe drugih. Iz organizacije znanja koje se oblikuje prema njihovim interesima i sklonostima tj. preferencijama (načelima, uvjerenjima i vrijednostima) u stvarnom svijetu nastali su brojni politički, društveni i sigurnosni problemi. Društvene mreže najprije se koristilo za marketinške i financijske svrhe, nakon toga političke stranke, pogotovo u SAD-u, počele su ih koristiti za poboljšavanje rezultata u političkim kampanjama. Međutim, ubrzo je postalo vidljivo da ih se može zloupotrebljavati za produbljivanje političkih i društvene podjela i potenciranje sigurnosne destabilizacije na lokalnim, regionalnim pa i globalnim razinama.

Nadziranje i (pre)oblikovanje obje kategorije osobnih podataka specifikum je industrije digitalnog marketinga. (Pre)oblikovanje pojedinačnih ili grupnih uvjerenja, vrijednosti i načela na društvenim mrežama pomoću tehnologija umjetne inteligencije koristi se za političke, društvene i korporativne interese te za planiranje i izvođenje informacijskih operacija u kojima se dezinformacije „kroje“ prema uvjerenjima, načelima i vrijednostima ciljanih publika. Pokazalo se da je ova činjenica postala veliki sigurnosni i politički problem. Društvene mreže koriste države, nedržavni akteri i korporacije čiji su motivi politički interesi. Oni mogu biti različiti od uplitanja u izborne procese[259], planskog i sustavnog produbljivanja društvenih i političkih podjela, poticanja na radikalizam i ekstremizam, pobuđivanja društvenih pobuna protiv vladajućih struktura do regrutiranja terorista i poticanja na terorizam. Opisani fenomeni u daljnjem istraživanju promatrat će se kao glavni čimbenici pomoću kojih navedeni akteri planiraju i stvaraju prijetnje ciljanim publikama iz kiber prostora.

U organizaciji podataka i informacija te znanja na društvenim mrežama na osnovi primjene algoritama i umjetne inteligencije nastao je niz negativnih posljedica na organizaciju korpusa javnog znanja:

259 Izborni procesi imaju dvije dimenzije: političku kao sukob različitih političkih ideja koje se bore za naklonost biračkog tijela; administrativnu kao proces kojim državne institucije organiziraju izbore u demokratskim procesima i po jasnim, za sve jednakim pravilima, procedurama i po jednakim pravima.

- Tehnike personaliziranog izlaganja ciljanim i prilagođenim informacijskim sadržajima na osnovi uvjerenja, načela i vrijednosti stvaraju negativne posljedice za političku i društvenu stabilnost;
- Omogućeno je stvaranje ogromnog broja dezinformacija koje su prilagođene korisničkim preferencijama;
- Dezinformacijama je povećana vidljivost u korpusu javnog znanja;
- U korpusu javnog znanja dodatno su naglašene postojeće društvene i političke podjele;
- Ojačane su dezinformacije koje podržavaju ekstremizam, radikalizam, terorizam;
- Različitim akterima u kiber prostoru omogućene su učinkovitije forme i načini planiranja i izvođenja (tajnih) informacijskih operacija čiji planeri i provoditelji imaju za cilj i svrhu ciljanim publikama stvarati različite forme prijetnji kroz kiber prostor s potencijalnim strateškim posljedicama.

2.11. Dezinformacije

Dezinformacije su jedna od važnijih negativnih posljedica opisanih mogućnosti i negativnih posljedica organizacije uvjerenja, načela i vrijednosti na društvenim mrežama. „Dezinformacije se „proizvode“ s namjerom da protivnika navedu da promijeni mišljenje te da donosi odluke i prosudbe u korist vlastite štete.“[260] Dezinformacija podrazumijeva namjernu uporabu lažnih podataka radi zavaravanja ciljanih publika. Ona uključuje sustavno širenje netočnosti, izmišljenih priča, slika i drugih provokativnih i razdvajajućih sadržaja kroz cijeli spektar dostupnih medijskih kanala. „Podrazumijeva iskrivljenu, nepotpunu te djelomično ili potpuno netočnu obavijest čiji je naručitelj i stvarni autor prikriven, kojoj je cilj da ciljane publike, utjecajem na kognitivnoj razini, navede na donošenje odluka koje im nanose štetu, odnosno kratkoročno i/ili dugoročno mijenja njihov korpus javnog znanja.“[261]

„Dezinformacije nastaju namjernom manipulacijom s jednim ili više uvjeta koji su pretpostavke kvalitetnoj i objektivnoj informaciji. Kvalitetu obavijesti određuje jezik razmjene obavijesti te potpunost, objektivnost, dostupnost i pouzdanost obavijesti. Kad neki od tih uvjeta nisu ostvareni, onda dolazi do pogreške u komunikaciji, do emitiranja pogrešnih obavijesti ili dezinformacija.“[262]

---

260 Tuđman, 2008., str. 129. i Tuđman Miroslav, Dezinformacija. Zbornik u čast Petru Strčiću, Povijesno društvo Rijeka, 2012., str. 205.-219. Dostupno na: https://www.researchgate.net/publication/281626713_Dezinformacija

261 Akrap, 2011., str. 312.

262 Tuđman, 2013., str. 97.

U pravilu cilj je dezinformacije ili navesti protivnika na pogrešnu odluku ili ga diskreditirati tako da ne bude u mogućnosti donositi odluke. Dezinformacija je namijenjena ili protivnikovoj javnosti, a cilj joj je diskreditirati protivnika, ili vlastitoj javnosti za potporu ciljevima koje javnost ne bi prihvatila kad bi znala istinu. Na osnovi logičkih relacija između parametara – što je cilj dezinformacije i kome je dezinformacija namijenjena, izvodi se nekoliko pravila dezinformiranja:[263]

Pravilo (1): „Dezinformacije su obmane kojima je cilj navesti protivnika na krivu odluku, a osigurati potporu javnosti vlastitom ponašanju, namjerama i odlukama. Svrha osiguravanja potpore javnosti u ovom slučaju ima za cilj izvršenje pritiska na donositelje odluka."

Pravilo (2): „Dezinformacije su obmane kojima je cilj diskreditiranje protivnika u javnosti, a svrha osiguravanje potpore vlastitom ponašanju, namjerama i odlukama.[264] U kiber prostoru dezinformacije se šire trenutačno, a implementiraju se globalno. Prešućivanje, izostavljanje ili prekrajanje bitnih podataka samo su neki od načina diskreditacije protivnika."[265]

Pravilo (3): „Dezinformacije imaju dvostruku zadaću i smisao: opravdati vlastito ponašanje, namjere i ciljeve pogrešnim (neistinitim, lažnim) tumačenjima tuđih ponašanja, namjera i ciljeva."[266]

Pravilo (4): Dezinformacije imaju dvostruku zadaću i smisao: tumačiti vlastite (pogrešne, promašene ili krive) odluke, namjere i ciljeve falsificiranjem tuđih odluka, namjera i ciljeva. Autor danu definiciju promatra kroz teoriju samoobmane i zablude, odnosno teoriju poklonstva u istinu, čak i kad se ona nalazi u dezinformaciji. Zato što vjeruju u istinu dezinformacije, ljudi su indoktrinirani sustavom, zarobljenici su potrošenih ideala, prestrašeni su promjenama, ograničeni u svojem ponašanju. Odnosno, ljudi vjeruju u dezinformacije dok im je to u interesu i osigurava probitke.[267]

Dezinformacije su postale vrlo tražen proizvod na informacijskom tržištu, osobito u informacijskom prostoru u kojem se vode informacijski ratovi. Zato, istraživanje

263 Ibid., str. 143.

264 Ibid., str. 148.

265 Ibid.

266 Ibid., str. 154.

267 Ibid., str. 160.

dezinformacija treba postati redovna zadaća informacijske znanosti. Može se to reći i na drugi način: treba istražiti sve ono što može narušiti integritet obavijesti da se obavijest ne bi pretvorila u dezinformaciju.[268]

Kontekst stvaranja i diseminacije dezinformacija u kiber prostoru pomoću društvenih mreža predmet je istraživanja iz nekoliko bitnih razloga:

- Dezinformacije se baziraju na osobnim i grupnim uvjerenjima, načelima i vrijednostima korisnika društvenih mreža temeljem kojih se utvrđuju društvene slabosti ciljanih publika;
- Dezinformacije je moguće stvarati na nove načine primjenom hibridne inteligencije;
- Dezinformacije zbog masovne „proizvodnje“ na društvenim mrežama imaju snažne negativne posljedice na organizaciju korpusa javnog znanja;
- Dezinformacije na društvenim mrežama čine osnovu stvaranja različitih formi prijetnji i s prijetnjama povezanih konstantnih (24/7) informacijsko-psiholoških pritisaka;
- Dezinformacije koje se stvaraju pomoću hibridne inteligencije na društvenim mrežama snažnije su i vjerodostojnije od dezinformacija koje se stvaraju na tradicionalnim medijima.
- Dezinformacije su postale učinkovitije, vjerodostojnije i snažnije, s potencijalnim strateškim posljedicama;
- Dezinformacije se uobličavaju i prilagođavaju društvenim slabostima ciljanih publika;
- Dezinformacije su anonimne, automatizirane, masovne i optimizirane;
- Dezinformacije na društvenim mrežama omogućavaju proizvodnju pseudoznanja, stvaranje nedogađaja odnosno pseudogađaja;

Dezinformacije na društvenim mrežama nastaju same po sebi iz nekoliko ključnih i evidentnih razloga. Prvo teško je očekivati da će 60% svjetske populacije koja koristi društvene mreže poštivati pravila i temeljna ljudska načela te da će stvarati i dijeliti isključivo točne, provjerene podatke, obavijesti i informacije. Drugo, na društvenim mrežama izvršena je podjela korisnika, stvorene su ogromne količine različitih virtualnih zajednica okupljenih, svaka za sebe, oko vlastitih ideja, ideologija, uvjerenja, načela i vrijednosti. Treće, u ovako globalno umreženoj komunikaciji, ali međusobno podijeljenim zajednicama korisnika, društvene mreže otvorile su mogućnosti masovnog stvaranja nepotpunih obavijesti koje mogu biti točne ali necjelovite u

268 Tuđman, 2008., str. 132.

sadržaju, što i jest osnova na kojoj nastaju dezinformacije.[269] Kao četvrto dezinformacije je na društvenim mrežama moguće stvarati anonimno i moguće ih je diseminirati na automatiziran i optimiziran način.

Funkcije i smisao djelovanja višedimenzionalnih tehnologija umjetne inteligencije na društvenim mrežama određeni su tvorničkim postavkama njihovih vlasnika. Rješenja koja tehnologije umjetne inteligencije nude algoritamskom sustavu rangiranja i preporuka posljedično utječu na veći angažman korisnika društvenih mreža, što znači da, po načelu preporuka i rangiranja, tehnologije umjetne inteligencije ostvaruju značajan i učinkovit potencijal u povećavanju vidljivosti dezinformacija.

Facebook se uzima za glavni primjer iz nekoliko razloga. Facebook je trenutno najpopularnija društvena mreža. Zajedno s aplikacijama u svom vlasništvu (WhatsApp, Facebook Messenger i Instagram) ukupno broji 7 milijardi i 376 milijuna korisnika, posjeduje najveću bazu osobnih podataka, ima vlastiti algoritamski sustav rangiranja i preporuka i razvijenu umjetnu inteligenciju za prikupljanje, pohranu, obradu i manipuliranje ogromne količine podataka koje stvaraju njegovi korisnici. Facebook je izvrstan alat za učinkovito širenje dezinformacija.[270] Njihova želja za profitom, uz nedostatak volje da otklone uzroke nastalih problema dezinformacija, postala je prvorazredno političko i sigurnosno pitanje.[271] Osim za širenje dezinformacija algoritmi osnaženi umjetnom inteligencijom na Facebooku koriste se i za stvaranje podjela.[272] Enorman porast dezinformacija rezultat je poslovnog pristupa i ideje vlasnika da algoritme i umjetnu inteligenciju podrede oglašavanju, privlačenju oglašivača i da maksimaliziraju angažman korisnika. Činjenica je da ovakav pristup donosi enormne prihode, ali jednako tako, očigledno da je bez odgovarajućih mjera zaštite došlo do monetizacije dezinformacija. Podređivanje tehnologija kako bi se maksimizirao angažman korisnika maksimaliziralo je stvaranje dezinformacija što je, iznad svega ostalog, svjesna odluka vlasnika Facebooka. Odgovornost u otklanjanju nastalog problema dezinformacija ne predstavlja problem algoritama i umjetne inteligencije nego vlasnika same platforme. Iako umjetnu inteligenciju koristi i za oblikovanje sadržaja, čime nastoji smanjiti vidljivost dezinformacija,

---

269 Ibid.

270 Oates Sarah, The easy weaponization of social media: why profit has trumped security for U.S. companies. Digi War 1, 2020., str. 17–122., dostupno na: https://doi.org/10.1057/s42984-020-00012-z

271 Ibid.

272 Usp. Kaput Mike, Facebook AI: An Honest Assessment, Marketing Artificial Intelligence Institute, 2021b, dostupno na: https://www.marketingaiinstitute.com/blog/how-facebook-uses-artificial-intelligence-and-what-it-means-for-marketers , pristup ostvaren 10.01.2022.

očigledno da Facebook ne čini dovoljno u otklanjanju nastalog problema.[273] Adekvatno ograničavanje primjene umjetne inteligencije dodatno otežava činjenica da često oni koji njome upravljaju ne mogu uvijek razumjeti kako umjetna inteligencija funkcionira. Njezin razvoj kojim upravlja ljudski faktor uznapredovao je do razina da umjetna inteligencija može samostalno djelovati i razvijati vlastite sposobnosti.

Višedimenzionalne tehnologije umjetne inteligencije primijenjene u sustav automatizirane povratne sprege na društvenim mrežama, kao i mogućnosti hibridne inteligencije, unijele su revolucionarnu novost u stvaranju dezinformacija. Stvaranje dezinformacija na društvenim mrežama oslanja se na kognitivnu hijerarhiju odnosa između podatka (cjeline percipiranih signala), obavijesti (prikaza pojava, podatka ili događaja) i znanja, odnosno odnosa između izvora (stvaratelja dezinformacije), poruka (dezinformacijskog sadržaja), prijamnika i prijenosnog kanala (društvenih mreža) i konteksta (dezinformacijskog) procesa. Kako osnova kiber prostora jesu logički odnosi koji omogućavaju procese i manipulaciju uvjerenjima, načelima i vrijednostima, a ovi podaci predstavljaju logičku, fizičku i kognitivnu vezu između sva tri sloja kiber prostora, umjetna inteligencija posredstvom društvenih mreža u kiber prostoru obavlja njihove matematičko-logičke interpretacije i obradu. U pogledu strukture kiber prostora i uzročno-posljedičnih odnosa, tehnologije umjetne inteligencije na društvenim mrežama, na istom mjestu prikupljaju, pohranjuju, manipuliraju osobnim podacima i obavijestima te stvaraju učinke u stvarnom svijetu. Ovaj proces odvija se u sustavu povratne sprege kroz matematičko-logičku interpretaciju i obradu uvjerenja, načela i vrijednosti kao ulaznih podataka koje stvaraju sami korisnici društvenih mreža. Sustav povratne sprege kroz njihovu matematičko-logičku interpretaciju i obradu objedinjuje kognitivnu, informacijsku i fizičku domenu kiber prostora. Kako se proces manipuliranja podacima i obavijestima odvija u logičkom području kiber prostora, ali unutar infrastrukture koja se prostire u fizičkom području, kroz infrastrukturu društvenih mreža, manipulacija uvjerenjima, načelima i vrijednostima na društvenim mrežama ima svoje uzroke i ostvaruje snažne učinke na fizički prostor i na korpus javnog znanja. Dezinformacije stvorene i oblikovane pomoću strojnog učenja, rudarenja podataka i drugim tehnologijama umjetne inteligencije u kombiniranju s ljudskim čimbenikom postale su moćnije nego ikad prije. Ključna promjena je da je primjena umjetne inteligencije na društvenim mrežama u nedostatku adekvatnih mehanizama kontrole omogućila „tkanje“ i „proizvodnju“ dezinformacija na način da se njima može manipulirati potpunošću ili objektivnošću na izvoru

273 Ibid.

obavijesti i dostupnošću i pouzdanošću na odredištu obavijesti. Vlasnici društvenih mreža omogućili su da algoritmi i tehnologije umjetne inteligencije kroz sustav povratne sprege upravljaju kognitivnim procesima korisnika svojih usluga, da se iskorištavaju njihove kognitivne pristranosti i druge slabosti prema kojima kroz logički sloj kiber prostora prilagođavaju i stvaraju učinkovite dezinformacije te time u fizičkom i informacijskom prostoru ciljanih publika stvaraju neposredne štetne posljedice po organizaciju njihovog korpusa javnog znanja. Platforme društvenih mreža obavijestima jesu izvorište (umjetna inteligencija obavijesti prikuplja i pohranjuje na osnovi ulaznih podataka o uvjerenjima, načelima i vrijednostima) i odredište preko kojih ih ciljane publike u (pre)oblikovanoj formi „konzumiraju“. Mogućnost da se na istom mjestu prikuplja, pohranjuje, obrađuje i manipulira ovom kategorijom osobnih podataka i prema njima generiranim novim obavijestima odnosno da ih uobličava prema stavovima, uvjerenjima, vrijednostima i interesima drugih, društvene mreže čini snažnim i moćnim alatom utjecaja za stvaranje dezinformacija i za napadanje protivničkih korpusa javnog znanja dezinformacijama. Time su dezinformacije stekle veću moć uvjeravanja i mogućnosti „hakiranja“ ljudskog uma, na dosad neviđene načine. Društvene mreže postale su najmoćniji alat za manipuliranje ljudskim umom – za stvaranje metapropagande: propagande koja na ishodištu i odredištu diskreditira propagandu druge strane.[274] Toffler metapropagandu opisuje kao osobito moćnu jer, umjesto da dovodi u sumnju istinitost jedne priče, ona dovodi u pitanje sve što dolazi od druge strane (neprijatelja). Zadaća je metapropagande razaranje jezika: na razini pristupa informacijama tj. medija i informacijskog sustava protivnika i to na razini sadržaja informacija, odnosno napadom na ishodištu informacijskog jezika na kojem je oblikovan sadržaj obavijesti i na odredištu poništavanjem sustava obavijesti za one poruke koje se žele isključiti iz komunikacije.[275] Društvene mreže koje objedinjuju ovaj proces koji se odvija u kiber prostoru postale su idealni alati za postizanje opisanog cilja metapropagande.

Činjenica je da automatizirani sustav povratne sprege društvenih mreža s primijenjenim algoritamskim rangiranjem i preporukama nudi "relevantan" informacijski sadržaj koji je osmišljen da pojačava i optimizira angažman prema određenom skupu preferiranih uvjerenja, načela i vrijednosti. Međutim, to ujedno znači da se na isti način na društvenim mrežama rangiraju dezinformacije i daju preporuke, odnosno da se zainteresiranost korisnika usmjerava na dezinformacije koje su prilagođene načelima, uvjerenjima i vrijednostima drugih. Algoritmi

274 Usp. Tuđman, 2008., prema Toffleru, str. 131.

275 Usp. Ibid., str. 131.-132.

preporuka i rangiranja dodatno naglašavaju postojeće razlike u vrijednostima, uvjerenjima i načelima između različitih virtualnih zajednica, dok unutar njih na osnovi istih i/ili sličnih uvjerenja, vrijednosti i načela osnažuju njihove kognitivne pristranosti. Na ovaj način ih se dodatno mobilizira za određeni cilj ili svrhu. Jednako tako, algoritam preporuka može smanjiti vidljivost informacija, čak i ako je informacijski sadržaj pouzdan, objektivan i točan.[276] Ovaj dio istraživanja o mogućnosti stvaranja metapropagande dezinformacijama na društvenim mrežama bitan je za daljnje dijelove istraživanja kojima će se nastojati potvrditi ili odbaciti hipoteza i odgovoriti na postavljena istraživačka pitanja. Očigledna je moć ovih tehnologija da utječu na razmišljanje i donošenje odluka. Algoritmi rangiranja i preporuka jednako tako određuju vidljivost dezinformacije. Primjerice u korisničkoj traci za Razmjenu sadržaja interesnih grupa koju ima svaka društvena mreža. Prema ovom načelu unutar homogenih virtualnih zajednica nastao je fenomen jeke koji pojačava učinak dezinformacija jer je cijeli proces automatiziran, anoniman a dezinformacije vjerodostojnije i učinkovitije.[277] Dezinformacijama se uobličavaju emocije koje pak stvaraju dojam te time određuju načine prema kojima se shvaćaju dezinformacije, vijesti i događaji te posljedično donose odluke. Algoritmi preporuka ne raspoznaju objektivnu točnost i istinitost dezinformacija, već ih automatizmom i na strojni način čine vidljivijim. Prema kriteriju popularnosti, ostvarenom prema broju pregleda i digitalnih tragova, pogoduje se stvaranju željene percepcije o nekom društvenom i političkom događaju koji uopće ne mora odgovarati stvarnom i činjeničnom stanju.

Do ovih podataka društvene mreže dolaze na osnovi osobnih podataka građana: njihovih preferencija, interesa, stavova, mišljenja, uvjerenja, načela i vrijednosti. Dezinformacije koje se „u virtualnom prostoru“ oblikuju prema uvjerenjima, načelima i vrijednostima, u stvarnom svijetu dodatno su produbile postojeće društvene podjele. Pojedinačna i/ili grupna strukturirana uvjerenja, načela i vrijednosti ciljanih publika društvene mreže pretvorile su u jednoobrazni objekt izlaganja dezinformacijama. U ovom dijelu istraživanja dezinformacije se promatraju

276 Saslow, 2021.

277 Flore i sur., Understanding Citizens` Vulnerabilities to Disinformation and Data-Driven Propaganda, Publications Office of the European Union, Luxembourg, 2019., dostupno na: doi:10.2760/919835, JRC116009. Autori ovo svoje zapažanje temelje na zaključcima istraživanja Vesnić-Alujević, Stehling M., Jorge A., Marôpo L., Springer, Algorithms and Intrusions: Emergent Stakeholder Discourses on the Co-option of Audiences' Creativity and Data, International Publishing, 2018; Newell S., Marabelli M., Strategic Opportunities and Challenges of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of Datification, Journal of Strategic Information Systems, 2015 i istraživanju Mittelstadt B., Allo P., Taddeo M., The Ethics of Algorithms: Mapping the Debate, Big Data & Society, Vol. 3(2), 2017.

kroz njihov utjecaj na izazivanje promjena i/ili oblikovanja mišljenja, ponašanja i ometanje i/ili mijenjanje odluka uz pomoć strojnog učenja, rudarenja podataka, hibridne inteligencije odnosno automatizacije cjelokupnog procesa kroz sustav povratne sprege kojom na društvenim mrežama upravlja umjetna inteligencija.

Na osnovi navedenog, višedimenzionalne tehnologije umjetne inteligencije koje koriste društvene mreže omogućile su proizvodnju nedogađaja koji mogu imati vrlo stvarnu snagu, dok stvarne događaje mogu prikazivati irelevantnima. Prema ovom načelu društvene mreže „stvaraju realnost koja nije više ta s pomoću koje se u informacijskom prostoru javnog znanja može jednostavno kontrolirati i verificirati točnost nekog prikaza. Posredstvom njih „moguće je manipulirati s realnošću , ali je isto tako moguće raditi preinake i mijenjati realnost.“[278] Tehnologije umjetne inteligencije koje koriste društvene mreže, u osnovi, temeljem prikupljenih, pohranjenih i (pre)oblikovanih uvjerenja, načela i vrijednosti upravljaju kognitivnim procesima svojih korisnika i u stvorenoj virtualnoj stvarnosti nude neviđene mogućnosti manipuliranja s realnošću, preinaka i mijenjanja realnosti. Na ovaj način društvene mreže su „omogućile manipuliranje s pouzdanošću i dostupnošću na odredištu obavijesti, što za posljedicu ima da neki „događaj prikažu kao nedogađaj.“[279] Nedogađaj kao prividni i nepostojeći događaj u realnom svijetu ne može se razobličiti objektivnim informacijama jer nedogađaj nije ni postojao. Argumenti prikaza nedogađaja usmjereni su na oblikovanje stavova i podilaženje uvjerenjima ciljane publike. Nedogađaj postaje zbiljski tek po posljedicama i učincima koje ima, odnosno postaje zbiljski onoliko koliko ga javnost prihvati ili pak onoliko koliko postaje dio institucionalnog ponašanja.[280] Istim tehnikama i postupcima kojima društvene mreže manipuliraju s nedogađajem, nastoji se zbiljski događaj krivotvoriti i od njega proizvesti pseudodogađaj: krivotvorinu, tj. fabricirani događaj. Pri tome se krivotvorina prikazuje kao objektivna informacija o zbiljskom događaju. Dezinformator konstruira krivotvorine da ih može koristiti kao argument za svoja uvjerenja, ostvarivanje svojih interesa ili opravdanje svojih odluka i ponašanja.[281] Manipulacije s „objektivnošću i potpunošću na izvoru obavijesti“ imaju za posljedicu stvaranje opisane metapropagande odnosno da se događaj proizvede u pseudodogađaj. Rezultat takvih dezinformacija čijem stvaranju doprinose

278 Tuđman, 2008., str. 124.-125.

279 Usp. Tuđman, 2013., str. 97.

280 Ibid., str. 107.

281 Ibid.

društvene mreže jest proizvodnja pseudoznanja. Njihovom masovnom i globaliziranom upotrebom „na djelu je manipulacija s prikazom zbilje s pomoću dezinformacija.“[282]„Posljedica manipulacije s obavijesti na odredištu proizvodnja je nadznanja. “Nadznanje osobnih podataka kao i obavijesti i informacija koje na društvenim mrežama stvaraju korisnici „postulira (novu) virtualnu zbilju s pomoću dezinformacija. Svaka je virtualna zbilja fikcija, konstrukcija... Takva je po svom nastanku, ali ne i po posljedicama. Učinci su virtualne stvarnosti na zbilju gotovo materijalni jer po svojim posljedicama virtualna stvarnost funkcionira kao realna društvena činjenica.“[283] Informacijska djelatnost bez kognitivne funkcije koja omogućava razumijevanje zbilje, proizvodi nadznanje i pseudoznanje. Hraniti javnost informacijama, nedogađajima i pseudodogađajima rezultira poluobrazovanom javnosti. Najbrži način da se javnost stavi pod kontrolu i drži pod njom jest da se osigura dominacija nadznanja i pseudoznanja u javnom prostoru.[284]

Tehnologije umjetne inteligencije koje na društvenim mrežama nadziru i (pre)oblikuju uvjerenja, načela i vrijednosti svojih korisnika doprinijele su širenju dezinformacija na više načina iz nekoliko dodatnih osnovnih razloga:

- pravila ponašanja u kiber prostoru nisu adekvatno regulirana;
- ne postoje adekvatna pravila kojima bi se na društvenim mrežama spriječila zloupotreba umjetne inteligencije;
- osobni podaci građana na društvenim mrežama nisu adekvatno zaštićeni;
- uvjerenjima, načelima i vrijednostima moguće je manipulirati na automatiziran i anoniman način;
- u stvaranju dezinformacija moguće je koristiti lažne profile.

Društvene mreže širenju dezinformacija dodatno daju snažan doprinos iz nekoliko razloga:

- lažni profili, pojedinačni ili grupni, nude anonimnost,
- nesvjesnost korisnika da šire dezinformacije pojačava vjerodostojnost dezinformacija,
- neposrednost i globalan doseg ciljanih publika,
- preopterećenost ogromnom količinom obavijesti, informacija, vijesti i događaja,
- teško razlikovanje dezinformacija od točnih informacija,

282 Ibid., str. 97. i Tuđman, 2008., str. 119.-132.

283 Tuđman, 2013., str. 97.

284 Ibid.

- sklonosti korisnika uvođenju prečaca u procjeni vjerodostojnosti poruka,
- sklonosti u prihvaćanju dezinformacija koje odgovaraju njihovom svjetonazoru, čak i ako su neistinite te vjerovanje deklaracijama i tvrdnjama koje vjerojatno nisu potkrijepljene činjenicama, odnosno prihvaćaju ih čak i ako su lažne.[285]

Anonimnost, automatiziranost, masovnost i optimiziranost dezinformacija pomoću hibridne inteligencije na društvenim mrežama i ostvarene podjele korisnika njihovih usluga postaju snažna i učinkovita prijetnja društvu, državnim politikama i organizaciji javnog znanja. Ovako nastale forme prijetnji i načini diseminacije dezinformacija na društvenim mrežama u pravilu pojačavaju se i nadopunjuju njihovim prenošenjem u korpus javnog znanja pomoću tradicionalnih medija (TV-a, tiska, radija) jer tradicionalni mediji nesvjesni dezinformacija koje na ovakav način nastaju na društvenim mrežama sve ih više prenose u korpus javnog znanja.

2.12. Dezinformacijske kampanje

Posljedica opisanog djelovanja jesu dezinformacijske kampanje na društvenim mrežama koje su neupitno postale glavne metode pomoću kojih se u kiber prostoru na planski i organiziran način u korpusu javnog znanja stvaraju i šire dezinformacije, stvaraju nedogađaji te se proizvodi pseudoznanje.

Prisilna promjena stavova pri tome predstavlja jedan od najzahtjevnijih ciljeva takvog djelovanja. Uzročna veza između namjere i stvarnog ishoda dezinformacija na ciljane publike nije uvijek linearna te nije jednostavno utvrditi niti mjeriti njihov ostvareni učinak. Unatoč moći koju su informacijsko-komunikacijske i računalne tehnologije (kroz sustav povratne sprege i zloupotrebu hibridne inteligencije) dale dezinformaciji, srednjoročne i dugoročne učinke dezinformacija nije jednostavno procijeniti. Dva su osnovna razloga: temeljni stavovi, uvjerenja i obrasci ponašanja ne podliježu lakoj i izravnoj manipulaciji[286], odnosno promijeniti nečija temeljna uvjerenja, načela i vrijednosti s pomoću dezinformacija nije jednostavna

285 Paikowsky Deganit i Matania Eviatar, Influence Operations in Cyber: Characteristics and Insights; The Cognitive Campaign, str. 102., u The Cognitive Campaign: Strategic and Intelligence Perspectives, Yossi Kuperwasser i David Siman-Tov, The Institute for National Security Studies, Tel Aviv, 2019., Siboni Gabi, The First Cognitive War, in Strategic Survey for Israel 2016-2017, eds. Anat Kurz i Shlomo Brom, Institute for National Security Studies, Tel Aviv, 2016.

286 Mazarr J. Michael, Bauer Ryan Michael, Casey Abigail, Heintz Sarah Anita, Matthews J. Luke, The Emerging Risk of Virtual Societal Warfare, Social Manipulation in a Changing Information Environment, RAND Corporation, SAD, 2019.

stvar.[287] Drugi razlog je složenost načina kojima bi se mjerili učinci dezinformacija u srednjoročnom i dugoročnom razdoblju. Mjerenje trenutnog utjecaja odnosno kratkoročnih učinaka moguće je, ono je jednostavnije a obavlja ga sama umjetna inteligencija na osnovi digitalnih tragova koje dezinformacije ostavljaju na društvenim mrežama.[288] Prema broju oznaka sviđanja, nesviđanja, pregleda ili prosljeđivanja. Primjerice, na Twitteru prema količini ponovno objavljivanih i proslijeđenih (engl. retweet) objava. Na Facebooku prema oznakama sviđanja ili na temelju drugih povratnih informacija koje bilježi sustav povratne sprege, primjerice o promjenama stavova kroz komentare. Po ovom načelu ostvaruju se mjerljivi indikatori koji se baziraju na vidljivim reakcijama i trenutnim promjenama u obrascima ponašanja ciljanih publika prema isporučenoj dezinformaciji. Algoritamski sustav nadziranja kroz sustav povratne sprege uz pomoć tehnologija umjetne inteligencije povratno daje upozorenja o kognitivnom statusu odnosno promjenama stavova, slijedom čega dezinformator, sukladno ostvarenom trenutnom utjecaju dezinformacije, modelira i prilagođava njezin sadržaj kako bi bila učinkovitija. Primjena ovakvog sustava u bilježenju promjena mišljenja i stavova kod kupovine političkih oglasa, primjerice na Facebooku sama po sebi nije protuzakonita, ali je na sivoj granici zakonitosti.[289] Međutim, kad se ovaj sustav koristi za stvaranje prijetnji dezinformacija sa političkim ciljem koji može varirati od produbljivanja društvenih ili političkih podjela, ciljanog kreiranja nepovjerenja u nositelje političke vlasti, poticanja na radikalizam, ekstremizam ili terorizam sa svrhom ispunjavanja političkih ciljeva u vidu izazivanja destabilizacijskih procesa, tada zloupotreba "tvorničkih postavki" umjetne inteligencije i algoritama „tehnologija uvjeravanja", prilagođenog i personaliziranog ciljanja mogu imati snažne strateške posljedice po organizaciju korpusa javnog znanja te stvarati niz različitih vrsta prijetnji demokratskim procesima koje proizlaze iz kiber prostora.

Postalo je evidentno da se tehnikama programiranog i automatiziranog personaliziranog izlaganja ciljanih publika (pre)oblikovanim načelima, uvjerenjima i vrijednostima kao i izvršenom podjelom prema istim kategorijama podataka, može učinkovito upravljati i

287 Usp. Assa Haim, Infuencing Public Opinion i Paikowsky Deganit i Matania Eviatar, Influence Operations in Cyber: Characteristics and Insights; u The Cognitive Campaign: Strategic and Intelligence Perspectives Yossi Kuperwasser and David Siman-Tov, The Institute for National Security Studies, Tel Aviv, 2019.

288 Usp. Mazarr, Bauer, Casey, Heintz, Matthews, 2019.

289 Cordey Sean, Cyber Influence Operations: An Overview and Comparative Analysis, Cyberdefense Trend Analysis, Center for Security Studies, ETH Zürich, 2019. Dostupno na: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf

dezinformacijama. Grupiranjem prema zajedničkim načelima, uvjerenjima i vrijednostima, ciljane publike na društvenim mrežama postale su jednostavnija meta dezinformacija sa snažnim učinkom uz niske troškove u realnom vremenu. Razlog tome je što su tehnologije koje upravljaju društvenim mrežama korpus javnog znanja ciljanih publika, kroz njihova strukturirana uvjerenja i vrijednosti, objedinile u jednoobrazni objekt napada. Na ovaj način pomoću društvenih mreža može se napadati čitav „informacijski sustav" ciljanog društva, odnosno njegovo opće znanje. Društvene mreže bez adekvatne zaštite ove kategorije osobnih podataka te normi kojima bi se ograničila zloupotreba umjetne inteligencije u njihovom (pre)oblikovanju za potrebe drugih, različitim akterima (državnim i nedržavnim) postale su multiplikator njihove moći u kiber prostoru. Različiti akteri stoga ih koriste kao ključne alate s pomoću kojih nastoje ostvariti vlastite informacijske strategije te s njima povezane ciljeve. Ono što određuje rezultat njihove zloupotrebe nije vladanje „činjenicama", nego manipuliranje osobnim i grupnim uvjerenjima, vrijednostima i načelima za prikrivene psihološke i političke svrhe. Višedimenzionalnost tehnologija umjetne inteligencije u višedimenzionalnom kiber prostoru osigurala je da naizgled sve bude transparentno, dok istovremeno stvarnu objektivnost, točnost i pouzdanost informacija može zamagliti a dezinformacije učiniti neprimjetnim. Ovim dijelom istraživanja dodatno će se u daljnjim dijelovima istraživanja nastojati potvrditi ili odbaciti hipotezu i odgovoriti na postavljena istraživačka pitanja.

Facebook koji predstavlja trenutno najpopularniju društvenu mrežu, mogućnost stvaranja dezinformacija pomoću opisanih tehnologija i sljedbenika lažnih profila na vlastitoj platformi nazvao je procesom „lažnog pojačavanja". Prema definiciji koju je dao sam Facebook, to podrazumijeva koordiniranje aktivnosti između lažnih i povezanih profila s ciljem manipuliranja javnog mnijenja (Facebook). Ove dvije mogućnosti nude nove opcije u izvođenju i planiranju dezinformacijskih kampanja te igraju vrlo važnu, ako ne i ključnu, ulogu u ispunjavanju zacrtanih ciljeva informacijskih strategija različitih aktera,

Za širenje dezinformacija koriste se sve raspoložive tehnološke mogućnosti koje nude društvene mreže:

Važnu ulogu u širenju dezinformacija imaju programska rješenja opisana kao *botovi*. U dezinformacijskim kampanjama *botovi* društvenih mreža upravljaju lažnim profilima i predstavljaju ono što u stvarnom ratovanju predstavljaju vojnici.[290] U zlonamjerne svrhe koriste

290 Bergh, 2019.

se za stvaranje i širenje ogromnog broja dezinformacija kojima se protivnički informacijski prostor znanja zagušuje ili se blokiraju javne rasprave koje nisu u interesu napadača.[291] Botovima se mogu širiti i zlonamjerni programi. Specifikum botova je da uz vrlo niske troškove oponašaju ljude i da računalnim sustavom automatizacije šire dezinformacije u ogromnim količinama i time dodatno pridonose ciljanom produbljivanju podjela među ciljanim publikama.

Automatizirani programi koji imaju sposobnost da upravljaju lažnim profilima nazivaju se trolovi koji mogu biti i stvarni ljudi. Sama tehnika kojom se upravlja lažnim profilima zove se tehnika trolanja i koristi se za dodatno povećavanje vidljivosti dezinformacija. Kad je ono dio planskog i ciljanog utjecaja i kad postoji više koordiniranih trolova, tada se ovakvo djelovanje trolova naziva astroturfingom i onda trolovi jesu dio šire dezinformacijske kampanje. Astroturfing podrazumijeva visoko organiziranu mrežu trolova koji rade u „tvornicama trolova“ ili pojedinačne trolove koji djeluju na manje organiziran način, ali su pod utjecajem napadača. Svrha im je stvoriti dojam većinskog mišljenja ili nekoj društvenoj ili političkoj temi podići popularnost koja je od interesa napadača, pokušati „nagovarati“ ciljane publike i prema njima sustavno komunicirati ideološke narative od interesa napadača. Dezinformacijama ove tehnologije i tehnike daju veću moć za produbljivanje podjela, prigušivanje suprotnog mišljenja, ometanje internetske rasprave i općenito ometanje formiranja javnog mišljenja.[292] Mogućnosti anonimnog komuniciranja u kiber prostoru i automatiziranog i strojnog upravljanja podacima glavni su čimbenici koji su omogućili da se primateljev informacijski sustav „bombardira“ i zagušuje protivničkim (dez)informacijama.

Za širenje dezinformacija koriste se sve raspoložive kombinacije digitalne obrade slikovnih, zvučnih i video zapisa koja se naziva fenomenom internetske „memetike“. Fenomen „memetike“ podrazumijeva korištenje dezinformacija u obliku kratkih tekstualnih, slikovnih i video sadržaja kojima se pažnja ciljanih publika ciljano privlači na dezinformacije koje su „tkane“ kroz humoristične i zabavne sadržaje na suptilan i prijetvoran način.[293] Njihova specifičnost je u suptilnom i prijetvornom načinu manipuliranja razmišljanjem i donošenjem

---

291 Fredheim Rolf, Robotrolling 2, NATO Strategic Communications Centre of Exellence, 2017, https://www.stratcomcoe.org/robotrolling-20172. U dokumentu se navodi da su tijekom druge polovice 2017. botovi na ruskom jeziku proizveli 70% poruka na temu NATO-a.

292 Cordey, 2019.; prema Pamment i sur., 2018.

293 Usp. Giesea Jeff, It's Time To Embrace Memetic Warfare, NATO Strategic Communications Centre of Excellence, Riga., 2017.

odluka ciljanih publika, iza čega se kriju napredniji ciljevi i planovi napadača koje ciljane publike ne mogu jednostavno prepoznati. Radi se o modernom tipu informacijskog i psihološkog ratovanja u kojem su društvene mreže zbog svog dizajna dezinformacijama dale dodatnu moć „oružja“.[294]

Memetika u kiber prostoru predstavlja novi čimbenik dezinformiranja o kojem će ovisiti ishodi budućih ideoloških, ali i oružanih konflikata.[295] Memetika podrazumijeva upotrebu memova, šaljivih slikovnih prikaza u digitalnom obliku. Dezinformacije u obliku slikovnih šaljivih i humorističnih prikaza postale su snažni alati kojima informacijski napadač potencijalno može steći prednost s mogućim strateškim posljedicama. Njihova snaga prepoznaje se kroz slikovne sadržaje kojima se utječe na ideje koje oblikuju uvjerenja koja potom generiraju i utječu na političke stavove i mišljenja.[296] Ona omogućava „izražavanje„ dezinformacija na šaljiv i humoristočan način, što ih čini privlačnim. Njihov međuljudski, dvosmislen i jednostavan dizajn dezinformacijama daje visoki potencijal prihvaćanja. Idealni su za legitimiziranje rubnih i/ili kontroverznih ideja, mišljenja i narativa, za ismijavanje, ponižavanje i šalu kojima se nastoji dodatno oslabiti monopol narativa struktura na vlasti u drugim državama. U globalnoj i masovnoj komunikaciji „mnoštva s mnoštvom“ ovako kreirane dezinformacije kroz „šale“ dobivene od virtualnih „prijatelja“ ili članova virtualnih grupa imaju veću vjerojatnost širenja. Kad se dezinformacija podijeli među „prijateljima„ ili članovima istih grupa ona je prihvatljivija i nastavlja se dijeliti, bez shvaćanja da se iza humorističnog sadržaja krije dezinformacija sa skrivenim političkim motivom.

U dezinformacijskim kampanjama koriste se sve dostupne tehnike koje se koriste na društvenim mrežama od toga kako se informacije generiraju, kako se distribuiraju, kako ih krajnji korisnici „konzumiraju“ odnosno načina kako pojedinci i grupe na društvenim mrežama obavljaju međusobne interakcije.[297] Zahvaljujući društvenim mrežama i hibridnoj inteligenciji izvode se kroz nekoliko faza. Automatizacija i optimizacija dezinformacija u svim predloženim fazama omogućena je primjenom hibridne inteligencije, strojnog učenja, automatiziranog

294 Usp. Singer W.P. i Brooking T. Emerson, LikeWar: The Weaponization of Social Media, 2018., str. 191.

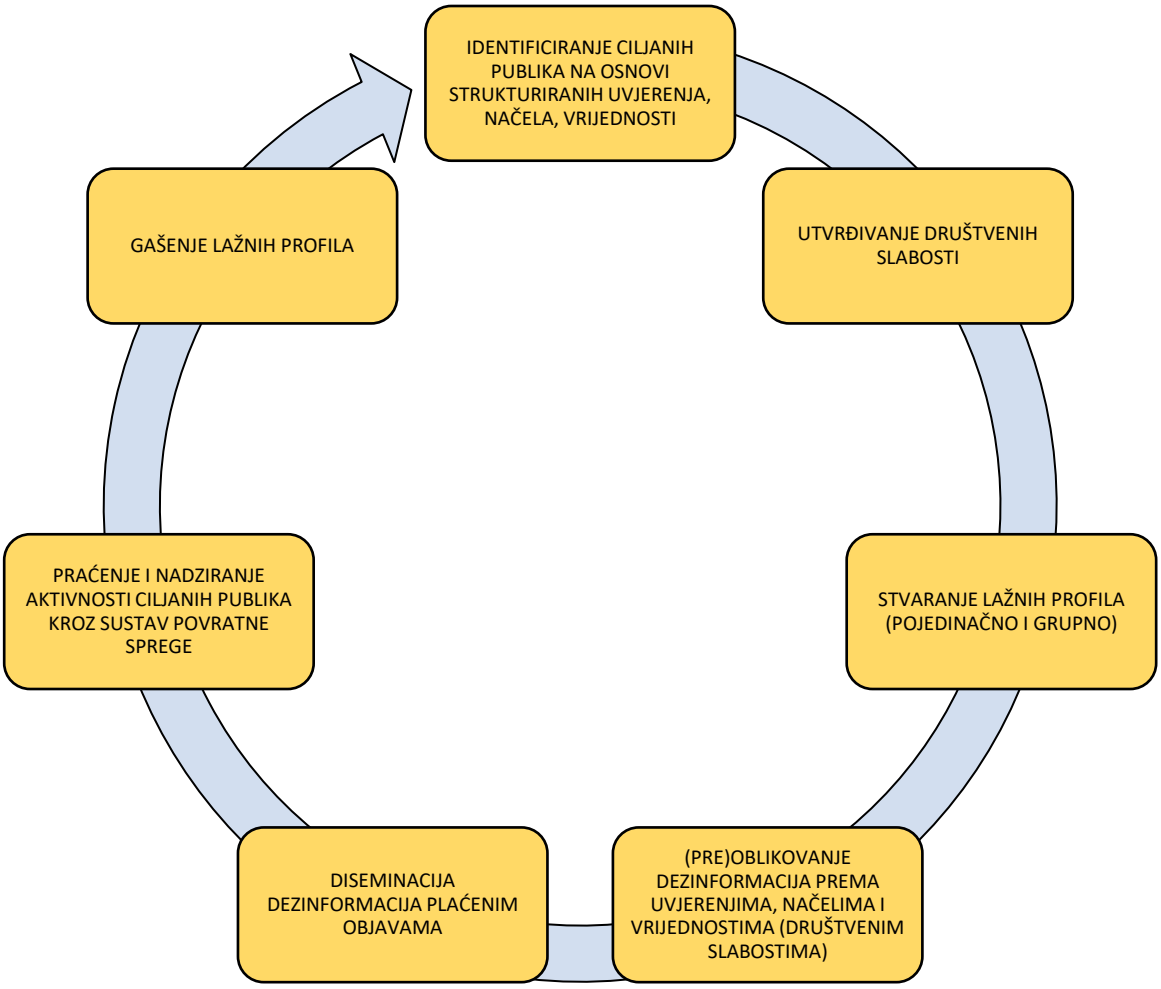
295 Ibid.

296 Ibid.

297 Usp. Cordey, 2019.

sustava povratne sprege i procesnim rudarenjem podataka. Svi navedeni čimbenici olakšavaju donošenje ključnih odluka tijekom kampanje s posljedicama na strateškoj razini.

1. faza na osnovi strukturiranih uvjerenja, načela i vrijednosti, podrazumijeva identificiranje ciljanih publika prema unaprijed određenom cilju:
2. faza podrazumijeva dodatno utvrđivanje njihovih sklonosti i interesa na osnovi kojih se utvrđuju društvene slabosti ciljanih publika. Ova faza podrazumijeva prikupljanje i analizu podataka s društvenih mreža i dodatnih podataka, obavijesti, informacija i vijesti iz korpusa javnog znanja ciljanih publika;
3. faza podrazumijeva stvaranje lažnih profila pojedinačno i/ili grupno prema sklonostima i interesima ciljanih publika;
4. faza podrazumijeva stvaranje dezinformacija prema korisničkim sklonostima i interesima. U ovoj fazi stvaraju se mreže sljedbenika i po toj osnovi dezinformacijama se nastoji graditi vjerodostojnost;
5. faza podrazumijeva diseminaciju dezinformacija plaćenim objavama vlasnicima društvenih mreža. Ova faza podrazumijeva korištenje lažnih profila, hastagova, botova, trolova i memeova te izvedenih tehnika kako bi se protivnički korpus javnog znanja zagušio dezinformacijama. Ujedno ova faza podrazumijeva (de)mobilizaciju ciljanih publika za potrebe planera i izvoditelja dezinformacijskih kampanja;
6. faza podrazumijeva praćenje i nadziranje aktivnosti ciljanih publika, dodatno modeliranje dezinformacija sukladno povratnim informacijama dobivenim kroz sustav povratne sprege;
7. faza je zadnja faza u kojoj se nakon ostvarenog cilja gase lažni profili, mrežne objave i drugi tragovi.



Slika 17.. Prikaz metodologije planiranja i izvođenja dezinformacijskih kampanja na društvenim mrežama pomoću lažnih računa, hibridne inteligencije i sustava povratne sprege koji dezinformacijama nude neprimjetnost u pravovremenom prepoznavanju.

Slikom 17. želi se prikazati hipotetski primjer dezinformacijske kampanje koju je moguće planirati i izvesti pomoću društvenih mreža s opisanim fazama, u kojima je cjelokupni proces, na osnovu sustava povratne sprege, automatiziran a na osnovu zloupotrebe hibridne inteligencije, uz korištenje lažnih računa, dodatno smanjena mogućnost pravovremenog prepoznavanja dezinformacija koje su, primjenom opisanih mogućnosti hibridne inteligencije i sustava povratne sprege, prilagođene uvjerenjima, načelima i vrijednostima ciljanih publika.

Umjetna inteligencija kroz sustav povratne sprege automatizmom planira, upravlja i nadzire cjelokupan proces kroz sve faze, po broju zabilježenih oznaka digitalnih tragova (broju klikova na određeni simbolički jezik) procjenjuje razine trenutnog uspjeha u željenim promjenama u uvjerenjima, načelima i vrijednostima, odnosno kontinuirano procjenjuje, ažurira podatke je li

ili nije ostvaren utjecaj na pojedinačne i/ili grupne profile, na koje jest a na koje nije te preispituje na koje je načine ostvaren veći utjecaj od planiranog. Ujedno pronalazi, analizira i predlaže najpogodnije profile korisnika društvenih mreža, koji nisu skloni njihovoj promjeni, ali koji su kroz vlastite komentare (digitalne tragove) izrazili određeno nezadovoljstvo ili kritiku prema isporučenim dezinformacijama koje se odnose na događaj određenog društvenog ili političkog karaktera, stanja ili pojave oko koje planer i izvođač dezinformacijskom kampanjom ciljanim publikama želi nametnuti vlastitu volju. Sustav povratne sprege dakle nudi povratne informacije kako bi se u stvarnom vremenu testirale i podešavale početne i daljnje ključne varijable dezinformacija, kao što su promjene u sastavu ciljanih publika, sadržaju i vremenu koje je potrebno dezinformacijama da postignu željeni učinak. Sustav automatizmom povratno izvještava o kognitivnom statusu odnosno upozorava o trenutnim promjenama u načelima, uvjerenjima i vrijednostima ciljanih publika, što omogućava daljnje modeliranje dezinformacija. Dodatno će se u daljnjem tijeku istraživanja nastojati potvrditi ili odbaciti postavljena hipoteza i postavljena istraživačka pitanja.

U dezinformacijskim kampanjama pomoću društvenih mreža primjenom hibridne inteligencije zloupotrebljavaju se osobni podaci, lažni profili, algoritmi, pojedinačni i/ili grupni, strojno učenje, rudarenje podataka, automatizirani sustav povratne sprege i sve raspoložive tehnološke mogućnosti širenja dezinformacija. Primjenom hibridne inteligencije ovi čimbenici stvaraju sinergijske učinke: pojačavaju učinak dezinformacija s potencijalnim strateškim posljedicama na korpus javnog znanja ciljanih publika. Anonimne, masovne, automatizirane i optimizirane dezinformacijske kampanje omogućavaju učinkovitije stvaranje različitih formi prijetnji ovisno o potrebama napadača:

- promoviranje vlastitih i/ili diskreditiranje tuđih uzoraka ili nekog problema; dezinformacijama se postojeće društvene slabosti mogu dodatno pojačavati ili smanjivati;
- poticanje nepovjerenja u političke institucije i/ili institucije civilnog društva; na strateškoj razini mogu se potkopavati ili pojačavati statusi određenih političkih institucija, osoba, grupa ili civilnog društva;
- produbljivanje postojećih podjela i (de)mobilizaciju ciljanih publika.

U dezinformacijskim kampanjama tri su osnovne tehnike informacijskih operacija koje se koriste u svijetu digitalnog marketinga. To su tehnika društvenog kognitivnog hakiranja kojom se volja napadača nastoji nametnuti velikim društvenim skupinama, tehnika psihografskog hakiranja kojom se volja nastoji nametnuti bitnim pojedincima i tehnika društvenog hakiranja

kojom se dodatno iskorištavaju sklonosti korisnika društvenih mreža da pripadaju određenoj grupi.[298] Sve tri tehnike „hakiranja“ ljudskog uma omogućavaju učinkovitije iskorištavanje kognitivnih slabosti, psihosocijalnih pokretačkih točaka, emocija (strah, bijes, mržnju, čast, interes, odanost itd.) te grupne sklonosti korisnika društvenih mreža da vjeruju u nešto u što vjeruju drugi, odnosno da usvajaju ponašanje grupe kojoj pripadaju. Primjena hibridne inteligencije pri tome daje učinkovitiju mogućnost „hakiranja ljudskog uma“. Članovi zatvorenih homogenih zajednica na društvenim mrežama na osnovi zajedničkih vrijednosti, uvjerenja ili načela u pravilu slijede određeni ideološki narativ. Članovi ovakvih grupa nalaze se u stanju „intelektualne izolacije” koje nastaje kad su njezini članovi izloženi selektivnim informacijama. Selektivna izloženost samo određenom skupu informacija, što omogućavaju algoritmi, pojačava njihovu grupnu pripadnost i onemogućava im dotok alternativnih izvora informacija. U ovakvim okolnostima unutar ovakvih zatvorenih i homogenih zajednica nastaje *učinak jeke.* U dezinformacijskim kampanjama iskorištava se upravo opisani proces. Unutar zatvorenih zajednica „intelektualna izolacija” i *učinak jeke* pojačavaju učinak dezinformacija koje dobivaju veću vjerodostojnost i multipliciraju moć utjecaja. *Učinak jeke* direktna je posljedica algoritama i izvršenih podjela. Na ovaj način dezinformacijama homogene zajednice mogu se dodatno mobilizirati ili se između njih mogu potencirati podjele, a između različitih grupa na nekoj od društvenih mreža mogu se dodatno produbljivati međusobne postojeće podjele. Ovaj cjelokupni proces je za potrebe vlasnika društvenih mreža automatiziran, optimiziran i anoniman čime su i dezinformacije postale automatizirane, anonimne i optimizirane. Ovu mogućnost koju nude društvene mreže različiti akteri zloupotrebljavaju kao diskretne metode kojima ciljanim publikama nastoje nametnuti vlastitu volju s potencijalnim strateškim posljedicama na demokratske procese i organizaciju znanja ciljanih publika.

Automatizirani sustav povratne sprege pomaže hibridnoj inteligenciji u uobličavanju dezinformacija prema utvrđenim društvenim slabostima. Automatizacijom i optimizacijom dezinformacija društvene mreže pospješile su i pojednostavile ono što se u teorijama o informacijskom ratovanju naziva pripremnom fazom psiholoških operacija. Masovna upotreba, popularnost, globalna dostupnost i visoka mrežna interakcija društvene mreže učinilo je učinkovitim alatima za prikupljanje širokog skupa podataka o tome kako ciljane publike promatraju i shvaćaju događaje, pojave ili stanja oko sebe, kako reagiraju, što ih pokreće da donose određene odluke na temelju obavijesti, informacija ili vijesti koje dobivaju. Primjena

[298] Ibid., str.11.

hibridne inteligencije omogućila je provjeravanje učinkovitosti dezinformacija koja je potrebna „kako bi se mogle prilagođavati novim izazovima, novim stanjima uz istovremeno praćenje njihovog učinka.“[299] Od najveće vrijednosti su podaci o uvjerenjima, vrijednostima i načelima ciljanih publika koje korisnici društvenih mreža nude besplatno kako bi se zauzvrat služili društvenim mrežama. Pri tome napadač, kako bi dodatno produbio postojeće podjele, koristi podatke o temama oko kojih među ciljanim publikama postoji najveći stupanj podjela. Napadaču automatizirani sustav povratne sprege na osnovi digitalnih tragova nudi uvid u njihove slabosti a hibridna inteligencija mu pomaže u prilagođavanju dezinformacija u skladu s potrebama i interesima te u istu svrhu izgrađuje mreže sljedbenika uz pomoć pojedinačnih i/ili grupnih lažnih profila.

Digitalna revolucija koju su tehnološke korporacije nametnule društvu kroz komercijalizaciju osobnih podataka i tehnologija zahtijeva nove pristupe u otklanjanju nastalih problema. Glavni problem predstavlja neadekvatna regulativa kojom bi se ograničila zloupotreba umjetne inteligencije koju koriste društvene mreže. Različitim akterima (državnim, nedržavnim i korporacijama) time je ostavljen prostor da zloupotrebljavaju društvene mreže za vlastite interese. Pri tome nemaju odgovornost ni oni koji ih zloupotrebljavaju niti odgovornost za iznesenu dezinformaciju snose društvene mreže. Činjenica je da korisnici društvenih mreža dobrovoljno i besplatno nude svoje osobne podatke u zamjenu za „besplatne usluge”, da umjetna inteligencija prepoznaje njihove slabosti koje različiti akteri uz pomoć iste tehnologije zloupotrebljavaju kako bi stvarali dezinformacije, produbljivali postojeće društvene i političke podjele odnosno kako bi na učinkovit način napadali sustav vrijednosti, uvjerenja i načela ciljanih publika za vlastite interese.

Daljnji tehnološki napredak koji propagira Četvrta industrijska revolucija doveo je do velikih promjena u planiranju i izvođenju psiholoških operacija. Kako se tehnologije umjetne inteligencije budu razvijale sljedeće generacije (dez)informacijskih kampanja pomoću društvenih mreža bit će učinkovitije. Dezinformacijske kampanje bit će najkritičnije područje zlouporabe umjetne inteligencije koje koriste društvene mreže pomoću kojih će se u kiber prostoru stvarati „naprednije“ verzije virtualne stvarnosti. Dezinformacije će se bazirati na umjetno stvorenim video i audio sadržajima. Automatizacija dezinformacijskih procesa, duboko lažiranje, umjetne automatizirane kampanje humanoidnih dezinformacija i strojno generiranje političkih astroturfing kampanja izgledan su nastavak dosadašnjih trendova

299 Usp. Akrap, 2011., str. 32.

zlouporaba umjetne inteligencije na društvenim mrežama.[300] Lažne događaje moći će se prikazivati kao stvarne, a stvarne će se prikazivati kao lažne. Umjetna inteligencija moći će samostalno stvarati i distribuirati sintetizirane lažne verzije stvarnih događaja. Tehnologije virtualne i proširene stvarnosti preko raznih aplikacija društvenih mreža bit će globalno dostupne, a razni akteri koristit će ih kako bi se lažnim sadržajima predstavljala željena stvarnost. S vremenom ove tehnologije bit će toliko sofisticirane da će biti sve teže raspoznavati razlike između stvarnih i lažnih događaja. Duboko lažiranje (*engl. deep fakes*) kao rezultat ovih tehnoloških dostignuća 2019. zahtijevalo je ljudsku intervenciju, no tijekom sljedećeg desetljeća tehnike dubokog lažiranja bit će u većoj mjeri automatizirane čime će njihovo pravovremeno uočavanje biti dodatno otežano.[301] Slični procesi već postoje na većini platformi društvenih mreža i relativno ih je lako razvijati. Tehnologije koje omogućavaju ovakve procese su jeftine, dostupne i široko prihvaćene i u skoroj budućnosti, ukoliko se ne reguliraju, može se očekivati da će se zloupotrebljavati za stvaranje i širenje dezinformacija na nove načine i u novim formama. Preko samo jedne aplikacije umjetna inteligencija moći će na više platformi društvenih mreža stvarati neograničen broj lažnih računa na kojima će automatizirano stvarati i širiti dezinformacije.[302] U geopolitičkim sukobima umjetna inteligencija koju koriste društvene mreže moći će slijediti koordinirani strateški cilj. Posljedice bi mogle biti dramatične jer će razni akteri umjetnu inteligenciju moći usklađivati sa strategijama vlastitih dezinformacijskih kampanja. Automatizirani proces masovnog dezinformiranja moći će slijediti koordiniranu strategiju i vrlo vjerojatno će biti glavna značajka sljedećeg desetljeća informacijskog rata. Automatizacija bi se u budućnosti mogla koristiti i za generiranje trenutnih odgovora na događaje. Primjerice, dezinformacijska kampanja kojom će upravljati umjetna inteligencija: umjetna inteligencija će moći prepoznati porast interesa za neku relevantnu temu, npr. popularnost nekog pojedinca ili akcije, na što će se generirati koordinirani automatski odgovor kako bi se automatizmom povećao interes i usmjerila pažnja ciljanih publika prema dezinformacijama koje se odnose na takvog pojedinca ili akciju. Obrasci ovako automatiziranih odgovora moći će uključivati i protuargumente, lažne vijesti, trolanje ili jeftinu propagandu.

300 Usp. Hartmann Kim i Giles Keir, The Next Generation of Cyber-Enabled Information Warfare, 2020. Dostupno na: https://ccdcoe.org/uploads/2020/05/CyCon_2020_13_Hartmann_Giles.pdf

301 Usp. Ibid.

302 Ibid.

2.13. Negativan utjecaj društvenih mreža na različite društvene pojave

Algoritamski sustav rangiranja i preporuka ukazuje da se na društvenim mrežama ciljano može širiti ekstremizam, radikalizam, terorizam i poticati nasilje. Algoritmi rangiranja i preporuka imaju ključnu ulogu u angažiranju ciljanih publika koje u ekstremizmu, radikalizmu i terorizmu pronalaze svrhu vlastitog djelovanja. Jedan od prvih zabilježenih sigurnosnih problema bio je problem zloupotrebe društvenih mreža za propagiranje vjerskog ekstremizma, radikalizma i terorizma.

Terorističkim organizacijama, njihovim ideolozima i vođama društvene mreže otvorile su prostor za učinkovitije širenje radikalnih i ekstremnih vjerskih ideja. Problem je postao još veći s pojavom prvih terorističkih napada koji su bili inspiriranim takvim sadržajima. Prva društvena mreža koja se počela zloupotrebljavati u ove svrhe bio je YouTube. Iste godine kada je stvoren, YouTube se počeo koristiti za prikazivanje i prenošenje radikalnih stavova terorističkih organizacija kojima su, skupljajući milijune pregleda, inspirirane desetine terorističkih napada diljem svijeta.[303] Glavnu ulogu u povećavanju njihove vidljivosti imao je YouTube algoritam preporuka koji je povećavao preglede video sadržaja kojima su se poticali teroristički napadi.[304] Kreirajući popis sličnih videa za svoje korisnike, YouTube algoritam preporuka upućivao je njihove korisnike na videa drugih terorističkih organizacija. Na ovaj način u društvu se povećavao stupanj prijetnji od terorističkih napada. Američka obavještajna zajednica uočila je da bi, nakon povećanog broja pregleda videa u kojima su se poticali teroristički napadi, slijedio povećani broj terorističkih napada.[305] Na isti način teroristi su ubrzo počeli koristiti Facebook i Twitter. Paradoksalno je da su terorističke organizacije koje unutar vlastitih organizacija žele uništiti slobodu govora, u Twitteru pronašle savršenu poveznicu s poslovnom politikom ove korporacije: posvećenost slobodi govora. Unatoč činjenici da su teroristi imali neometani pristup platformi Twitter, vlasnici ove korporacije odbacivali su pritužbe da je njihova platforma teroristima dala prostor za djelovanje. Međutim, prekretnica u tumačenju ovakvog pristupa uslijedila je nakon terorističkog napada u kojem su teroristi iskoristili Twitter za širenje dezinformacija koje su prenosile zapadne medijske kuće koje su objave terorista na Twitteru ujedno koristile kao jedan od izvora informacija. Najveći iskorak u iskorištavanju Twittera napravila je teroristička organizacija Islamska država (ISIL) koja ga je, zajedno s Facebookom,

303 Singer i Brooking, 2018., str. 234.

304 Ibid.

305 Ibid.

iskoristila za širenje ekstremističkih i radikalnih vjerskih narativa, za mobilizaciju pristaša oko ideje Islamskog kalifata te za regrutiranje terorista u političkom ratu protiv Zapada.[306] Zloupotreba Facebooka, Twittera i YouTubea od strane terorističkih organizacija bila je vrlo jednostavna jer su teroristi iskoristili mogućnosti koje su vlasnici ovih društvenih mreža pružili svim korisnicima svojih usluga: registriranje lažnih računa te automatizirano ubrzavanje i optimizirano širenje poruka, obavijesti i informacija prilagođenih korisničkim sklonostima i interesima. Kao rješenje nastalih problema do kraja 2016. vodeće tehnološke korporacije Facebook, Microsoft, Twitter i Google lansirali su bazu podataka za „nasilne terorističke prikaze", iako su prije svega nekoliko godina inzistirali na tome su da je takav sustav nemoguć. Tada su svoju nespremnost opravdavali činjenicom kako je definicija „terorizma" bila odviše subjektivna da bi mogla biti definirana nekim programskim rješenjem koje bi moglo uklanjati račune terorističkih organizacija.[307]

Drugi sigurnosni problem nastao je kad su društvene mreže počeli koristiti za propagiranje političkog i ideološkog ekstremizma i radikalizma. Ekstremne i radikalne grupacije počele su ih otvoreno koristiti za iskazivanje mržnje, poticanje nasilja i diskriminacije. Google, Facebook i Twitter na ove pojavnosti, kao i u slučaju terorizma, nisu reagirali na vrijeme što su opravdavali time da cenzuriranje nije njihov posao, iako su priznali da se na njihovim platformama širi rasizam i predrasude.[308] No, po obrascu kako su izvršili pritisak na teroriste i njihove pristaše uklanjanjem računa sa svojih društvenih mreža na isti način su, očito pod političkim pritiskom, pristupili borbi protiv ekstremizma. Prvi korak je bio gašenje osobnih i službenih računa pojedinaca, skupina i organizacija konzervativnog i desno orijentiranog političkog krila američke političke scene. Ovo je bio veliki preokret jer su od osnivanja društvenih mreža njihovi vlasnici ustrajali na tvrdnji da njihovi servisi i usluge nude „tržišta ideja" kojima će dominirati oni koji budu obdareni najvećim vrlinama i racionalnošću. Međutim, ubrzo su shvatili da su njihove platforme, preko kojih su umrežavali ideje, postale bojišnica s ozbiljnim posljedicama u stvarnom svijetu, u vidu jačanja terorizma, nasilja i ekstremizma.

306 Ibid.

307 Ibid., str. 237.

308 Ibid.

Treći sigurnosni problem nastao je kad su se društvene mreže počele koristiti u političke svrhe za planiranje i organiziranje fizičkih prosvjeda, demonstracija, društvenih nemira i kriza.[309] Podjednako su se počele koristiti za planiranje i izvođenje vojnih psiholoških operacija i u vidu potpore vojnom djelovanju u kinetičkim borbama. Brojni primjeri sa svjetskih žarišta govore o tome da su društvene mreže odigrale ključnu ulogu u iniciranju građanskih nemira, organiziranju društvenih i političkih pokreta, u mobilizaciji, poticanju demonstracija i organiziranju uličnih protesta. Primjenom novih tehnoloških rješenja u prikupljanju i obradi podataka (uvjerenja, načela i vrijednosti), izvršenim podjelama, uz mogućnost masovne i globalno distribuirane komunikacije „svatko sa svakim" u stvarnom vremenu, Facebook je bio prva društvena mreža koja je stvorila paradigmatski pomak u tradicionalnim načinima planiranja i organiziranja društvenih pokreta i masovnih prosvjeda. U njihovom planiranju i organiziranju iskorištavaju se sve prednosti koje je Facebook pružio u kiber prostoru: globalni doseg i odabir potencijalnih publika na lokalnoj, regionalnoj globalnoj razini, prema određenim interesima, visoku razinu interakcija i povezanost, ravnopravnost u raspravama, neposrednost i anonimnost djelovanja. Omogućio je masovno i neposredno širenje informacijskih sadržaja (fotografija, audio i video sadržaja) te prenošenje aktivnosti iz virtualnog prostora na ulice i trgove.[310] Time je Facebook postao snažan mrežni stroj za ostvarenje političkih ciljeva i nezaobilazni alat za planiranje i izvođenje vojnih psiholoških operacija. Uz ostale društvene mreže omogućio je zaobilaženje izravnih vojnih sukoba, uz učinkovito umanjivanje volje protivnika.[311] Ova hipoteza potvrđena je istraživanjem koje se metodološki temeljilo na komparaciji američkih vojnih doktrina koje sugeriraju korištenje društvenih mreža u vojnim psihološkim operacijama unutar nekonvencionalnog ratovanja sa znanstvenim radovima o ulozi društvenih mreža u organiziranju pokreta otpora i literaturama koje se bave izučavanjem kako su društvene mreže strukturalno promijenile informacijsko okruženje u kojem djeluju pojedinci i organizacije.

Prvi zabilježeni slučaj u kojem je neki politički pokret iskoristio moć globalne informacijske infrastrukture za organiziranje političke akcije bio je El Ejército Zapatista de Liberación

309 Van Niekerk Brett, Manoj Maharaj, Social Media and Information Conflict, International Journal of Communication 7, str. 1162–1184., 2013. Dostupno na: https://ijoc.org/index.php/ijoc/article/view/1658

310 Burnore Nathanael, Social Media Applications for Unconventional Warfare, U.S. Army Command and General Staff College, SAD, 2013. Dostupno na: Homeland Security Digital Library https://www.hsdl.org/?abstract&did=761246.

311 Usp. Ibid.

Nacional, osnovan 1994. u Meksiku. Španjolski sociolog Manuel Castells nazvao ga je "prvim informacijskim gerilskim pokretom". Njihove aktivnosti uz pomoć interneta privukle su pozornost svjetske javnosti. Iako tada društvene mreže nisu postojale u formi u kakvoj ih danas koristimo, Web 2.0 tehnologije i internet pomogao im je u političkoj borbi.[312] Sljedeći korak u političkom aktivizmu bile su tekstualne (SMS) poruke. S pomoću SMS poruka 2004. u Ukrajini pokrenuta je Narančasta revolucija koja je rezultirala smjenom vlasti. Prvi put u organiziranju političkog i društvenog aktivizma Facebook je iskorišten u Revoluciji šafrana u Burmi 2005., svega godinu dana od njegovog osnivanja, preko Facebook stranice "Podržite prosvjed monaha u Burmi". Prvi put Facebook i YouTube korišteni su u oružanom sukobu koji je izbio između Hezbollaha i Izraela u pojasu Gaze 2008/9. Oba aktera s pomoću društvenih mreža vodili su borbu za percepciju javnosti za legitimitet vlastitog djelovanja. Facebook i Twitter odigrali su važnu ulogu u popularno nazvanoj Twitter revoluciji u Moldaviji 2009. koja je, kao u Burmi i Ukrajini, rezultirala smjenom vladajućih struktura.

Proces započet 2010./2011. poznat kao Arapsko proljeće jedan je od najboljih primjera najmasovnijih društvenih i političkih promjena pokrenutih pomoću društvenih mreža. U državama sjeverne Afrike i Bliskog istoka Facebook i Twitter odigrali su ključnu ulogu u mobilizaciji društvenih pokreta, aktivista i prosvjednika.[313] Na tragu revolucija u Tunisu i Egiptu, nazvani Dani bijesa proširili su se 2011. arapskim svijetom: 07. siječnja u Alžiru, 12. siječnja u Libanonu, 14. siječnja u Jordanu, 17. siječnja u Mauritaniji, 17. siječnja u Sudanu, 17. siječnja u Omanu, 27. siječnja u Jemenu, 14. veljače u Bahreinu, 17. veljače u Libiji, 18. veljače u Kuvajtu, 20. veljače u Maroku, 26. veljače u Zapadnoj Sahari, 11. ožujka u Saudijskoj Arabiji, 18. ožujka u Siriji. U nekoliko slučajeva (Saudijska Arabija, Libanon, Kuvajt, UAE, gdje se zapravo malo toga dogodilo), protesti su zgasnuli iz različitih razloga. U drugim slučajevima ustanci su ugašeni mješavinom represivnih mjera i ustupaka od strane režima (Maroko, Jordan, Alžir, Oman). U Jemenu, Libiji i Siriji, prvobitno miroljubivi pokreti bili su izloženi krajnjem nasilju od strane vlasti i izrodili su se u građanske ratove koji su ove zemlje pretvorili u bojna polja na kojima se geopolitički rivali bore za utjecaj. U Libiji je bila presudna izravna strana vojna intervencija, dok je bitni čimbenik u evoluciji sirijskog ustanka postao strani geopolitički utjecaj. Ovi različiti pokreti nastali su iz motiva koji su specifični za svaku zemlju, a evoluirali su u skladu s uvjetima konteksta i osobnostima svake pobune.

312 Ibid.

313 Ibid.

„Međutim, sve su to bile spontane poruke, nadahnute nadom i uspjehom tuniske i egipatske revolucije, uz pomoć slika i poruka s interneta i arapskih satelitskih televizijskih mreža.“[314] Bez ikakve sumnje, iskra revolta i nade koja je rođena u Tunisu i koja je srušila Mubarakov režim i time dovela do demokratskog Tunisa i protudemokratskog Egipta brzo se proširila na druge arapske zemlje, po istom modelu: pozivanjem na internetu, umrežavanjem u kiber prostoru i pozivima da se zauzme urbani prostor kako bi se izvršio pritisak na vladu da podnese ostavku i pokrene proces demokratizacije.[315]

U slučaju arapskih ustanaka, kada je riječ o preciznoj ulozi digitalnih mreža, Castells tvrdi da je moguće osloniti se na istraživanje koje su obavili Philip Howard i Muhammad Hussain sa svojim suradnicima. Kako navodi Castells, tehnologija ne determinira društvene pokrete niti bilo koje drugo društveno ponašanje. Međutim, on smatra da „mreže interneta i mobilnih telefona nisu samo sredstva, nego su i organizacijske forme, kulturni izrazi i specifične platforme za političku autonomiju“.[316]

Castells dalje navodi kako je Howard u svome djelu 'Digitalno porijeklo diktature i demokracije: informacijske tehnologije i politički islam iz 2011.' (koje je napisano prije arapskih ustanaka, na temelju komparativne analize 75 zemalja, bilo muslimanskih ili sa značajnim udjelom muslimanskog stanovništva) utvrdio da, iako zadani brojnim kontekstualnim faktorima, širenje i upotreba informacijsko-komunikacijskih tehnologija favoriziraju demokratizaciju, osnažuju demokraciju i povećavaju sudjelovanje građana i autonomiju civilnog društva, čime je otvoren put za demokratizaciju države, kao i preispitivanje diktatura. Castells u cijelosti navodi zaključak P. Howarda[317], no ovdje bismo se ograničili samo na jedan dio zaključka:

„U svakom pojedinačnom slučaju, početni incidenti Arapskog proljeća bili su na neki način digitalno posredovani. Informacijska struktura u obliku mobilnih telefona, osobnih računala i društvenih medija bila je dio uzročno-posljedične priče o Arapskom proljeću. Ljudi su bili inspirirani na proteste iz mnogo različitih i uvijek osobnih razloga. Informacijske tehnologije

314 Usp. Manuel Castells: Mreže revolta i nade, društveni pokreti u doba interneta, JP Službeni glasnik, 2018., str. 91.-92.

315 Ibid.

316 Ibid., str. 99.

317 Ibid., str. 100. i 101.

posredovale su to nadahnuće, tako da su se revolucije događale jedna za drugom u roku od nekoliko tjedana i imale su u znatnoj mjeri slične obrasce. Naravno, bilo je različitih političkih ishoda, ali to ne umanjuje značaj uloge digitalnih medija u Arapskom proljeću. Ali, što je još važnije, ovo je istraživanje pokazalo da zemlje koje nemaju civilno društvo koje je prihvatilo digitalne medije imaju mnogo manje šanse da dožive pojavu narodnih pokreta za demokraciju – zapažanje do kojeg smo došli na osnovi objašnjenja čitave konstelacije uzročnih varijabli koje su prethodile početku uličnih protesta, a ne samo na osnovi kratkoročne upotrebe digitalnih tehnologija tijekom kratkog razdoblja političkog previranja".

Castells u nastavku tvrdi da su arapski ustanci bili spontani procesi mobilizacije do kojih je došlo pozivima koji su potekli s interneta i bežičnih komunikacijskih mreža, kako digitalnih, tako i onih neposrednih i osobnih, koje su postojale u društvu.[318] Digitalne mreže i zauzimanje urbanih prostora, u bliskom međusobnom djelovanju, osigurali su platformu za autonomnu organizaciju i deliberaciju, na čijim su temeljima zasnovane pobune te stvorili otpornost koja je bila neophodna da pokreti izdrže žestoke udare državnog nasilja do trenutka kada su, u nekim slučajevima, zbog instinkta samoobrane, i sami postali kontra država.[319]

Neminovno da su društvene mreže kroz njihovu aktivnu upotrebu u svrhu organiziranja društvenih i političkih nemira pridonijele svrgavanju režima.[320] Tadašnja vlast u Egiptu pokušala je prekinuti usluge internetskog mobilnog servisa i na taj način ugušiti prosvjede. Međutim, nije shvatila da moć, zbog ogromne zasićenosti informacijama više nije u informaciji koliko u privlačenju pažnje, a upravo je to bio ključni okidač širih društvenih promjena.[321] Na primjeru Egipta inicijalni povod društvenih nemira bila je smrt mladog aktivista i blogera Khaleda Saida. Međutim, do masovne mobilizacije prosvjednika, kako navodi isti autor, došlo je nakon što je izvršni direktor Googla na Facebooku pokrenuo stranicu "Svi smo Khaled Said", nakon čega su pokrenute slične stranice podrške čelniku egipatske oporbe preko kojih su se u vrlo kratkom vremenu mobilizirale stotine tisuća prosvjednika.[322]

---

318 Ibid., str. 101.

319 Ibid., str. 102.

320 Usp. Affaya Noureddine Mohammed, The Arab Spring: Breaking the chains of authoritarianism and postponed democracy, Contemporary Arab Affairs, 2011. Dostupno na: https://online.ucpress.edu/caa/article-abstract/4/4/463/25971/The-Arab-Spring-breaking-the-chains-of?redirectedFrom=fulltext

321 Burnore, 2013.

322 Ibid.

Na primjeru oružanog sukoba u Siriji društvene mreže odigrale su još važniju ulogu: Terorističke grupe koristile su Facebook kao alat za strateško komuniciranje prema svjetskoj javnosti, Twitter su iskoristile kao učinkovito sredstvo za regrutiranje i mobilizaciju terorista, a YouTube za dodatno vizualno propagiranje vlastitih ideologija i ideja. Svi uključeni akteri, državni i nedržavni, koristili su društvene mreže kao strateške komunikacijske alate preko kojih su se borili za legitimitet vlastitog djelovanja.[323] Još je svježiji primjer Rusije koja se, prilikom pripojenja Krima 2014./2015. sa svrhom pružanju podrške pobunjenicima protiv vlasti u Ukrajini uz kinetičku silu, služila društvenim mrežama kao učinkovitim alatima za planiranje i izvođenje vojnih psiholoških operacija, širenje dezinformacija, (de)mobiliziranje i demoraliziranje ciljanih publika te izvođenje tehnoloških napada preko kiber prostora na protivničke informacijske sustave kako bi onemogućila adekvatne, brze i učinkovite protuodgovore.

Četvrti sigurnosni problem nastao je kad je postalo očito da se društvene mreže mogu zloupotrebljavati i u razdobljima mira za planiranje i izvođenje informacijskih operacija sa svrhom potenciranja društvenih i političkih kriza te za vanjska uplitanja u izborne procese u drugim državama. Najplastičniji primjer bio je slučaj Facebook – Cambridge Analytica i ruske „Agencije za istraživanje interneta“ tijekom predsjedničkih izbora u SAD-u 2016. Primjer zloupotrebe društvenih mreža u izbornoj kampanji za izbor američkog predsjednika pokazao je složenost i isprepletenost unutarnjeg političkog i društvenog sukoba u SAD-u, postojećih društvenih i ideoloških rascjepa unutar američkog društva te interesa Rusije da produbi takva stanja i iskoristi ih za vlastite političke ciljeve. Međusobna isprepletenost ovih čimbenika izazvala je dodatne kontroverze o zlouporabi društvenih mreža i odgovornosti njihovih vlasnika koji ih razvijaju i njima upravljaju.

Izvršene podjele i tehnologije umjetne inteligencije koje omogućavaju „programirano izlaganje“ prema uvjerenjima, vrijednostima i načelima u javnosti su na primjeru SAD-a 2016. izazvale snažan negativan publicitet. Međutim, tek nakon izbijanja slučaja Facebook – Cambridge Analytica i nakon što je na vlast stupio predsjednički kandidat Republikanske stranke Donald Trump, tvrtka Cambridge Analytica javno je prozvana da je na manipulativan način iskoristila osobne podatke korisnika Facebooka za politički interes Republikanske stranke u izbornom procesu kandidata za predsjednika SAD-a. Smatramo potrebnim naglasiti da je

323 Lynch Marc, Freelon Deen, Aday Sean, Syria’s Socially Mediated Civil War, United States Institute of Peace, 2014. Dostupno na: https://www.usip.org/publications/2014/01/syrias-socially-mediated-civil-war

korištenje tehnike „personaliziranog izlaganja informacijskim sadržajima“ prema korisničkim preferencijama za vođenje političkih kampanja u industriji digitalnog marketinga dio općeprihvaćenih tržišno diktiranih pravila i standarda koji se primjenjuju u SAD-u. U SAD-u političke stranke i kandidati od 2000-tih, u svrhu ostvarivanja boljih rezultata u političkim kampanjama, koriste usluge tvrtki kao što je Cambridge Analytica koje informacijske operacije nude kao komercijalnu uslugu i u kojima se koriste Facebookom. Iako je velika pažnja javnosti bila usmjerena na Cambridge Analyticu, skandal je naglasio simptom i upozorenje na nešto puno šire što će neminovno promijeniti način promišljanja društva o štetnim posljedicama neadekvatne regulacije umjetne inteligencije i zaštite osobnih podataka građana na društvenim mrežama. Problem je predstavljala činjenica da se u primjeru američkih predsjedničkih izbora tehnologija umjetne inteligencije koje koriste društvene mreže zlouporabila za uplitanje strane države u izborne procese, da osobni podaci građana u posjedu velikih tehnoloških korporacija koje upravljaju društvenim mrežama nisu zaštićeni i da trgovina ovim podacima nije na adekvatan način regulirana djelatnost. Unatoč tome, političke stranke u SAD-u nakon 2016. nastavile su voditi političku borbu koristeći se uslugama Facebooka i tvrtki kao što je Cambridge Analytica.

U vezi s tadašnjom pobjedom republikanskog kandidata Donalda Trumpa, vlasnik Facebooka Mark Zuckeberg komentirao je kako je ideja da je njegova platforma utjecala na rezultat ičijeg glasanja „prilično bedasta“. Međutim, nakon žestokih reakcija od strane američkih liberalnih medija i političara, Facebook je bio prisiljen objaviti dokument pod nazivom „Informacijske operacije“ kojim je morao objasniti metodologiju suptilne zloupotrebe svoje platforme. U ovom uratku Facebook je čak izrijekom kazao da je njegov protivnik bila Vlada Ruske Federacije. Primjer su bili ruski hakeri iz farme trolova iz St. Petersburga, ruske „Agencije za istraživanje interneta“, koji su Facebook iskoristili za pokretanje masovne dezinformacijske kampanje prema američkom glasačkom tijelu, kako bi se postigli vanjskopolitički ciljevi. Pokrenutom masovnom dezinformacijskom kampanjom u kojoj su se koristile sve mogućnosti koje je Facebook omogućio svim svojim korisnicima, ruski hakeri iskoristili su ove tehnologije protiv američkog biračkog tijela. Postoje i brojni drugi primjeri operacija utjecaja koje se vode preko Twittera, Facebooka ili Instagrama[324] o kojima će detaljnije biti riječi u nastavku istraživanja.

---

324 Cohen Daniel i Bar’el Ofir, The Use of Cyberwarfare in Influence Operation, Blavatnik Interdisciplinary Cyber Research Cente, Tel Aviv University, 2017. dostupno na: https://icrc.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf

Slučaj Facebook – Cambridge Analytica u javnosti je podignuo percepciju o ustaljenoj praksi u industriji digitalnog marketinga, a to je da izvršene podjele korisnika na društvenim mrežama prema interesima i grupiranim identitetskim pripadnostima uz „programirano izlaganje“ prema korisničkim preferencijama nude savršen način manipuliranja obavijestima, informacijama i samim kognitivnim procesima u ljudskom razmišljanju i donošenju odluka. Ove metode pokazale su se naročito štetnim u američkoj predsjedničkoj kampanji, kad su američki građani donosili odluke o budućnosti upravljanja državom.[325] Problem je, kao i kod svih drugih oblika manipulacija, da se „programirano izlaganje“ ne može jednostavno prepoznati zbog suptilnosti isporučenog sadržaja koji je sustavom povratne sprege i primjenom hibridne inteligencije prilagođen krajnjem korisniku. Manipulativnost ove tehnike proizlazi iz pretpostavke da umjetna inteligencija algoritamskom obradom korisničkih preferencija, kroz sustav povratne sprege, zna više o ponašanju ciljanih publika od njih samih i da razmjena podataka i informacija nije jasna i transparentna. Ovdje se zapravo radi o zloupotrebi osobnih podataka i kognitivnih slabosti korisnika društvenih mreža. Kako sustav povratne sprege omogućava nadziranje osobnih podataka i interesa te primjenom hibridne inteligencije prilagođava informacije prema interesima, znatno je otežano pravovremeno uočavanje manipulativne namjere. Opisana kritika temelji se na činjenici da „programirano izlaganje“ ne pruža samo objektivne obavijesti i informacije o budućim ponašanjima nego se na osnovi korisničkih preferencija stvaraju učinkovitiji utjecaji na buduće odluke.[326] Ne stvaraju se novi oblici kontroliranja ljudskog uma niti se stvaraju značajniji učinci u promjenama temeljnih uvjerenja, vrijednosti i načela, već se uočene slabosti dodatno čini vidljivima i na taj način se neminovno utječe i na smjer razmišljanja i donošenje odluka. „Programirano izlaganje“ dodatno iskorištava izvršenu podjelu prema vrijednostima, uvjerenjima i načelima. Ova podjela osnova je svake daljnje manipulacije informacijama na društvenim mrežama. Grupirani interesi su izloženiji mogućnostima utjecaja jer im se mogu prilagođavati informacije.[327] Tamo gdje „programirano izlaganje“ isporučuje preferirani informacijski sadržaj u obliku objave ili novinskog članka, umjetna inteligencija je kroz podjele korisnika na društvenim mrežama identificirala njihove

325 Henriksen Ellen Emilie, Big data, microtargeting, and governmentality in cybertimes, The case of the Facebook-Cambridge Analytica data scandal, Master thesis in political science, Department of Political Science University of Oslo, 2019. Dostupno na: https://www.duo.uio.no/handle/10852/69743

326 Usp. Hofmann, J. Mediated democracy – Linking digital technology to political agency. Internet Policy Review, 2019., dostupno na https://doi.org/10.14763/2019.2.1416 i Kreiss, D. Micro-targeting, the quantified persuasion. Internet Policy Review, 2017., dostupno na https://doi.org/10.14763/2017.4.774

327 Usp. Henriksen, 2019.

slabe točke i ranjivosti prema kojim se onda isporučuju njima prilagođene informacije. Objave, vijesti ili novinski članci koji se „konzumiraju“ unutar homogene grupe, tumače se na drugačiji način unutar druge grupe s drugačijim stavovima, mišljenjima i uvjerenjima. Izvedena podjela i mogućnost manipuliranja informacijama time je postala osnova svake daljnje manipulacije.[328]

Na osnovi primjene tehnologija umjetne inteligencije u obavljaju ovih osnovnih zadaća na društvenim mrežama tehnološke korporacije poput Facebooka, Twittera i YouTubea postale su globalni upravitelji moći. Preko njihovih platformi različiti akteri mogu mobilizirati, regrutirati vlastite pristaše i simpatizere, mogu širiti dezinformacije i voditi informacijske i psihološke operacije u borbi za pažnju, način razmišljanja i donošenje odluka ciljanih publika za vlastite interese. Ove korporacije stekle su moć da u političkoj borbi utječu na izbor pobjednika. Njihove poslovne odluke i tvorničke postavke algoritama i druge tehnologije umjetne inteligencije odredile su pravila koja oblikuju bojišnicu kiber prostora u kojem se njihovim tehnologijama odlučuje o pobjednicima i gubitnicima u ratu i politici.

328 Ibid.

3. NACIONALNE INFORMACIJSKE STRATEGIJE, DRUŠTVENE MREŽE I OPERACIJE UTJECAJA U KIBER PROSTORU

3.1. Informacijske strategije i kiber prostor

Pojavom kiber prostora nastali su novi strateški planovi najrazvijenih zemalja koji polaze od dogme da je informacija jedan od četiri ključna izvora nacionalne moći i da će „informacijska superiornost omogućiti dominaciju u odlučivanju (…) i odlučnu prednost nad budućim protivnicima“.[329]

Svjetska je politika i službeno prihvatila panaceju: nove informacijske i komunikacijske tehnologije vode u „novu civilizaciju“, u „informacijsku revoluciju“, odnosno u „društvo znanja“. Takvu viziju najavio je 1994. potpredsjednik SAD-a Al Gore zagovarajući projekt globalne informacijske infrastrukture: „Globalna informacijska infrastruktura opasat će zemljinu kuglu s informacijskim veleprometnicama /superhighways/ po kojima će svi ljudi putovati. Ove prometnice – ili preciznije, mreže distribuirane inteligencije – omogućit će nam da dijelimo informacije, da se spojimo i komuniciramo kao globalna zajednica.“[330] Ubrzo je grupa najrazvijenih zemalja G-7, na inicijativu SAD-a, odlučila o politici implementacije navedenog projekta te su u nizu održanih nacionalnih i kontinentalnih konferencija odaslale osnovne poruke: „bez primijenjenih nacionalnih informacijskih i komunikacijskih politika, strategija i razvojnih planova, zemlje neće biti u stanju u potpunosti sudjelovati u globalnom informacijskom društvu“.[331]

Nova je informacijska tehnologija promijenila ne samo prirodu znanja, nego i socijalne uloge i zadaće novouspostavljenog informacijskog poretka.[332] Novi informacijski poredak u globalnoj informacijskoj infrastrukturi dobio je novi prostor za ostvarivanje programa globalnih informacijskih dominacija. Novim informacijsko-komunikacijskim i računalnim tehnologijama informacijski poredak u globalnoj informacijskoj infrastrukturi dobio je učinkovite alate za ostvarivanje takvih programa. Nastali su novi uvjeti i nova pravila prema kojima je akterima na globalnoj sceni omogućeno stvaranje informacijske dominacije punog spektra.[333] „Informacija

329 Tuđman, 2013., str. 88.; prema Joint Vision 2020 - America's Military: Preparing for Tomorrow. Washington, D.C., US Governmment Printing Office, June 2020.

330 Tuđman 2013., str. 177.; prema Hamelink.

331 Tuđman 2013., str. 177.

332 Ibid., str. 180.

333 Ibid., str. 183.

je postala oružje za sređivanje političkih, gospodarskih, kulturnih, društvenih odnosa na globalnim i lokalnim razinama, a informacijski prostor i mediji postali su bojišnicom.“[334] „Informacija (i njene izvedenice) u cijelom spektru djelovanja dobila je ključnu ulogu, a vojna opcija prestala je biti glavna prijetnja i krajnje rješenje.“[335]

Za razliku od industrijskog doba u kojem su „zemlje koje su imale prevlast na moru i u zraku vladale svijetom, u informacijskom dobu zemlje koje dominiraju informacijskim prostorom imaju dominaciju u svijetu.“[336] „Države uspješne na globalnom planu, a pogotovo one koje žele osigurati dominaciju i hegemoniju u svijetu, prema novim uvjetima i pravilima pristupile su razvoju novih nacionalnih informacijskih strategija.“[337] „Zemlje koje su usvojile nacionalne informacijske strategije, razvile doktrine informacijskog ratovanja, osigurale potrebnu infrastrukturu za provođenje informacijskih operacija, podredile i uskladile djelovanje svojih državnih, vojnih nevladinih i gospodarskih djelatnosti prema stranim javnostima – danas dominiraju i vladaju u svijetu.“[338]

Cilj je nacionalnih informacijskih strategija:[339]

1. „objedinjavanje i koordinacija djelovanja na polju informacijskih operacija svih institucija i ustanova koje se u svom radu koriste tom vrstom djelovanja“,
2. „prilagođavanje njihove aktivnosti novim stvarnostima“,
3. „stvaranje uvjeta uz pomoć kojih se može izvršiti ključni utjecaj na strateške razine odlučivanja druge strane (političke, vojne, gospodarske, sigurnosne, društvene, vjerske), na oblikovanje prostora javnog znanja, a time i svijesti, percepcije i volje pripadajućeg i/ili onog koji može vršiti utjecaj, javnog mnijenja.“

Novim doktrinarnim pristupima državni akteri kroz kiber prostor nastoje ispuniti ciljeve vlastitih politika te ispuniti konačni cilj nacionalnih informacijskih strategija: „osigurati informacijsku nadmoć radi vlastitih interesa, odnosno osigurati barem dominaciju onih

---

334 Tuđman, 2008, str. 154. i Tuđman, 2013., str. 180.

335 Ibid.

336 Usp. Tuđman, Miroslav, Informacijske operacije i mediji ili kako osigurati informacijsku superiornost, 2011., dostupno na: https://www.researchgate.net/publication/281069630_Informacijske_operacije_i_mediji_ili_kako_osigurati_informacijsku_superiornost

337 Ibid.

338 Tuđman, 2013., str. 179.

339 Akrap, 2011., str. 39.

informacija koje će onemogućiti protivničkoj strani razvoj oporbenih informacija.“ Prema prikazanim ciljevima nacionalnih informacijskih strategija, informacijska nadmoć „ogleda se u postizanju bitne prednosti u procesima prikupljanja, obrade, promjene odnosno manipulacije, distribucije (prikrivene i javne) obavijesti (i njezinih izvedenica) prema različitim ciljanim publikama, na strateškoj razini odlučivanja, djelovanja i utjecanja te mogućnosti bitnog utjecaja na učinkovitost protivničkog informacijsko-komunikacijskog sustava.“ Uvođenje novih strategija bilo je nužno radi iskorištavanja svih prednosti koje pruža kiber prostor i nove tehnologije, kako u zaštiti vlastitog prostora javnog znanja tako i u ovladavanju za vlastite aktivnosti prema protivničkom prostoru javnog znanja. Naime, „ukoliko netko nije u stanju koristiti njihove prednosti ili pak nije u stanju odgovoriti na izazove koje pred njega i njegovu nacionalnu informacijsku strategiju postavlja protivnička strana, njihov je prostor javnog znanja uvelike oslabljen i time izložen i podložan brzim promjenama u, za napadača, poželjnim pravcima.“[340] Informaciji kao oružju suvremenih imperijalnih politika cilj je trajno osigurati i sebi podrediti informacijski prostor svojih protivnika. Drugim riječima, cilj je informacijskih strategija dobiti rat, a ne voditi stalno nove bitke u istom prostoru. Zato kontrola javnog znanja protivnika ima dva cilja: prvo, trajno dominirati u informacijskim prostoru, što se može ostvariti nametanjem pravila za institucionalno tumačenje zbilje „odozgo“; drugo, osigurati sebi lojalnu profesionalnu skupinu koja će održavati željeni informacijski poredak.[341]

Stvaranjem kiber prostora nove informacijske bojišnice dolazi do „tri bitne promjene i u filozofiji međunarodnih odnosa: prvo *„mekana moć“* dobiva prednost nad uporabom „tvrde sile“, odnosno javna diplomacija ima prioritet u odnosu na vojne operacije; drugo informacija postaje jedan od četiri osnovna instrumenta nacionalne moći; a treće u rješavanje međunarodnih sukoba uvedena je doktrina sukoba niskog intenziteta.“[342]

Mekana moć

U međunarodnim odnosima moć se tradicionalno smatra sposobnošću postizanja željenog cilja na temelju dva osnovna koncepta. Prva mogućnost temelji se na konceptu *mekane moći* odnosno na sposobnosti napadača da uobliči neki podatak, obavijest i/ili informaciju na način da privuče i uvjeri ciljanu publiku da dobrovoljno provodi njegovu volju, dobrovoljno prihvati

340 Ibid.

341 Tuđman, 2013., str. 188.

342 Ibid., str. 178.

napadačeve ideje, njegovu kulturu, jezik, ideologije i politike odnosno njegov sustav vrijednosti, uvjerenja i načela. Druga mogućnost je koncept *tvrde moći* koja se, kao krajnje rješenje u nametanju napadačeve volje, temelji na vojnoj ili ekonomskoj prisili. „Joseph Nye definirao je pojam *mekane moći* kao „sposobnost da dobijete ono što želite kroz privlačnosti, prije nego prisilom ili plaćanjem. Privlačnost jedne zemlje, nacije, politike, kulture, gospodarstva postiže se javnom diplomacijom. Zato *mekana moć* postaje ključni pojam u redefiniranju politike javne diplomacije kojoj je cilj uvjeriti druge da prihvate i slijede norme i institucije koje proizvode poželjno ponašanje.“[343]

Primjena hibridne inteligencije za rješavanje međunarodnih sukoba kroz kiber prostor promijenila je dosadašnje shvaćanje primjene *mekane moći* u rješavanju međunarodnih sukoba. Kao posljedica nastale paradigme, *mekana moć* se u kiber prostoru pretvorila u tzv. *oštru moć*. *Oštra moć* nastaje kad uobličavanje podataka, obavijesti i/ili informacija od dobrovoljnosti pređe u obmanu i takav čin u svojoj biti postaje prisilan. Prisilna obmana briše element dobrovoljnosti i ne predstavlja više *mekanu moć* već ona postaje *oštra moć*.[344] Između *mekane* i *oštre moći* osnovna razlika je u različitom pristupu uobličavanju informacija. *Mekana moć* primarno se provodi informacijskim operacijama javne diplomacije, dok *oštra moć* primarno djeluje i provodi se u kiber prostoru psihološkim operacijama. *Oštra moć* teže je primjetna zbog anonimnosti, masovnosti, automatizacije i optimiziranosti psiholoških operacija prema društvenim slabostima ciljanih publika. Dodatnoj prikrivenosti i neprimjetnosti pridonosi činjenica da ih provode obavještajni sustavi s pomoću lažnih računa na društvenim mrežama, čime se dodatno otežava pravovremeno uočavanje i odvraćanje.

Oštru moć promatra se kroz sposobnost uobličavanja dezinformacija prema društvenim slabostima uz pomoć hibridne inteligencije s prikrivenim političkim interesima.

343 Ibid., str. 178.

344 Usp. Nye, 2019. i Walker Christopher, Kalathil Shanthi i Ludwig Jessica, The Cutting Edge of Sharp Power, Journal of Democracy Volume 31, Number 1, National Endowment for Democracy and Johns Hopkins University Press, 2020. Dostupno na: https://www.ned.org/wp-content/uploads/2020/01/Cutting-Edge-Sharp-Power-Walker-Kalathil-Ludwig.pdf

Oštra moć objedinjuje kiber napade na kritične infrastrukture[345] i dezinformacijske kampanje u vidu psiholoških operacija. Kod *mekane moći* fokus je na "osvajanja srca i umova", a kod *oštre moći* na „ubacivanju“ dezinformacija u politički i medijski diskurs ciljanih publika. Na ovaj način *oštra moć* koristi se za stvaranje novih oblika prijetnji iz kiber prostora. Osnovne karakteristike *oštre moći* su: velika brzina prenošenja dezinformacija, nizak trošak sudjelovanja, odabir optimalnog vremena odnosno fleksibilnost u planiranju i izvođenju dezinformacijskih kampanja u stvarnom vremenu, mogućnosti (de)mobilizacije pristaša i/ili protivnika ovisno o napadačevim potrebama, anonimnost i dovoljan stupanj poricanja. *Oštra moć* promatra se kroz cjelokupni skup napadačkih taktika koje u strateškom smislu u konačnici daju sveukupnu učinkovitost u nametanju volje i stjecanju stanja informacijske nadmoći.[346] Čimbenici koji podižu taktičku i stratešku učinkovitost, odnosno koji *mekanu moć* pretvaraju u *oštru moć* su otvorenost kiber prostora, maskiranost napadačevih namjera i sposobnost provođenja državne kontrole nad planiranim taktičkim koracima u stvaranju informacijsko-psihološkog pritiska na razmišljanja i donošenje odluka. Neupitno je da je od presudnog značaja pri tome postala primjena hibridne inteligencije na društvenim mrežama.

Oštra moć na Zapadu primarno se veže za sposobnost Rusije u stvaranju prijetnji koje su usmjerene protiv SAD-a i njezinih saveznika. Vlastite nedostatke i ograničenja *meke moći* u promicanju i privlačenju podrške idejama i ideologijama tradicionalizma, državnog suverenizma i nacionalnih politika[347] Rusija je nadoknadila primjenom *oštre moći* u kiber prostoru.[348] Pomoću društvenih mreža uspjela je upravljati društvenim i političkim procesima

345 Kritične infrastrukture su infrastrukture od vitalne važnosti jer omogućavaju temeljno funkcioniranje gospodarskog sustava neke države i njezinog društva u cjelini. Kritične infrastrukture čine sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti: gospodarske, energetske, političke, kulturne, sportske, sigurnosne, medijske, informacijsko-komunikacijske itd. Vidi više: Zakon RH o kritičnim infrastrukturama, dostupno na https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama

346 Usp. Leonova O. Sharp Power – the New Technology of Influence in a Global World. Mirovaya ekonomika i mezhdunarodnye otnosheniya, 2019, vol. 63., No. 2., str. 21.-28. https://doi.org/10.20542/0131-2227-2019-63-2-21-28

347 Nye, 2019. Autor se referira na pružanje podrške desno populističkim strankama u pojedinim državama EU-a koje propagiraju ideje tradicionalizma, konzervativizma, suverenizma i nacionalnih politika naspram različitih ideja globalizacije i srodnih termina koji se vežu za ideje liberalne demokracije na društvenom, ekonomskom, političkom i kulturnom području.

348 Usp. Walker Christopher i Ludwig Jessica, From ‘Soft Power’ to ‘Sharp Power’, Rising Authoritarian Influence in the Democratic World, National Endowment for Democracy, 2017. Dostupno na https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf

u drugim državama za vlastite vanjskopolitičke ciljeve i interese.[349] Učinkovitom primjenom hibridne inteligencije u stvaranju dezinformacija i psiholoških pritisaka u kiber prostoru, Rusija je pokazala je da se *mekana moć* od pasivnog utjecaja uz pomoć društvenih mreža može pretvoriti u način djelovanja za uspostavljanje aktivne kontrole[350] nad političkim i društvenim procesima u drugim državama. Ova paradigmatska promjena dovela je do radikalnih promjena u promišljanju o planiranju i vođenju sukoba kroz kiber prostor. NATO savez nastalu promjenu paradigme u ruskom pristupu opisao je sposobnošću pretvaranja informacija u oružje (engl. *weaponization of information*) primjenom strategije „4-D" koja se oslanja na četiri bitne stavke: odbaci kritike, iskrivi činjenice, odvrati od glavnog pitanja i zastraši publiku.[351] „Kao plastičan primjer suvremenih shvaćanja trajne uporabe operacija utjecaja vrijedno je istaknuti sadržaj koji je u svom radu 2013. istaknuo načelnik stožera Oružanih snaga Ruske Federacije general Gerasimov.[352] U tom je radu naglasio promjenu paradigme napada u novim sukobima, koji ne moraju prerasti u ratove, u kojima prevladavaju aktivnosti iz spektra informacijskog ratovanja u odnosu na ratovanje klasičnim kinetičkim ubojitim sredstvima u omjeru 4 : 1 u korist informacijskog ratovanja. Druga novina koju naglašava general Gerasimov jest prihvaćanje činjenice da se aktivnosti iz spektra hibridnih prijetnji mogu i trebaju planirati i provoditi bez prestanka (24/7) i bez obzira na to vlada li stanje apsolutnog mira, krize, rata ili poraća."[353]

Iako je ruski pristup u korištenju društvenih mreža „u planiranju nekinetičkih operacija pobudio zanimanje široke javnosti, potrebno je jasno reći da na Zapadu nije nepoznato da operacije nekinetičkim sredstvima (operacije utjecaja) imaju iznimno važno mjesto u sukobima u odnosu na operacije u kojima se upotrebljavaju kinetička ubojita sredstva."[354]

---

349 Usp. Orttung Robert i Walker Christopher, Russia's International Media Poisons Minds, Moscow Times, 2014, Dostupno na: https://themoscowtimes.com/articles/russias-international-media-poisons-minds-40194

350 Usp. Kuzio Taras i D'anieri Paul, The Sources of Russia's Great Power Politics, E-International Relations, Bristol, England 2018. Dostupno na: https://www.e-ir.info/publication/the-sources-of-russias-great-power-politics-ukraine-and-the-challenge-to-the-european-order/

351 Brooking i Singer, 2020.

352 Gerasimov Valery, The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, MILITARY REVIEW January-February 2016., str. 23-29. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

353 Akrap, 2019.

354 Ibid., str. 41.

Upotreba hibridne inteligencije, lažnih računa i svih raspoloživih tehnologija koje koriste društvene mreže za procesuiranje podataka za uobličavanje anonimnih dezinformacija prema kulturnim i identitetskim simbolima odnosno uvjerenjima, vrijednostima i načelima ciljanih publika ključna je novost u planiranju i izvođenju psiholoških operacija u kiber prostoru. Raspoložive tehnologije u proteklom desetljeću u planiranju i izvođenju psiholoških operacija u kiber prostoru prema uvedenoj doktrini sukoba niskog intenziteta počele su primjenjivati SAD i Rusija s međusobnim razlikama i sličnostima.

Javna diplomacija

„Prema američkoj službenoj doktrini četiri su instrumenta i izvora nacionalne moći: javna diplomacija, informacija, vojska i gospodarstvo (John Bokel). Redoslijed u nabrajanju nije nebitan. Informacija kao instrument nacionalne moći na drugom je mjestu, prije vojske i gospodarstva, a to znači da je i težište američke nacionalne i sigurnosne politike stavljeno prije na informacijske operacije, nego na vojne i gospodarske. Uloga i zadaća javne diplomacije, odnosa s javnošću i psiholoških operacija u strateškim informacijskim operacijama vrlo je precizno definirana.“[355] „Javna diplomacija danas je suvremeni termin koji je zamijenio nepopularne nazive propaganda i informacijske operacije.“[356] „Javna je diplomacija relativno nova doktrina u međunarodnim odnosima koja polazi od teze da je uporaba *“mekane moći”* (dakle, informacija i medija) učinkovitija od vojnih operacija ili ratova.“[357] „Pod javnom se diplomacijom podrazumijeva djelovanje jedne suverene zemlje prema javnostima u drugim zemljama kako bi se utjecalo na stavove i mišljenja javnosti u drugim zemljama, s namjerom da se prihvate i promiču nacionalni ciljevi i interesi strani tim zemljama.“[358] Odnosno, javna diplomacija predstavlja napore vlade jedne države da utječe na javno mišljenje i mišljenje elita u drugoj državi s ciljem da se u svoju korist promijeni vanjska politika ciljane države.[359] Javna diplomacija „podrazumijeva plasiranje informacija prema inozemstvu iako inozemna publika kojoj se te informacije obraćaju ne mora biti njihov primarni cilj, dok odnosi s javnošću podrazumijevaju plasiranje informacija domaćoj publici iako domaća publika ne mora biti

355 Tuđman, 2011., str. 30.

356 Tuđman, 2008., 135.

357 Tuđman, 2011., str. 30.

358 Ibid.

359 Tuđman, 2008., str. 135.

njihov primarni cilj.“[360] „Javna diplomacija postala je javna doktrina velesila u međunarodnim odnosima, tj. odnosima između država. Pod tim se podrazumijeva “legalizacija” uporabe medija, agencija za odnose s javnošću, nevladinih organizacija, Pool agencija, razmjene stručnjaka itd., s ciljem da se “privole” strane javnosti i strani političari da se ponašaju i donose odluke na vlastitu štetu. Strateški cilj javne diplomacije je osigurati informacijsku superiornost i dominaciju vlastitih informacija.[361] „Informacijske operacije koje provodi javna diplomacija u svojem operativnom, izvedbenom dijelu, nisu javne.“[362]

Sve donedavno za opisivanje sukoba bila su potrebna četiri instrumenta moći. Za one koji su željeli voditi i planirati sukobe i ratove bilo je važno imati mogućnost korištenja nekih od onih instrumenata poznatih pod akronimom DIME (Diplomacy, Information, Military, Economy). Glavna poluga nametanja vlastite volje ciljanim publikama temeljila se na vojnoj moći i na sposobnosti (vojne moći) brzog, učinkovitog, potpunog prijenosa, odnosno sigurnog, potpunog i neometanog prebacivanja na željeno područje i angažiranja prema individualnim ciljevima, u onoj mjeri i razini koja omogućuje brzu pobjedu u oružanom sukobu. Postizanje ukupne pobjede, s druge strane, zahtijevalo je brzu i potpunu transformaciju pregovaračkih sposobnosti u moć korištenja prisile i njezino ponovno aktiviranje nakon što se kinetički sukob približio svom kraju.[363]

Sukobi niskog intenziteta

U sukobima niskog intenziteta „u osnovi se vode borbe za ljudsko mišljenje“ (..) a u njima su „psihološke operacije postale važnije od primjene vojne sile ... kognitivna domena postala je primarna bojišnica, informacijska domena sekundarna, a fizička tek tercijarna.“[364] Kao posljedica globalizacije informacijskog prostora obavijest je postala oružje, kiber prostor bojišnica sukoba niskog intenziteta u kojima dominiraju javna diplomacija, informacijske napadačke aktivnosti psihološke operacije i medijske operacije, a izvode se primarno kroz kiber prostor pomoću informacijsko-komunikacijskih i računalnih tehnologija i rješenjima koja nudi umjetna inteligencija. U kiber prostoru koji je postao bojišnicom i u sukobima niskog intenziteta

360 Ibid.

361 Tuđman, 2011., str. 30.

362 Ibid.

363 Akrap Gordan, Ivica Mandić, Why Security Science, Security Science Journal, Vol. 1 No. 2, 2020

364 Akrap, 2009.

u kojima se vode borbe za ljudsko mišljenje a informacija je postala oružje za ostvarivanje informacijskih strategija, postalo je očito i neizbježno da su informacijsko-komunikacijske i računalne višedimenzionalne tehnologije umjetne inteligencije na društvenim mrežama dobile novu zadaću: „osigurati informacijsku nadmoć odnosno osigurati barem dominaciju onih informacija koje će omogućiti protivničkoj strani razvoj oporbenih informacija.“[365] Društvene mreže s primijenjenim rješenjima koja hibridna inteligencija nudi u prikupljanju, pohrani, obradi i isporuci informacija postale su oružje u rukama onih koji imaju dovoljno znanja i vještina, financijsku podršku i razrađene strateške ciljeve.

3.2. Operacije utjecaja u kiber prostoru

U rješavanju međunarodnih sukoba i u teoriji o informacijskom ratovanju termin koji obuhvaća informacijske operacije, medijske operacije, javnu diplomaciju i odnose s javnošću jesu operacije utjecaja, a navedene sastavnice u funkciji su njihove provedbe.[366] Operacije utjecaja kroz sinergiju informacijskih i medijskih operacija, javne diplomacije i odnosa s javnošću za konačan cilj imaju postizanje informacijske nadmoći nad prostorom javnog znanja ciljanih publika. Operacije utjecaja u kiber prostoru sve više zauzimaju glavno mjesto u napadačkim informacijskim operacijama. Razlog je u prostoru u kojem se izvode. Njihovo planiranje i izvedba u kiber prostoru dovelo je do paradigmatske promjene. Teško ih je nekome pripisati, time nose mali rizik od eskalacije sukoba u ratna stanja. Međutim, kada je u pitanju definiranje svih elemenata koji čine stratešku primjenu moći u informacijskoj domeni na Zapadu još uvijek nedostaje konsenzus budući da postoji velika zbrka što se tiče upotrebe izraza i postoje brojne proturječne definicije pojmova koji se koriste u različitim kontekstima za opisivanje različitih ciljeva i radnji, ovisno koriste li se u razdobljima mira ili rata.[367] Glavni razlog tome je što operacije utjecaja zahvaljujući globalnom digitaliziranom informacijskom prostoru i društvenim mrežama, više nisu ograničene na vojne operacije, već mogu biti dio bilo koje vrste sukoba, uključujući i one koji se vode u diplomatskoj areni. Neupitno je da su kiber prostor i informacijsko-komunikacijski sustavi i tehnologije umjetne inteligencije koje koriste društvene

365 Ibid.

366 Usp. Tuđman, Informacijske operacije i mediji ili kako osigurati informacijsku superiornost', National security and the future, 10(3-4), 2009, str. 25-45, str. 29.. Preuzeto s: https://hrcak.srce.hr/80565 (Datum pristupa: 09.12.2021.)

367 Ova primjedba odnosi se na pojmove i izraze Informacijski rat, Psihološke operacije, Operacije utjecaja, Strateške komunikacije, Operacije računalne mreže i Vojna obmana. Pojmovi kao što su informacijski rat, psihološke operacije i vojna obmana obuhvaćaju aktivnosti s informacijama isključivo za vojna djelovanja, dok operacije utjecaja i strateške komunikacije podrazumijevaju i korištenje informacija izvan vojnog djelovanja. Detaljnije o razlikama bit će izneseno u nastavku istraživanja.

mreže otvorili nove mogućnosti za njihovu provedbu i izvan konteksta vojnog djelovanja. Operacije utjecaja dio su šireg nastojanja različitih aktera da steknu informacijsku nadmoć nad korpusom javnog znanja ciljanih publika i nisu više nužno vezane za vojno djelovanje. U načelu operacije utjecaja uspjeh ostvaruju kroz: „upotrebu nevojnih [nekinetičkih] sredstava, s ciljem umanjivanja protivnikove snage volje, zbunjivanja i ograničavanja donošenje odluka i potkopavanja javne potpore, tako da se pobjeda može postići bez kinetičke prisile“.[368] Stoga termin operacije utjecaja obuhvaća sve operacije u informacijskoj domeni, uključujući sve aktivnosti *mekane i oštre moći*. Iako su u principu nenasilne, mogu biti dio pripremnih aktivnosti za planiranje i vođenje vojnih operacija.[369] One uključuju sve napore u miru ili tijekom oružanog sukoba koje poduzimaju države ili bilo koje druge skupine kako bi utjecale na ponašanje ciljane publike. Različiti pristupi planiranju i provođenju operacija utjecaja u kiber prostoru u razdobljima mira detaljnije će se iznijeti u nastavku istraživanja u kojem će se opisati različiti pristupi SAD-a i Rusije u primjeni operacija utjecaja ovisno o kontekstu i potrebama. Ovdje je dovoljno istaknuti da je na Zapadu pristup operacijama utjecaja transparentniji i ograničen na vojno djelovanje, nasuprot ruskom koji je cjelovitiji i podrazumijeva upotrebu ovih operacija i izvan vojnog djelovanja.

Operacije utjecaja predstavljaju dobro poznatu metodu informacijskih operacija kojom se ostvaruju politički, vojni, ekonomski i društveni ciljevi. Za ostvarivanje rečenih ciljeva koriste se svi raspoloživi alati i metode *mekane i oštre moći* kako bi se ciljane publike privlačilo da donesu odluke u interesu napadača. Kao što informacijske strategije oduvijek koriste informacije kako bi poboljšale ciljeve i politike svojih donositelja tako ni sukobi nikada nisu bili ograničeni na vojno područje djelovanja.[370] Glavna pretpostavka operacija utjecaja je da one, putem širenja informacija i prenošenja poruka, mijenjaju stavove i oblikuju mišljenja[371] te time ostvaruju trenutne učinke na promjenu u stavovima, načelima i vrijednostima ciljanih publika. Kiber prostor i društvene mreže u ovom kontekstu unijele su paradigmatsku promjenu.

---

368 Brangetto Pascal i Veendendaal Matthijs, Influence Cyber Operations: the Use of Cyberattacks in Support of Influence Operations. 8th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2016. Dostupno na: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf; prema Anne Applebaum, Edward Lucas, Wordplay and War Games, 19 June, 2015, http://www.cepa.org/content/wordplay-and-war-games

369 Brangetto, Veendendaal, 2016., str. 115.

370 Ibid. str 1.; prema Qiao Liang i Wang Xiangsui, Unrestricted Warfare, PLA Literature and Arts Publishing House, 1999, str. 189.

371 Usp. Hutchinson William, Influence Operations: Action and Attitude, 2010. Dostupno na: https://ro.ecu.edu.au/isw/33/

Kao novo područje borbenog djelovanja kiber prostor postao je idealan za provođenje operacija utjecaja u kojima je „hakiranje“ umova i oblikovanje okruženja u kojem se odvija politička rasprava postalo važnije od uništavanja i onesposobljavanja kritičnih infrastruktura.[372] Nastali su novi, učinkovitiji prisilni načini utjecaja na razmišljanje i donošenje odluka ciljane publike koji ostaju u području informacija, ali se više ne mogu smatrati dijelom primjene *mekane moći* budući da više nisu dizajnirani za postizanje ciljeva isključivo kroz moć 'privlačenja'.[373]

Osnovne prednosti i veću učinkovitost operacija utjecaja u odnosu na one koje se vode preko tradicionalnih medijskih kanala (televizije, radija i tiskanih medija) omogućili su kiber prostor i društvene mreže.

Ciljane publike i strategije utjecaja ostale su iste kao i kod tradicionalnih operacija utjecaja. Međutim, razlika je višeznačna: u prostoru u kojem se odvijaju; u korištenim alatima, tehnikama, akterima koji ih provode i u razmjerima učinaka. U operacijama utjecaja koje se planiraju i izvode u kiber prostoru iskorištava se čitav spektar nekinetičkih mogućnosti sa svrhom postizanja maksimalnog strateškog učinka.

Novina je da se operacije utjecaja planiraju i provode u kiber prostoru, a u njemu nema pravila prema kojima bi se ovakve operacije mogle adekvatno pratiti. Dodatnu prednost operacijama utjecaja u kiber prostoru dale su tehnologije umjetne inteligencije koje na društvenim mrežama nadziru i (pre)oblikuju uvjerenja, načela i vrijednosti ciljanih publika. U nereguliranom kiber prostoru društvene mreže postale su snažan i učinkovit medijski kanal za upravljanje, preoblikovanje i daljnje prenošenje i prezentiranje informacija u skladu s napadačevim potrebama. Zajednička poveznica kiber prostora i društvenih mreža u operacijama utjecaja je u mogućnostima njihove zloupotrebe. Planerima operacija utjecaja društvene mreže omogućile su učinkovitije iskorištavanje glavnih prednosti koje nudi kiber prostor a to su asimetričnost, neposrednost i anonimnost.

Vlasnici društvenih mreža omogućili su zloupotrebu osnovnih čimbenika koji određuju poslovanje društvenih mreža:

---

372 Usp. Brangetto i Veendendaal, 2016.; prema; Ben Quinn, ‘Revealed: the MoD’s secret cyberwarfare programme’, The Guardian, 16 March 2014, http:// www.theguardian.com/uk-news/2014/mar/16/mod-secret-cyberwarfare-programme.

373 Ibid., prema; Joseph Nye, ‘Soft Power, the means to succeed in world politics’, Public Affairs 2004, p. x.

- Osobnih i grupnih uvjerenja, načela i vrijednosti, koji su kao „roba koja ima tržišnu vrijednost“ u posjedu vlasnika društvenih mreža;
- Izvršene podjele; prema uvjerenjima, načelima i vrijednostima;
- Lažnih računa koji mogu biti pojedinačni i/ili grupni;
- Hibridne inteligencije;
- Tehnologija umjetne inteligencije koje povećavanju domet, ubrzavaju i usmjeravaju dezinformacije prema ciljanim publikama;

Iz ovih osnovnih razloga zloupotrebe društvenih mreža proistekle su specifične mogućnosti na temelju kojih su kiber operacije utjecaja ujedno postale učinkovitije od tradicionalnih operacija utjecaja:

- U pravilu izvode ih obavještajne vojne i/ili civilne službe pomoću lažnih profila pojedinačnih i/ili grupnih koji nude dodatnu anonimnost;
- Sustav povratne sprege kroz primjenu hibridne inteligencije, uz anonimnost omogućava brzinu, prilagodljivost i automatiziranost u planiranju i izvođenju dezinformacijskih kampanja koje su prilagođene društvenim slabostima; kiber operacije utjecaja su prema ovom kriteriju dodatno prikrivene, što posljedično dodatno onemogućava pravovremeno uočavanje.
- Društvene mreže omogućavaju globalni doseg ciljanih publika; njihova umreženost na osnovi grupiranih podataka pretvorila ih je u jednoobrazni objekt napada, time su postale izloženije i jednostavnije mete unaprijed isplaniranih ciljeva, što predstavlja ključnu stratešku prednost;
- Nude ekonomičnost; usluge su „besplatne“ i dostupne svima, omogućavaju neposredan doseg ciljanim publikama pojedinačno i/ili grupno u realnom vremenu;
- Nude učinkovitiju (de)mobilizaciju ciljanih publika za potrebe napadača. Izgradnja povjerenja i isticanje prijetnji dio su kontinuirane strategije mobiliziranja pristaša ili demobiliziranja ciljanih publika. Međutim, novost je da su društvene mreže proces (de)mobilizacije učinile anonimnim a sam proces su pospješile, automatizirale i optimizirale prema potrebama napadača.
- Nude poticanje radikalizma, ekstremizma i terorizma, ovisno o potrebama.

Kiber prostor i društvene mreže nude brojne nove mogućnosti za planiranje i izvođenje operacija utjecaja, bez obzira primjenjuju li se u ratu ili miru. Brangetto i Veendendaal iz NATO Cooperative Cyber Defense u svom radu uvode termin kiber operacije utjecaja kojim opisuju primarno tehničke aspekte napadnog djelovanja kroz kiber prostor. Drugi termin koji uvode su

Operacije informiranja i utjecaja (engl. Inform & Influence Operations) koje obuhvaćaju aktivnosti u cilju informiranja, utjecaja ili uvjeravanja ciljanih publika kroz radnje, govorne iskaze, signale ili poruke'.[374] Na sličan način Cordey iz Centra za sigurnosne studije[375] operacije utjecaja u kiber prostoru dijeli prema dvije osnovne kategorije ciljeva koji se mogu postići iskorištavanjem društvenih mreža: na kiber operacije tehnološkog utjecaja (engl. cyber-enabled technical influence operations) i kiber operacije društvenog utjecaja (engl. cyber-enabled social influence operations). U kiber operacijama tehnološkog utjecaja primarna svrha društvenih mreža je stvaranje posrednih informacijsko-psiholoških pritisaka pomoću tehnoloških napada na kritične infrastrukture. Ovom vrstom kiber napada nastoji se postići dva cilja. Jedan je izazvati tehnološke poremećaje ili prekid funkcionalnosti primarno informacijsko-komunikacijskih i gospodarsko-energetskih kritičnih infrastruktura. Drugi je iz kritičnih infrastruktura prikupiti štićene podatke i informacije.[376] U kontekstu ove vrste napada predmet napada su sustavi za dostavu informacija, poslužitelji podataka i mrežni čvorovi. U svom opisu mogu biti dio napadačkog ili obrambenog elektroničkog ratovanja (koje nije predmet istraživanja). Ova vrsta kiber operacija u kontekstu stvaranja psiholoških pritisaka je sekundarna. Međutim, služe kao priprema i potpora izvođenju složenijih napada dezinformacijskih kampanja koje se izvode kiber operacijama društvenog utjecaja odnosno operacijama informiranja i utjecaja, koje su u biti jedno te isto. U ovoj vrsti operacija primarna zadaća društvenih mreža je stvaranje neposrednih informacijsko-psiholoških pritisaka, u koju svrhu se dezinformacije i druge vrste prijetnji koje se stvaraju u kiber prostoru prilagođavaju društvenim slabostima koje su utvrđene na osnovi prikupljenih uvjerenja, načela i vrijednosti ciljanih publika. Društvene mreže služe za stvaranje i za (pre)usmjeravanje pažnje ciljanih publika na dezinformacije pomoću kojih se kratkoročno ili dugoročno nastoji (pre)oblikovati temeljna uvjerenja, vrijednosti i načela prema potrebama napadača.

Donedavno su se kiber napadi uglavnom promatrali u kontekstu funkcionalnog oštećenja vojnih ili civilnih kritičnih infrastruktura. Ovakvi napadi neupitno predstavljaju napade na nacionalnu sigurnost i ekonomsku otpornost ciljanih publika. Međutim, posljednjih godina svjedočimo

374 Brangetto i Veendendaal, 2016., str. 116.

375 Cordey, 2019., str. 16.

376 To su u prvom redu štićeni podaci i informacije i drugi podaci koji su dobiveni krađom podataka iz e-pošti; elektroničkih korespondencija; krivotvorenjem podataka protokola; ubacivanjem zlonamjernog programa u zaštićene informacijske sustave kritičnih infrastruktura; uklanjanje web stranica; uništavanje mrežnih usluga i važnih računalnih mreža.

porastu kiber napada kojima je primarni cilj dezinformacijama ometati političke i društvene procese u drugim državama. Kiber operacijama utjecaja podjednako se napada cjelokupno protivničko okruženje – njegova fizička infrastruktura, materijalna imovina (poput znanja ili tajni) i njegova nematerijalna imovina (poput ugleda ili povjerenja). Cilj više nije toliko u nanošenju funkcionalnog oštećenja kritičnih infrastruktura, već u ostvarivanja informacijske nadmoći nad korpusom javnog znanja ciljanih publika.

Glavni argumenti ove paradigmatske promjene leže u kiber prostoru i činjenici da su tehnologije koje se na društvenim mrežama koriste za (pre)oblikovanje uvjerenja, načela i vrijednosti unijele ključnu konceptualnu paradigmu u planiranju i izvođenju operacija utjecaja u kiber prostoru: napadaču su omogućile neposredan fizički i kognitivni utjecaj na ciljane publike u realnom vremenu. Omogućile su objedinjavanje vremenske i prostorne dimenzije djelovanja. S aspekta uzročnih veza koje nastaju u kiber prostoru posljedice se u fizičkom prostoru odvijaju u realnom vremenu. Kiber prostor i fizički prostor postali su neodvojivi u planiranju i izvođenju napadačkih informacijskih operacija (psiholoških operacija). Kroz vremensku i prostornu dimenziju djelovanja ove nove vrste operacija informiranja i utjecaja (kako ih nazivaju Brangetto i Veendendaal) odnosno društvenog utjecaja (kako ih naziva Cordey) integrirale su fizičku, kognitivnu i informacijsku domenu kiber prostora. Dezinformacija je dobila dodatnu moć utjecaja. Zbog ove činjenice dezinformacije i društvene mreže koriste se za vođenje operacija utjecaja koje imaju svrhu stvarati učinkovitije informacijsko-psihološke pritiske bez obzira radi li se o ratu ili miru.

Boljoj učinkovitosti operacija utjecaja pridonijela je izvršena podjela znanja na društvenim mrežama koje je grupirano prema uvjerenjima, vrijednostima i načelima ciljanih publika. Produbljivanje podjela jedan je od osnovnih ciljeva u planiranju i izvođenju vojnih psiholoških operacija i vojne obmane.[377] Tehnologije umjetne inteligencije koje koriste društvene mreže donijele su nove mogućnosti prikupljanja podataka i informacija iz ciljeva psiholoških operacija te su, shodno tome, znatno utjecale na novi način u njihovom osmišljavanju, planiranju i provođenju.[378] Na osnovu zajednica i grupa podijeljenih prema različitim načelima i vrijednostima kojima je ograničena mogućnost pristupa alternativnim informacijama

377 Iskorištavanje Facebooka za potrebe planiranja i izvođenja vojnih psiholoških operacija i vojne obmane u istraživanju se promatra kroz primjer intervencije SAD-a protiv ISIL-a tijekom rata u Siriji i kroz primjer ruske intervencije protiv Ukrajine na Krimu. Ovi primjeri su ujedno primjeri kiber operacija u hibridnom ratu.

378 Akrap, 2019., str. 69.

jednostavnije je produbljivati postojeće društvene i političke podjele između različitih društvenih zajednica te je po toj osnovi jednostavnije ciljano destabilizirati društvene, političke ili sigurnosne procesa koji, ukoliko je to nekome u interesu, mogu eskalirati u nasilni i oružani sukob.

Prednosti u odnosu na tradicionalne operacije utjecaja su u dodatnoj anonimnosti i u tome što su ciljane publike u realnom vremenu u većoj ili manjoj mjeri nesvjesno povezane s inicijatorom podjela. Kiber operacije utjecaja zato često ostaju neotkrivene te ih je teže dokazati. U pravilu planiraju ih i provode obavještajne strukture i jedinice za specijalizirano planiranje i izvođenje psiholoških operacija. „Za razliku od stvarnog svijeta, u kojemu postoje pravila ratovanja i međunarodno prihvaćene institucije koje te procese na neki način mogu kontrolirati i penalizirati, napadačko djelovanje u kiber prostoru nije ograničeno. U njemu ne postoje međunarodno prihvaćene norme ponašanja ni pravila sukobljavanja i ratovanja, a još manje međunarodno priznate i prihvaćene institucije koje bi takva pravila pratile i po potrebi sankcionirale njihovo kršenje.“[379] Njihovoj neprimjetnosti pogoduju „tvorničke postavke“ društvenih mreža koje su omogućile korištenje lažnih profila koji dodatno omogućavaju zamagljivanje skrivenih namjera, taktika i ciljeva. Naročito ih je teško uočiti kad se provode na strateškoj razini tj. kada su usmjerene na populaciju i političko vodstvo. Jedna od najočitijih prednosti u odnosu na tradicionalne operacije jest mogućnost zagušivanja protivničkog korpusa javnog znanja automatiziranom i masovnom diseminacijom anonimnih dezinformacija koje su uz to prilagođene društvenim slabostima ciljanih publika. Ova činjenica dodatno otežava pravovremeno uočavanje, kontroliranje i penaliziranje te nudi određeni stupanj poricanja, čak i tamo gdje je izvor napada bio manje ili više utvrđen.[380] Neprimjetnosti dodatno doprinosi činjenica da korisnici društvenih mreža dezinformacije u pravilu obrađuju nekritički ili ih nesvjesno šire, čime dodatno otežavaju praćenje tragova autora dezinformacija, podložniji su manipulacijama i potencijalno čine štetu za svoju okolinu. Ove mogućnosti koje nudi kiber prostor i društvene mreže unijele su dramatičnu novost u planiranju, izvođenju i ostvarivanju planiranih ishoda.

Moć utjecaja proizlazi iz samog kiber prostora ali i načina na koji su osmišljene društvene mreže i postavke umjetne inteligencije i algoritama koji procesuiraju podatke i informacije. Primjena

379 Akrap, 2019.

380 Brangetto i Veenendaal, 2016.

umjetne inteligencije na društvenim mrežama dodatno je sinkronizirala nelinearnost kiber prostora i kognitivne elemente informacijskog ratovanja, načine razmišljanja i donošenja odluka. Temeljem činjenice da se na društvenim mrežama prikuplja i preoblikuje podatke, pomoću društvenih mreža postalo je moguće iskorištavati društvene slabosti na nove načine, ovisno o okolnostima i potrebama napadača. Moguće ih je koristiti za planiranje i stvaranje dezinformacija koje je sad moguće prilagoditi taktičkim i strateškim ciljevima. Operacije utjecaja u kiber prostoru predstavljaju novu subverzivnu metodu napadačkog djelovanja i s pomoću njih se mogu učinkovito destabilizirati društveni, politički i sigurnosni procesi u drugim državama. Ovaj dio istraživanja bitan je iz razloga što će se u daljnjim dijelovima istraživanja potvrditi ili odbaciti hipoteza te će se odgovoriti na prvo i drugo postavljeno istraživačko pitanje.

„Na vojnim se sveučilištima SAD-a posebna pozornosti poklanja odnosu doktrine informacijskih operacija te medijskih operacija i operacija odnosa s javnošću.“[381] „Naime, globalne komunikacijske mreže imaju za posljedicu da se ne može vlastitoj javnosti plasirati jedna priča, a stranim (protivničkim i/ili neprijateljskim) javnostima druga.“[382] „Istovremeno, sustav nacionalne sigurnosti ne smije se ni u jednom svom segmentu (barem u demokratskim zemljama i po demokratskim pravilima ponašanja) rabiti za dezinformiranje i obmanjivanje vlastite javnosti. Zato su medijske operacije i operacije s odnosima s javnošću vrlo osjetljive. Posebna se pažnja u tim odnosima posvećuje relacijama između civilnog i vojnog sektora. Salomonsko je rješenje pronađeno tako što se u američkoj teoriji, a za javnost, razdvajaju medijske od informacijskih operacija. Pojednostavljeno rečeno: medijske operacije imaju za cilj osigurati komunikacijske kanale za plasiranje informacija. Medijske operacije su manje-više javne i ostvaruju se posredstvom vladinih, nevladinih i privatnih organizacija.“[383] Informacijske operacije što ih provodi javna diplomacija, kako je prethodno spomenuto, u svojem operativnom, izvedbenom dijelu, nisu javne.

3.3. Informacijske operacije

Informacijske operacije u sklopu provođenja operacija utjecaja imaju bitnu i temeljnu ulogu s ciljem promjene organizacije znanja u javnom informacijskom prostoru kako bi se osigurala informacijska nadmoć. U svojoj biti informacijske operacije usmjerene su na to kako ljudi misle

381 Tuđman, 2011.; prema Gary S. Patton.

382 Tuđman, 2011., str. 33.

383 Ibid.

ili, još preciznije, kako donose odluke.[384] Pojavom kiber prostora ostvaren je paradigmatski pomak u planiranju i izvođenju informacijskih operacija. Pojavom društvenih mreža dodatno je osnažena ova uloga kiber prostora.

Koliko god informacijske operacije bile tajne, doktrina informacijskog ratovanja postala je javna, kao i činjenica da je neskriveni cilj informacijskih operacija usmjeren „protiv bilo kojeg dijela znanja i vjerovanja protivnika".[385] Cilj je informacijskih operacija globalan: utjecati na javnost protivnika tako da prisili svoje vođe na odluke na vlastitu štetu.

Dezinformacije zato više nisu usmjerene na uski krug ljudi koji donose odluku, nego na javno znanje ciljane publike da bi javnost odbila prihvatiti odluke svojih vođa kad su te odluke u suprotnosti s interesima dezinformatora. Mediji odnosno globalni informacijski prostor postao je tako bojišnicom na kojoj se sukobljavaju ne samo domaći protivnici, nego djeluju i međunarodni čimbenici da bi oblikovanjem medijskih poruka i kontrolom domaćeg javnoga znanja „lokalnoj" javnosti nametnuli svoje ciljeve.[386] Plasiranje dezinformacija u protivnički informacijski prostor prethodno se izvodilo specijalnim operacijama[387] primarno za vojne potrebe kroz prikrivene ili tajne operacije. Danas se informacijske i specijalne operacije izvode pomoću društvenih mreža kroz kiber prostor na svim mogućim razinama djelovanja: lokalnoj i/ili globalnoj razini, pojedinačno i/ili grupno, neovisno radi li se o ratu ili miru. Između informacijskih operacija i specijalnih operacija nema bitnih razlika u pogledu metoda i tehnika djelovanja. Razlika je u strategijama i ciljevima. Cilj je informacijskih operacija globalni: utjecati na promjenu sadržaja i organizaciju znanja u informacijskom prostoru protivnika. „Cilj je specijalnih operacija partikularni: plasirati dezinformaciju da bi se trenutačno zavarao protivnik. Razlika je i u strategiji nastupa."[388] Specijalne operacije provode se kao tajne ili prikrivene operacije, u pravilu ih vode obavještajne strukture s prikrivenim političkim ciljevima svojih vlada, dok informacijske operacije sve češće djeluju na otvoren način. „Provode se kroz medijske operacije, odnose s javnošću, javnu diplomaciju te one nisu u isključivoj nadležnosti vojnih i sigurnosno-izvještajnih službi i struktura. Informacijskim operacijama se sve više i sve

384 Usp. Tuđman, 2008., str. 137.

385 Tuđman, 2013., str. 58.; prema Szafranski, 1995.

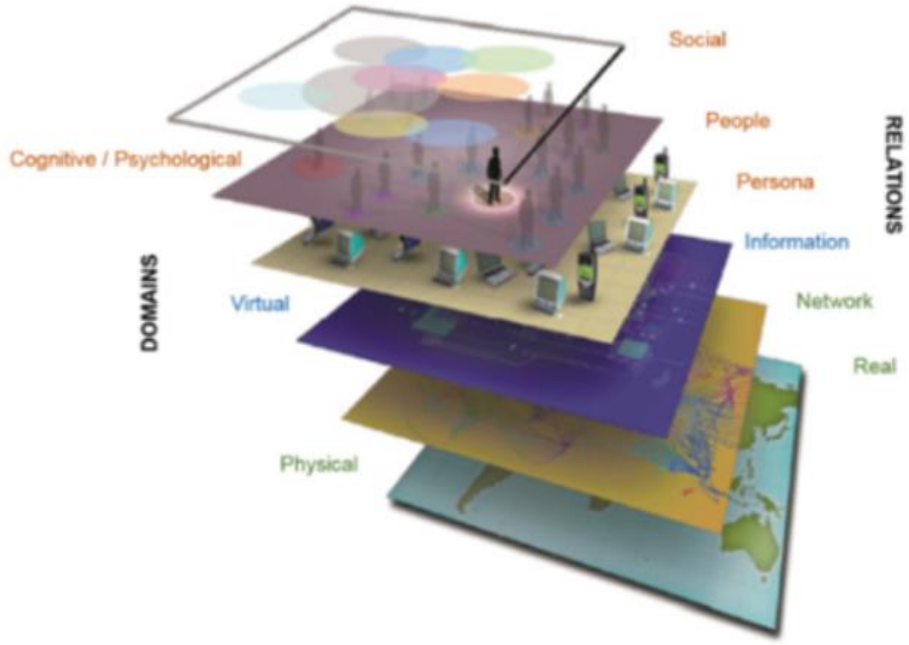
386 Tuđman, 2013., str. 58.

387 Tuđman, 2008., str. 136. Autor navodi da su u uporabi različiti nazivi specijalnih operacija: psihološki rat, propaganda, politički rat, agitacija, ideološko ratovanje, ideološka agresija, ideološka diverzija, indoktrinacija, ispiranje mozga, širenje glasina, subverzija, diverzija itd.

388 Ibid.

učinkovitije, za postizanje vlastitih ciljeva, bave i civilne strukture, vladine i nevladine organizacije, tvrtke, institucije i udruge.“[389] Visokotehnološke korporacije koje upravljaju i razvijaju društvene mreže poput Facebooka ogledni su primjer alata koje navedeni akteri koriste za vlastite ciljeve i interese. Zahvaljujući umjetnoj inteligenciji koja se koristi na društvenim mrežama, informacijske operacije je moguće učinkovito provoditi u svim postojećim dimenzijama: prostor, vrijeme, virtualnost.

Prema NATO-u i Ministarstvu obrane SAD-a, informacijske operacije definiraju se kao „integrirano korištenje, tijekom vojnih operacija, sposobnosti povezanih s informacijama u skladu s drugim linijama djelovanja kako bi se utjecalo, ometalo, korumpiralo ili uzurpiralo donošenje odluka protivnika i potencijalnih protivnika, istovremeno štiteći naše vlastite.“[390]



Izvor: Kiesler Jack, A Next Generation National Information Operations Strategy and Architecture, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2021.

Slika 18. Okruženje informacijskih operacija.

389 Akrap, 2011., str. 42.

390 Joint Chief of Staff. Joint Publication 3-13. Information operations. [online] 2014 [cit. 2019-04-30]. Dostupno na https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf. Vidi također: US Department of Defense, Directive 3600.01., 2013., str. 12.

Slika 18. pokazuje okruženje informacijskih operacija koje obuhvaća i agregira brojne društvene, kulturne, kognitivne, tehničke i fizičke atribute koji djeluju i utječu na znanje, razumijevanje, uvjerenja, svjetonazore i, u konačnici, djelovanje pojedinca, grupe, sustava, društva, zajednice ili organizacije. Informacijsko okruženje kroz fizičku domenu stvarnog svijeta, informacijsku (virtualnu) i kognitivnu/psihološku domenu kiber prostora, izravno utječe i nadilazi sva radna okruženja unutar kojih postoje odnosi i procesi gdje se (kroz stvarni svijet, mreže tj. infrastrukturu, informacije koje se u njima stvaraju, kroz osobe, zajednice i društvo) odvijaju informacijske operacije.[391] Kiber prostor koji objedinjuje domene informacijskog okruženja i odnose svih navedenih čimbenika i atributa stoga je postao okruženje u kojem se dominantno planiraju i izvode informacijske operacije.

Informacijske operacije predstavljaju napadačke i obrambene mjere usmjerene na stvaranje učinkovitog utjecaja na odluke protivnika, manipuliranje informacijama i informacijskim sustavima. One također uključuju mjere koje štite procese donošenja odluka u zemlji, informacije i informacijske sustave. Informacijske operacije mogu utjecati na sve tri domene informacijskog okruženja odnosno kiber prostora. Fizička domena pokriva ljudska bića, ali i zapovjedne i kontrolne objekte i informacijsko-komunikacijske sustave. Ono što je važno jest da fizička domena zahvaljujući društvenim mrežama nije povezana samo s vojnim ili nacionalnim sustavima i procesima. U fizičkoj i virtualnoj domeni utječe se na sadržaj i protok informacija. Posljednje je, ali ne i najmanje važno, djelovanje informacijskih operacija u kognitivno psihološkoj domeni informacijskog okruženja. U njoj informacijske operacije utječu na umove onih koji prenose, primaju, reagiraju na informacije ili djeluju na njih. Kognitivna dimenzija obuhvaća pojedince i zajednice, njihova individualna i kulturna uvjerenja, norme, ranjivosti, motivacije, emocije, iskustva, obrazovanje, mentalno zdravlje, identitete i ideologije. Na ovaj način ostvaruju potencijal u utjecanju na načine na koje se informacije prikupljaju, obrađuju, pohranjuju, šire i štite te time mogu utjecati na sustave zapovijedanja i kontrole, na ključne donositelje odluka i prateću infrastrukturu.[392]

Informacijske operacije „definiraju se kao skup mjera, radnji i djelovanja poduzetih prema protivničkom informacijama, informacijsko-komunikacijskim sustavima, osobama i kognitivnim procesima s ciljem uništavanja, onemogućavanja i usporavanja njihovog

391 Usp. Joint Concepts - Operating in the Information Environment.Pdf

392 Usp. Joint Chief of Staff, Joint Publication 3-13, Information operations, 2014 (30.04.2019.). Dostupno na : https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

djelovanja ili pak preuzimanja nadzora nad njihovim djelovanjem, uz istovremeno osiguravanje primjene razine zaštite vlastitih informacija, kognitivnih procesa, informacijsko-komunikacijskih sustava i osoba.“[393] „Informacije utjecaja stoga imaju za cilj djelovati na "kognitivnu domenu" tj. na shvaćanje i ponašanje lidera, grupa i cijelih populacija kako bi oni, protivnici, promijenili svoje odluke.“[394]

„Informacijskim operacijama želi se utjecati na dva ključna dijela društva, odnosno pojedine zajednice:“[395]

- „Na donositelje ključnih političkih, gospodarskih i drugih odluka kako bi ih se nagnalo na donošenje odluka na vlastitu štetu“;
- „Na pripadajuće javno mnijenje kako bi se isto potaknulo da svojim djelovanjem otežа poziciju vladajuće/upravljačke strukture, onemogući njihovo racionalno djelovanje te potakne masu na traženje promjena u zajednici, društvu, državi, ako treba i primjenom nasilnih sredstava i metoda.“

Dobro razumijevanje odnosa između domena kiber prostora i relacija u informacijskom okruženju između ciljanih publika ključno je za učinkovito planiranje i izvođenje informacijskih operacija kako bi se na najbolji način stekla informacijska nadmoć nad njihovim korpusom javnog znanja. Informacijske operacije nisu samo skup pojedinačnih informacijskih aktivnosti. One su ujedno procesi kojima se integriraju učinci pojedinačnih informacijskih aktivnosti koji zajedno dovode do učinkovitog utjecaja. Tako informacijske operacije integriraju psihološke operacije, sigurnost operacija, informacijsku sigurnost, obmanu, elektroničko ratovanje, kinetičke akcije, angažman ključnih vođa i operacije računalnih mreža. Svi zajedno ciljaju na volju ciljanih publika za borbu, njihovo razumijevanje situacije i njihove sposobnosti. Informacijske operacije usmjerene su na stvaranje utjecaja na protivnika, uglavnom na donositelje odluka koji imaju sposobnost utjecati na određene situacije. Aktivnosti u ovom slučaju uključuju propitivanje legitimiteta političkih vođa, podrivanje morala stanovništva ili vojske, polariziranje društva i tako dalje. Informacijske aktivnosti koje utječu na razumijevanje situacije nastoje utjecati na informacije koje su dostupne ciljanim publikama kako bi se u korist napadača utjecalo na trenutne i dugoročne promjene u njihovim uvjerenjima,

393 Akrap, 2011., str. 42.

394 Tuđman, 2009., str. 25.-45.

395 Akrap, 2011., str. 41.

načelima i vrijednostima. To uključuje širenje dezinformacija, zavaravanje neprijateljskih radarskih sustava, namjerno curenje iskrivljenih informacija, uništavanje ili manipulaciju informacijama u informacijskim sustavima protivnika, itd. Treća vrsta informacijskih aktivnosti je djelovanje na sposobnosti ciljanih publika, pokušaji da se poremeti njihova sposobnost razumijevanja informacija i promicanje volje napadača. To uključuje niz pomno planiranih aktivnosti u rasponu od prekidanja internetskih veza, fizičkog uništavanja infrastrukture, kiber napada i slično.

Informacijske operacije ponekad se pogrešno nazivaju strateškom komunikacijom. Iako se ova dva pojma mogu činiti vrlo sličnima, među njima postoje bitne razlike. Strateška komunikacija pokreće se s političke, strateške razine; njen doseg su i globalne publike i djeluje samo u kognitivnoj dimenziji informacijskog prostora. Nasuprot tome, informacijskim operacijama upravlja se s operativne, vojne razine, imaju dobro definiran opseg djelovanja i publike i djeluju u sve tri dimenzije informacijskog okruženja.[396] Strateško komuniciranje je širi pojam kojemu su podređene informacijske operacije i ono se na strateškoj razini provodi izvan konteksta vojnog djelovanja. S druge strane, informacijske operacije koncentriraju informacijsko-tehnološke i informacijsko-psihološke aktivnosti tijekom vojnih operacija. I u jednom i u drugom evidentno je da postoje elementi koji se odnose na psihološke operacije i na ciljeve koji se ovom vrstom operacija nastoje postići.

3.4. Psihološke operacije

Kao što je spomenuto, psihološke operacije definiraju se kao jedna od aktivnosti koja pripada informacijskim operacijama. Allied Joint Doctrine AJP 3-10.1 iz 2014. psihološke operacije opisuje kao „planirane aktivnosti u kojima se korištenjem metoda komunikacije i drugih sredstava usmjerenih na ciljanu publiku nastoji utjecati na percepciju, stavove i ponašanje i postizanje političkih i vojnih ciljeva.“[397]

„Psihološke operacije su glavna informacijska sastavnica napadnih informacijskih operacija, a podrazumijevaju skup planiranih djelovanja, u cijelom vremenskom spektru događanja, prema

396 Vejvodová Petra, Information and Psychological Operations as a Challenge to Security and Defence, Vojenské rozhledy, 2019., str. 85., dostupno na: 10.3849/2336-2995.28.2019.03.083-096; prema; DIVIŠOVÁ, Vendula, Strategická komunikace v protipovstaleckých operacích NATO, Obrana a strategie, str. 105-118.

397 NATO Standardization Office, Allied Joint Doctrine for Psychological Operations AJP 3-10., Brussels, 2014, (30.04.2019), dostupno na:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

ciljanim publikama na određenom području s ciljem stjecanja informacijske nadmoći, odnosno oblikovanja informacijskog prostora (nadzorom nad informacijama, informacijskim sustavima, kognitivnim procesima)“[398] u korist napadača. Psihološke operacije promatramo kroz združene oblike civilne i vojne suradnje, kao dio napadačkih informacijskih operacija i oblika djelovanja u okviru strateškog utjecaja nacionalnih informacijskih strategija prema određenim ciljevima.[399] „Psihološkim operacijama pokušava se utjecati na emocije, percepciju, volju, odluke i ponašanje ciljane zajednice, grupe i/ili pojedinca, na oblikovanje njihovog znanja, na njihove postupke i djelovanje.“[400] „Psihološkim operacijama ciljanim publikama nastoji se onemogućiti racionalno razmišljanje i uvjeriti ih da je sustav „napadača“ odnosno planera informacijskih operacija (iza kojih se krije „naručitelj“), ispravan i poželjan.“[401] Dakle, unaprijed planiranim aktivnostima korištenjem informacijsko-komunikacijske tehnologije, komunikacijskih metoda usmjeravaju se prema ciljanim publikama kako bi se izazvali poželjni odgovori, što u širem kontekstu doprinosi ispunjavanju specifičnih političkih i/ili vojnih ciljeva. Svaka psihološka operacija temelji se na određenoj temi (glavnoj, pažljivo pripremljenoj pripovijesti ili idejama) s ciljem izazivanja psiholoških posljedica na njihovo razumijevanje i, shodno tome, donošenju odluka u korist onog tko ih provodi. Što je veća osjetljivost ciljane publike na specifične alate kojima se izvode psihološke operacije, to je veća vjerojatnost uspjeha cijele psihološke operacije.[402]

Društvene mreže i mogućnosti primjene hibridne inteligencije za prikupljanje, pohranu i (pre)oblikovanje uvjerenja, načela i vrijednosti u dezinformacije unijele su paradigmatski pomak u planiranju i izvođenju psiholoških, specijalnih i medijskih operacija iz dva bitna razloga. Vrše prijem i obradu obavijesti u stvarnom vremenu, ujedno su mjesto prikupljanja osobnih ili grupnih uvjerenja, načela i vrijednosti, njihove obrade i alat kojim se u realnom

---

398 Akrap, 2011., str. 52.

399 Druga dva oblika djelovanja kroz koja se vrši strateški utjecaj nacionalnih informacijskih strategija su javna diplomacija i odnosi s javnošću. Međutim, oni nisu predmet dubljeg istraživanja. Javnu diplomaciju i odnose s javnošću prethodno smo definirali radi boljeg razumijevanja psiholoških operacija kao posebnog oblika djelovanja koje provode posebne, civilne i vojne ustanove i institucije, bez primjene kinetičke sile kao krajnjeg sredstva utjecaja.

400 Akrap, 2011., str. 52.

401 Ibid.

402 NATO Standardization Office, Allied Joint Doctrine for Psychological Operations AJP 3-10.1., 2014 (30.04.2019). Dostupno na:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

vremenu mogu stvarati dezinformacije koje se ujedno na učinkovit i anoniman način mogu širiti u protivnički korpus javnog znanja. Društvene mreže time su u kiber prostoru postale izuzetno snažan i po ostvarivanju ciljeva moćan alat za planiranje i izvođenje psiholoških operacija i za ostvarivanje željenih psiholoških učinaka. Na lokalnoj, regionalnoj ili globalnoj razini omogućavaju masovnu diseminaciju širokog spektra audio, video i foto (dez)informacijskih sadržaja kojima napadač može učinkovitije uobličavati emocije, percepciju i volju ciljanih publika kako bi, kratkoročno ili dugoročno, utjecao na promjenu u njihovim stavovima, mišljenju i donošenju odluka za vlastitu korist. Zbog načina na koji su osmišljene društvene mreže podjelom na grupna uvjerenja, vrijednosti i načela, ciljane publike na društvenim mrežama postale su lakša meta psiholoških operacija. Na temelju toga uspjesi u vođenju informacijskih operacija u marketinškim kampanjama podjednako se ostvaruju i u psihološkim operacijama koje izvode državni i nedržavni akteri za skrivene političke interese, bez obzira na stanje rata ili mira. Ovaj dio istraživanja bitan je jer će se na osnovu njega u daljnjem dijelu istraživanja potvrditi ili odbaciti hipoteza i odgovoriti na prvo i drugo istraživačko pitanje.

Važnost psiholoških operacija temelji se na uvjerenju da je psihološka priroda sukoba jednako važna kao i fizička. Stavovi i ponašanje ljudi utječu na tijek i ishod sukoba te na prirodu okruženja u kojem se sukob odvija. Za dobro provedenu psihološku operaciju važno je poznavati ciljanu publiku, njezinu volju i motivaciju. „U metodologiji planiranja i izvođenja psiholoških operacija raščlanjuju se prikupljene obavijesti kako bi se identificirale utjecajne osobe, utjecajne grupe i zajednice, pojedinci i grupe koje bi u doglednoj vremenskoj perspektivi mogle postati utjecajne ili koje bi mogle najbolje ispuniti postavljene ciljeve i zadaće njihovih planera.“[403] Tehnologije umjetne inteligencije koje koriste društvene mreže i mogućnost primjene hibridne inteligencije unijeli su značajne promjene u metodologiji planiranja i izvođenja psiholoških operacija. Društvene mreže postale su idealan alat za prikupljanje potrebnih podataka, obavijesti i informacija. Tehnologije umjetne inteligencije nude njihovu sveobuhvatnu obradu i davanje rješenja za djelotvornije psihološke (kognitivne) učinke. Planeri psiholoških operacija u njihovom izvođenju rade upravo sa spomenutim elementima i imaju za cilj utjecati na njih, slabiti protivnikovu volju jačajući opredijeljenost ciljane publike i dobivajući podršku i suradnju neodlučnih ciljanih publika. Iz logike danih definicija, psihološkim operacijama pomaže se ostvarivanju ciljeva informacijskih operacija na informacijsko-psihološkoj razini. Ciljajući na kognitivnu dimenziju informacijskog prostora,

403 Akrap, 2011., str. 72.

psihološkim operacijama utječe se na percepciju, stavove i ponašanje ciljane publike, što bi posljedično trebalo dovesti do učinka i na donositelje odluka.

Dakle, psihološke operacije su potkategorija informacijskih operacija, koordinirane kroz procese informacijskih operacija. Zajednička doktrina NATO saveza AJP 3-10.1 za psihološke operacije navodi da se one provode u cijelom spektru vojnih operacija.[404] Međutim, problem u sagledavanju njihovih učinaka predstavlja nedoumica oko neupitne činjenice da su društvene mreže postale alati pomoću kojih se planiranje i provođenje ovakvih operacija može učinkovito izvoditi i u razdobljima mira i kriza tj. izvan konteksta vojnih operacija.

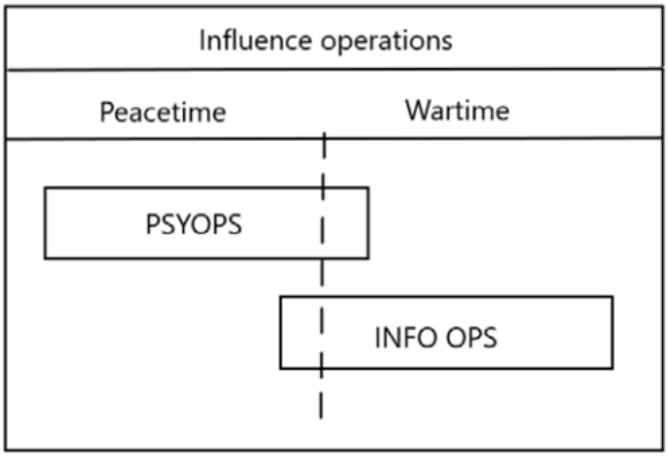
3.5. Psihološke operacije i strateško komuniciranje u razdobljima mira

Prethodno spomenute razlike između strateške komunikacije i informacijskih operacija (utjecaja) odnosno psiholoških operacija kao njihove napadačke odrednice potrebno je dodatno pojasniti radi konteksta istraživanja planiranja i izvođenja psiholoških operacija s pomoću društvenih mreža izvan spektra vojnih operacija, oružanog sukoba ili rata. Bitna kontradikcija između strateškog komuniciranja i psiholoških operacija je što i strateško komuniciranje podrazumijeva informacijsko-psihološke aktivnosti, ali izvan konteksta vojnog djelovanja a često se shvaćaju kao psihološke operacije, što one u svojoj osnovi i jesu. Cordey u svojoj komparativnoj analizi između tradicionalnih operacija utjecaja i kiber operacija utjecaja uzima definiciju Schmidt-Felzmanna koji operacije utjecaja definira kao koordiniranu, integriranu i sinkroniziranu primjenu nacionalnih diplomatskih, informativnih, vojnih, ekonomskih i drugih sposobnosti u mirnodopsko vrijeme, u vrijeme kriza, sukoba i post konflikta s ciljem utjecaja na odluke, percepcije i ponašanje političkih lidera, stanovništva ili određenih ciljanih skupina (poput stručnjaka, vojnog osoblja ili medija) i postizanja ciljeva sigurnosne politike državnog aktera. Prema Uredu za standardizaciju NATO saveza, psihološke operacije vezuju se isključivo za vojni kontekst djelovanja tijekom oružanog sukoba tj. rata. Međutim, nesporna je činjenica da su društvene mreže u kiber prostoru omogućile planiranje i izvođenje psiholoških operacija izvan konteksta rata primjerice za dezinformiranje, mijenjanje, kompromitiranje, uništavanje ili krađu podataka i informacija iz informacijskih sustava i mreža s ciljem stvaranja konstantnih (24/7) informacijsko-psiholoških pritisaka. Potrebu za redefiniranjem neusklađenosti između pojmova psiholoških operacija i strateškog komuniciranja u razdobljima

404 NATO Standardization Office, Allied Joint Doctrine for Psychological Operations AJP 3-10.1., 2014 (30.04.2019). Dostupno na:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

mira naglašavaju npr. Brangetto i Veenendaal koji navode da se psihološke operacije, kao i strateška komunikacija, poduzimaju i u vrijeme mira. Govore o kategoriji operacija koje opisuju kao „stratešku komunikaciju i propagandu".[405]



Izvor: Vejvodová, Petra. Information and Psychological Operations as a Challenge to Security and Defence, 2019., str. 87.

Slika 19. Prikaz neusklađenog odnosa psiholoških operacija i informacijskih operacija u razdobljima mira i rata

Slika 19. prikazuje odnos psiholoških operacija i informacijskih operacija u razdobljima mira i rata iz kojeg je vidljiva opisana neusklađenost između pojmova psiholoških operacija i informacijskih operacija koje se provode u razdobljima mira. U istraživanju Brangetta i Veenendaala 'Information and Psychological Operations as a Challenge to Security and Defence'[406] prikazanom neusklađenošću dodatno se ukazuje na terminološku nedoumicu pri miješanju strateškog komuniciranja i psiholoških operacija. Nedoumica proizlazi iz činjenice da se, u terminologiji koju koristi NATO savez, psihološke operacije zamjenjuju strateškom komunikacijom. S jedne strane, Allied Joint Doctrine AJP 3-10.1 definira psihološke operacije kao podređene strateškoj komunikaciji i ispunjavanju cilja i potpore ciljevima, politikama, operacijama i aktivnostima NATO saveza, uključujući strateški narativ. S druge strane, psihološke operacije definira istim načelima kao i strateško komuniciranje, naročito u pogledu atribucije, vjerodostojnosti, dosljednosti i istinitosti. Kaže se da se psihološke operacije moraju temeljiti na istinitim informacijama i očuvanju vjerodostojnosti Saveza, tako da se općenito

405 Brangetto i Veendendaal, 2016.

406 Ibid.

mogu pripisati NATO savezu, partnerskoj državi ili organizaciji. Strateške komunikacije i propagandne aktivnosti spadaju u ovu kategoriju, kao i namjerno širenje dezinformacija kako bi se zbunile publike.[407] Psihološke operacije svrstavaju se također u strateški narativ i cjelokupnu informacijsku strategiju.[408] Spomenuto istraživanje međutim navodi da ovakvo razumijevanje može biti problematično, odnosno da se psihološke operacije preklapaju sa strateškom komunikacijom s naglaskom na narativ. Ipak, u spomenutom istraživanju ističe se kako se za razliku od strateškog komuniciranja, psihološke operacije u teoriji mogu koristiti dezinformacije i propagandu te mogu pokušati manipulirati ciljanom publikom lažnim ili obmanjujućim informacijama. Poput propagande, psihološke operacije mogu se podijeliti na bijele, sive i crne na temelju izvora i točnosti informacija te korištenih metoda. Planeri i sponzori bijele propagande otvoreno priznaju aktivnosti. Kod sive propagande ne otkrivaju svoje izvore u potpunosti, dok kod crne propagande obmanjuju i pretvaraju se da je izvor neki drugi. U ovim terminima psihološke operacije podređene su konceptu strateške komunikacije a prema danom opisu podudaraju se osobito s bijelim psihološkim operacijama.[409] Međutim, činjenica je da psihološke operacije mogu ići daleko izvan okvira i načela strateške komunikacije i da koriste dezinformacije i obmanu. Zapadne demokracije smatraju da takve operacije treba povezivati samo s vojnim operacijama i da izvan njih, obmanu, dezinformacije i propagandu treba izbjegavati, odnosno temelje se na uvjerenju da pažljivo razvijeni narativi mogu biti učinkoviti samo ako su poruke pouzdane i dosljedne. U ovakvom pristupu također se računa da je istinita priča ona koja pobjeđuje.[410] Međutim, evidentan porast zloupotreba društvenih mreža u kiber prostoru za stvaranje dezinformacija izvan konteksta vojnog djelovanja ukazuje da ovakav pristup može biti ograničenje u izgradnji i uspostavi adekvatnih mehanizama za odvraćanje i ublažavanje potencijalnih strateških posljedica dezinformacija koje se stvaraju na društvenim mrežama za postizanje političkih ciljeva.

3.6. Medijske operacije

Posljedica je globalizacije i globalnih informacijskih procesa da je „ ...prvi put u povijesti, medijska podrška postala bitno pa čak i središnje strateško sredstvo međunarodne zajednice za iznošenje širokog spektra stavova, od političkih do socijalnih pitanja“. Ali umjesto svestrane

407 Ibid. str. 116.

408 Vejvodová, 2019.; prema NATO Standardization Office. Allied Joint Doctrine for Psychological Operations AJP 3-10.1., 2014.

409 Vejvodová, 2019., str. 88.

410 Brangetto i Veendendaal, 2016.

informiranosti, međunarodne povezanosti i proklamiranog informacijskog društva, „medijska podrška je uistinu jedan od najispolitiziranijih oblika strane pomoći“. Za tranzicijske zemlje, u kojima su međunarodni čimbenici insistirali na uspostavi „slobodnih medija“ kao mjere demokratizacije, pokazalo se da je ta maksima bila tek paravan za oblikovanje domaćih javnosti po mjeri stranih interesa: „Izravna pomoć medijima, kao i pomoć u medijskom sadržaju … bila je usmjerena na ispunjavanje postavljenih političkih i društvenih ciljeva„.[411] Mogućnosti današnjih informacijsko-komunikacijskih i računalnih tehnologija koje koriste društvene mreže omogućavaju prijenos neslućenih količina obavijesti i njihovu, gotovo trenutnu, globalnu dostupnost. Suvremeni mediji obilato koriste te nove tehnike i tehnologije. Zato imaju nemjerljivo veću mogućnost utjecaja na javnost i ciljane publike negoli ikad ranije.[412] U planiranju i provođenju informacijskih operacija ta se mogućnost svestrano koristi jer su društvene mreže najbrži put ka ciljanim publikama.

Društvene mreže ne služe više samo za prijenos obavijesti s ciljem obavještavanja dijela javnosti koja ih koristi. Kao snažan i učinkovit netradicionalan medij društvene mreže „danas nastoje snažno oblikovati javno znanje ciljanih publika, uzrokovati i voditi procese promjene tog znanja ili pak održavati njegovu trenutnost, djelovati sukladno interesima koji ih pokreću i koje im predlažu (i traže od njih) njihovi politički i/ili gospodarski sponzori.“[413] Društvene mreže kao netradicionalni učinkovit medijski kanal imaju globalnu dostupnost i mogućnost trenutačnog umrežavanja medijskih operacija i ciljanih publika. Ova ključna prednost napravila je paradigmatski pomak u mogućnostima plasiranja dezinformacija u medijski prostor javnog znanja ciljanih publika na svim ravnima: globalnoj, regionalnoj, lokalnoj, masovnoj, grupnoj i pojedinačnoj. Jednako tako, društvene mreže kao komercijalni proizvod dostupne su svima: planerima i provoditeljima informacijskih i medijskih operacija i ciljanim publikama. Planerima medijskih i informacijskih operacija nude anonimnost i trenutne učinke, pri čemu publike u većoj ili manjoj mjeri nisu svjesne njihovih ciljeva, bez obzira radi li se o skrivenim komercijalnim ili političkim ciljevima. Paradigmatski pomak napravljen je u činjenici da planeri i izvoditelji napadačkih informacijskih operacija i medijskih operacija za vlastite potrebe koriste osobne podatke korisnika društvenih mreža. Zbog planetarne dostupnosti i dosega te mogućnosti personaliziranog usmjeravanja vlastitih sadržaja tradicionalni mediji

411 Tuđman, 2013., str. 88.-89.; prema A Rodhes, 2007., str. 15 i 18.

412 Akrap, 2011., str. 87.

413 Ibid.

(tisak, tv, radio) i tvrtke oglašivači postali su snažno zavisni od algoritama, botova i drugih formi umjetne inteligencije primijenjene na društvenim mrežama. Sintagma da je za mnoge medije najbolja vijest ona koja najbolje prodaje medije, koja je marketinški privlačna a da točnost i pouzdanost padaju u drugi plan[414] na najbolji način opisuje tradicionalne medije koji društvene mreže koriste kako bi učinkovitije utjecali na „objavljivanje, oblikovanje ili pak zaustavljanje pojedinih (dez)informacija kako u gospodarske, tako i u političke svrhe (protiv vladajuće strukture koja namjerava donijeti jedan ili više zakona koji tom/tim gospodarskim i/ili političkim subjektima iz nekog razloga ne odgovaraju).“[415] „Time mjere vrijednosti i kvalitete obavijesti i informacije a objektivnost, točnost, istinitost, vjerodostojnost, korisnost u oblikovanju javnog znanja gube na važnosti i vrijednosti.“[416]

Mogućnost (pre)oblikovanja uvjerenja, načela i vrijednosti korisnika društvenih mreža za radikalizaciju i mobilizaciju ciljanih publika za skrivene političke ciljeve napose dolazi na vidjelo uz fenomen samoradikalizacije, kad osoba koja je u fizičkom svijetu introvertirana na osnovi vlastitih korisničkih preferencija i algoritama preporuka i rangiranja njezinih interesa, postane ekstrovertirana prvo u virtualnom, a potom i u stvarnom svijetu. Ova činjenica ukazuje na evidentan učinak tehnologija koje koriste društvene mreže na kognitivne procese u logičkom sloju kiber prostora, kojima je u fizičkom svijetu sad moguće prilagođavati potrebe planera informacijskih i medijskih operacija. Društvene mreže i hibridna inteligencija unijele su paradigmatsku novost u činjenici da je izvršena raščlamba korisnika društvenih mreža uz visok stupanj njihovih međusobnih interakcija planerima informacijskih i medijskih operacija omogućila učinkovitiju prilagodbu dezinformacija i na osnovu njih mobilizaciju radikalnih pojedinaca ili grupa. Ovaj dio istraživanja bitan je iz razloga što će se u daljnjem dijelu istraživanja koristiti kako bi se potvrdila hipoteza i kako bi se odgovorilo na prvo i drugo istraživačko pitanje.

Društvene mreže pridonijele su većoj učinkovitosti medijskih operacija po nekoliko osnova. Učinkovitijim mogućnostima u prikupljanju mnoštva nestrukturiranih podataka i informacija o stavovima, mišljenjima i vrijednostima koje korisnici društvenih mreža stvaraju i dijele u

414 Usp. Ibid., str. 91.

415 Usp. Ibid.

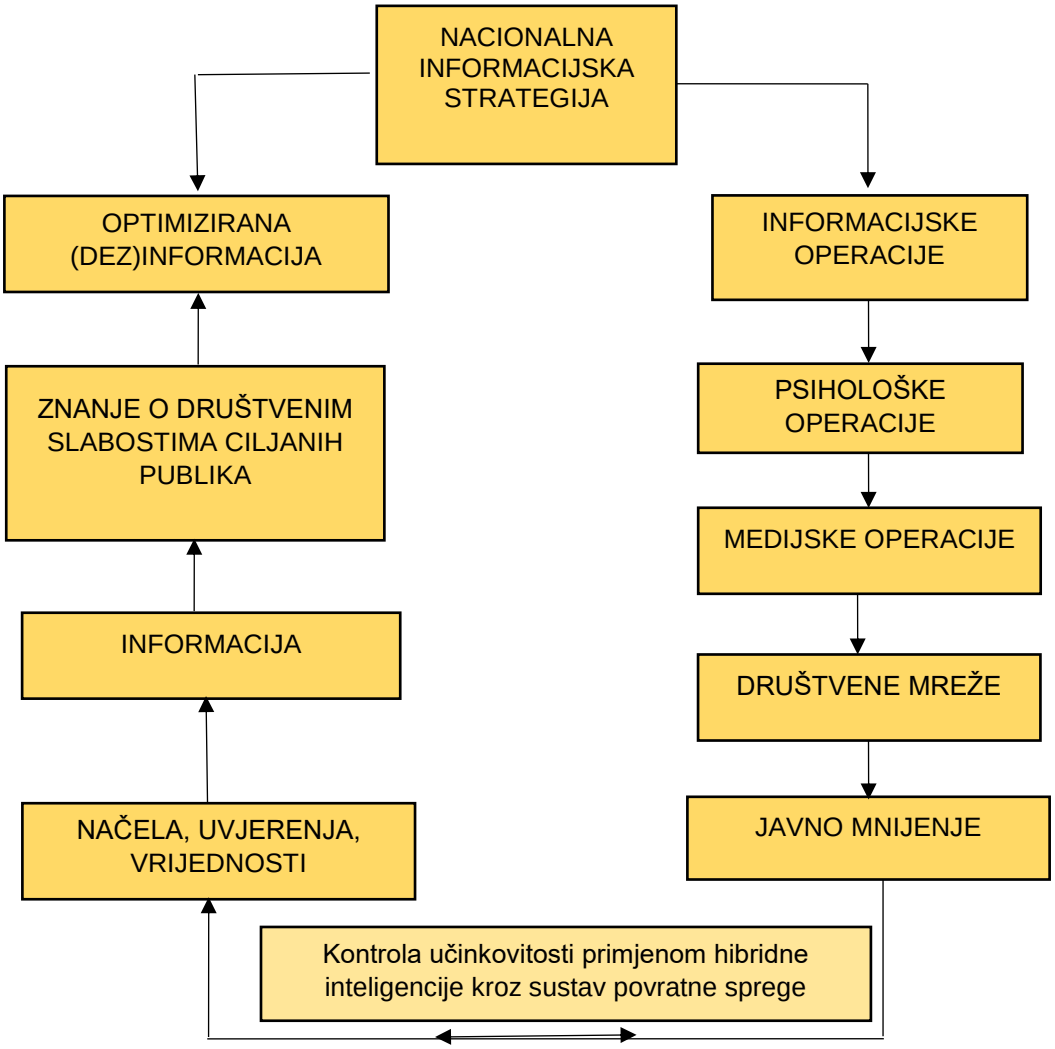
416 Ibid.

informacijskom i medijskom prostoru, a odgovaraju interesima i planerima informacijskih i medijskih operacija, odnosno olakšavaju prikupljanje i obradu obavijesti i informacija:

- Prema preferencijama na društvenim mrežama utvrđuju se kategorije ciljanih publika kojima se treba obratiti na temelju prikupljenih i obrađenih podataka o njihovim ranjivostima, odnosno na koga i kako bi se mogao imati najsnažniji utjecaj,
- Sukladno čemu se različitim oblicima psihološkog djelovanja i medijskim operacijama može ostvariti podržavanje ciljeva i ispunjavanje postavljenih zadaća,
- Analiziraju se različite kategorije ciljanih publika na pojedinačnom geografskom području bilo da se radi o pojedincima, manjim i većim grupama, manjim i većim zajednicama koje na neki način mogu sudjelovati u procesu donošenja odluka (ili će to tek postati) te pojedinaca i malih grupa osoba koji donose odluke i čije su odluke ključne za grupu, zajednicu, tvrtku, narod, državu.[417]

Društvene mreže opisanim mogućnostima postale su idealan alat za planiranje i stvaranje utjecaja u informacijskim i medijskim operacijama, odnosno za uspješnost djelovanja procesa utjecanja, učinkovitosti i brzine utjecaja. Odgovor je trenutan temeljem izvršene raščlambe prikupljenih strukturiranih podataka o uvjerenjima, načelima i vrijednostima zahvaljujući algoritmima i tehnologijama umjetne inteligencije. Na osnovu prikupljenih strukturiranih podataka automatiziranim sustavom povratne sprege hibridna inteligencija stvara gotovo idealne uvjete za učinkovito nametanje volje napadača i stjecanje informacijske nadmoći. Time se ostvaruju ciljevi iz nacionalnih informacijskih strategija, pojednostavljuju se procesi planiranja i provođenja informacijskih operacija, psiholoških operacija i medijskih operacija. Primjenom hibridne inteligencije moguće je kratkoročno ili dugoročno preoblikovati uvjerenja, načela i vrijednosti ciljanih publika u skladu s potrebama nacionalnih informacijskih strategija. To uključuje plasiranje dezinformacija i na osnovu njih napadanje ključnih društvenih slabosti ciljanih publika pri čemu primjena strojne inteligencije u procesu povratne sprege nadzire njihovu učinkovitost.

417 Usp. Ibid., str. 94.-95.



Slika 20. Prikaz procesa planiranja i provođenja nacionalnih informacijskih strategija pomoću društvenih mreža

Slika 20. prikazuje opisani proces planiranja i provođenja nacionalnih informacijskih strategija pomoću društvenih mreža. Želi se naglasiti kako primjena hibridne inteligencije u nadzoru nad procesom „tkanja dezinformacija“ od načela, uvjerenja i vrijednosti omogućava učinkovitije stjecanje znanja na osnovu kojeg se dezinformacije prilagođavaju utvrđenim strukturiranim društvenim slabostima, što je potpuno u skladu s predviđenim djelovanjima. Iako su preostali dijelovi ovog procesa bitni, oni se mogu mijenjati i biti manje ili više intenzivni. Automatizirani proces prikupljanja i obrade podataka, kontrole i nadzora nad podacima pomoću hibridne inteligencije osigurava mogućnost nadzora nad sadržajem koji se objavljuje ili pak treba objaviti kroz informacijske, psihološke i medijske operacije koje se planiraju i provode društvenim mrežama. Društvene mreže planerima ovih operacija osigurale su njihovo uspješno i učinkovito provođenje jer posredstvom društvenih mreža imaju kontrolu nad osobnim podacima (načelima, uvjerenjima i vrijednostima) i sadržajima koje korisnici društvenih mreža

stvaraju i dijele, na koje se kroz sustav povratne sprege i primjenom hibridne inteligencije izravno utječe na pojedine ciljane publike.[418] Ovaj dio istraživanja bitan je za daljnji dio istraživanja kojim će se potvrditi ili odbaciti hipoteza i odgovoriti na drugo istraživačko pitanje.[419]

418 Usp. Akrap, 2011., str. 97.

419 Istraživačko pitanje 2 glasi: Na koji način se društvene mreže i umjetna inteligencija koriste kao alati utjecaja za ostvarivanje vlastitih energetskih politika, za izazivanje društvenih nemira i oružanih sukoba te vlastitih ciljeva u izbornim kampanjama ciljanih publika?

4. HIBRIDNI SUKOBI I NOVI INSTRUMENTI MOĆI U KIBER PROSTORU

4.1. Transformacija sukoba i kiber prostor

Uvođenjem novih informacijskih strategija i sukoba niskog intenziteta u rješavanje međunarodnih odnosa na globalnoj pozornici sukobljavanja nametnute su nove doktrine informacijskog rata.[420] Globalne informacijske mreže postale su dio potpuno nove forme informacijskog rata[421] odnosno nove forme planiranja i izvođenja operacija utjecaja. Od prvotne ideje da osigura stvaranje i dijeljenje znanja, globalni informacijski prostor pretvorio se u žarište psiholoških operacija u borbi za ljudsko mišljenje i donošenje odluka. Globalne informacijske mreže u kiber prostoru stvorile su nove instrumente moći.

Kiber prostor koji je nastao za vojne potrebe i koji je osmišljen vojnim promišljanjem o korištenju umjetne inteligencije za obrambeno-napadačke svrhe, u znatnoj mjeri odredio je i oblikovao nove načine planiranja i upravljanja ratovima i sukobima. Tehnologije umjetne inteligencije koje koriste društvene mreže postale su novi instrumenti moći u kiber prostoru u kojem su ovakve tehnologije proširile mogućnosti i time povećale učinkovitost psiholoških operacija. Protivnički centar odlučivanja postao je ranjiviji i izloženiji psihološkim operacijama. Novi instrumenti moći uveli su nove obrasce psihološkog djelovanja, nove metodologije, nove alate i nove aktere koji se njima koriste. Novu paradigmu i transformaciju ratova i sukoba iz 20. st. američki teoretičari informacijskog rata Arquilla i Ronfeld najavili su djelima 'The Cyberwar is Coming!' i 'The Advent of Netwar'.[422] U njima su najavili ratove i sukobe u kiber prostoru koje su predstavili kroz termin mrežni rat (engl. netwar)[423] a koji je proizašao iz obilježja nove bojišnice. Tehnologije umjetne inteligencije koje koriste društvene mreže kao novi instrumenti moći u kiber prostoru pružile su nove mogućnosti u stvaranju različitih prijetnji i informacijsko-psiholoških pritisaka. Pored državnih aktera u mrežni rat uključili su se novi akteri, računalni hakeri i različite mrežno organizirane strukture kojima su

420 Usp. Tuđman, 2008., str. 135.

421 Tuđman, 2008. str 16.

422 Arquilla John i David Ronfeldt, The Advent Of Netwar. Santa Monica, RAND Corporation, 1996. https://www.rand.org/pubs/monograph_reports/MR789.html

423 Tuđman, 2008., str. 16.; prema Arquilla, John i David Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, RAND, 2001.

društvene mreže u kiber prostoru omogućile da mogu djelovati anonimno i da se u njemu organiziraju i koordiniraju bez preciznih i središnjih naredbi.[424]

Novi instrumenti moći, tehnologije umjetne inteligencije, postale su snažni i učinkoviti alati s pomoću kojih je u realnom svijetu postalo moguće izgraditi nove realnosti, rušiti postojeće i na njihovom mjestu izgraditi nove. Društvene mreže postale su primarni alati kojima se ciljanim publikama „nastoji prekinuti, oštetiti ili modificirati ono što zna ili misli da zna o sebi i o svijetu oko sebe“[425]. Postalo je moguće bez primjene kinetičke (vojne) sile uzrokovati političke promjene, što je u prošlosti uzimalo godine priprema i djelovanja.[426] „SAD i Velika Britanija kao začetnici ideje o stvaranju kiber prostora postepeno su u vojne strategije i doktrine počeli uvoditi nove vojne strukture s većim brojem manjih, sinkroniziranih vojnih jedinica kojima su novi instrumenti moći omogućili umrežavanje, veću efikasnost i operativnost. Ideja umrežavanja bila je osnova novog modela ratovanja u kiber prostoru poznatog kao mrežnocentrično ratovanje.“[427] Mrežnocentričnost vojne organizacije SAD-a bila je ključan čimbenik zbog kojeg je bio neophodan razvoj strukture kiber prostora i sposobnosti zasnovanih na njemu. Za vojsku SAD-a postojanje i funkcioniranje kiber prostora bilo je jedini način stvaranja optimalnog organizacijskog sustava globalno distribuirane vojne strukture. Ideja i zamisao SAD-a o mrežnocentričnom ratovanju u kiber prostoru trebala je osigurati učinkovito korištenje novih instrumenata moći za učinkovitije nametanje vlastitih ideja i ideologija ciljanim publikama bez direktnog masovnog sukobljavanja s protivničkim vojnim snagama.

---

424 Usp. Arquilla John i Ronfeldt David, The Advent of Netwar, Networks and Netwars: The Future of Terror, Crime, and Militancy, RAND, 2001. U mrežne organizacije autori ubrajaju organizacije i razne druge oblike nedržavnih elemenata od društvenih revolucionara, radikalnih grupacija, pobornika različitih anarhističkih i nihilističkih stavova do raznih drugih oblika aktivističkih grupa i organizacija, transnacionalnih, terorističkih, kriminalnih, fundamentalističkih ili etnonacionalističkih grupacija. Nove vrste organizacija globalne informacijske i komunikacijske mreže počele su koristiti za kreiranje i širenje vlastitih ideologija.

425 Brooking i Singer, 2018., str. 183.

426 Ibid.

427 Mladenović, 2016., str. 92

Ruski znanstvenik i teoretičar informacijskog ratovanja Aleksandar Dugin američkom modelu mrežnocentričnog ratovanja u kiber prostoru suprotstavlja ruski model protudjelovanja u koji kao ideološku matricu uvodi ideju euroazijanizma.[428] Dugin tumači da su SAD informacijske strategije mrežnocentričnog rata i dominaciju punog spektra pokrenule s namjerom da novim instrumentima moći na globalnoj razini prošire ideje i ideologije euroatlantizma koje su uobličene prema američkim vanjskopolitičkim interesima te da su nove strategije vođene idejom da u međunarodnim sukobima učinkovitije nameću vlastiti sustav vrijednosti bez primjene vojne sile. Pod euroatlantizmom podrazumijeva se ukupnost veza i odnosa postavljenih između SAD-a i zemalja zapadne Europe koje su u prvom redu vidljive u institucionaliziranom obliku njihove vojne suradnje kao temelja euroatlantskog zajedništva. Na tim vojnim osnovama izgrađeni su svi ostali oblici euroatlantskih veza koji nastaju kao sekundarni oblik povezivanja.[429] Temeljne zajedničke ideologije i prihvaćene vrijednosti snažno su ujedinile zapadnoeuropske američke saveznike i ojačale su euroatlantske veze.[430] Ideološka matrica ideje euroatlantskih veza ima za cilj stvaranje sigurnog tržišta za američko gospodarstvo, uspostavu transatlantskih ekonomskih veza i jačanje transatlantske vojne suradnje. U ovom smislu, mrežnocentrični model ratovanja, prema Duginu, SAD-u treba kako bi osigurala nadmoć ideje kako je vojna konfrontacija sa SAD-om besmislena.[431] Euroazijska ideja pak nastoji provoditi sustavnu i neophodnu reviziju političke, ideološke, etničke i vjerske povijesti čovječanstva te predlaže novi sustav klasifikacije meta političkih kategorija koje nadmašuju klasične klišeje.[432] Euroazijska ideja je strategija na globalnoj razini koja uzima u

---

428 Fridman Ofer, The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political and Public Discourse, Defence Strategic Communications, The official journal of the NATO Strategic Communications Centre of Excellence, Volume 2, 2017., str. 72. Dostupno na: https://www.stratcomcoe.org/ofer-fridman-russian-perspectiveon-information-warfare-conceptual-roots-and-politicisation-russian (pristup 5.8.2020.); prema Dugin, A., Voyna kontinentov - sovremennyy mir v geopoliticheskoy sisteme koordinat, str. 240.–258., str. 246.

429 Čehulić Lidija, Euroatlantizam, Politička kultura, Zagreb, 2003., str. 42.

430 Ibid. str. 40. Temelje euroatlantske suradnje odredilo je potpisivanje Atlantske povelje između SAD-a i Velike Britanije, a bipolarna ideologijska podijeljenost Europe učvrstila je euroatlantske veze. Pri pokusaju Washingtona da vlastite nacionalne interese ostvari putem univerzalističkih aspiracija kreiranja svijeta prema vlastitim vrijednostima, Europa je imala posebno značenje. Krilatica: štovatelji demokracije i liberalizma američki su prijatelji, svi ostali američki su neprijatelji, bila je potka formiranja saveza SAD-a s ostalim zemljama. Beatrice Heuser smatra da je upravo Europa u povijesti bila glavno poprište borbe između zagovornika; s jedne strane euroatlantske univerzalističke vjere u razvoj liberalne demokracije, slobode, tržišne ekonomije, a s druge raznih nacionalizama, jednopartijskih sistema, državnog socijalizma, centraliziranih ekonomija i raznih drugih nesloboda pojedinca i društva. Čehulić, 2003, prema; B. Heuser. Transatlantic Relations., str. 13.

431 Usp. Fridman, 2017., str. 61.- 86.

432 Vujić Jure, Rat svjetova, Euroazijanizam protiv atlantizma, Zagreb, 2012., str. 63.- 64.

obzir objektivnost globalizacije i kraj modela „država-nacija“, ali ujedno suvremenoj globalizaciji nudi alternativu koja se ne referira na unipolarni globalni model i globalnu vladavinu. Takva ideja predlaže multipolarni model globalizacije s raznim globalnim poljima. Euroazijanizam drži da je paradigma globalizacije ujedno i paradigma atlantizma. Globalizacija je jednodimenzionalni fenomen s jednim vektorom koji nastoji univerzalizirati zapadni (anglosaksonski i američki) model i osigurati američku kulturnu, političku i gospodarsku hegemoniju kao zajedništvo u svijetu.[433] Suprotno atlantizmu koji nastoji nametnuti jedinstveni gospodarski liberalno-kapitalistički model, euroazijski pokret smatra da ekonomski model potječe od zasebnih povijesnih i kulturnih tradicija, razvoja naroda i društva, stoga zagovara pluralnost ekonomskih modela i slobodni gospodarski razvoj, ali pojedini strateški sektori (vojno-industrijski kompleks, strateški resursi, komunikacije, transport) ostaju pod strogom državnom kontrolom.[434]

Prema Duginu, borbe za ovakve ideje i ideologije odvijaju se kroz četiri međuovisne domene ljudskih aktivnosti: fizičku, informacijsku, kognitivnu i društvenu[435] u kojima pobjede odnosi ona strana koja na učinkovitiji način iskorištava „široku upotrebu informacijskih, društvenih, kognitivnih i drugih čimbenika...“ Informacijska domena ljudskih aktivnosti glavno je poprište strateških informacijskih operacija te njima podređene, medijske, diplomatske, gospodarske i tehničke podrške. U ovoj domeni ostvaruje se potpuna i apsolutna kontrola nad svim sudionicima stvarnih i mogućih vojnih aktivnosti i manipulira se procesima za vrijeme trajanja rata, na njegovom vrhuncu ili za vrijeme mira.[436]

Američku ideju o mrežnocentičnom ratovanju „prethodno je u tehnološkom i operativnom smislu formalno uobličio američki admiral Ovens s konceptom “sustav sustava”.[437] „Prema Ovensu, vojna organizacija u vođenju sukoba predstavlja “sustav sustava”, odnosno usklađeno združeno funkcioniranje svih postojećih, organizacijski specifičnih vojnih komponenti za čiju je učinkovitost kao jedinstvene cjeline potrebna posebna i prilagođena doktrina planiranja,

433 Ibid.

434 Ibid. str. 97.- 98.

435 Fridman, 2017., str. 61-86.

436 Ibid.

437 Mladenović, 2016, str. 99., prema; William A. Owens, „Emerging US system-of-systems,“ Strategic Forum, 1996.

organiziranja i izvođenja vojnih operacija“.[438] S vremenom je mrežnocentrično vojno okruženje oružanih snaga SAD raslo i s ubrzanom digitalizacijom sustava preraslo je u koncept “sustav sustava”. Koncept „sustav sustava“ odredio je nastanak kiber prostora te predstavlja direktnu primjenu teorije ili znanosti sustava (Systems science) na organiziranje vojnog djelovanja i model vođenja svih kasnijih nastalih sukoba. „Budući da je bio blisko povezan s upotrebom informacijskih sustava, iz ovog koncepta nastala je potreba za razvijanjem sposobnosti za pokazivanje nacionalne moći utemeljene na kiber prostoru.“[439]

U tehnološkom pogledu, koncept “sustav sustava” omogućen je razvojem i primjenom informacijsko-komunikacijskih sustava i tehnologija umjetne inteligencije. „Proces vođenja sukoba i rata ovisi o mnoštvu čimbenika, kao što su vojna organizacija, raspolaganje sredstvima oružane sile, materijalni i ekonomski resursi, stupanj organizacije i morala i dr., a „sustav sustava“ povezuje sve te elemente u jedinstvenu, funkcionalnu i učinkovitu cjelinu. To je razlog zbog kojeg je kiber prostor proglašen petim područjem vojnih operacija.“[440] U kiber prostoru stvorenom kao „sustav sustava“ operativno je moguće djelovati isključivo primjenom informacijsko-komunikacijskih tehnologija[441], kao i odgovarajućom organizacijskom strukturom (…), zasnovanom na načelima nelinearnosti, složenosti i kaosa.[442] „Sustav sustava“ predstavlja sinergiju informacijskih tehnologija i umjetne inteligencije koja je izgradila kiber prostor te skup pravila koja unutar takvog prostora određuju ponašanje pojedinaca, zajednica ili određene političke i društvene strukture.

Unutar nereguliranog „sustava sustava“ (kiber prostora) na načelima nelinearnosti, složenosti i kaosa pomoću društvenih mreža kao novih instrumenata moći kojima upravlja umjetna inteligencija, odvija se borba aktera za spomenute ideje i ideologije, na način da se društvene mreže koriste za utjecanje na ponašanje ciljane političke ili društvene strukture. Unutar ovakvog „sustava sustava“ prevladava determinirani kaos. Pojam determiniranog kaosa promatra se kao način rješavanja međunarodnih sukoba kroz kiber prostor. „Postavlja se pitanje što je

438 Ibid.

439 Mladenović, 2016., str. 94.

440 Ibid. str. 96., prema; „War in the Fifth Domain,“ The Economist, 2010, i Robert J. Bunker and Charles „Sid“ Heal, eds. Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War—A Terrorism Research Center Book (Bloomington, IN: iUniverse LLC, 2014)

441 Ibid.; prema James R. Blaker, Transforming Military Force, The Legacy of Arthur Cebrowski and Network Centric Warfare, (Westport, CT: Preager Security International, 2007).

442 Mladenović, 2016., str. 96.

determinirani kaos?“[443] „To je nered „kojim se određuju granice… Nakon što su zadane njegove granice, nered koji nastaje ostaje unutar tih granica tako da postaje *nadziran* odnosno *upravljiv*.“[444] „Determinirani kaos prostor je međunarodnih igara, prostor koji je omeđen međunarodnim odlukama i naporima, da bi ostao ograničen unutar zadanih granica nereda.“[445] „Kontrolu tog nereda nije moguće ostvariti bez kontrole komunikacija. Jednako kao i dimenzije kaosa, tako i kriterije *nadziranja* i *upravljanje komunikacija* određuju centri moći u međunarodnoj zajednici uz prešutni pristanak svojih članica. Jedna od posljedica kontroliranih javnih komunikacija (medija) jest nadzor nad javnim pamćenjem.“[446] „Mehanizmi upravljanja pamćenjem u determiniranom kaosu jesu selekcija informacija, uspostava logike dvostrukih mjerila i dominacija kontroliranih informacija u informacijskom prostoru[447]. Zašto? Zato što obrazac proizvodnje determiniranog kaosa vrijedi samo za strane izolirane unutar omeđenog prostora. Nadziranjem pamćenja štite se vanjski čimbenici, tj. „upravljači krizom“ i „proizvođači kaosa „od širenja kaosa i od odgovornosti za proizvodnju nereda.“[448]

Prema teoriji kaosa američkog generala Stevena Manna iznesenoj 1992. u djelu 'Teorija kaosa i strateška misao'[449], informacijske i komunikacijske tehnologije od presudnog su značaja za iskorištavanje određenih slabosti i ranjivosti unutar nekog ciljanog „sustava sustava“ koji čine pojedinci, zajednice ili određene političke i društvene strukture. Pomoću informacijskih i komunikacijskih tehnologija „sustav sustava“ postaje podložan vanjskom utjecaju. Unutar njega unatoč kaosu koji se u njemu stvara, prepoznaje se redoslijed pomno isplaniranog djelovanja s potencijalnim strateškim posljedicama. Posljedice vanjskog djelovanja ovise o slabostima ciljanog „sustava sustava“. Izazivanjem determiniranog kaosa pomoću društvenih mreža u ciljanom „sustavu sustava“ zbog anonimnosti djelovanja umanjuju se mogućnosti pravovremenog predviđanja i brzog reagiranja, pri čemu ovisno o potrebi napadača „naoko

443 Tuđman, 2008., str. 169.

444 Ibid., str. 169.-170.; prema Domazet, Davor, Hrvatska i veliko ratište, Zagreb, Udruga Sv. Jurja, 2002., str. 282.-283.

445 Ibid., str. 170.

446 Ibid.

447 Ibid.

448 Ibid.

449 Mann, Steven R. Chaos Theory in Strategic Thought // Parametes, 1992. Dostupno na: https://archive.org/stream/1992Mann/1992+mann_djvu.txt

nepredvidljivi događaji mogu se manifestirati državnim udarom“.[450] Stvaranje determiniranog kaosa podrazumijeva nelinearnu formu planskog i sustavnog iskorištavanja društvenih slabosti koje je preko kiber prostora moguće osnažiti društvenim mrežama. One kao novi instrumenti moći u kiber prostoru služe za pokretanje procesa destabilizacija a u koju svrhu je pomoću društvenih mreža moguće iskorištavati čitav spektar društvenih slabosti unutar ciljanog „sustava sustava“: njihove etničke, religijske, političke i ideološke razlike i podjele, različite interpretacije povijesnih događaja, društvene, klasne i ekonomske razlike.

Skup pravila koja unutar „sustava sustava“ određuju ponašanje pojedinaca, zajednica ili određene političke i društvene strukture predstavljaju logičku osnovu napadnute strukture. Najviši opći “sustav sustava” ukupne primjene informacijskih tehnologija predstavlja kiber prostor. „Njegova ključna sposobnost, a to je umrežavanje, ostvaruje se na raznim razinama, uključujući i razinu podataka. Suvremeni sustavi informacijskih tehnologija nisu s vremenom evoluirali iz “nemrežnih” u “mrežne” sustave; oni su to oduvijek bili, zahvaljujući sposobnosti informacija da u digitalnom zapisu budu beskonačno puta umnožene i međusobno uspoređene i obrađivane po značenju.“[451] Umrežavanje računalnih informacijskih sustava postepeno je postalo automatizirano, da bi se došlo do suvremenog automatskog umrežavanja povezivanja „sustava sustava” kroz proces koji je poznat kao koncept umjetno stvorenog svijeta oko nas koji postaje razumljivo mrežni i virtualan. Hibridna inteligencija, u kojoj se koristi sve ono najbolje od strojne i ljudske inteligencije za stvaranje utjecaja, kroz automatizaciju obrade uvjerenja, načela i vrijednosti ciljanih publika unutar „sustava sustava” predstavlja novi iskorak u dobivanju kvalitetnijeg uvida u slabosti struktura koje se unutar takvog sustava napadaju. Kroz automatizirani sustav povratne sprege procesi prikupljanja, pohrane, obrade podataka, obavijesti i informacija koje stvaraju sami korisnici društvenih mreža postali su automatizirani time i učinkovitiji. Na osnovi strukturiranih podataka korisnika društvenih mreža umjetna inteligencija unutar „sustava sustava” prepoznaje slabosti društva na osnovi prikupljenih načela, uvjerenja i vrijednosti. Primjenom hibridne inteligencije takvi podaci i informacije (pre)uobličavaju se u dezinformacije. U kiber prostoru kao „sustavu sustava“ vojna, gospodarska i politička moć počiva na podacima o uvjerenjima, načelima i vrijednostima. Putem podatkovnih i komunikacijskih mreža društvene mreže s primijenjenim algoritmima i

450 Usp. Korybko Andrew; Haddad Hamsa, Chaos Theory, Global Systemic Change and Hybrid Wars, Comparative Politics Russia, 2016, No. 4, str. 25-35. Dostupno na https://www.comparativepolitics.org/jour/article/view/543

451 Mladenović, 2016., str. 98.

umjetnom inteligencijom svaki sa svojim zadaćama donose i nude optimizirana rješenja na nove načine. U svijetu stalne mrežne povezanosti ovi podaci predstavljaju "novu naftu", a društvene mreže nove „naftne platforme". Baš kao što sirovu naftu treba rafinirati kako bi se stvorili upotrebljivi proizvodi poput benzina, tako je podatke potrebno pročistiti kako bi se dobile upotrebljive informacije.[452] Bez obzira hoće li se primjenjivati u ratu ili izvan ratnog konteksta, umjetnu inteligenciju na društvenim mrežama moguće je zloupotrebljavati za postizanje širokog spektra ciljeva od strateških do taktičkih razina. Primjena umjetne inteligencije na društvenim mrežama ubrzala je procese donošenja odluka: temeljem strukturiranih pojedinačnih i grupnih uvjerenja pospješeno je prepoznavanje društvenih slabosti koje se prema iznesenoj teoriji kaosa, iskorištava za pokretanje željenih procesa i njihovo usmjeravanje u željenim pravcima.

Primjena umjetne inteligencije u prikupljanju, pohrani i obradi uvjerenja, načela i vrijednosti, u globalnoj informacijskoj infrastrukturi društvenih mreža, promijenila je političke, društvene i ekonomske sustave. Jednako tako, promijenila se forma ratovanja i sukobljavanja. Informacijska i komunikacijska tehnologija otvorila je nove načine prikupljanja, pohrane, manipulacije i distribucije podataka i informacija te stvaranja znanja. U nevojnim operacijama (operacijama utjecaja) novi instrumenti informacijama su dali potrebnu moć. Stečena moć koristi se za nanošenje štete funkcijama fizičkih infrastruktura, omogućava pristup podacima i informacijama i stvaranje učinkovitijeg utjecaja na pojedince, interesne skupine i države na globalnoj razini.[453] Neupitna je činjenica da tehnologije i informacije time ostvaruju sve veći utjecaj na rješavanje međunarodnih sporova i upravljanje sukobima. Vođena velikim podacima i algoritmima, umjetna inteligencija utječe na gotovo svaki aspekt života, od razvoja učinkovitijih načina za educiranje ljudi do obrane i napada u gotovo svim domenama.[454] Računalna znanost i informacijsko-komunikacijske tehnologije promijenile su načine života i rada ljudi, i konačno, promijenile su i same ljude. Na taj način tehnologije su utjecale i na sukobe: promijenila su se sredstva kojima se vode sukobi, promijenili su se akteri u sukobima i metode vođenja sukoba. Tehnologije neupitno utječu na forme sukoba koje društvene grupe

452 Thiele Ralph i Schmid Johann, Hybrid Warfare – Orchestrating the Technology Revolution, The Institute for Strategic, Political, Security and Economic Consultancy, No. 663, 2020., dostupno na https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf

453 Ibid.

454 Usp. Schmidt Eric, Work Robert, In Search of Ideas: The National Security Commission on Artificial Intelligence Wants You", War on the Rocks, 2019, dostupno na: https://warontherocks.com/2019/07/in-search-of-ideas-the-national-security-commission-on-artificial-intelligence-wants-you/

vode između sebe, na njihove sposobnosti koje razvijaju i usmjeravaju za vlastite ciljeve. Umjetna inteligencija jedna je od ključnih tehnologija u procesima digitalizacije[455] koja je odredila i uspostavila nova pravila. Umjetna inteligencija predvodnik je digitalne transformacije i snažno utječe na sva područja društva, uključujući industriju i gospodarstvo, kao i na državne domene, poput obrane i sigurnosti.[456] Vojno-obrambeni, politički i društveni sektori nalaze se pod snažnim pritiskom transformacije koju diktira umjetna inteligencija. Tehnologija koja obrađuje velike podatke trenutno se razvija ogromnom brzinom te jednakom brzinom ostvaruje snažan utjecaj i na transformaciju sukoba.[457]

Na vjerojatnost izbijanja sukoba ne utječe primarno sama tehnologija, već ona utječe na način kako se sukobi vode. „Veću vjerojatnost za izbijanje unutrašnjeg sukoba u nekoj državi nose brojni drugi čimbenici poput ekonomskih i političkih nestabilnosti“.[458] „Tehnologije, međutim, imaju ključni utjecaj na prirodu, trajanje i ishod sukoba.“[459] Automatizacija i anonimnost u prikupljanju, pohrani i obradi uvjerenja, načela i vrijednosti na društvenim mrežama omogućuju učinkovitije pronalaženje postojećih društvenih slabosti koje se na adekvatan način mogu iskoristiti za stvaranje nestabilnosti. Glavnu ulogu u povezivanju ciljanih publika, događaja i željenih procesa u kiber prostoru, kao novoj bojišnici, ima umjetna inteligencija koja na društvenim mrežama nadzire i upravlja načelima, uvjerenjima i vrijednostima. Primjerice algoritmi optimizacije pomažu identificirati ključne točke u vremenu ili prostoru koje vrijedi pratiti. Praćenje cilja u stvarnom vremenu omogućava trenutno djelovanje, odmah se mogu predložiti nove opcije za preraspodjelu cilja.[460] Algoritmi za prepoznavanje uzoraka omogućuju obradu velikih količina informacija. Algoritmi za rasuđivanje kombiniraju dostupne

455 Harhoff Dietmar, Heumann Stefan, Berlin Nicola Jentzsch i Lorenz Philippe, Outline for a German Strategy for Artificial Intelligence, July 2018, str. 6. Dostupno na: https://www.ip.mpg.de/fileadmin/ipmpg/content/aktuelles/Outline_for_a_German_Artificial_Intelligence_Strategy.pdf.

456 Thiele i Schmid, 2020.

457 Usp. Thiele Ralph, Artificial Intelligence – A key enabler of hybrid warfare, Hybrid CoE Working Paper 6, 2020. Dostupno na: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-6-artificial-intelligence-a-key-enabler-of-hybrid-warfare/

458 Mladenović, 2016.; prema Havard Hegre, Ranveig Gissinger, and Nils Petter Gleditsch. "Globalization and Internal Conflict,“ in Globalization and Conflict, eds. Gerald Schneider, Katherine Barbieri and Nils Petter Gleditsch (Boulder, CO: Rowman and Littlefield, 2003): 251-75.

459 Mladenović, 2016., str. 176.

460 Usp. Thiele, 2020.

informacije i pretvaraju ih u dobro strukturiran i koherentan prijedlog.[461] Oni moraju biti stalno dostupni, pouzdani i sigurni. Ovi podaci koji kontinuirano i u realnom vremenu pomoću društvenih mreža stižu do planera psiholoških operacija, objedinjeni i shvaćeni predstavljaju znanje o kompleksnom borbenom prostoru. Značaj informacija u borbenom prostoru u kojem prevladava automatizacija u njihovom stvaranju, prijemu, odašiljanju i obradi kroz podatke, sustav koji dakle neprekidno funkcionira, očigledno je veći nego što je ikada bio. Informacija je dobila odrednicu strateškog djelovanja i dodatnu moć utjecaja. Bez pravovremenih, potpunih, sigurnih i brojnih informacija različiti elementi iz „sustava sustava" ne mogu biti uspješno povezani i ne može se ostvariti sinergijski učinak djelovanja u „nadziranom kaosu" kako bi se u stvarnom fizičkom svijetu ostvarili zacrtani ciljevi s potencijalnim strateškim posljedicama.

Automatizacija predstavlja temeljnu promjenu pristupa procesu nadzora informacija u kiber prostoru koja je nesumnjivo utjecala na transformaciju sukobljavanja. Na društvenim mrežama automatizacija i nadzor kroz grupiranje podataka omogućuje identifikaciju i pravovremeno uočavanje obrazaca o društvenim slabostima u ogromnim skupovima strukturiranih podataka. Automatizacija nadzora uočenih obrazaca potom se koristi za prilagođavanje zacrtanih ciljeva na svim razinama ciljanih publika, masovnoj, grupnoj i pojedinačnoj. Iz strukturiranih podataka o uvjerenjima, vrijednostima i načelima primjenom strojnog učenja, dubokog učenja, procesnog rudarenja mogući su kvalitetniji uvidi u društvene slabosti. Strukturiranje ogromnih količina različitih podataka o uvjerenjima, načelima i vrijednostima algoritmima omogućava neovisno generiranje predviđanja u odnosu na još nepoznate podatke i, u idealnom slučaju, autonomno poboljšanje vlastite izvedbe tijekom vremena. To se pokazalo posebno vrijednim za iskorištavanje potencijala hibridne inteligencije u planiranju i izvođenju dezinformacijskih kampanja u psihološkim operacijama u nepredviđenim situacijama, kada je potrebno otkriti pomicanje/promjenu težišta u razmišljanju i stavovima ciljanih publika. Preopterećenost informacijama pri tome ne predstavlja problem, dapače ona postaje korisna. Inteligentna i automatizirana evaluacija podataka vođena umjetnom inteligencijom omogućuje procjenu i obradu svih relevantnih podataka te njihovu pravovremenu i učinkovitu primjenu.[462]

Društvene mreže po ovoj osnovi postale su ključni alati za planiranje i izvođenje učinkovitijih informacijsko-psiholoških pritisaka prema strukturiranim ciljanim publikama unutar „uzročno-

461 Kerbusch Philip, Keijser Bas, Smit Selmar, Roles of AI and Simulation for Military Decision Making, TNO 2018, https://pdfs.semanticscholar.org/885b/182170db541d48ca7f0380bc0447ce56c9ae.pdf.

462 Thiele, 2020., str. 9.

posljedičnog prostorno i vremenski isprepletanog multiverzuma (multidimenzionalog okruženja)“[463]. Osnovni čimbenici koji omogućavaju umreženost i izrazitu interakciju ciljanih publika, sustava, događaja i procesa u borbenom prostoru „sustava sustava“ (kiber prostora) su podaci koje automatizirani sustavi na društvenim mrežama prikupljaju, pohranjuju, obrađuju, preoblikuju i diseminiraju u obliku dezinformacija. Primjena informacijskih tehnologija i automatiziranih sustava u planiranju i izvođenju psiholoških operacija time je postala neupitna. U tom smislu promatraju se kao novi snažni instrumenti moći koji u kiber prostoru diktiraju transformaciju sukoba sa stvarnim implikacijama u fizičkom svijetu te koji na učinkovit način utječu na procese razmišljanja i donošenje odluka ciljanih publika od interesa napadača.

Pojavom automatiziranih tehnologija došlo je do evolucije u planiranju i provođenju sukoba niskog intenziteta, operacija utjecaja te u konačnici ratova kao krajnjeg načina rješavanja međunarodnih sporova. Globalna umreženost, robotika i umjetna inteligencija doprinijeli su iskorištavanju informacija od strane svih koji imaju definirane ciljeve, dovoljno znanja i financijskih sredstava za njihovu provedbu. Novi oblici dezinformacijskih kampanja primarno su psihološke naravi. Neosporno je da se automatizacija obrade podataka odvija u kiber prostoru u kojem se dezinformacijskim kampanjama napadaju kritične društvene slabosti. Čimbenici automatizacije i anonimnosti postali su ključni. Ranjivosti se u ovom kontekstu promatraju kroz kognitivne slabosti u razmišljanju i donošenju odluka koje se utvrđuju na temelju prikupljenih i obrađenih uvjerenja, načela i vrijednosti.

Činjenica je da automatizacija obrade podataka stvara učinke na kognitivne procese bez obzira radi li se o stanju mira ili rata. „I u ratu i u miru moguće je izvoditi nasilne akcije nad drugom stranom, ali to nasilje ne ispunjava se samo nad objektima i ljudima (u fizičkom okruženju), već i nad njihovim dušama, odnosno svijesti (u informacijsko-kognitivnom okruženju)“.[464] Konačno, „razvoj logičkog okruženja i sposobnosti tehničkih sustava kako bi funkcionirali kreativno i smisleno poput čovjeka“[465] kroz sustave umjetne inteligencije omogućio je stvaranje konstantnih (24/7) informacijsko-psiholoških pritisaka na razmišljanje i donošenje odluka.

Prema ovom načelu globalizacija informacijsko-komunikacijskih tehnologija, kiber prostor, automatizacija i umjetna inteligencija koju koriste društvene mreže predstavljaju glavne

463 Mladenović, 2016., str. 100.

464 Mladenović, 2016., str. 108.; prema Đuro Šušnjić, Ribari ljudskih duša (Beograd: Čigoja, 2008).

465 Ibid.

čimbenike koji su promijenili forme sukobljavanja. Krivo bi bilo tumačiti da su stari sukobi prestali i da su nastali novi sukobi. Sukobi nisu prestali, već su se nastavili u novim pojavnim oblicima i vode se novim instrumentima moći - tehnologijama umjetne inteligencije koje koriste društvene mreže.

U kiber prostoru fizičko djelovanje, informacijski, društveni i politički „sustavi sustava" pomoću društvenih mreža učinkovitije su se povezali na taktičkoj, operativnoj i strateškoj razini. Društvene mreže su u njemu omogućile pronalaženje ključnih društvenih slabosti na osnovi strukturiranih uvjerenja ciljanih publika. Ovakav pristup utječe i na razumijevanje odnosa između taktičkih, operativnih i strateških informacijskih i psiholoških operacija kroz kiber prostor. Sustavi koji su postali umreženi i automatizirani tako su objedinili aktivnosti kojima se planira i upravlja informacijskim operacijama u svim domenama kiber prostora: fizičkoj, logičkoj (informacijskoj) i kognitivnoj. „Teorijski modeli ovakvog načina vođenja sukoba u suvremenoj međunarodnoj praksi različito se nazivaju, poput specijalnog ratovanja (engl. Special Warfare), nelinearnog ratovanja (engl. Non-linear Warfare), mrežnocentričnog ratovanja (Network-Centric Warfare), asimetričnog ratovanja (Assymetric Warfare), ratovanja četvrte generacije (Fourth Generation Warfare), neograničenog ratovanja (Unrestricted Warfare), hibridnog ratovanja (Hybrid Warfare) i drugih."[466] „Svi navedeni koncepti ratovanja razlikuju se po teorijskom modelu i nastali su sukcesivno u različitim vremenskim razdobljima. Međutim, svi oni imaju zajedničku karakteristiku, a to je da ne određuju formu budućih sukoba, već da su njihovi modeli kreirani opisivanjem postojećih sukoba. Pobjeda u sukobu s drugom državom je krajnji cilj svake države. Pošto je sam opstanak države ulog u sukobu, države nemaju razloga ograničavati se na samo određeni oblik vođenja sukoba."[467] U građanskim ratovima, društvenim, političkim prevratima i uličnim nemirima, naizgled, sve se odvija kaotično bez reda i pravila. To ukazuje da se u skladu s vremenom, razvojem novih informacijskih strategija, primjenom novih informacijskih instrumenata moći u vođenju sukoba i povećavanjem broja aktera povećala složenost sukobljavanja prema kojima su različiti akteri morali usklađivati informacijske strategije. Automatizirane tehnologije umjetne inteligencije koje koriste društvene mreže u tolikoj su mjeri integrirane u informacijske strategije da ih se s pravom smatra aktivnim pomagačima u ispunjavanju njihovih ciljeva.[468]

466 Ibid., str. 101.

467 Ibid.

468 Usp., Thiele, 2020., str. 6.

Opisana transformacija sukoba u kiber prostoru započela je koncem 1980-ih teorijom ratovanja četvrte generacije[469] koja je unijela najradikalnije promjene u načinu ratovanja još od Vestfalskog mira iz 1648.[470;471] Države su pojavom kiber prostora izgubile monopol na rat, tzv. kulturni ratovi ponovno su postali aktualni a imigracije su postale jednako opasne kao upadi oružani snaga u teritorij drugih država.[472;473] Teorija ratova četvrte generacije uvela je kiber prostor u borbena djelovanja i naglašeniju primjenu asimetrije te veću ulogu nedržavnih pokreta. „Usprkos tome što vojno razvijenija strana posjeduje očiglednu vojnu nadmoć, asimetrično djelovanje u kiber prostoru i široka dostupnost informacijsko-komunikacijskih tehnologija vojno slabijem protivniku omogućilo je izvođenje konstantnih, prikrivenih i neočekivanih napada. Primjenom asimetričnih djelovanja u kiber prostor postalo je moguće vršiti neprekidan pritisak na vlast države kako bi angažirala sve raspoložive resurse u cilju borbe čime se, u dužem periodu, dovodi do njezinog ekonomskog, društvenog i organizacijskog sloma.“[474]

Kiber prostor i njegova struktura omogućili su četvrtoj generaciji ratova i sukoba istovremeno djelovanje u fizičkoj, informacijskoj i kognitivno-psihološkoj domeni, pri čemu je kognitivno-psihološka domena ključna jer se preko nje dezinformacijama nastoji utjecati na uvjerenja, načela i vrijednosti ciljanih publika za vlastitu korist.

---

469 Prethodne generacije sukobljavanja nisu predmet istraživanja.

470 Vestfalski mir ili Münsterski mir, mirovni ugovor zaključen u Münsteru u Vestfaliji 1648. između rimsko-njemačkog cara Ferdinanda III. s jedne strane, a Šveđana, Francuza i njihovih protucarskih saveznika među njemačkim državnim staležima s druge strane. Njime je bio okončan Tridesetogodišnji rat (1618–48) između Habsburgovaca te Francuske i Švedske sa saveznicima za političku i vjersku prevlast u Europi. Vestfalski mir imao je veliko značenje: ograničio je autoritet rimsko-njemačkog cara, izmijenio političku ravnotežu u Europi ojačavši utjecaj Francuske i Švedske, pridonio širemu poimanju slobode savjesti i vjerskoj snošljivosti. Naglašavanjem državnog suvereniteta i suradnje postao je temeljem novog europskog poretka, zasnovanoga (teoretski) na načelu ravnopravnih država. Vestfalski mir. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Prestupljeno 21. 1. 2022. http://www.enciklopedija.hr/Natuknica.aspx?ID=64409

471 Lind S William, Understanding Fourth Generation War, 2004., Homeland Security Digital Library, dostupno na : https://www.hsdl.org/?view&did=482203

472 Ibid., str. 13.

473 Usp. Lind William, Nightengale Keith, Schmitt John, Sutton Joseph i Wilson I. Gary, The Changing Face of War: Into the Fourth Generation, Marine Corps Gazette, 1989, str. 22-26, dostupno na: https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html

474 Mladenović, 2016., str. 143. Autor navodi da je ovakav model sukoba primijenjen u periodu takozvanog “Rata protiv terora” koji je nastupio nakon terorističkog napada Al-Kaide na SAD 2001. Pa ipak, u području ratnih operacija i u vremenu u kojem se sukob vodio, terorizam ne samo da nije uništen, već je značajno ojačao i dobio je formu nove organizacije sa svojstvom države, ISIL-a, koja je svojim aktivnostima pokrivala područja više bliskoistočnih država zahvaćenih sukobima.

„Sukobi četvrte generacije vode se na holistički način: u medijskoj, političkoj, ekonomskoj, društveno-civilnoj i konačno, kao krajnje sredstvo u vojnoj sferi. Posljedica toga je da organizacijska struktura sudionika u sukobu četvrte generacije ne teži širenju i učvršćivanju, već nestalnosti i elastičnosti. Ta struktura je po obliku mrežna, a po trajanju nestalna.“[475] U ratovanju četvrte generacije mrežne organizacije funkcioniraju i djeluju samostalnije, bez formalne strukture organizacije te je smanjen značaj direktnog vojnog nadmetanja oružanom silom. Ove male veličine organizacijskih elemenata i struktura u sukobu ističu svoju prilagodljivost i prikrivenost u djelovanju. Teorija sukoba i ratova četvrte generacije unijela je novu paradigmu: na fizičkom bojnom polju umjesto vojnika koriste se mrežne organizacije te razni oblici društvenog i političkog aktivizma, odnosno civili koji se de facto preko informacijskih mreža uključuju u izazivanje društvenih nemira.

Digitalizacija informacijskog prostora, daljnji napredak tehnologija umjetne inteligencije i sama automatizaciju procesa prikupljanja, pohrane i obrade ogromnih količina strukturiranih podataka i informacija, nesumnjivo je odredila daljnji iskorak u transformaciji četvrte generacije u petu generaciju sukoba i ratova. „Treba napomenuti da u definiranju pete generacija ratovanja postoji veliko razmimoilaženje u pogledima vodećih teoretičara rata.“[476] „George Friedman je 2007. govorio o razvoju pete generacije ratovanja u kontekstu suprotstavljanja novim oblicima ratovanja koje će dolaziti od strane Rusije i Kine (Friedman, 2007:60), a Daniel H. Abbott u svojoj knjizi 5th Generation Warfare navodi da su temelji pete generacije ratovanja nekinetičke operacije i mrežni sustavi.“[477] „Neki teoretičari, kao što je Samuel Liles, petu generaciju ratovanja nazivaju i kiber ratom (Liles, 2007: 1).“[478] „Iako se prelazak iz četvrte u petu generaciju čini nejasnim, s obzirom na to da se sudeći po dostupnoj literaturi on dogodio u vrlo kratkom vremenskom periodu, takozvana peta generacija ratovanja počiva većim dijelom na upotrebi tehnologija za širenje i obranu vlastitih ideja u informacijskom prostoru.“[479] U svakoj dosadašnjoj tranziciji ratova i sukoba pa tako i u ovoj posljednjoj ključnu ulogu imale su tehnologije[480] na način da su se koristile kao alati za učinkovito nametanje ideja i ideologija. Kako su tehnologije umjetne inteligencije na

475 Ibid., str. 145.

476 Brzica, 2018, str. 39.-40.

477 Ibid.

478 Ibid., str. 40.; prema Abbot, 2010.

479 Ibid., str. 40.

480 Lind i sur., 1989.

društvenim mrežama omogućile automatizaciju u prikupljanju, nadziranju i (pre)uobličavanju načela, uvjerenja i vrijednosti informacije su na društvenim mrežama postepeno u međunarodnim sukobima povećavale moć utjecaja a smanjivale potrebu primjene tradicionalne vojne sile i oružja. Primjena vojne sile time je postala tek krajnja opcija za nametanje napadačeve volje. Sukobi su se nastavili voditi u kiber prostoru kao petoj dimenziji sukobljavanja, u novoj bojišnici pomoću tehnologija umjetne inteligencije koja upravlja i održava osnovne funkcije društvenih mreža. Društvene mreže stoga u današnjim ratovima i sukobima dominiraju kao snažni i učinkoviti alati u borbi za ideje i ideologije, stvaranje utjecaja na kulturne i identitetske simbole, načela, sustave vrijednosti i uvjerenja.

4.2. Nastanak hibridnih sukoba i glavna obilježja

Glavna obilježja hibridnih sukoba su u novim formama planiranja i izvođenja informacijsko-psiholoških pritisaka u kiber prostoru. Te nove forme najviše se prepoznaju kroz mogućnosti preoblikovanja uvjerenja, načela i vrijednosti u učinkovite dezinformacije, automatiziranost i masovnost takvih dezinformacija, njihova anonimnost, da se mogu uobličavati prema društvenim slabostima, u kombinaciji s javnim diplomatskim mjerama, političkim i kulturološkim subverzijama, novim mogućnostima stvaranja konstantnih informacijsko-psiholoških pritisaka, korištenjem mrežnih organizacija, računalnih hakera i osnivanjem vlastitih medijskih sustava u drugim državama.

Termin hibridnost za opisivanje novih oblika sukoba prvi put se pojavio u Nemethovoj studiji iz 2002. pod naslovom 'Future War and Chechnya: A case for hybrid warfare'. Termin hibridnosti predstavljen je kroz tezu da će moć vojnih snaga u novim sukobima primarno ovisiti o sposobnosti uporabe novih tehnologija za borbena djelovanja. Kad je postalo očito da se kiber prostor i tehnologije umjetne inteligencije koje koriste društvene mreže sve naglašenije koriste za planiranje i izvođenje i nekinetičkih operacija, termin hibridnosti postepeno je postao prihvaćen u akademskim, znanstvenim, političkim i vojno-sigurnosnim krugovima za opisivanje primjene opisanih tehnologija kao nekinetičkih sredstava borbe. Sam termin hibridnosti dakako nije bio ni nov niti potpuno originalan. Nastao je još u antičkom dobu i njime se opisivala primjena ratnih strategija i kombiniranje takvih strategija s primjenom tehnoloških rješenja i mogućnosti za njihovu realizaciju.[481] Hibridni rat/sukob u biti nije ništa novo.

481 Popescu Nicu, Hybrid Tactics: Neither New Nor Only Russian, The European Union Institute for Security Studies, 2015., dostupno na: https://www.iss.europa.eu/content/hybrid-tactics-neither-new-nor-only-russian

Međutim, tehnološki trendovi sugeriraju da će se opasnosti koje proizlaze iz hibridnog djelovanja širiti vrlo brzo.[482] Svojim potencijalom otvaraju nove načine nasilnog djelovanja i primjene sile u ratovima i sukobima.[483]

Ovdje je vrijedno ponovno spomenuti model mrežnocentričnog ratovanja kao forme korištenja tehnologija za nametanje ideja i ideologija. Ideju euroazijanizma Dugin je uveo u ruski akademski i politički diskurs 2007., u svojoj knjizi 'Geopolitika Postmoderna', iste godine kada je američki teoretičar informacijskog ratovanja Frank G. Hoffman u svojoj knjizi 'Sukobi u 21. stoljeću: Uspon hibridnih ratova' najavio „novi“ oblik sukoba i ratova. Nadovezujući se na Nemethov koncept kombiniranja vojnih taktika i novih informacijskih i komunikacijskih tehnologija, Hoffman je termin hibridnosti iskoristio za prvu definiciju hibridnog ratovanja. Povod je bio sukob niskog intenziteta koji je izbio između Hezbollaha i Izraela 2006. Jedna od karakteristika ovog sukoba bila je da su oba aktera, svaki za svoje interese i potrebe, koristili prvu društvenu mrežu Facebook koja se pojavila 2004. Hoffman je hibridno ratovanje definirao kroz prizmu različitih prijetnji koje proizlaze iz kiber prostora koji državni i nedržavni akteri koriste za različite forme ratovanja. Naknadno 2009. Hoffman je proširio ovu definiciju u kojoj je u osnovi hibridno ratovanje definirao kao poduzimanje različitih radnji na nekom geografskom području u svrhu postizanja sinergijskih učinaka u fizičkoj i psihološkoj dimenziji sukoba. Terminom hibridnosti označio je konvergenciju različitih aktivnosti kroz fizičku, informacijsku i kognitivnu domenu kiber prostora pomoću informacijskih i komunikacijskih sustava i tehnologija. Kontinuirano unaprjeđivanje ovih sustava i tehnologija i njihova primjena na društvenim mrežama s vremenom su dovele do činjenice da su se društvene mreže počele sve intenzivnije koristiti kao učinkovit alat za planiranje i izvođenje psiholoških operacija.

Hibridne taktike stare su kao i sam fenomen sukoba. Pojavom društvenih mreža i njihovom zlouporabom, termin hibridnosti poslužio je kako bi se u međunarodnim sukobima naglasila rastuća uloga kiber prostora i informacijsko-komunikacijskih i računalnih tehnologija za planiranje i izvođenje kinetičkog (vojnog) i nekinetičkog djelovanja (operacija utjecaja).

---

482 Usp. Schmid Johann i Thiele Ralph, Hybrid Warfare – Orchestrating the Technology Revolution. In Robert Ondrejcsak & Tyler H. Lippert (Eds.), STRATPOL. NATO at 70: Outline of the Alliance today and tomorrow, Special Edition of Panorama of Global Security Environment 2019, Bratislava December 2019, str. 211–225, https://www.stratpol.sk/wp-content/uploads/2019/12/panorama_2019_ebook.pdf.

483 Za razumijevanje koncepta hibridnog ratovanja vidi: Schmid, J. COI S&D Conception Paper: Hybrid Warfare – a very short introduction, Helsinki, 2019., ISBN: 978-952-7282-20-5.

U ovom dijelu istraživanja bitno je razlučiti razlike između hibridnog ratovanja i hibridnih sukoba.

Za potrebu ovog istraživanja i u svrhu prikazivanja razlika između hibridnog ratovanja i hibridnih sukoba dovoljno je navesti osnovnu definiciju i osnovna obilježja hibridnog ratovanja. Hibridno ratovanje definira se kao sinkronizirana upotreba višestrukih instrumenata hibridne moći koji se prilagođavaju specifičnim slabostima ciljanih publika u cijelom spektru društvenih funkcija (MCDM 2019).[484] Pod hibridnim instrumentima moći podrazumijevaju se vojni, ekonomski, politički, financijski, sigurnosni i informacijski instrumenti moći.[485]

Hibridni sukobi odvijaju se izvan konteksta hibridnog rata, otvorenih međunarodnih, unutarnjih ili posredničkih (*engl. proxy*) sukoba. U hibridnim sukobima, kao i u hibridnom ratovanju, podjednako se kombiniraju tradicionalne i netradicionalne metode planiranja i izvođenja psiholoških operacija. Koriste se dakle tradicionalni mediji (tisak, tv, radio) i društvene mreže kao dominantan netradicionalni medij sa svrhom stjecanja informacijske nadmoći nad korpusom javnog znanja ciljanih publika. Primjena kinetičke sile u hibridnim sukobima tek je krajnja opcija za nametanje volje napadača koja je rezervirana za hibridno ratovanje. Upotreba kinetičke sile dakle, osnovna je razlika između hibridnog sukoba i hibridnog ratovanja. Hibridni sukob predstavlja širi pojam od hibridnog rata. Varijacije psihološkog djelovanja kroz kiber prostor nešto su složenije nego u hibridnom ratovanju.

U hibridnim sukobima informacijski instrumenti hibridne moći u odnosu na ostale instrumente moći imaju važniju ulogu i oni su alati koji se primarno koriste za stvaranje informacijsko-psiholoških pritisaka. U informacijske instrumente hibridne moći, uz tradicionalne medije, ulaze informacijsko-komunikacijski sustavi i sve raspoložive računalne tehnologije i sustavi za umreženo i globalno komuniciranje. U hibridnim sukobima svi dostupni hibridni instrumenti moći: ekonomski, politički, financijski (osim vojnih kao krajnjeg sredstva) primarno se iskorištavaju kroz kreativnost, dvosmislenost i nelinearnost kiber prostora pomoću informacijsko-komunikacijskih sustava i tehnologija umjetne inteligencije koje koriste društvene mreže. Njihovom sinergijom u kiber prostoru stvara se cijeli niz prijetnji u kojima se na učinkovit način iskorištavaju društvene slabosti protivničke strane.

---

484 A Multinational Capability Development Campaign project (MCDC) Countering Hybrid Warfare Project: Countering Hybrid Warfare, 2019. Serija MCDC inicijativa je koju vode Sjedinjene Američke Države osmišljena za zajednički razvoj i procjenu koncepata i sposobnosti NATO saveza za rješavanje izazova povezanih s provođenjem zajedničkih, multinacionalnih i koalicijskih operacija, izradu smjernica za planere vojno-strateške i operativne razine radi suzbijanja hibridnih prijetnji ili djelovanja aktera hibridnog ratovanja.

485 Ibid.

Ključnu novost unijele su informacijsko-komunikacijske tehnologije koje su postale temelj hibridnog ratovanja[486] i hibridnih sukoba. Ove tehnologija su glavni čimbenici koji su omogućili kombiniranje različitih instrumenata hibridne moći.[487] Hibridni instrumenti moći imaju dvije glavne funkcije. Jedna je nanošenje selektivne štete, a druga je podrška donošenju odluka na dvije razine: kako bi vlastite odluke bile superiornije u odnosu na protivnika i kako bi protivnik donosio pogrešne odluke na vlastitu štetu. Donositeljima odluka tehnologije koje koriste društvene mreže i primjena hibridne inteligencije na njima pružaju podršku u donošenju kvalitetnijih odluka. Višedimenzionalne tehnologije umjetne inteligencije koje na društvenim mrežama obrađuju načela, uvjerenja i vrijednosti te daju zaključke i rješenja dodatno su proširile mogućnosti u planiranju i izvođenju psiholoških operacija. Strojno učenje igra posebnu ulogu. Strojno učenje koristi se kako bi se ažuriralo znanje o operativnom okruženju. Uvođenje dubokog učenja u kombinaciji s besplatnim pristupom ogromnoj količini strukturiranih uvjerenja, načela i vrijednosti povećalo je mogućnosti pravovremenog uočavanja društvenih slabosti na osnovi čega se poboljšala učinkovitost željenog djelovanja i smanjili su se politički troškovi dugotrajnih vojnih angažmana.[488] Istodobno, strukturiranje podataka o uvjerenjima, načelima i vrijednostima u stvarnom vremenu vođeno umjetnom inteligencijom omogućilo je bolje razumijevanje obrazaca ponašanja, struktura i procesa koji se odvijaju u korpusu javnog znanja ciljanih publika.[489]

Strojno učenje, duboko učenje bazirano na primjeni dubokih neuronskih mreža, robotska automatizacija procesa njihove obrade, procesno rudarenje podataka i algoritmi kroz primjenu sustava povratne sprege na društvenim mrežama proširili su mogućnosti informacijsko-psiholoških pritisaka. Ove tehnologije postale su novi instrumenti moći jer su integrirale prednosti kiber prostora i kognitivne elemente informacijskog ratovanja. Omogućile su ostvarivanje željenog utjecaja na razmišljanja i donošenje odluka ciljanih publika na nove načine: automatizirane i optimizirane načine prema okolnostima i slabostima ciljanih publika i potrebama napadača. Primjena ovih tehnologija kroz sustav povratne sprege, na osnovi ulaznih podataka i njihove automatizirane i optimizirane obrade, na društvenim mrežama omogućila je prilagođavanje informacijsko-psiholoških pritisaka prema društvenim slabostima ciljanih

---

486 Thiele i Schmid, 2020.

487 Ibid., str. 6.

488 Usp. Thiele, 2020.

489 Usp. Daniel Egel, Eric Robinson, Charles T. Cleveland, Christopher Oates, "AI and Irregular Warfare: An Evolution, Not a Revolution", War on the Rocks, October 31, 2019, https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/

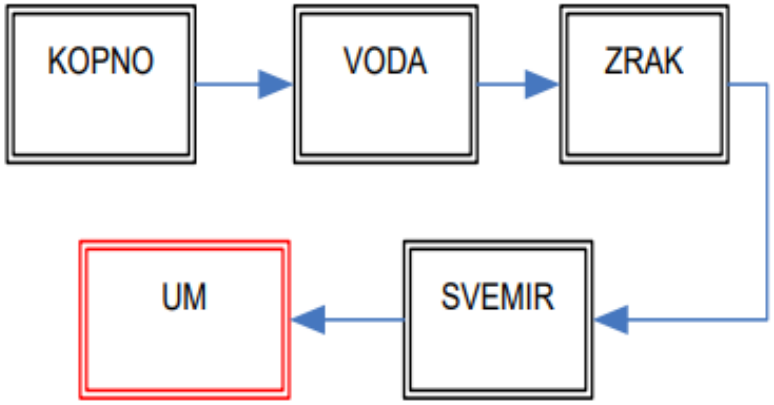
publika. Ključna uporišna točka koja se pri tome koristi u hibridnim sukobima je nametanje volje napadača na njihova temeljna uvjerenja, vrijednosti i načela, pitanja identiteta, kulture i jezika sa svrhom njihovog (pre)oblikovanja za potrebe napadača, bez primjene kinetičke sile. Mogućnost zloupotrebe hibridne inteligencije kroz primjenu strojne i ljudske inteligencije dodatno nudi mogućnosti i rješenja da se dezinformacije stvaraju i prilagođavaju prema utvrđenim društvenim slabostima.

Time su „tvorničke postavke" tehnologija umjetne inteligencije koje koriste društvene mreže neupitno postale ključni alati za ostvarivanje željenih psiholoških učinaka. Uobličavanjem dezinformacija prema društvenim slabostima, njihovim optimiziranjem, automatiziranošću i anonimnošću informacijsko-psihološki pritisci postali su snažniji i učinkovitiji, mogu se provoditi konstantno (24/7) bez primjene kinetičke sile koja je stalno prisutna kao krajnja prijetnja.

Hibridni sukobi, dakle, sukobi su u kojima je naglasak na iskorištavanju informacijskih tehnologija i globaliziranih, umreženih medija i globalne informacijske infrastrukture (interneta) kojima se umanjuje protivnička volja i borbena spremnost.[490] Hibridni sukobi se planiraju i izvode primarno kroz kiber prostor tehnologijama koje održavaju osnovne funkcije društvenih mreža. Hibridni sukobi su sukobi ideja i ideologija, a vode se svim raspoloživim tehnologijama strojne i ljudske inteligencije. Društvene mreže zbog niza očitih prednosti koje nude u kiber prostoru ovdje služe kao snažan i učinkovit instrument utjecaja. Pomoću njih moguće je učinkovito provoditi nacionalne informacijske strategije i psihološke operacije. Ovaj dio istraživanja bitan je iz razloga što će se na osnovu njega u daljnjem dijelu istraživanja potvrditi ili opovrgnuti hipoteza i dodatno odgovoriti na prvo i drugo istraživačko pitanje.

Hibridni sukobi jesu sukobi u kojima se borbe prvenstveno vode za um protivnika, odnosno za njegovo mišljenje i donošenje odluka. U borbi za um, mišljenje i donošenje odluka automatizirane tehnologije koje su primijenjene na društvenim mrežama omogućile su da psihološka djelovanja napadača budu optimizirana prema društvenim slabostima ciljanih publika. One čine osnovu novih instrumenata moći s pomoću kojih se na učinkovitiji način u kiber prostoru vode informacijske, psihološke i medijske operacije.

490 Akrap, 2019.



Izvor: Akrap, 2009., Informacijske strategije i oblikovanje javnoga znanja.

Slika 21. „Promjena težišta strateškog djelovanja ratnih operacija tijekom vremena.“

Slika 21. pokazuje da je u skladu s opisanim razvojem novih tehnika i tehnologija došlo do promjene gravitacijskog središta djelovanja, odnosno težišta djelovanja u prostoru u kojem je moguće steći odlučujuću prednost. Iz prikaza jasno proizlazi da je novo težište strateškog djelovanja u 21. stoljeću postao um osobe, grupe, zajednice; pojedinačni i grupni kognitivni procesi s ciljem oblikovanja njihovih mišljenja, stavova, zaključaka, odluka, kako bi se utjecalo na njihovo djelovanje i na percepciju stvarnosti koja se ne temelji na istini i činjenicama.[491]

U hibridnim sukobima podaci o društvenim slabostima primarno se prikupljaju pomoću društvenih mreža na osnovi podataka o uvjerenjima, načelima i vrijednostima ciljanih publika. Da bi se postojeće slabosti društva iskoristile na što učinkovitiji način, društvene mreže koriste se za stvaranje dezinformacija iz razloga što na njima dezinformacije mogu biti prilagođene društvenim slabostima. Ovakvim dezinformacijama jednostavnije se produbljuju postojeće slabosti za vlastite ciljeve, a društvene mreže ujedno služe da se dezinformacijama povećava vidljivost u protivničkom korpusu javnog znanja te da se na taj način dodatno pojačavaju ostale forme prijetnji ciljanim publikama. Dezinformacije su učinkovitije jer su automatizirane, masovne, anonimne i optimizirane. Zbog toga, onaj tko njima upravlja može ih jednostavnije poricati. Mogućnost poricanja vlastitog djelovanja, skrivanje namjera i ciljeva jedno je od temeljnih obilježja hibridnih sukoba. Brzi i sveobuhvatni razvoj informacijskih i komunikacijskih tehnologija, sredstava i tehnika, razvoj društva u smjeru njegove digitalizacije

491 Akrap, 2009., str. 77.-151. (23.02.2022.)

i stvaranje snažne ovisnosti o digitalizaciji stvorili su uvjete za gotovo potpunu promjenu paradigme u procesima nametanja svoje volje drugima.[492]

Promjenu paradigme omogućila je automatizacija obrade potrebnih podataka, masovnost, anonimnost i optimiziranost dezinformacija. Neprimjetnost dezinformacija u primateljevom sustavu jedna je od odlika hibridnih sukoba. Međutim, jednako tako i drugi instrumenti hibridne moći prilagođavaju se da ostanu ispod očitih pragova otkrivanja i međunarodnopravnih odgovora. Raznolikost primijenjenih taktika maskiranih u planirani redoslijed stvaranja prijetnji omogućile su društvene mreže. Njihova anonimnost u stvaranju, automatizacija i masovnost u širenju i u optimizaciji prema društvenim slabostima omogućila je primjenu taktika koje zamagljuju razlike između rata i mira. Primjenom lažnih profila identitet napadača na društvenim mrežama ostaje prikriven. Značajnu, ako ne i presudnu, ulogu osim lažnih profila pri tome igra brzina i volumen dezinformacija koje se pomoću društvenih mreža ubacuju u protivnički korpus javnog znanja. Stoga nema jasnih razlika između aktivnosti vojske i civila, a informacijsko-psihološke pritiske moguće je provoditi kroz čitav spektar instrumenata moći, uz stalnu prijetnju kinetičkom silom. Upravo zbog toga dezinformacije nije jednostavno predvidjeti, kako i u kojem stupnju bi se pojedini instrumenti moći mogli pojavljivati te kako će biti sinkronizirani. Hibridne sukobe zato je teško prepoznati na vrijeme pa su otežane i sposobnosti obrane te postupci donošenja odluka i reagiranja. Kao informacijski instrument moći, društvene mreže ključne su u cjelokupnom procesu nametanja napadačeve volje i postizanju stanja informacijske nadmoći nad primateljevim informacijskim i medijskim sustavom.

Hibridne sukobe primarno promatramo kroz formu psiholoških operacija u kojima primjena hibridne inteligencije na društvenim mrežama omogućava učinkovito uobličavanje podataka, obavijesti i informacija. Lažni profili omogućavaju neprimjetnost psihološkog djelovanja napadača. Hibridnom inteligencijom i lažnim profilima moguće je učinkovitije zadobiti podršku ciljanih publika za vlastite ciljeve. Višedimenzionalne tehnologije na prilagodljive asimetrične i sinkronizirane forme utjecaja ovdje daju ključan doprinos.[493] Kombiniranje informacijsko-psiholoških pritisaka na ovako dizajniran način i korištenje dezinformacija kojima se društvene slabosti nastoje dodatno produbiti u kombinaciji s drugim instrumentima

492 Akrap, Mandić, 2020.

493 Akrap, 2019.

hibridne moći, hibridnim sukobima daju višedimenzionalnost i sinergiju, a ciljanim publikama nameće se veća neizvjesnost i nemogućnost pravovremenog otkrivanja i odvraćanja prijetnji.

Hibridni sukobi nalikuju trajnom stanju sukoba u kojem se intenzitet sukoba mijenja i prilagođava specifičnim društvenim slabostima i razinama otpornosti ciljanih publika. Popularnost i globalna dostupnost društvenih mreža ključni su čimbenici koji omogućuju da se težište informacijske borbe s vojnih simbola kroz kiber prostor učinkovitije prebaci na kulturne, društvene i ideološke simbole. Moć automatiziranog umrežavanja, globalna komunikacija i razmjena podataka, obavijesti i informacija u realnom vremenu postala je neizbježna i poželjna za planiranje i izvođenje psiholoških operacija u kiber prostoru. Hibridni sukobi su zbog toga nelinearni, decentralizirani, fluidni, neizravni, amorfni i dodatno teže predvidljivi. Sposobnost stalnog obavljanja dubinskih analiza specifičnih izazova, povezanih aktera i strategija postala je ključna sposobnost u planiranju i upravljanju sukobima. Društvene mreže omogućile su potpuno razumijevanje informacijskog okruženja, a time su doprinijele kvalitetnijim odlukama. Mogućnost otkrivanja slabosti društva na osnovi automatiziranog analiziranja uvjerenja, načela i vrijednosti u stvarnom vremenu predstavlja ključnu novost. Hibridne sukobe, dakle, primarno promatramo kroz interes napadača da pomoću informacijsko-komunikacijskih sustava i tehnologija koje (pre)oblikuju uvjerenja, načela i vrijednosti na društvenim mrežama, preko kiber prostora kroz psihološke operacije iskorištava protivničke slabosti i ranjivosti. Psihološkim operacijama nastoji potaknuti niz destruktivnih manifestacija i ostvariti njihovu sinergiju, a da ciljane publike nisu potpuno svjesne da ovakva djelovanja pogađaju sve sektore društva i države.[494]

Dva dodatna obilježja hibridnih sukoba su njihova asimetrična i subverzivna priroda. Pod asimetričnom prirodom hibridnih sukoba podrazumijevamo iskorištavanje nekinetičkih visokotehnoloških multidisciplinarnih i neizravnih pristupa kojima napadač nastoji poremetiti protivničku psihološku ravnotežu.[495] Neizravni pristupi i narušavanje protivničke psihološke ravnoteže dio su psiholoških operacija iz asimetričnog ratovanja u kojem državni akteri za

494 Usp. Danyk Yuriy, Zborovska Oleksandra Development and Implementation of a new Concept of Crisis situation syndrome: Syndrome of a Hybrid War, Eureka, Health Sciences, Number 6, 2018., dostupno na: http://eu-jr.eu/health/article/view/797

495 Pod neizravnim pristupima podrazumijeva se iskorištavanje neočekivanih i neizravnih taktika kako bi se ciljanim publikama poremetila psihološka ravnoteža. Usp. Liddell Hart, B. H., The Strategy of Indirect Approach, Internet Archive, 1954. Dostupno na:

https://archive.org/stream/strategyofindire035126mbp/strategyofindire035126mbp_djvu.tx

vlastite ciljeve koriste nedržavne aktere protiv drugih državnih aktera. U hibridnim sukobima ova paradigma je promijenjena. U hibridnim sukobima državni i nedržavni akteri djeluju koordinirano i u sinergiji kako bi državni akteri izbjegli međusobnu direktnu kinetičku konfrontaciju. Neizravni pristupi i narušavanje psihološke ravnoteže protivnika u hibridnim sukobima provodi se kroz kiber prostor, a društvene mreže pritom igraju važnu ulogu zbog niza prednosti. Psihološke operacije koje se izvode pomoću društvenih mreža kombiniraju se s gospodarskim, političkim, diplomatskim i drugim oblicima pritisaka i služe za učinkovitije stvaranje različitih prijetnji. Društvene mreže pri tom daju veliki doprinos budući da je pomoću njih protivnički korpus javnog znanja moguće zagušiti masovnim, automatiziranim, anonimnim i optimiziranim dezinformacijama koje se usmjeravaju prema pojedinačnim, grupnim ili masovnim ciljanim publikama, lokalno, regionalno ili globalno – ovisno o taktičkim i strateškim potrebama napadača a sve sukladno utvrđenim razinama slabosti ciljanih publika.

Pod subverzivnom prirodom hibridnih sukoba podrazumijevamo upotrebu širokog spektra nedržavnih i nevojnih sposobnosti kojima se ciljane publike preko kiber prostora s pomoću društvenih mreža izlažu učinkovitijim konstantnim (24/7) informacijsko-psihološkim pritiscima. Subverzivne aktivnosti, kako se objašnjava u Cambridgeovu rječniku, označavaju pokušaje izazivanja promjena ili slabljenja vlada radeći potajno unutar njenog teritorija. Ovo je cilj i kod asimetričnog ratovanja. Međutim, u hibridnim sukobima subverzivno djelovanje podrazumijeva suptilnije metode narušavanja društvenog i moralnog integriteta.[496]

Subverzivna priroda hibridnih sukoba podudarna je teoriji ruskog znanstvenika i teoretičara informacijskog ratovanja Evgenija Eduardovicha Messnera (1891.-1974.) koji je, tada, buduće sukobe predvidio kao primarno subverzivne. Prema Messneru, subverzivni ratovi primarno se odvijaju u psihološko-informacijskoj dimenziji. Umjesto vojski, glavni akteri su društveni pokreti i cjelokupno stanovništvo.[497] Prema Messneru, preko informacijsko-psihološke dimenzije, društveni pokreti i cijela društva postali su subjekti političkih sukoba i ratova. Svoju tezu o subverzivnim sukobima i ratovima Messner je temeljio na fenomenima tadašnjih revolucija u kojima su se preko informacijsko-psihološke dimenzije rušile tadašnje protivničke ideološke pozicije, psihološka moć i produbljivale podjele. Prema Messneru, sve veća uključenost društvenih pokreta i cjelokupnog stanovništva u političke i vojne poslove učinila ih

496 Usp. Caliskan Murat, Cramers Paul-Alexander, What Do You Mean by Hybrid Warfare? A Content Analysis on the Media Coverage of Hybrid Warfare Concept, 2018. dostupno na https://www.researchgate.net

497 Fridman, 2017.; prema Messner, Myatezh.

je primarnim metama informacijsko-psiholoških pritisaka. Glavni cilj subverzivnog djelovanja jest rušenje ideoloških položaja, unošenje podjela i društvenog nesklada.[498]

Iznesena Messnerova teorija i predviđanja savršeno odgovaraju onome što danas predstavljaju hibridni sukobi i čemu danas svjedočimo u kiber prostoru. Informacijsko-psihološku dimenziju o kojoj govori Messner danas predstavlja kiber prostor, društvene mreže predstavljaju učinkovite instrumenti moći i alate pomoću kojih su društveni pokreti i cijela društva postali sudionici sukoba i pomoću kojih se dezinformacije na učinkovit način usmjeravaju na njihova uvjerenja, vrijednosti i načela sa svrhom rušenja ideoloških položaja i unošenje podjela.

Sasvim je opravdano tvrditi da su hibridni sukobi u virtualnom, kiber prostoru razvili obilježja novih formi ideoloških i političkih ratova. U američkom RAND-u ovaj fenomen opisuju formom društvenog ratovanja u virtualnom prostoru.[499] Prema definiciji koju daje RAND, društveno ratovanje predstavlja namjernu i plansku informacijsku agresiju pomoću novih tehnoloških rješenja koja nude računalne tehnologije i sustavi, a ima za cilj narušiti temeljne gospodarske i društvene funkcije protivnika. Ono je virtualno jer uglavnom ne uključuje izravno fizičko nasilje ili uništenje kritičnih infrastruktura, atribut društvenog ima jer se proteže kroz cijelo društvo s ciljem narušavanja njegovog funkcioniranja, međusobnog povjerenja i društvene stabilnosti. Atribut ratovanja sadrži jer napadač nastoji postići informacijsku nadmoć. Uvođenjem „virtualnog društvenog ratovanja“ kao nove forme sukobljavanja i ratovanja u kiber prostoru autori nastoje ukazati na doseg višedimenzionalnih tehnologija u upravljanju procesima s podacima i informacijama u kiber prostoru te na moć iskorištavanja protivničkih slabosti i mogućnosti (pre)oblikovanja uvjerenja, načela i vrijednosti ciljanih publika u korist napadača pomoću društvenih mreža. Društvene mreže prostor virtualne „stvarnosti“ učinile su globalno dostupnim. Neupitno da će tehnologije umjetne inteligencije koje se koriste u prostoru „virtualne stvarnosti“ u skoroj budućnosti ovaj prostor učiniti poprištem novih formi sukobljavanja kako bi se utjecalo na djelovanje i na percepciju stvarnosti koja se ne temelji na istini i činjenicama s dalekosežnijim posljedicama. Društvene mreže, duboko učenje, strojno učenje, rudarenje podataka, složeniji oblici umjetne inteligencije, mobilne aplikacije, pametni telefoni predstavljaju infrastrukturu i tehnologije pomoću kojih se na učinkovitije načine iskorištavaju društvene slabosti. Dodatnim usavršavanjem ovih tehnologija umjetna inteligencija moći će samostalno stvarati umjetne i automatizirane dezinformacije, moći će

498 Ibid.

499 Mazarr i sur., 2019.

oponašati stvarne osobe i stvarati realnije sintetičke tekstove, video i audio sadržaje te fotografije[500] koje će različiti akteri koristiti za produbljivanje podjela, izazivanje sukoba i narušavanje protivničkih političkih, ekonomskih i ideoloških položaja. Razumijevanje ovih procesa tek je u nastajanju, no jasno je da ovu snažnu tehnološku tranziciju društva diktiraju tehnologije umjetne inteligencije koje na društvenim mrežama nisu na adekvatan način regulirane.

„Primjena višedimenzionalnih tehnologija u procesima obrade podataka i informacija, nepostojanje adekvatnih pravila ponašanja u kiber prostoru i na društvenim mrežama posljednjih 30 godina dovelo je do hibridnih multimodalnih oblika sukobljavanja.“[501] Zapadna literatura povezuje ih s nizom prijetnji koje imaju za cilj nametanje volje izazivanjem i potenciranjem destabilizacijskih procesa političkog, društvenog ili sigurnosnog predznaka kroz kiber prostor te za umreženo i globalno komuniciranje uz postojanje stalne prijetnje uporabe kinetičke sile, kroz međusobnu povezanost takvih prijetnji s upotrebom digitalnih informacijsko-komunikacijskih sustava i tehnologija.

500 Usp. Ibid.

501 Akrap, 2019.

5. NOVI INSTRUMENTI MOĆI: HIBRIDNE PRIJETNJE I HIBRIDNE OPERACIJE

5.1. Hibridne prijetnje kao nova paradigma prijetnji iz kiber prostora

Globalnom dostupnošću tehnologija umjetne inteligencije i informacijsko-komunikacijskih sustava na osnovi kojih su društvene mreže ljudsku komunikaciju učinile globalnom i masovnom pojavom, proširio se krug aktera koji takve tehnologije i sustave koriste za ciljeve informacijskih strategija. Novi komunikacijski sustavi i tehnologije kratkoročnim ili dugoročnim (pre)oblikovanjem uvjerenja, načela i vrijednosti ciljanih publika omogućili su ostvarivanje ovih ciljeva, bez otkrivanja ili prelaska bilo kakvog jasnog praga za odgovorom na prijetnje koje stvaraju.[502] Informacijsko-psihološki pritisci na ciljane publike preko kiber prostora pomoću društvenih mreža time su evoluirali u nove složene oblike koji zahtijevaju identifikaciju i kategorizaciju. Spomenute promjene paradigme sukoba i ratova: u redoslijedu korištenja instrumenata moći (kao i u njihovom redoslijedu uporabe), ciljeva koji se napadaju (došlo je i do promjene redoslijeda meta koje se napadaju primarno, sekundarno i tercijarno) i u domenama koje su meta napadačkih aktivnosti, dolazimo u situaciju da moramo prepoznati, razumjeti i redefinirati nove prijetnje.[503]

Četvrta industrijska revolucija 21. stoljeća dodatno je potaknula sinergiju kiber prostora i umjetne inteligencije te je ubrzala eksponencijalno širenje i upotrebu strojnog učenja.[504] Koncepti prijetnji, ratovanja i sukobljavanja na osnovi mogućnosti zloupotreba hibridne inteligencije i srodnih tehnologija u planiranju i izvođenju prijetnji u kiber prostoru dio su materije koja se sve snažnije izučava unutar strateških studija[505] i obavještajnih studija[506]. Mogućnosti primjene hibridne inteligencije u stvaranju novih obrazaca prijetnji u kiber prostoru postale su ključno i najrelevantnije pitanje koje se trenutno razmatra unutar obrambene, akademske i sigurnosne zajednice. Ključnu komponentu koja konfigurira aktualni obrazac

---

502 Usp. Akrap, Mandić, 2020.

503 Ibid.

504 Usp. Gonçalves, Carlos Pedro, *Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats*., 2019., str. 1., dostupno na: https://www.intechopen.com/chapters/68561

505 Ibid. Strateške studije uključuju proučavanje strategija, križanje različitih disciplina, uključujući vojnu znanost, znanost odlučivanja, političke znanosti pa čak i znanost o sustavima i kognitivne znanosti.

506 Ibid. Pod inteligencijom autor podrazumijeva sve aktivnosti koje su uključene u proizvodnju znanja potrebnog za strateško i/ili taktičko odlučivanje. Studije obavještajne službe su, dakle, područja istraživanja koja se bave svim aktivnostima uključenim u takvu proizvodnju znanja, uključujući, ali ne ograničavajući se na špijuniranje.

prijetnji i taktika koje se planiraju i izvode kroz sukobe u kiber prostoru čine hibridne strategije i hibridne taktike.

Primjena hibridnih strategija i taktika ostvaruje se operacijama utjecaja koje se planiraju i izvode u kiber prostoru pomoću tehnologija umjetne inteligencije.[507] Hibridna strategija podrazumijeva stvaranje sinergijskih učinaka tradicionalnih operacija utjecaja i netradicionalnih operacija utjecaja koje se planiraju i izvode pomoću informacijsko-komunikacijskih sustava i tehnologija umjetne inteligencije.[508] Hibridne taktike podrazumijevaju korištenje prednosti višestrukih (lažnih) taktičkih računa na društvenim mrežama i primijenjenu automatizaciju u generiranju dezinformacija kako bi se ciljanim publikama isporučile one dezinformacije koje će na najučinkovitiji način privući njihovu pozornost te kako bi ih publike učinkovito diesminirale. Radeći s podacima algoritmi strojnog učenja na društvenim mrežama mogu se uvježbati u predviđanju struktura informacijskih sadržaja koji će pospješiti njihovu diseminaciju. Ova mogućnost dodatno pridonosi da su dezinformacije neprimjetne i aktualne. Upotrebom taktičkih lažnih računa i različitih taktičkih alata u kiber prostoru, poput hashtagova i botova, dezinformacije se učinkovito diseminiraju u korpus javnog znanja ciljanih publika.[509]

Sinergija kiber prostora, društvenih mreža i umjetne inteligencije podigla je razinu prijetnji koje proizlaze iz kiber prostora, čineći takve prijetnje središnjim dijelom onog što se naziva hibridnim prijetnjama. Hibridne prijetnje predstavljaju novi koncept subverzivnog djelovanja u kiber prostoru kroz nekinetičke operacije utjecaja, a služe kako bi se na strateškoj razini narušili strateški interesi konkurenata.[510] Kad se hibridnim prijetnjama u nekom trenutku sukoba pridoda kinetički element (oružana prisila) onda se govori o hibridnom ratu kojem, u pravilu, prethode hibridni sukobi i hibridne prijetnje. Koncept hibridnih prijetnji predstavlja ključnu brigu za obrambene i sigurnosne zajednice. Hibridne operacije koje su omogućene i poboljšane

507 Usp. Atkinson, Carol, "Hybrid Warfare and Societal Resilience: Implications for Democratic Governance, Information & Security, An International Journal 39, no. 1., 2018, str. 63-76. Dostupno na: http://dx.doi.org/10.11610/isij.3906

508 Gonçalves, 2019., str. 1.

509 Usp. Ibid., prema; Nemr C, Gangware W. Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age. 2019.

510 Akrap, 2019.

kroz kiber prostor, povećale su opseg, učestalost, brzinu i razine prijetnji upravo zbog sinergije koja proizlazi iz upotrebe rješenja koja se temelje na upotrebi kiber prostora i strojnog učenja.[511]

Mogućnosti (pre)oblikovanja podataka, obavijesti i informacija u dezinformacije, optimiziranje dezinformacija prema društvenim slabostima, njihovo masovno automatizirano i anonimno diseminiranje predstavlja ključnu paradigmatsku promjenu u planiranju i izvođenju operacija utjecaja u kiber prostoru. Ove mogućnosti čine bitnu komponentu hibridnih strategija taktika i prijetnji. Prijetnje koje se stvaraju pomoću informacijsko-komunikacijskih sustava i tehnologija umjetne inteligencije (strojnog učenja, rudarenja podataka i dr.) u kombinaciji s primjenom hibridne inteligencije postaju složenije i teže uočljive. Hibridne prijetnje promatraju se kroz stvaranje informacijsko-psiholoških pritisaka izvan konteksta oružanih sukoba, odnosno odvijaju se i izvode preko kiber prostora za vrijeme mira, kriza i poraća. Dakako, hibridne prijetnje mogu biti i dio priprema za rat.

Sve donedavno informacijske i psihološke operacije koje se planiraju i izvode u kiber prostoru predstavljale su specifičnu podskupinu aktivnosti koje su bile isključivo vezane za obrambena i sigurnosna pitanja u kontekstu vojnog djelovanja, odnosno rata. Hibridnim prijetnjama opisuje se nova paradigma napadačkih psiholoških operacija utjecaja u kiber prostoru koje se planiraju i izvode uz pomoć tehnologija umjetne inteligencije i u kojima se zloupotrebljavaju osobna uvjerenja, načela, vrijednosti i hibridna inteligencija. Ove znakovite promjene u napadačkim aktivnostima kroz kiber prostor ostvarene su zahvaljujući globalnoj dostupnosti društvenih mreža i neadekvatnoj reguliranosti njihove upotrebe. Na osnovi njih nastale su značajne promjene u procesima, vektorima i instrumentima napada i utjecaja kojima napadač, koristeći kiber prostor, ciljanim publikama učinkovitije nameće svoju volju i postiže informacijsku nadmoć. U svim ovim aktivnostima društvene mreže omogućile su napadaču da, prema vlastitim potrebama, stvara hibridne prijetnje i pojačava informacijsko-psihološke pritiske. Prijetnje i pritisci primarno su usmjereni na narušavanje političke, gospodarske i sigurnosne stabilnosti država. Primjerice, Europsko Vijeće navodi kako su društvene mreže izvorište hibridnih prijetnji poput kiber tehnoloških napada, dezinformacijskih kampanja i uplitanja u izborne procese.[512]

511 Gonçalves, 2019.

512 Europsko Vijeće, Vijeće Europske unije: https://www.consilium.europa.eu/hr/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/

Hibridne prijetnje odnose se na širi raspon metoda ili aktivnosti koje neprijateljski raspoloženi državni ili nedržavni akteri koriste na koordiniran način kako bi ciljali društvene slabosti demokratskih država i institucija, a realiziraju se ispod praga formalno objavljenog rata.[513] Najznačajnije društvene slabosti koje se iskorištavaju za potrebe stvaranja hibridnih prijetnji jesu unutarnji sukobi, podijeljenost društva, nedostatak političke suglasnosti o upravljanju budućnošću društva i države između struktura na vlasti i opozicije, korupcija, neučinkovitost u provođenju zakona, nedostatak prirodnih resursa i ovisnosti o vanjskim faktorima itd.[514]

Oznaka 'hibridnosti' često se koristi naizmjenično s drugima kao što su 'ispod praga' ili 'sive zone' djelovanja, ali karakteristike temeljnih pojava ostaju iste.[515]

Koncept hibridnih prijetnji koji je dao Zajednički istraživački centar Europske komisije i Europski centar izvrsnosti za suzbijanje hibridnih prijetnji[516], može se sažeti na sljedeći način: podrazumijevaju neprijateljske aktivnosti u kojima se namjerno kombinira i sinkronizira djelovanje, posebno ciljajući ranjivosti unutar sustava demokratskih društava, na načine koji izvore imaju u taktikama autoritarnih država, revizionističkih sila, odmetničkih država i nedržavnih aktera, koji nastoje potkopati sustave demokratskih država, pokušavaju održati svoju moć, vršiti kontrolu i oslabiti protivnike.[517] Koncept također naglašava namjeru koja je skrivena iza ovakvih radnji i koja se može okarakterizirati sljedećim:

- Korištenje više sinkroniziranih sredstava (u načelu, nevojnih) i linearnih i nelinearnih učinaka;
- Stvaranje dvosmislenosti (prikriveno i uvjerljivo poricanje) i skrivanje stvarne namjere;
- Pokazivanje namjerne manipulacije u 'sivoj zoni' djelovanja kada u pitanje dolazi otkrivanje i davanje odgovora;
- Iskorištavanje višeslojnosti i različitih jurisdikcija demokratskih društava;

---

513 Akrap, 2019.

514 Yanakiev Yantsislav, Dimov Petko i Bachvarov Daniel, Conceptualizing The Role of Societal Resilience In Countering Hybrid Warfare, Information & Security: An International Journal, 2018, str. 77-89, https://doi.org/10.11610/isij.3907

515 Heap Ben, Hansen Pia, Gill Monika, Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, NATO Strategic Communications Centre of Excellence, Riga, 2021.

516 Giannopoulos Georgios, Smith Hanna, Theocharidou Marianthi, The landscape of Hybrid Threats: A conceptual model, 2021. Dostupno: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

517 Ibid.

- Često uključuje element koji odvlači pažnju, poput aktivnosti koje su usmjerene na jedno mjesto dok se stvarna meta nalazi negdje drugdje.[518]

NATO Centar za stratešku komunikaciju taksativno navodi vrste hibridnih prijetnji i pripadajuću stratešku logiku djelovanja takvih prijetnji prema ciljanim publikama.[519]

Vrste hibridnih prijetnji:

- stvaranje izravnog utjecaja na javno mnijenje;
- pogoršavanje društvenih podjela;
- agitacija i građanski nemiri;
- uplitanje u izborne procese u drugim državama;
- smanjenje povjerenja ciljanih publika u nositelje vlasti;
- potkopavanje upravljanja i državnih funkcija u drugim državama;
- operacije utjecaja u kiber prostoru;
- poticanje na terorizam i nasilni ekstremizam;
- diplomatski pritisci;
- ekonomske poluge;
- špijunaža;
- teritorijalni sporovi.

Strateška logika hibridnih prijetnji predstavljena je kroz niz međusobno povezanih aktivnosti koje imaju različite taktičke ciljeve sa strateškim posljedicama:[520]

- Strateška logika stvaranja izravnog utjecaja na javno mnijenje podrazumijeva osnivanje, financiranje ili davanje potpore akademskim, obrazovnim ili kulturnim institucijama, uspostavljanje pratećih medija i kanala vijesti, uspostavljanje vlasništva nad medijima i reklamne kampanje; stvaranje pritisaka na novinare i širenje dezinformacija;
- Strateška logika pogoršavanja društvenih podjela podrazumijeva financiranje, podržavanje i promicanje nacionalnih, vjerskih ili političkih ekstremističkih organizacija; nastojanja za polarizacijom političkih rasprava radi potkopavanja određenog političkog programa; iskorištavanje etničkih ili kulturnih identiteta za potkopavanje društvene kohezije.

518 Ibid.

519 Heap i sur. 2021.

520 Ibid.

- Strateška logika agitacije i građanskih nemira podrazumijeva agitiranje ciljanih društvenih, kulturnih, vjerskih ili etničkih skupina pozivanjem na promjenu politike ili iniciranje prosvjeda u ciljanoj naciji; podrazumijeva remećenje političkih ili gospodarskih procesa prosvjedima ili bojkotima te povećanje rizika od radikalizacije i eskalacije nasilja.
- Strateška logika uplitanja u izborne procese u drugim državama ima za cilj uplitanja vanjskih aktera u izborne procese u drugim državama radi utjecaja na biračko ponašanje ciljanih publika.
- Strateška logika smanjenja povjerenja ciljanih publika u nositelje vlasti podrazumijeva aktivnosti koje imaju za cilj smanjivati povjerenje javnosti u vladu i vojsku; diskreditirati ciljane vlade i javne institucije; potkopavati vjerodostojnost i legitimnost njezinih politika i operacija te stvarati javnu nesigurnost kroz isticanje društvenih slabosti kao što su korupcijski skandali, ucjene i iznude.
- Strateška logika potkopavanja upravljanja državnih funkcija podrazumijeva strano državno pokroviteljstvo političkim strankama ili političkim akterima; poticanje korupcije, stvaranje kriminalnih mreža i organiziranog kriminala te uspostavljanje paralelnih neformalnih struktura vlasti kroz informacijske, obrazovne (…) sustave u drugoj državi.
- Strateška logika diplomatskih pritisaka je smanjiti diplomatske i domaće opsege djelovanja ciljane vlade putem pritisaka, prijetnji upotrebom sile, zastrašivanja, prisile i povećavanjem ovisnosti; diskreditirati ciljanu vladu i narušiti njezin međunarodni ugled, pogoršati njezine odnose s međunarodnim partnerima i saveznicima; povećati rizik da ciljana država postane platforma za proxy sukobe te u potenciranju regionalne nestabilnosti.
- Strateška logika ekonomskih poluga je u stvaranju ekonomskog pritiska ili energetske ovisnosti; korištenje sankcija.
- Strateška logika kiber operacija utjecaja je u izazivanju poremećaja u komunikacijskim tokovima i digitalnim infrastrukturama; pokazivanju namjera i sposobnosti; stvaranju psiholoških učinaka, poticanju javne nesigurnosti i smanjivanju povjerenja te političkom i javnom sramoćenju.
- Strateška logika terorizma i nasilnog ekstremizma podrazumijeva poticanje nacionalnog, vjerskog i političkog ekstremizma; povećavanje rizika od domaćeg terorizma, oživljavanje bivših terorističkih organizacija; potenciranje etnički motiviranih djela nasilja te izazivanje eskalacija društveno-političkih protesta i sektaškog nasilja.

- Strateška logika teritorijalnih sporova je u izazivanju regionalne nestabilnosti; prelijevanju učinaka na druge teritorijalne sporove; stvaranju separatističkih regija unutar državnih granica i jačanju separatističkih pokreta.
- Strateška logika špijunaže je u stvaranju financijskih, fizičkih, sigurnosnih i reputacijskih šteta i gubitaka radi smanjivanja povjerenja javnosti u institucije; špijunaža u tom kontekstu može biti korporativna, kiber i politička.

Glavna ideja hibridnih prijetnji usmjerena je prema ciljanim publikama na više razina i na više područja:[521]

1) na slabljenje obrane;
2) na ciljanje društva njegovim vlastitim slabostima;
3) destabiliziranje i poticanje da donose odluke od volje napadača;
4) utjecanje na prostor javnog znanja.

Navedene i opisane strateške logike i glavne ideje hibridnih prijetnji planiraju se i izvode operacijama utjecaja u kiber prostoru koje se, kako je prethodno navedeno, i same promatraju kao hibridna prijetnja koja se kroz ovu vrstu operacija utjecaja usmjerava na četiri glavne ideje prijetnji, kroz njih nastoji iskoristiti sve društvene slabosti ciljanih publika te se, na osnovi toga, kroz kiber prostor nastoji potkopavati autoritet i dovoditi u pitanje legitimitet vlasti. Ciljanje slabosti nekog društva ili države odgovara onome što je Margolis identificirao kao izvore tri vrste kriza:[522]

- krize vlasti (autoriteta) koje proizlaze iz nesposobnosti države da provodi vladavinu prava i nesposobnost da kontrolira vlastiti teritorij odnosno da provodi vlastite zakone;
- krize otpornosti koje proizlaze iz nesposobnosti države da se prilagodi različitim poremećajima;
- krize legitimiteta koje proizlaze iz stava društva da je vlast izgubila pravo na vladavinu jer je pogrešna ili nepravedna.

521 Akrap, Mandić, 2020.

522 Gonçalves, 2019., str. 6.; prema Margolis JE. Estimating state instability. Studies in Intelligence, 56(1), 2012, str. 3-24. Available from: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-1/pdfs-vol-56.-no.-1/Estimating%20State%20Instability%20-Extracts-Mar12-20Apr12.pdf [Accessed: April 24, 2019]

Slika 22. Hibridne prijetnje kao nova paradigma prijetnji iz kiber prostora.

Slikom 22. želi se prikazati da se opisane vrste kriza u stvarnom svijetu potenciraju iz kiber prostora operacijama utjecaja, u kojima napadač kroz mogućnosti kratkoročnog ili dugoročnog preoblikovanja uvjerenja, načela i vrijednosti ciljanih publika planski i sustavno iskorištava njihove postojeće društvene slabosti kako bi opisane krize usmjeravao u pravcima prema vlastitim težnjama i potrebama.

Glavna metodologija koju različiti akteri koriste za stvaranje učinkovitih hibridnih prijetnji promatra se kroz operacije utjecaja u kiber prostoru, konkretno kroz psihološke operacije koje se planiraju i provode zloupotrebama društvenih mreža i hibridne inteligencije. Psihološke operacije utjecaja u kiber prostoru smatraju se ključnim nositeljima hibridnih prijetnji iz dva razloga. Prvi je u primjeni i mogućnostima zloupotrebe hibridne inteligencije na društvenim mrežama za stvaranje učinkovitih dezinformacija. Drugi je da su, zahvaljujući društvenim mrežama i umjetnoj inteligenciji, u kiber prostoru psihološke operacije zauzele ključnu ulogu u planiranju i provođenju hibridnih strategija i hibridnih taktika za stvaranje hibridnih prijetnji i na učinkovit način provođenje strateške logike takvih prijetnji koje u konačnici imaju za cilj: stjecanje stanja informacijske nadmoći odnosno (pre)oblikovanje korpusa javnog znanja ciljanih publika u korist napadača. Strojno učenje, algoritmi, automatizacija procesa, umjetne neuronske mreže koje na društvenim mrežama obrađuju uvjerenja, načela i vrijednosti, zloupotreba hibridne inteligencije, lažnih računa, mogućnosti stvaranja automatiziranih,

masovnih, anonimnih dezinformacija koje je moguće optimizirati prema društvenim slabostima, jesu ključni čimbenici koje se neupitno koristi za ispunjavanje strateške logike hibridnih strategija, taktika i prijetnji. Evidentno je da se hibridne strategije, taktike i prijetnje u kiber prostoru na najučinkovitiji način realiziraju i stvaraju kombiniranjem dezinformacija i psiholoških operacija na osnovi čega je u stvarnom svijetu moguće planirati i realizirati hibridne sukobe i ratove. Navedene tehnologije koje koriste društvene mreže planerima ovih operacija omogućile su veći stupanj svjesnosti o protivničkom informacijskom okruženju i učinkovitije pokrivanje cijelog spektra djelovanja, od prikupljanja i obrade potrebnih podataka do planiranja i izvođenja samih operacija, stvaranja prijetnji i ostvarivanja strateške logike takvih prijetnji. Ovim dijelom istraživanja potvrđena je hipoteza istraživanja da se u hibridnim sukobima umjetna inteligencija koju koriste društvene mreže koristi kao snažan alat utjecaja za stjecanje informacijske nadmoći. Ujedno je potvrdno odgovoreno na prvo istraživačko pitanje da su društvene mreže i umjetna inteligencija postali dominantni alati utjecaja te su navedena tri ključna razloga: opisane mogućnosti (pre)oblikovanja uvjerenja, načela i vrijednosti u učinkovite dezinformacije, mogućnosti njihove automatizirane, masovne i anonimne diseminacije u korpusu javnog znanja čime se na učinkovitiji način iskorištavaju slabosti društva.

Hibridne prijetnje u kiber prostoru izvan konteksta hibridnog ratovanja postale su time „zamaskirane", sve suptilnije i sve veći sigurnosni izazov za demokratske procese i sigurnost država. Hibridne prijetnje u većoj ili manjoj mjeri jesu tajne radnje. Njihovoj tajnosti doprinosi nekoliko čimbenika. Prvi je da ih provode sigurnosno-obavještajne strukture i službe. Drugi je da se mogu konstantno optimizirati prema potrebama napadača i društvenim slabostima. Treći je mogućnost zloupotrebe lažnih profila i svih drugih mogućnosti strojne, automatizirane, neprekidne i masovne diseminacije dezinformacija. Zloupotreba lažnih profila, hibridne inteligencije uz anonimnost djelovanja, automatiziranost i optimiziranost dezinformacija prema društvenim slabostima dodatno daje prostor za poricanje uloge napadača i za stalno zagušivanje protivničkog korpusa javnog znanja dezinformacijama i strateškim narativima. Zagušivanjem protivničkog korpusa javnog znanja dezinformacijama i narativima napadač za vlastite potrebe može kratkoročno ili dugoročno na učinkovit način preoblikovati uvjerenja, vrijednosti i načela ciljanih publika i nametati im vlastite ideje i ideologije. „Tvorničke postavke" društvenih mreža otežale su pravovremeno prepoznavanje ovakvih prijetnji i podizanje percepcije o izloženosti dezinformacijama. Drugim riječima, omogućile su učinkovito provođenje psiholoških operacija i stvaranje hibridnih prijetnji.

„Hibridne prijetnje važna su novost u promjeni paradigme nedavnih sukoba. Naime, koncept hibridnih prijetnji podrazumijeva stvarnost prema kojoj radnje i procesi na taktičkoj razini mogu dati značajne rezultate na strateškoj razini. Istodobno, nevojna sredstva mogu postići ciljeve u vojnoj i nevojnoj domeni i obrnuto: vojna sredstva mogu snažno utjecati na vojna i nevojna područja. Agresija pomoću nekih aktivnosti iz spektra hibridnih prijetnji može se neprimjetno upotrijebiti prema određenoj ciljanoj publici. Drugim riječima, ciljane publike ne moraju biti svjesne da su pod hibridnim napadom.“ [523] „Hibridne prijetnje, kao skup mogućih pojavnih oblika, planiraju se i izvode operacijama utjecaja u kiber prostoru. Svrha im je usmjereno i organizirano djelovanje prema pojedinoj ciljanoj publici u cilju iskorištavanja (poticanja, produbljivanja) njezinih slabosti, stvaranja novih slabosti, poticanja osjećaja podjela, nesigurnosti, defetizma, nemoći, beznađa, dvojbenosti, sumnjičavosti, narušavanja i urušavanja demokratskih struktura i procesa te slabljenja i kontroliranja obrambenog sustava.“[524]

Temeljem dezinformacija koje su optimizirane i prilagođene društvenim slabostima, planiranje i izvođenje hibridnih prijetnji postalo je jednostavnije i učinkovitije. Nesumnjivo da su takve dezinformacije jedan od najučinkovitijih načina kojim se ostvaruju ciljevi takvih prijetnji s potencijalnim strateškim posljedicama. Kako je pokazano, dezinformacijama koje se planiraju i izvode u psihološkim operacijama u kiber prostoru na osnovi zloupotrebe hibridne inteligencije na društvenim mrežama, moguće je na učinkovit način stvarati i ostale prijetnje kojima napadač, prema vlastitim potrebama, na učinkovit način može ostvarivati više strateških negativnih učinaka na političku, gospodarsku i sigurnosnu stabilnost u drugim državama.

Da bi se bolje razumjelo kako hibridne prijetnje djeluju kao poluge utjecaja na ciljane publike, fokus je potrebno pomaknuti sa stvarnog, fizičkog svijeta u kojem se odvijaju događaji i radnje. Fokus je potrebno usmjeriti na međusobnu povezanost kognitivne, fizičke i informacijske domene kiber prostora i mogućnosti koje hibridna inteligencija ostvaruje u procesima s uvjerenjima, načelima i vrijednostima unutar tih domena. Ključna je mogućnost umjetne inteligencija da, kroz automatizirani sustav povratne sprege analizom ulaznih podataka s društvenih mreža, na osnovi strukturiranih uvjerenja, načela i vrijednosti pojedinaca i zajednica identificira društvene slabosti ciljanih publika te prema njima daje i optimizira rješenja prema

523 Akrap, Mandić, 2020., str. 14.

524 Akrap, 2019.

kojima planer psiholoških operacija prilagođava hibridne prijetnje što ih dodatno čini učinkovitim. Zlouporabom uvjerenja, načela, vrijednosti i umjetne inteligencije moguće je na učinkovitiji način stvarati hibridne prijetnje. Ovim dijelom istraživanja dodatno je potvrđena hipoteza rada te je dodatno potvrdno odgovoreno na prvo i drugo istraživačko pitanje. Hibridni sukobi ne moraju prerasti u hibridni rat jer im višedimenzionalnost sustava povratne sprege omogućava konstantno prilagođavanje i izlaganje ciljanih publika neprestanim (24/7) informacijsko-psihološkim pritiscima i konstantno provođenje strateške logike različitih hibridnih prijetnji, ovisno o potrebama napadača i otpornosti ciljanih publika na takve napade. Hibridni rat koristi se kao krajnja nužnost i krajnji način rješavanja međunarodnih sporova.

5.2. Društvene mreže kao alati za stvaranje hibridnih prijetnji

Na osnovi prikupljanja, pohrane te obrade osobnih podataka korisnika društvenih mreža umjetna inteligencija na društvenim mrežama upravlja i oblikuje obavijesti i informacije. Prema kriterijima koje određuju vlasnici društvenih mreža na njima nastaju nove obavijesti i informacije prema sklonostima i potrebama samih korisnika. Upravljajući osnovnim funkcijama i zadaćama društvenih mreža, umjetna inteligencija upravlja i organizacijom znanja. Društvene mreže tako su postale stvaratelji, nadzornici i posrednici u distribuciji znanja. Stvorene su, prema predviđanjima vojnih stratega s početka 1990-ih, nove mogućnosti i prilike za (pre)oblikovanje načina ljudskog razmišljanja i donošenja odluka. Društvene mreže postale su snažni alati utjecaja i nositelji novih načina stvaranja dezinformacija i drugih formi informacijsko-psiholoških pritisaka i organizacije znanja u korpusu javnog znanja ciljanih publika i u njemu novih načina stvaranja informacijske nadmoći.

Na platformama društvenih mreža ostvarena je sinergija moći kiber prostora i hibridne inteligencije i ova dva čimbenika svestrano se koristi za stvaranje učinkovitih hibridnih prijetnji. Time je osnaženo psihološko djelovanje, a društvene mreže postale su snažni i učinkoviti alati uvjeravanja. Društvene mreže i hibridna inteligencija u kiber prostoru postali su glavni nositelji dezinformacija, hibridnih prijetnji, taktika i strategija. Pomoću društvenih mreža kroz kiber prostor napadači dezinformacijama mogu učinkovitije pojačavati i ostvarivati stratešku logiku svih vrsta hibridnih prijetnji, ovisno o potrebama: produbljivati postojeće podjele i stvarati nove, potkopavati povjerenje ciljanih publika u državne institucije, narušavati stabilnost i pouzdanost činjenica kao i postojećih narativa koji okružuju ciljane publike u njihovom korpusu javnog znanja. Društvene mreže koriste se u borbi za javno mišljenje i

legitimitet vlastitog djelovanja[525] i ostvarivanje političkog utjecaja. Anonimnost, automatiziranost i masovnost dezinformacija optimiziranih prema društvenim slabostima, onome tko zloupotrebljava društvene mreže ne može se pripisati agresija niti se prema takvom akteru mogu primijeniti pravila koja vrijede za oružane sukobe. Stvaranje hibridnih prijetnji na osnovi dezinformacija uobličenih na osnovi uvjerenja, načela i vrijednosti jedna je od ključnih mogućnosti koja se svestrano koristi. O kojoj vrsti hibridne prijetnje će biti riječ ovisi o taktičkim ili strateškim ciljevima napadača i otpornosti ciljanih publika na takve prijetnje.

Umjetna inteligencija koju su vlasnici društvenih mreža primijenili za vlastite potrebe može identificirati društvene slabosti. Također je omogućena zloupotreba hibridne inteligencije i po navedenim osnovama omogućeno je stvaranje hibridnih prijetnji.

Paralelno s digitalizacijom kiber prostora njegovi tvorci nisu uspjeli izgraditi i uspostaviti adekvatna pravila prema kojima bi se reguliralo ponašanje unutar kiber prostora niti su uspjeli izgraditi pravila kojima bi se na društvenim mrežama adekvatno regulirala (zlo)upotreba umjetne inteligencije. Zbog globalne dostupnosti i nereguliranosti društvenih mreža, različiti akteri (državni, nedržavni i korporacije) mogu koristiti tehnologije koje koriste društvene mreže za različite ciljeve. Visokotehnološke korporacije koje razvijaju i upravljaju društvenim mrežama nametnule su vlastita pravila interakcija i komunikacijskog procesa za vlastite potrebe. Izvršena podjela korisnika, mogućnosti anonimnog komuniciranja, ubrzavanja, uobličavanja podataka i informacija u stvarnom vremenu, a bez stvarne i adekvatne odgovornosti za napisanu i podijeljenu riječ, postala su načela prema kojima se u kiber prostoru planiraju i izvode psihološke operacije i u kojima njihovi planeri koriste sve raspoložive tehnologije za stvaranje hibridnih prijetnji.

Primarne mete hibridnih prijetnji postale su kulturni i drugi identitetski simboli ciljanih publika odnosno njihovi temeljni sustavi vrijednosti, uvjerenja i načela s ciljem njihovog kratkoročnog ili dugoročnog preoblikovanja prema potrebama napadača i stvaranja informacijske nadmoći nad protivničkim korpusom javnog znanja. U ovom kontekstu dezinformacije su postale najučinkovitiji način za stvaranje hibridnih prijetnji i stjecanje informacijske nadmoći.

525 Nissen Thomas, The Weaponization of Social Media, Royal Danish Defence College, NATO Strategic Communications Centre of Excellence, Publication, 2015. Dostupno na: https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media

Korištenje dezinformacija u cilju stvaranja prijetnji i informacijske nadmoći nije novost koja je nastala pojavom društvenih mreža. Novost je u brzinama, dometu, neposrednosti i mogućnostima stvaranja dezinformacije prilagođenih društvenim slabostima koje se utvrđuju na osnovi uvjerenja, načela i vrijednosti i na toj osnovi mogućnosti stvaranja ostalih vrsta hibridnih prijetnji.

Brojni primjeri nepobitno ukazuju da različiti akteri koriste trenutno najpopularnije društvene mreže Facebook, Twitter, YouTube kao i aplikacije za dopisivanje Facebook Messenger, WhatsApp, Instagram, Viber, Telegram i druge za učinkovito planiranje i izvođenje hibridnih prijetnji. Nakon nastanka Facebooka, prve društvene mreže sredinom 2000-tih, postalo je evidentno da su informacije u kiber prostoru postale od presudne važnosti za upravljanje, planiranje i izvođenje psiholoških operacija i za ostvarivanje političkih ciljeva izvan konteksta oružanih sukoba ili rata. Društvene mreže su se od komercijalnog proizvoda pretvorile u ključni čimbenik i snažni alat utjecaja za postizanje širih ciljeva. Zahvaljujući „tvorničkim postavkama“ strojnog učenja, procesnog rudarenja podataka, robotske automatizacije podataka, algoritama preporuka i rangiranja sadržaja, informacija je na društvenim mrežama u potpunosti postala strateško borbeno sredstvo za planiranje i izvođenje operacija utjecaja te stjecanje stanja informacijske nadmoći. Ovim je dodatno odgovoreno na prvo istraživačko pitanje.[526] “Informacija je postala četvrti instrument na kojem se pored diplomatske, vojne i gospodarske, temelji moć suvremene države.“[527] Pojavom društvenih mreža nastala je nova paradigma u planiranju i izvođenju psiholoških operacija. Društvene mreže u ovom kontekstu jesu nove potrebne infrastrukture pomoću kojih se planiraju i djelotvorno provode psihološke operacije u kiber prostoru. Ovim je dodatno odgovoreno na drugo istraživačko pitanje. Postalo je očito da su tehnologije umjetne inteligencije koje su primijenjene na društvenim mrežama psihološkim operacijama i dezinformacijama u kiber prostoru omogućile veću učinkovitost nego na tradicionalnim medijskim kanalima. Činjenica je da je globalna upotreba društvenih mreža omogućila da se operacije utjecaja s tradicionalnih tiskanih medija, televizije i radija „premjeste“ prema prostorno bezgraničnom i zakonodavno nedovoljno reguliranom kiber prostoru.

526 Istraživačko pitanje 1. glasi: Postaju li društvene mreže i umjetna inteligencija dominantna sredstva utjecaja za vođenje strateških operacija utjecaja za postizanje informacijske nadmoći preko kojih informacijski napadač želi promijeniti i manipulirati prostorom javnog znanja ciljane publike?

527 Akrap, 2011., str., 38.

Ova činjenica otvorila je nove mogućnosti: stvaranje učinkovitih dezinformacija i na osnovu dezinformacija učinkovitije stvaranje hibridnih prijetnji. Nedovoljno i neadekvatno regulirano korištenje umjetne inteligencije i neadekvatna zaštita osobnih podataka na društvenim mrežama, temeljni su razlozi zbog kojih su hibridne prijetnje postale učinkovitije.

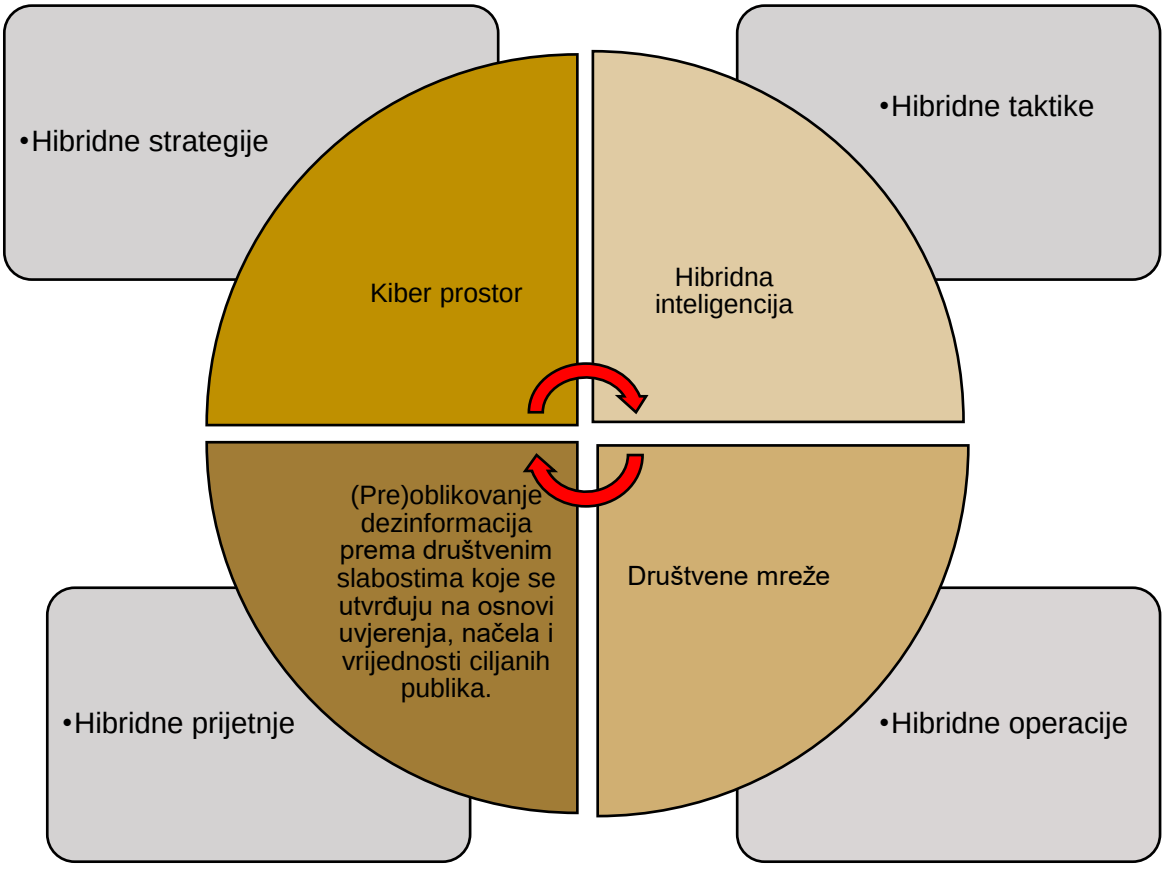
Psihološke operacije koje se u kiber prostoru izvode pomoću društvenih mreža u hibridnim sukobima promatraju se kao ključna metodologija kojom se društvene mreže iskorištavaju kao važan, ako ne i presudan informacijski instrument hibridne moći u realizaciji ciljeva. Društvene mreže na osnovi opisanih zloupotreba jesu glavni napadački alati za stvaranje hibridnih prijetnji i učinkovitiju realizaciju strateške logike takvih prijetnji. Moguće ih je koristiti prema potrebama i zacrtanim ciljevima, moguće ih je usmjeravati prema ciljanim publikama bez otkrivanja ili prelaska bilo kakvog jasnog praga za odgovorom. Ovu vrstu pritisaka omogućila je sinkronizacija kiber prostora i umjetne inteligencije koja se primjenjuje na društvenim mrežama u procesima obrade podataka (uvjerenja, načela i vrijednosti). Nove tehnologije su, kroz obradu ovih podataka u informacijskoj domeni kiber prostora, omogućile stvaranje učinaka u realnom vremenu na kognitivnoj razini ljudskog razmišljanja i na stvarne događaje u fizičkom svijetu. Razumijevanje procesa sinkronizacije kiber prostora i kognitivnih elemenata psiholoških operacija utjecaja kroz primjenu hibridne inteligencije na društvenim mrežama daje bolji uvid u suštinu hibridnih sukoba. Ova činjenica neupitno je dovela do promjene paradigme i stvaranja novog težišta strateškog djelovanja u 21. stoljeću. Kako je prethodno već navedeno, novo težište „postaje um osobe, grupe, zajednice; pojedinačni i grupni kognitivni procesi s ciljem oblikovanja njihovih mišljenja, stavova, zaključaka, odluka, kako bi se utjecalo na njihovo djelovanje i na percepciju stvarnosti koja se ne temelji na istini i na činjenicama.“[528] Druga krajnost je uporaba kinetičke moći koja je rezervirana za hibridni rat kao krajnje sredstvo za nametanje vlastite volje ciljanim publikama, kad u istom cilju, kombiniranje ostalih instrumenata moći ne rezultira željenim interesima i potrebama. Činjenica je da je u psihološkim operacijama, pomoću globaliziranih informacijskih i komunikacijskih sustava, kognitivna domena primarna bojišnica, informacijska domena sekundarna, a fizička tek tercijarna.[529]

Psihološke operacije utjecaja u kiber prostoru s primjenom hibridne inteligencije jesu ključna metoda kojom se na učinkovit način stvaraju hibridne prijetnje organizaciji znanja u

528 Ibid., str. 284.

529 Ibid., str. 37.

protivničkom korpusu javnog znanja. Stvaranje informacijsko-psiholoških pritisaka primarno promatramo kroz dezinformacije i dezinformacijske kampanje. Zahvaljujući društvenim mrežama psihološke operacije postale su višedimenzionalne jer ih je moguće provoditi sa stvarnim učincima u kognitivnoj domeni tj. u razmišljanju i donošenju odluka ciljanih publika sa stvarnim učincima u realnom vremenu u stvarnom svijetu. U kognitivnoj domeni manifestiraju se kroz preoblikovanje mišljenja ciljanih publika, a u stvarnom svijetu manifestiraju se za različite potrebe koje mogu varirati od regrutacije i mobilizacije, organizacije prosvjeda, terorističkih skupina, jačanja ekstremizma i radikalizma do uništavanja ili narušavanja funkcioniranja kritičnih infrastruktura. Društvene mreže omogućile su nove forme prijetnji koje se pomoću njih mogu usmjeravati prema svim razinama ciljanih publika (pojedinačnim, grupnim i masovnim) i prostora (lokalnom, regionalnom, globalnom), ovisno o potrebama napadača. Ovim poglavljem u potpunosti je potvrđena hipoteza rada.



Slika 23. Hibridne prijetnje i hibridne operacije kao nova paradigma prijetnji iz kiber prostora.

Slikom 23. želi se prikazati sinergija kiber prostora, hibridne inteligencije i društvenih mreža za stvaranje učinkovitih dezinformacija koje se osnovom toga mogu (pre)oblikovati prema

društvenim slabostima. Opisana sinergija (označena crvenom bojom) naziva se hibridna moć koja se u hibridnim operacijama, novoj formi operacija utjecaja u kiber prostoru, koristi kako bi se provodile hibridne strategije, taktike i prijetnje. Hibridna moć napadaču omogućava da dezinformacije (pre)oblikovane prema društvenim slabostima sinkronizira s političkim, diplomatskim i gospodarskim instrumentima moći te s vojnim instrumentima moći, ukoliko je to potrebno.

5.3. Hibridne operacije utjecaja

Hibridne operacije utjecaja primarno se promatraju kroz psihološke operacije u kiber prostoru. Promatraju se kroz sinergiju kiber prostora i mogućnosti hibridne inteligencije za stvaranje hibridnih prijetnji pomoću društvenih mreža.

Terminom hibridnih operacija želi se naglasiti moć hibridne inteligencije na društvenim mrežama u (pre)oblikovanju znanja ciljanih publika na osnovi mogućnosti stvaranja učinkovitih dezinformacija i prijetnji koje su nastale kao direktna negativna posljedica organizacije znanja na društvenim mrežama. Ova mogućnost pokazala se iznimno korisnom u planiranju i izvođenju svih kategorija hibridnih prijetnji. U hibridnim operacijama primjena hibridne inteligencije na društvenim mrežama koristi se kao snažno sredstvo utjecaja za planiranje i izvođenje psiholoških operacija u kojima dezinformacije potencijalno mogu imati strateške posljedice: postići stanje informacijske nadmoći u korpusu javnog znanja ciljanih publika. Također, promatraju se kroz sposobnost umrežavanja planera i izvoditelja, različitih (proxy) aktera i ciljanih publika kroz kiber prostor pomoću društvenih mreža. Povezanost ovih čimbenika kroz hibridne operacije ne može se sagledavati odvojeno jer upravo sinergija kiber prostora i umjetne inteligencije, posebice putem strojnog učenja, čini ono što određuje sadašnji strateški i taktički zamah hibridnih operacija. Psihološke operacije u kojima se koristi kiber prostor, društvene mreže i umjetna inteligencija čine osnovu hibridnih operacija.

Hibridne operacije možemo nazvati psihološkim, medijskim, subverzivnim, specijalnim i kognitivnim operacijama u kiber prostoru. Hibridne operacije sadrže osnovne elemente navedenih vrsta operacija. One su primarno usmjerene na um ciljanih publika, a pomoću društvenih mreža kroz kiber prostor moguće je upravljati procesima i usmjeravati ih u željenom pravcu u korpusima javnog znanja ciljanih publika. Cilj ovih operacija je stvarati hibridne prijetnje i produbljivati postojeće krize. U pravilu su strateške prirode i podrazumijevaju pružanje političke podrške ciljanim publikama u drugim državama kako bi se pojačale podjele a, u pravilu, izvode ih državne vojne i civilne obavještajne strukture, bez obzira radi li se o ratu

ili miru. „Brzina promjene i dostupnost objavljenih dezinformacija, mogućnost interakcije primatelja i sadržaja kao i mogućnost prikrivanja autorstva nad dezinformacijama doveli do toga da svijet virtualnog ima neposredne i realne učinke u stvarnom svijetu.“[530] Evidentno da je njihovom porastu i popularnosti doprinio konstantan rast upotrebe društvenih mreža, mobilnih telefona i mobilnih aplikacija za komuniciranje poput WhatsAppa, Vibera, Telegrama, Instagrama, Reddita, Tik toka i drugih. Njihov globalni doseg, popularnost i rasprostranjenost i nedovoljna reguliranost omogućili su planiranje i izvođenje psiholoških operacija u neviđenim razmjerima brzine, dosega, neposrednosti i anonimnosti.

Hibridne operacije koriste se kao glavne poluge utjecaja pomoću kojih se na prilagodljive i višeznačne načine drugoj državi otežava provođenje politika i potkopava učinkovito upravljanje kriznim stanjima. Društvene mreže unijele su paradigmatski pomak u nametanju volje napadača i postale su nositelji kulturnih, društvenih, psiholoških i moralnih dimenzija (nekinetičkih) težišta borbe. Uspjeh na ovim područjima informacijske borbe predstavlja ujedno ključan dio političkog utjecaja država i ostvarivanje uspjeha.

Hibridnim operacijama u kiber prostoru vodi se moderni oblik onog što se naziva političkim ratovanjem. Naime, kiber prostor i društvene mreže omogućile su sinergiju tri ključna elementa političkog ratovanja a to su stvaranje dezinformacija, strateških narativa i suradničkih mreža.[531]

Strateški narativi, u hibridnim strategijama, taktikama, operacijama, sukobima i prijetnjama, djeluju na tri razine: na razini međunarodnog sustava, na razini politika i na razini identiteta. Na razini međunarodnog sustava politički akteri (države, međunarodne organizacije, interesne grupe) strateškim narativima oblikuju percepciju ciljanih publika na željeni način i u željenom smjeru. Na razini politike promiču vlastite interese kako bi utjecali i usmjeravali tijek međunarodnih dogovora ili kako bi posredovali u sporovima između drugih za vlastite potrebe. Na razini identiteta izgrađuju i projiciraju željene prikaze vlastitih identitetskih odrednica. Narativima objašnjavaju situacije, definiraju probleme i/ili nastoje mijenjati početne situacije kako bi pružili vlastito rješenje. Ako politički akteri sa svojim strateškim ciljevima uspiju

530 Ibid., str. 286.

531 Usp. Nestoras Antonios, Political Warfare: Competition in the Cyber Era, Policy Brief, The Wilfried Martens Centre for European Studies, Brussels, 2019. Dostupno na https://martenscentre.eu/publications/political-warfare-competition-cyber-era

uskladiti narative o sustavu, politici i identitetu, to im u međunarodnim odnosima daje veće šanse za povećanje vlastitog utjecaja.[532]

Izgradnja otvorenih i/ili prikrivenih suradničkih mreža predstavlja jednu od metoda psiholoških operacija. U hibridnim operacijama i hibridnim sukobima suradničke mreže stvaraju se preko kiber prostora pomoću društvenih mreža kako bi hibridne prijetnje bile učinkovitije. Društvene mreže omogućavaju njihovo anonimno stvaranje na pojedinačnoj i/ili grupnoj razini. Izgradnja mrežnih organizacija o kojima govore Ronfeldt i Arquilla u svom djelu 'The Advent of Netwar' s početka 1990-ih danas je u potpunosti moguća i ostvariva pomoću društvenih mreža. Pomoću njih se na anoniman način može stvarati utjecaj na utjecajne osobe, grupe i zajednice, među pojedincima i grupama koje bi mogle postati utjecajne ili koje bi mogle najbolje ispuniti postavljene ciljeve i zadaće. Pomoću suradničkih mreža sljedbenika lažnih pojedinačnih i grupnih profila na društvenim mrežama preko kiber prostora hibridnim operacijama mogu se učinkovitije stvarati hibridne prijetnje. Podrivanje političkih procesa, poticanje radikalnih, ekstremističkih ili populističkih elemenata u drugim državama, ovisno o potrebama napadača i društvenim slabostima ciljanih publika, samo su neke od mogućnosti.

Teza o hibridnim operacijama kao obliku političkog ratovanja podudarna je s teorijom ruskog teoretičara o informacijskom ratovanju Igora Panarina: „Politička aktivnost [po svojoj definiciji] je informativna borba za kontrolu uma političkih elita i [drugih] društvenih skupina.“[533] Panarin vođenje informacijsko-psiholoških sukoba promatra kroz sposobnost manipuliranja informativnim slikama koje služe za ostvarivanje političke koristi i za kontroliranje protivničkih informacijskih tokova. To se postiže manipulacijom informacijama, dezinformacijama, izmišljanjem informacija, lobiranjem, ucjenjivanjem ili bilo kojim drugim načinom izvlačenja željenih informacija ili pak pukim demantiranjem protivničkih informacija. Baze velikih podataka o uvjerenjima, načelima i vrijednostima, analitika velikih podataka, botovi, trolovi, memetika, hashtagovi i hibridna inteligencija otvorili su nove mogućnosti u kiber prostoru zbog kojih su društvene mreže postale tako snažni i učinkoviti alati u onome što

532 Roselle Laura, Miskimmon Alister i O'Loughlin Ben, Strategic narrative: A new means to understand soft power, Media, War & Conflict, 2014., str. 3., dostupno na: https://www.researchgate.net/publication/274484086_Strategic_narrative_A_new_means_to_understand_soft_power

533 Fridman, 2017.; prema Panarin 2006.

Panarin naziva „informativnom borbom za kontrolu uma političkih elita i [drugih] društvenih skupina“.[534]

Zbog snažnog djelovanja tehnologija na procese donošenja odluka odnosno učinaka koji se odvijaju u kognitivnoj domeni kiber prostora, hibridne operacije znanstvena i stručna literatura opisuju kognitivnim operacijama odnosno smatraju se dijelom onog što se u njima opisuje kao kognitivno ratovanje.[535] Kognitivne operacije promatraju se kao nova forma utjecaja na um ciljanih publika kroz kiber prostor pomoću tehnologija umjetne inteligencije koje održavaju funkcije društvenih mreža.

Hibridne operacije u kiber prostoru su višeznačne i objedinjavaju sinergiju više segmenata hibridne moći. Kroz informacijske instrumente hibridne moći hibridne operacije objedinjuju diplomatske, ekonomske i financijske instrumente hibridne te vojne instrumente moći kao krajnju mogućnost za rješavanje hibridnih sukoba. U kiber prostoru pomoću društvenih mreža hibridne operacije objedinjuju psihološke operacije i napade na kritične infrastrukture, prijetnje, potenciranje kriza, informacijsko-psihološke pritiske, dezinformacije, zloupotrebe hibridne inteligencije koja nadzire i upravlja uvjerenjima, načelima i vrijednostima u korpusima znanja ciljanih publika. Hibridna inteligencija ovdje ima zadaću povećati učinke dezinformacija i prijetnji na nove učinkovitije načine. U hibridnim operacijama planiraju se i izvode dezinformacijske kampanje i stvaraju se konstantni informacijsko-psihološki pritisci. Kiber napadi na kritične infrastrukture dio su tehnoloških napada koji imaju potpornu ulogu i služe za prikupljanje potrebnih podataka i/ili za stvaranje dodatnih psiholoških pritisaka. Hibridne operacije stoga promatramo kao krovni pojam i aktivnosti kojima se preko kiber prostora pomoću društvenih mreža objedinjuju operacije utjecaja i svi elementi napadačkih informacijskih aktivnosti koje su usmjerene prema ciljanim publikama s krajnjom svrhom: stvaranja učinkovitih hibridnih prijetnji, planskog i smišljenog iskorištavanja društvenih slabosti demokratskih država i institucija te, u konačnici, stjecanja informacijske nadmoći nad korpusom javnog znanja ciljanih publika. Društvene mreže ovdje daju snažan doprinos.

534 Ibid.

535 Brojni autori ovim terminom opisuju procese nametanja napadačeve volje ciljanim publikama pomoću društvenih mreža koje se koriste za planiranje i izvođenje operacija utjecaja u kiber prostoru. Usp. Rugge Fabio, Mind Hacking Information Warfare In The Cyber Age, Analysis No. 319, 2018., Underwood Kimberly, Cognitive Warfare Will Be Deciding Factor in Battle, SIGNAL Magazine, 2015., Bienvenue Emily, Rogers Zac, Troath Sian, Cognitive Warfare: The Fight We’ve Got**,** Cove, 2019., The Weaponization of Information, The Need for Cognitive Security, RAND Corp., 2017., Kuperwasser Yossi i Siman-Tov David, Editors, The Cognitive Campaign: Strategic and Intelligence Perspectives, Disinformation Campaigns and Influence on Cognition: Implications for State Policy, Institute for National Security Studies, Tel Aviv, 2019.

Pomoću društvenih mreža napadač, ovisno o svojim potrebama, hibridne prijetnje može stvarati skupno ili svaku zasebno te ih prema ciljanim publikama može usmjeravati grupno, pojedinačno, lokalno, regionalno ili globalno. Automatizirane, anonimne i masovne dezinformacije koje su primjenom hibridne inteligencije optimizirane prema društvenim slabostima ciljanih publika ovdje imaju ključnu ulogu. Pojačavaju stratešku logiku svih vrsta hibridnih prijetnji. Hibridne operacije stoga smatramo glavnom prijetnjom koja proizlazi iz kiber prostora.

Neupitno je da se hibridna moć u kiber prostoru ostvaruje zloupotrebom hibridne inteligencije i tehnologija umjetne inteligencije koje koriste društvene mreže. Mogućnosti njihove zloupotrebe omogućile su višestruke operativne i taktičke mogućnosti sa strateškim posljedicama. Nude automatiziranu i time učinkovitiju obradu, analizu i evaluaciju prikupljenih strukturiranih podatka o društvenim slabostima ciljanih publika iz različitih izvora prema kojima ljudskom faktoru predlažu odluke u stvaranju optimiziranih dezinformacija i prijetnji, mnogo brže i učinkovitije nego što je bilo moguće prije pojave društvenih mreža. Zlouporaba hibridne inteligencije za stvaranje dezinformacija, prijetnji i kriza postala je ključni prioritet i način planiranja i izvođenja hibridnih (psiholoških) operacija u kiber prostoru na političko-strateškoj, operativnoj i na taktičkoj razini.

Slika 24. Tri razine iskorištavanja hibridne moći kroz zloupotrebe hibridne inteligencije na društvenim mrežama za stvaranje dezinformacija, hibridnih prijetnji i kriza.

Slikom 24. želi se prikazati kako se hibridna moć u hibridnim operacijama ostvaruje kroz zloupotrebu hibridne inteligencije na društvenim mrežama na tri glavne razine djelovanja:

- Na političko-strateškoj razini, sustavi umjetne inteligencije iz strukturiranih uvjerenja, načela i vrijednosti na društvenim mrežama nude bolje uvide u protivničko informacijsko okruženje i tekuća društveno-politička stanja i krize;
- Na operativnoj razini, na osnovi prikupljenih podataka osiguravaju relevantna saznanja i informacije o ključnim uporišnim točkama i njihovim slabostima na osnovi kojih se planiraju hibridne prijetnje i prema kojima se usklađuju dezinformacijske kampanje;
- Na taktičkoj razini, pružaju saznanja i informacije u realnom vremenu o promjenama u ponašanju i reakcijama ciljanih publika na dezinformacijske kampanje, nude optimizaciju i podršku strateškom i operativnom planiranju, prilagodbama i povećavanju njihove učinkovitosti.

Dezinformacije je moguće širiti globalno, regionalno i lokalno prema pojedincima, grupama i masama na svim razinama (političko-strateškoj, operativnoj i taktičkoj) jer su aktivnosti na društvenim mrežama objedinjene i stvaraju učinke u fizičkom i virtualnom prostoru. Zbog ove i niza drugih prednosti (anonimnost, automatizacija, masovnost, neposrednost, optimiziranost, brzina) primjenom hibridne inteligencije društvene mreže postale su ključni informacijski alati hibridne moći s pomoću kojih se planiraju i izvode hibridne operacije u kojima se s pomoću dezinformacija projiciraju i pospješuju, prema potrebama napadača, ostale vrste hibridnih prijetnji pomoću kojih napadač nastoji postići strateške posljedice u korpusu javnog znanja ciljanih publika u vlastitu korist: nadmoć vlastitih dezinformacija u javnom prostoru znanja ciljanih publika.

Automatizacija procesa obrade uvjerenja, načela i vrijednosti i drugih potrebnih podataka i informacija na društvenim mrežama, botovi, trolovi, lažni računi i zloupotreba hibridne inteligencije otvorili su nove i učinkovitije mogućnosti oblikovanja svijesti ciljanih publika, nove oblike strateškog utjecaja i jednostavnije i učinkovitije narušavanje funkcioniranja protivničkog korpusa javnog znanja preko kiber prostora i u njemu provođenje hibridnih operacija i hibridnih prijetnji bez učinkovitog protivljenja druge strane.

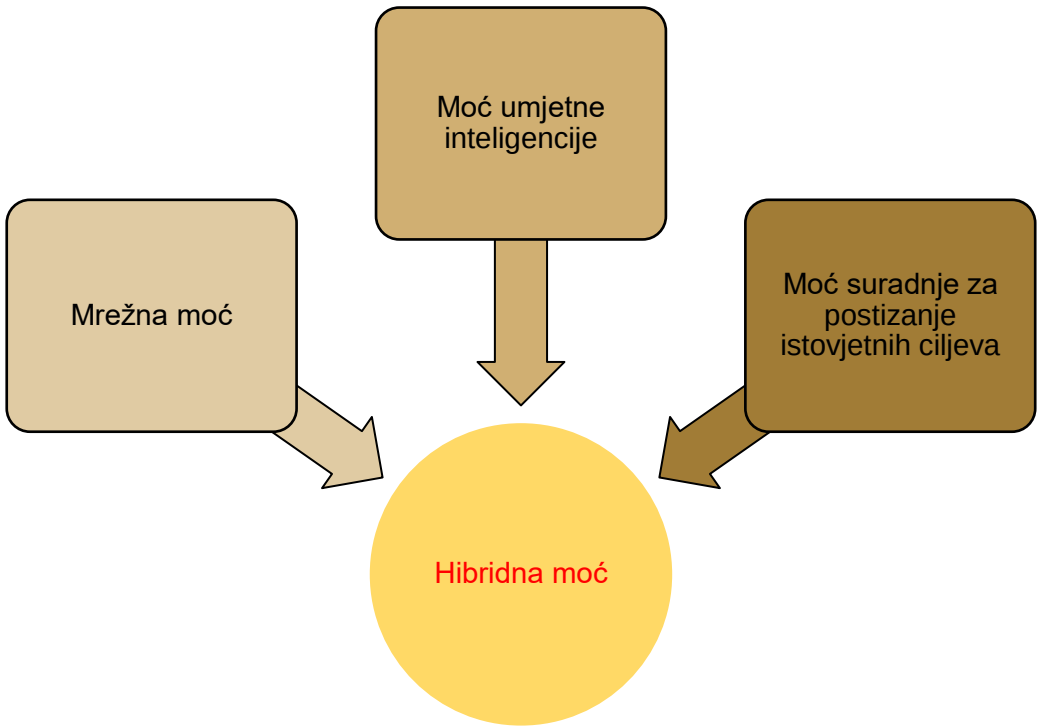
Hibridne operacije podrazumijevaju kombiniranje tradicionalnih i netradicionalnih operacija utjecaja i stvaranje njihovih sinergijskih učinaka u kiber prostoru pomoću društvenih mreža. Hibridne operacije kao sastavni dio hibridne strategije podrazumijevaju sposobnost postizanja strateških ciljeva.

Hibridne strategije, taktike, prijetnje i operacije obuhvaćaju tri glavne dimenzije hibridne moći:[536]

• Mrežnu moć,

• Moć umjetne inteligencije,

• Moć suradnje (mobilizacije) ciljanih publika za istovjetne ciljeve;



Slika 25. Provođenje hibridne moći kroz tri razine djelovanja prema ciljanim publikama.

Slikom 25. želi se prikazati hibridna moć kroz tri razine željenog djelovanja prema ciljanim publikama koje se ostvaruje hibridnim operacijama za potrebe ispunjavanja ciljeva hibridnih strategija, taktika i stvaranja hibridnih prijetnji.

Mrežna moć omogućena je pojavom društvenih mreža i sposobnosti da ih se u kiber prostoru koristi za sve forme ratovanja koje se odnose na informacije: od propagande, dezinformacijskih kampanja do širenja računalnih virusa i izvođenja tehnoloških napada na zaštićene informacijsko-komunikacijske sustave s ciljem izazivanja poremećaja u redovnom funkcioniranju kritičnih infrastruktura i/ili krađe štićenih podataka i informacija te njihovo

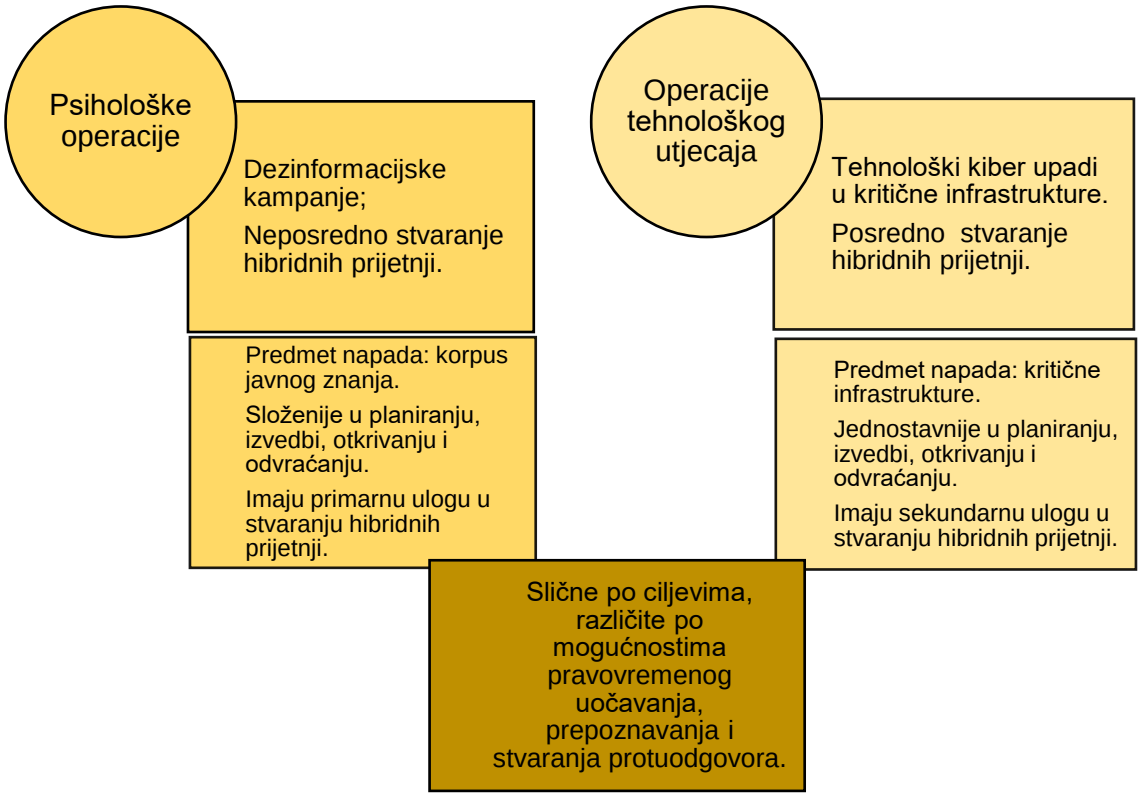
536 Gonçalves, 2019., str. 2.

javno objavljivanje ciljanim publikama. Moć umjetne inteligencije uključuje korištenje umjetne inteligencije, posebno strojnog učenja kao učinkovitog sredstva podrške ispunjavanja ciljeva hibridne strategije i taktika. Raspon korištenja umjetne inteligencije u napadima na ciljane publike u kiber prostoru može varirati od psiholoških operacija koje iskorištavaju moć mreže za stvaranje dezinformacija do kiber tehnoloških napada u kojima se moć mreže iskorištava za stvaranje dodatnih psiholoških pritisaka. Moć mobilizacije ciljanih publika za istovjetne ciljeve specifična je za današnje obrambeno-sigurnosno okruženje, a uključuje suradnju u kiber prostoru pomoću društvenih mreža različitih državnih i nedržavnih aktera, među kojima su, na primjer, organizirane nevladine organizacije, kriminalne skupine i terorističke skupine koje mogu međusobno surađivati, podržavati i unapređivati međusobne hibridne operacije.[537]

U kontekstu iskorištavanja tehnologija umjetne inteligencije koje koriste društvene mreže u hibridnim operacijama psihološki pritisci stvaraju se na temelju dvije osnovne kategorije kiber napada. Jedni su napadi tehnološke prirode koji se provode kiber tehnološkim operacijama utjecaja, a drugi su dezinformacijski napadi koji se provode psihološkim operacijama. Iako su po načinu izvođenja različiti, među njima postoje određene sličnosti. Sličnosti su u konačnom cilju, dok se osnovne razlike odnose na predmet napada, mogućnost pravovremenog uočavanja i prepoznavanja te stvaranje protuodgovora. Kiber psihološke operacije utjecaja su složenije u izvedbama i one su privlačnije zbog neposrednih učinaka na razmišljanje i donošenje odluka ciljanih publika. Tehnološki napadi podrazumijevaju klasične, javnosti dobro poznate tradicionalne upade u štićene informacijsko-komunikacijske sustave različitih kategorija kritičnih infrastruktura. Tehnološkim napadima nanose se lako uočljive funkcionalne i fizičke štete, oni se lakše uočavaju pa se time lakše otkrivaju i preveniraju. Napadima dezinformacijama nastoji se izazvati izravna šteta u procesu razmišljanja i donošenja odluka i predstavljaju daleko složeniju zadaću u planiranju i izvođenju, ali i u otkrivanju jer su manje primjetni i teži u pravovremenom prepoznavanju i odvraćanju. Dezinformacije su prvenstveno usmjerene na percepciju ciljanih publika. Kako su dezinformacije na društvenim mrežama automatizirane, masovne, anonimne i optimizirane prema uvjerenjima, načelima i vrijednostima ciljanih publika time su odgovori u odvraćanju rizika i prijetnji koji iz takvih dezinformacija proizlaze daleko složeniji. U kiber operacijama tehnološkog utjecaja napadač se daleko lakše izlaže kompromitaciji. Međutim, neupitno je da i ova vrsta kiber napada utječe

537 Usp. Ibid.

na kognitivne procese u čemu se ove dvije kategorije kiber napada preklapaju i imaju zajedničku karakteristiku.



Slika 26. Glavna podjela hibridnih operacija

Slikom 26. prikazana je glavna podjela hibridnih operacija prema vrstama i predmetima napada u kiber prostoru, međusobne razlike u složenosti planiranja, izvođenja, otkrivanja i međusobnim sličnostima u ciljevima.

Dakle, dezinformacijske kampanje i tehnološki kiber napadi imaju za cilj jačati hibridne prijetnje stvaranjem informacijsko-psiholoških pritisaka na razmišljanje i donošenje odluka, ali na različite načine s obzirom na predmet napada. Tehnološkim kiber napadima primarno se napadaju kritične infrastrukture, a dezinformacijama se primarno napada percepcija, odnosno um ciljanih publika. Izravna funkcionalna šteta na kritičnim infrastrukturama posredno može prouzrokovati značajan kognitivni učinak na ciljane publike. U određenim situacijama kognitivni učinci koji proizlaze iz tehnoloških napada mogu imati veću kognitivnu štetu po društvo od štete koja je nanesena samim kritičnim infrastrukturama. Shodno tome, tehnološki napadi također mogu biti motivirani pobudom da stvaraju strah, neizvjesnost i nepovjerenje. Primjerice, kad ciljane publike postanu svjesne štete uzrokovane tehnološkim napadom, posredno se izazivaju učinci na spoznaju o vlastitim slabostima odnosno o snazi i

sposobnostima napadača.[538] Prekidanje pristupa internetu također jest očit ratni čin koji ima i jasno rješenje, no infiltriranje dezinformacija u informacijski i medijski prostor ciljanih publika predstavlja daleko složeniju mogućnost za pojačavanje prijetnji i generiranje kriza.

Hibridne operacije mogu se definirati kao korištenje vojnih i nevojnih sredstava za postizanje strateških ciljeva. To znači da se umjesto otvorene borbe mogu koristiti sva druga raspoloživa sredstva i načini borbe kako bi se stekla prednost nad protivnikom: od obavještajnih aktivnosti do različitih oblika subverzija.[539] U hibridnim operacijama strateško djelovanje nije ograničeno na bojno polje, već uključuje djelovanje na onome što je danas poznato kao psihološko ratovanje,[540] uključuje djelovanje na ekonomskoj, financijskoj, društvenoj i političkoj razini kao način izbjegavanja otvorenog rata ili kako bi se oslabilo protivnika da ga se, ako se otvoreno ratovanje ipak dogodi, na vojnom polju može lakše pobijediti.[541]

Hibridne operacije podrazumijevaju „cijeli niz aktivnosti usmjerenih prema postizanju stanja informacijske nadmoći i oblikovanja napadnutog cilja u skladu s napadačevim potrebama.“[542] „Hibridne prijetnje i hibridne operacije podrazumijevaju usmjereno i organizirano djelovanje prema pojedinoj ciljanoj publici u cilju iskorištavanja (poticanja, produbljivanja) njezinih ranjivosti, stvaranja novih ranjivosti, poticanja osjećaja podjele, nesigurnosti, defetizma, nemoći, beznađa, dvojbenosti, sumnjičavosti, narušavanja i urušavanja demokratskih struktura i procesa te slabljenja i kontroliranja obrambenog sustava.“[543] Strateška logika hibridnih operacija je u stvaranju hibridnih prijetnji kroz kiber prostor kako bi se ciljane publike u državama natjerale da se okrenu protiv kreatora nacionalnih politika koje nisu po volji napadača. Zloupotrebe društvenih mreža i hibridne inteligencije jedno su od ključnih sredstava koje olakšava ovaj proces. Ova činjenica ponovno se počela razmatrati u razmišljanjima o današnjem obrambenom i sigurnosnom okruženju i predmet je istraživanja u različitim

538 Cordey, 2019. Primjerice, kod višesatne nestašice električne energije ili vode u velikom gradu, kad javnost otkrije da je ona rezultat namjernog tehnološkog napada, vjerojatno će rezultirati panikom, strahom, neizvjesnošću i nesigurnošću. Time tehnološki kiber napad može nanijeti veću kognitivnu štetu od izravne funkcionalne štete koja je nastala zbog nedostatka električne energije ili vode.

539 Gonçalves, 2019., str. 2.; prema Sawyer RD, The Seven Military Classics of Ancient China, United States: Basic Books, 2007., str. 568.

540 Gonçalves, 2019., str. 3.

541 Ibid., prema; Cummins A, Minami Y. The Book of Ninja: The First Complete Translation of the Bansenshukai, Japan’s Premier Ninja Manual. London: Watkins Publishing; 2013. str. 512.

542 Akrap, 2019., str. 37.-49.

543 Ibid.

zemljama. S ruske strane, kako su naglasili Čekinov i Bogdanov[544], dvojica ruskih stručnjaka za obranu, informacijske tehnologije čine novo lice ratovanja u kojem će dominirati informacijsko i psihološko ratovanje. Središnja pokretačka snaga hibridnih operacija u 21. stoljeću su kiber psihološke operacije u kojima informacijska nadmoć igra ključnu ulogu. Kao što je istaknuto u prethodnom poglavlju, novo lice sukoba čine nekinetičke operacije u kojima se za ispunjavanje ciljeva koriste informacijsko-komunikacijski sustavi i tehnologije umjetne inteligencije protiv javnih institucija u ciljanoj zemlji. Iako ovo ilustrira rusku perspektivu sukoba u dvadeset i prvom stoljeću, slično stajalište ima i Treverton[545], bivši predsjednik američkog Nacionalnog obavještajnog vijeća. Treverton je, u obrascu hibridnih operacija, identificirao tipične taktike informacijskog ratovanja koje se zasnivaju na psihološkim operacijama: korištenje propagande, lažnih vijesti, strateško puštanje u javnost štićenih informacija, financiranje organizacija i potpora političkim strankama, organiziranje protestnih pokreta pomoću društvenih mreža, korištenje sredstava u kiber prostoru za špijunažu, izvođenje kiber napada i manipuliranje informacijama, korištenje ekonomskih poluga utjecaja, posrednika, pružanje potpore paravojnim organizacijama i nepriznavanje vlastitog sudjelovanja u ratu.[546] Hibridne operacije su vidljivo kroz kiber prostor objedinile sve forme informacijskog i gerilskog ratovanja, uz nužnu napomenu da se rat podrazumijeva isključivo kao krajnji način rješavanja međunarodnih sporova.

Koncept hibridnih operacija i njihova relevantnost u strateškom razmišljanju i doktrinama dvadeset i prvog stoljeća proizlaze iz kiber prostora u kojem (strateške operacije) imaju veću učinkovitost. Kiber prostor je postao određujući čimbenik u promjeni paradigme obrambenih i sigurnosnih prijetnji koje proizlaze iz hibridnih operacija. Kiber prostor je omogućio da hibridne operacije u dvadeset i prvom stoljeću mogu provoditi i državni i nedržavni akteri, što implicira veliki pomak u strateškoj moći, gdje pojedinci i grupe koje ne moraju djelovati pod pokroviteljstvom države, mogu koristiti kiber prostor i sustave temeljene na umjetnoj

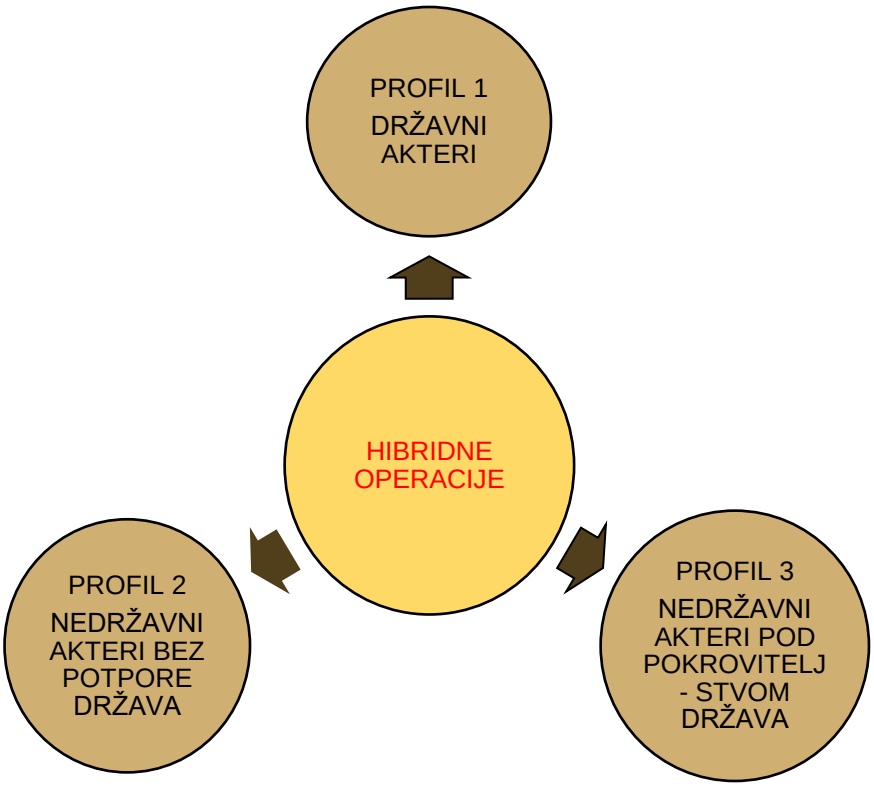
544 Gonçalves, 2019., str. 3. prema Chekinov SG, Bogdanov SA. The nature and content of a new-generation war. Military Thought: A Russian Journal of Military Theory and Strategy. 2013;4:12-23

545 Ibid, prema; Treverton GF. The intelligence challenges of hybrid threats: Focus on cyber and virtual realm. Sweden. Center for Asymmetric Threat Studies. 2018. str. 36. ISBN: 978-91-86137-75-5. Available from: http://fhs.diva-portal.org/smash/get/diva2:1250560/FULLTEXT01.pdf

546 Gonçalves, 2019., str. 3.-4.

inteligenciji za provedbu hibridnih operacija koje mogu imati značajan utjecaj na upravljanje određenom zemljom.[547]

Ovom novom paradigmom napada u kiber prostoru na osnovi znanja organiziranog na društvenim mrežama stvaraju se učinkovite dezinformacije, učinkovitije se mogu pojačavati prijetnje i iskorištavati krize vlasti, krize otpornosti i krize legitimiteta. Prema ovom načelu i obrascu planiraju i izvode nove kategorije operacija utjecaja u kiber prostoru koje su daleko kompleksnije po pitanju obrane i odvraćanja od tradicionalnih operacija utjecaja. Temeljem ovih novih mogućnosti razlikuju se tri (3) profila hibridnih operacija i prijetnji:[548]



Slika 27. Podjela hibridnih operacija prema akterima koji ih planiraju i provode u kiber prostoru.

Slikom 27. želi se prikazati moć hibridnih operacija kroz koje različiti akteri u kiber prostoru mogu kombinirati različite mogućnosti samostalnog ili udruženog djelovanja. Slikom se želi

547 Ibid.

548 Ibid.

prikazati tri profila hibridnih operacija kroz tri kategorije aktera koji koriste hibridnu moć za vlastite ciljeve:

- Profil 1: hibridne operacije i hibridne prijetnje koje sponzorira država, odnosno provodi ih određena zemlja ili zemlje. Uključuje ljudske i tehničke resurse oružanih snaga i obavještajnih struktura;
- Profil 2: hibridne operacije i hibridne prijetnje koje ne sponzorira država, već ih provode nedržavni akteri i skupine, odnosno ne podržava ih nijedna država ni financijski niti politički i logistički;
- Profil 3: hibridne operacije i hibridne prijetnje koje su pod pokroviteljstvom države, a provode ih nedržavni akteri. Podrazumijeva korištenje hakera i drugih oblika plaćenika, pružanje političke, financijske i logističke podrške nedržavnim akterima i skupinama te provedbu zajedničkih operacija (što im daje dodatnu razinu i mogućnosti uvjerljivog poricanja).

Hibridne operacije Profila 1 (koje provode državne vojne i vojno-civilne obavještajne strukture i agencije) oduvijek su bile sastavni dio strateškog razmišljanja, doktrina vojnog djelovanja i nacionalnih informacijskih strategija, taktika i načina na koji države nastoje postići ciljeve bez upotrebe konvencionalnih vojnih snaga. To uključuje tajne tradicionalne operacije utjecaja i netradicionalne operacije utjecaja koje se vode kroz kiber prostor, specijalne i subverzivne operacije i informacijsko ratovanje. Društvene mreže i hibridna inteligencija samo su pojačale potencijal i učinkovitost operacija u kiber prostoru, čime su hibridne operacije i prijetnje učinile temeljnom dimenzijom vojnih doktrina, hibridnog ratovanja i hibridnih sukoba u 21. stoljeću.

Hibridne operacije Profila 2 (koje provode nedržavni akteri bez potpore država) karakteristične su za novu paradigmu i promjenu u dinamici strateške moći koja je ostvarena zahvaljujući kiber prostoru i društvenim mrežama. Pojavu ove vrste operacija i njihov eksponencijalni rast omogućila je globalna dostupnost tehnologija umjetne inteligencije i predstavlja specifičan oblik izazova s kojima se trenutno susreću nacionalni i međunarodni obrambeno-sigurnosni sustavi. U njima male grupe ili čak dovoljno obrazovani i motivirani pojedinci i skupine, ponekad uključeni u kriminalne organizacije, s dovoljno sofisticiranim vještinama hakiranja mogu izvoditi hibridne operacije, koristeći prednosti kiber prostora i dostupnost tehnologija umjetne inteligencije, mogu ih usmjeravati prema državama sa svrhom nanošenja štete i ometanja njezinih funkcija s gotovo istom učinkovitošću kao i hibridne operacije koje sponzorira država. Činjenica je da su sustavi umjetne inteligencije slobodno dostupni svima i

da različiti alati u kiber prostoru poput zlonamjernih programa, botova i trolova imaju nisku cijenu korištenja, zbog čega ovaj tip hibridnih operacija ima ogroman potencijal. Eksponencijalni trend njihovog rasta povezan je s globalizacijom društvenih mreža, strojnog učenja, dinamikom razvoja tehnologija koju nudi Četvrta industrijska revolucija, trendom koji je povezan s internetom stvari i mogućnostima korištenja kiber prostora, uključujući mračni web (dark web) za povezivanje s pojedincima i istomišljenicima koji su voljni podržati kiber napade protiv određenih politika. Glavni problem leži u činjenici da se hibridne operacije mogu implementirati uz znatno manje ulaganja. Slabijim akterima, kako državnim tako i nedržavnim, Četvrta industrijska revolucija otvorila je mogućnost učinkovitijeg angažmana protiv jačeg protivnika s jačim vojnim snagama, smanjujući protivnikovu komparativnu prednost. Mrežna moć i moć umjetne inteligencije omogućuju nedržavnim akterima pokretanje hibridne operacije na ciljane publike s bilo kojeg mjesta na svijetu, teško im se može pripisati lokacija tj. određeni fizički/nacionalni teritorij prema kojem se onda ne može primijeniti konvencionalni vojni odgovor. Dovoljno sofisticirana skupina može ostati anonimna pa čak i biti transnacionalna u sastavu svojih članova, što ovaj tip operacija izdiže iz tradicionalnih pitanja obrane te zahtijeva daleko složenije institucionalne odgovore. Zbog trendova koje diktira Četvrta industrijska revolucija, snažnog utjecaja i učinka tehnologija uz niske troškove ulaganja u operativne mogućnosti, ova vrsta operacija prepoznaje se kao sve veća prijetnja društvu te je neupitno da će rasti u primjenama i mogućnostima.[549]

Hibridne operacije Profila 3 potencijalno mogu nanijeti najveću štetu jer uključuje zajedničku suradnju državnih i nedržavnih aktera. Ovaj posljednji profil hibridnih operacija bazira se na moći suradnje u kiber prostoru koju pospješuju društvene mreže. Iskorištavaju se prednosti mrežne suradnje između različitih nedržavnih aktera, uključujući terorističke skupine i različite kriminalne organizacije; suradničkih mreža i mrežnih organizacija između različitih zemalja te suradnja između državnih i nedržavnih aktera. Suradnja državnih i nedržavnih aktera može postati glavni izvor hibridnih prijetnji koje sponzorira država[550]; umjesto da se upuštaju u

549 Usp. Treverton, 2018., Atkinson, 2018. i Normak Magnus, How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks, The European Centre of Excellence for Countering Hybrid Threats, 2019. https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_15_Non-state-Actors.pdf

550 Gonçalves, 2019.; prema Normak, 2019. i Raugh David, Is the hybrid threat a true threat? Journal of Strategic Security, 2016, str. 1-13.

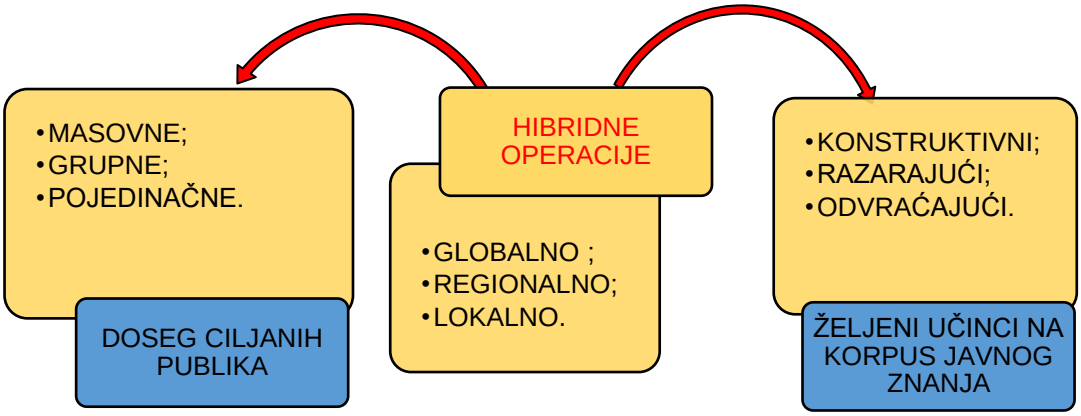
sukobe s drugim državama, različite države mogu podržavati nedržavne aktere i s njima usklađivati vlastita djelovanja.[551]

Profili hibridnih operacija 1 i 3 objedinjuju informacijske aktivnosti svih vladinih ustanova i institucija kroz snažnu i aktivnu koordinaciju s ciljem njihovog učinkovitog usmjeravanja prema ostvarenju informacijske nadmoći države napadača. Bit hibridnih operacija je u strateškom informacijsko-psihološkom djelovanju iz kiber prostora i njegovom usmjeravanju ka stvaranju hibridnih prijetnji, ovisno o potrebama. Algoritmi preporuka i rangiranja sadržaja na društvenim mrežama, hibridna inteligencija koja uobličava i optimizira dezinformacije prema pojedinačnim i grupnim uvjerenjima, načelima i vrijednostima, automatizirani botovi i trolovi koji ubrzavaju i šire njihovu vidljivost na svim mogućim prostornim razinama (lokalno, regionalno, globalno) pospješuju jednostavnije i učinkovitije postizanje informacijske nadmoći. Ove tehnologije omogućavaju masovnu i automatiziranu diseminaciju dezinformacija kao i učinkovito nadziranje, predviđanje i (pre)oblikovanje kognitivnih procesa u razmišljanju i donošenju odluka. „Svrha je natjerati ciljanu publiku da donosi odluke koje joj kratkoročno i dugoročno mogu nanijeti ozbiljne štete.“[552]

Protivnički korpus javnog znanja hibridnim operacijama moguće je napadati dezinformacijama i hibridnim prijetnjama geografski i prostorno neograničeno (globalno, regionalno i lokalno). Prema načelu izvršenih podjela korisnika društvenih mreža, dezinformacije i hibridne prijetnje hibridnim operacijama mogu biti usmjeravane na masovne, grupne i pojedinačne ciljane publike, pri čemu dezinformacije i hibridne prijetnje mogu biti uobličene za stvaranje konstruktivnih, razarajućih i odvraćajućih učinaka na korpus javnog znanja ciljanih publika.

551 Gonçalves, 2019.

552 Akrap, 2019., str. 42.



Slika 28. Podjela hibridnih operacija prema dosegu ciljanih publika i prema željenim učincima na korpuse javnog znanja.

Slikom 28. želi se prikazati da se hibridnim operacijama dezinformacije i hibridne prijetnje na masovnoj razini mogu usmjeravati prema javnim/društvenim infrastrukturama, kulturnim i drugim identitetskim simbolima te srodnim politikama, idejama i ideologijama. Na grupnoj razini dezinformacije i hibridne prijetnje mogu biti usmjerene prema određenim društvenim grupama s različitim društveno-demografskim karakteristikama (dobnim, spolnim, nacionalnim, političkim, vjerskim, religijskim i ideološkim identitetskim odrednicama, načelima i uvjerenjima). Na pojedinačnoj razini dezinformacije i hibridne prijetnje mogu biti usmjerene prema utjecajnim pojedincima i donositeljima političkih odluka koji bi u doglednoj vremenskoj perspektivi mogli postati utjecajni ili koji bi mogli najbolje ispuniti postavljene ciljeve i zadaće.

U hibridnim operacijama dezinformacije i hibridne prijetnje mogu imati konstruktivni učinak kada napadač ima za cilj dezinformacijama i prijetnjama mobilizirati ciljane publike za vlastite ideje i ideologije. Dezinformacije i hibridne prijetnje mogu imati razarajući učinak kada napadač ima za cilj narušiti koheziju ideja i ideologija koje prevladavaju u korpusima znanja ciljanih publika. Dezinformacije i hibridne prijetnje mogu imati odvraćajuće učinke kada napadač ciljanim publikama nastoji odvratiti pažnju s neke teme koja nije u interesu napadača odnosno kad dezinformacije i hibridne prijetnje imaju za cilj pažnju ciljanih publika usmjeriti u pravcima željenog djelovanja.

Konstruktivni, razarajući i odvraćajući učinci dezinformacija i hibridnih prijetnji u hibridnim operacijama mogu se provoditi na svim razinama ciljanih publika (masovno, grupno i pojedinačno) s potencijalnim strateškim posljedicama na njihov korpus znanja: stvaranje informacijske nadmoći i njegovo preoblikovanje u željenim pravcima.

U ovom poglavlju potvrđena je hipoteza rada da se umjetna inteligencija koju koriste društvene mreže koristi kao učinkovito sredstvo utjecaja za oblikovanje prostora javnog znanja prema napadačevim potrebama i za postizanje informacijske nadmoći u njegovu korist. Potvrdno je odgovoreno na prvo istraživačko pitanje da su društvene mreže i umjetna inteligencija postale dominantna sredstva za vođenje strateških operacija utjecaja kojima se na učinkovit stječe informacijska nadmoć nad protivničkim korpusom javnog znanja. U tom kontekstu strateške operacije utjecaja u kiber prostoru prikazane su kroz hibridne operacije, kao nova kategorija operacija utjecaja u kiber prostoru u kojima se zloupotrebom hibridne inteligencije na društvenim mrežama na učinkovit način planiraju i izvode napadačke informacijske operacije - psihološke operacije, u kojima se društvene mreže i hibridna inteligencija zloupotrebljavaju za stvaranje učinkovitih dezinformacija i različitih formi prijetnji s potencijalnom strateškom posljedicom – stjecanjem informacijske nadmoći. Time je odgovoreno na drugo istraživačko pitanje. Pokazano je da se društvene mreže i umjetna inteligencija koriste za ostvarivanje različitih politika i ciljeva: od energetskih politika, izazivanja društvenih nemira, oružanih sukoba do uplitanja u izborne procese, što predstavlja dio hibridnih prijetnji, koje je na učinkovit način moguće ostvariti u kiber prostoru pomoću društvenih mreža.

5.4. Razlikovanje hibridnih operacija od drugih vrsta informacijskih operacija

Hibridne operacije razlikuju se od drugih vrsta informacijskih operacija koje se u pravilu vode za marketinške i političke svrhe. Između ovih dviju vrsta operacija postoje dvije osnovne razlike. To su razlike u akterima koji ih provode i razlike u ciljevima. Alati s pomoću kojih se izvode su isti, a metodologija nije bitno drugačija.

Provoditelji hibridnih operacija utjecaja su državni i/ili nedržavni akteri sa specifičnim, u pravilu skrivenim političkim ciljevima i ambicijama. Imaju sigurnosni kontekst iz kojeg proizlaze politički, društveni i sigurnosni rizici te predstavljaju značajnu prijetnju demokratskim i političkim procesima. Razlike u ciljevima između informacijskih operacija koje se izvode u marketinške/političke svrhe i hibridnih operacija koje se izvode pomoću društvenih mreža mogu se opisati na sljedeći način: Namjerni pokušaj države A (napadača) da preko treće strane C (korporacija koje upravljaju društvenom mrežom kao alatom utjecaja) koja je izvan pravne kontrole napadača, lažnim profilima pojedinačnim i/ili grupnim, kod građana (ciljane publike) u državi B generiranjem hibridnih prijetnji i diseminacijom dezinformacija preko društvenih mreža, potakne vjerovanje ciljanih publika da određena regija države B povijesno pripada državi A. Dugoročni cilj mogao bi biti preuzimanje kontrole nad regijom, ako je

potrebno i putem kinetičke prisile odnosno hibridnim ratom kao krajnjim načinom rješavanja međunarodnog spora. Vlast u državi B (koja se brani) može se pokušati obraniti protumjerama. Komercijalna tvrtka C (tj. akter koji upravlja društvenom mrežom) posreduje u stvaranju hibridnih prijetnji širenjem dezinformacija koje je A prilagodio prema društvenim slabostima države B kako bi podržale intenciju države A, ali ne zato što C dijeli istu ideologiju s A, već kako bi zaradila od oglašavanja dezinformacija.[553] S druge strane, u industriji digitalnog marketinga i u političkim kampanjama informacijskim operacijama trgovci ili tvrtke oglašivači i političke stranke stvarnim profilima na društvenim mrežama (tvrtka C) u pravo vrijeme s pravom porukom nastoje doći do pravog kupca da kupi neki proizvod ili uslugu, odnosno da dā svoj glas određenoj političkoj opciji. Na ovom primjeru najbolje se vidi sigurnosni rizik koji akter C omogućava kroz anonimnost hibridnih operacija i stvaranja hibridnih prijetnji države A prema državi B. U ovom cjelokupnom procesu stvaranja hibridnih prijetnji jedan od najbitnijih čimbenika su društvene slabosti u ključnim uporišnim točkama ciljanih publika koje hibridna inteligencija utvrđuje na osnovi prikupljenih pojedinačnih i/ili grupnih podataka o uvjerenjima, vrijednostima i načelima te na osnovi kojih A prilagođava dezinformacije, nastoji preoblikovati uvjerenja, vrijednosti i načela te nastoji nametnuti vlastitu volju kako bi postigao informacijsku nadmoć nad B preko C. Iz navedenog primjera vidljiva je moć društvenih mreža i hibridne inteligencije za učinkovitije nametanje volje napadača. Pomoću društvenih mreža i primjenom hibridne inteligencije hibridnim operacijama ciljane publike se nastoje dodatno dijeliti prema utvrđenim slabostima, (de)mobilizirati i (de)motivirati za prikrivene političke svrhe. Po istom obrascu dezinformacijske kampanje i informacijsko-psihološki pritisci mogu biti usmjereni na njihov (ne)izlazak na izbore, za (ne)odaziv na ulične prosvjede ili u svrhu podizanja percepcije ciljanih publika o nekom političkom, društvenom stanju i/ili događaju. Po istom obrascu regrutiraju se teroristi, podiže se stupanj radikalizacije u društvu i u konačnici pokreće hibridni sukob, a po potrebi i hibridni rat.

Osobni podaci korisnika društvenih mreža mogu biti razni, a napadač ih koristi ovisno za koju hibridnu prijetnju su potrebni. Kad je interes stvoriti dezinformacije kako bi se produbile društvene i političke podjele i nepovjerenje prema nositeljima vlasti, zloupotrebljavat će se podaci koji otkrivaju politička, religijska, ideološka i svjetonazorska uvjerenja, vrijednosti i načela. Kad je interes narušavati i pogoršavati sigurnosnu stabilnost, poticati radikalizam ili ekstremizam u nekoj državi ili na nekom geografskom području, zloupotrebljavat će se podaci

553 Usp. Bergh, 2019.

o sklonostima radikalizmu, ekstremizmu i terorizmu. Osobni podaci koriste se za (de)mobilizaciju ciljanih publika, radikaliziranje ili potenciranje i drugih prijetnji. Primjena hibridne inteligencije za obradu podataka kroz sustav povratne sprege omogućava nadziranje „popularnosti" dezinformacija, njihovo rangiranje i povećavanje vidljivosti. Dezinformacijama u kombinaciji s algoritmima preporuka i rangiranja može se sugerirati da neki politički plan ili program ima podršku, dok u stvarnosti takve podrške nema. Postojeći stavovi mogu se „pogurati" prema ekstremnim, ekstremni se mogu „normalizirati" i pretvoriti u općeprihvaćenu kategoriju ili ih se, ovisno o potrebama napadača, može „usmjeravati" prema ciljanim publikama da izražavaju nasilje i organiziraju ulične prosvjede koji se inače ne bi dogodili.

Društvene mreže s lažnim profilima cjelokupnom procesu nude anonimnost djelovanja, čime se podiže učinak hibridnih operacija. Ciljane publike u većem ili manjem obimu nisu svjesne da su izložene spomenutim procesima i da njima ciljano i planirano na prikriveni način upravljaju obavještajne službe i druge srodne državne agencije i strukture koje ih (de)mobiliziraju za vlastite potrebe i potrebe svojih pokrovitelja. Mogućnost poticanja svih vrsta hibridnih prijetnji posredstvom društvenih mreža hibridnim operacijama daje potencijalni strateški učinak na ishode planiranog utjecaja.

Neosporna je činjenica da je u planiranju i izvođenju hibridnih operacija preuzeta digitalna arhitektura uvjeravanja, odnosno algoritamsko upravljanje ljudskim emocijama[554] što je specifikum industrije digitalnog marketinga. Državni i nedržavni akteri u hibridnim operacijama koriste ovaj specifikum za planiranje dezinformacijskih kampanja i za stvaranje konstantnih informacijsko-psiholoških pritisaka s mogućim strateškim posljedicama: za stjecanje informacijske nadmoći nad korpusom javnog znanja ciljanih publika kako bi ostvario šire geopolitičke, geostrateške ili geoekonomske interese.

Hibridne operacije promatraju se kao nova forma indoktrinacije ciljanih publika. Primjenom hibridne inteligencije na društvenim mrežama postalo je moguće planski preoblikovati i manipulirati pamćenje ciljanih publika odnosno svoditi ga na dezinformacije. Hibridne operacije postale su dio „informacijskih strategija koje imaju za cilj svesti pamćenje samo na onaj skup podataka koji se sustavno i planski projektira i memorira u informacijskom prostoru."[555] „Poznato je da su indoktrinacije najveće kad se ostvaruju manipulacijom

554 Usp. Tufecki, Zeymep. We're Building a Dystopia Just to Make People Click on Ads, Ted Talk, 2017.

555 Usp. Tuđman, 2008., str. 158.

pamćenja. To se može ostvariti prešućivanjem postojećih dokumenata i dokaza; kad se promjenom konteksta dokumentima pridaju nova značenja i kad se „novim obavijestima“ i porukama mijenja pamćenje prema matrici koja je definirana informacijskim strategijama.“[556] U hibridnim operacijama njihovi planeri pomoću botova, trolova i algoritama preporuka i rangiranja zagušuju korpus javnog znanja ciljanih publika masovnim, automatiziranim, anonimnim i optimiziranim dezinformacijama, dok primjena hibridne inteligencije omogućava učinkovitu interpretaciju podataka, prilagođavanje dokaza ciljevima informacijskih strategija i, prema potrebama, omogućava učinkovitije stvaranje „novih dokaza“. Ujedno hibridnim operacijama pomoću društvenih mreža ciljanim publikama pružaju se ograničene obavijesti, informacije, vijesti i događaji o kojima one nemaju prethodnih saznanja niti imaju znanja o stvarnom činjeničnom stanju. Anonimnim, automatiziranim, masovnim i optimiziranim dezinformacijama uz pomoć algoritama preporuka i rangiranja, botova i trolova ubrzava se i određuje doseg i brzina njihovog širenja kao i širenja djelomično točnih podataka. Na ovaj način dugoročno i učinkovito mogu se napadati kognitivne pristranosti ciljanih publika i tako ih se može neprimjetno kratkoročno ili dugoročno navoditi na pogrešne zaključke. Tehnologije su omogućile da za vlastitu korist planeri hibridnih operacija hibridnom inteligencijom stvaraju željenu, projiciranu sliku stvarnosti koja im daje mogućnost da učinkovitije manipuliraju pamćenjem i da posljedično, kratkoročno ili dugoročno, dođe do potpune indoktrinacije. Primjenom hibridne inteligencije kroz sustav povratne sprege i uz pomoć višedimenzionalnih tehnologija mogu jednostavnije i učinkovitije mijenjati „kontekst dokumenata te im pridavati nova značenja“, a novim „obavijestima“ i porukama mijenjati pamćenje prema matrici koja je definirana informacijskim strategijama.“[557] Automatizirano, masovno, konstantno stvaranje i širenje dezinformacija pogoduje memoriranju dezinformacija, odnosno njihovom kratkoročnom i dugoročnom pamćenju u korpusu javnog znanja ciljanih publika. Automatizirani sustav povratne sprege i u njemu primjena višedimenzionalnih tehnologija umjetne inteligencije jesu najzaslužniji čimbenici koji su društvene mreže pretvorili u snažne i učinkovite alate utjecaja za ostvarivanje širih ciljeva s potencijalnim strateškim posljedicama. Ovim dijelom ujedno je dodatno odgovoreno na prvo i drugo istraživačko pitanje. Strateške posljedice iz grupe hibridnih prijetnji i hibridnih operacija kratkoročno i dugoročno mogu nanijeti ozbiljne štete demokratskim procesima. Njihova moć najviše dolazi do izražaja upravo

556 Ibid.

557 Ibid.

u hibridnim psihološkim operacijama u hibridnim sukobima kad se (kod prvih naznaka mogućeg izbijanja krize te rasta napetosti, a prije izbijanja većeg sukoba) traži „osjetljiva ravnoteža između istine, poluistine i propagande“.[558] Primjena hibridne inteligencije na društvenim mrežama predstavlja očitu prednost jer se dezinformacije mogu prilagođavati hibridnim prijetnjama koje se pak mogu uključivati ili isključivati prema potrebi (i kontekstu). Hibridne prijetnje uglavnom su nesmrtonosne, privremene i reverzibilne, čime dodatno smanjuju rizik od eskalacije sukoba i penalizacije prema primjeni međunarodnog prava. Društvene mreže prema ovom načelu jesu snažni alati za „ostvarivanje strateških utjecaja iz daljine“[559] s pomoću kojih se, ovisno je li to potrebno na određenoj regionalnoj ili lokalnoj razini, može pokrenuti ili militarizirati određeni međunarodni spor, kontrolirati tok i učinak hibridnih prijetnji i ujedno suzbijati protivničke hibridne prijetnje, u realnom vremenu, na manje ili više anoniman način. Algoritmi i tehnologije umjetne inteligencije, naročito strojno učenje, automatizacijom i stalnim učenjem iz baza podataka na društvenim mrežama o ciljanim publikama osiguravaju potrebnu moć i služe kao učinkoviti alati za planiranje i izvođenje hibridnih prijetnji. Iz ovoga je vidljivo da se društvene mreže, sukladno usvojenim informacijskim strategijama, koriste za planiranje i upravljanje hibridnih psiholoških operacija s mogućim strateškim posljedicama. Umreženost ciljanih publika na društvenim mrežama osigurava bolji uvid u informacijsko okruženje i slabosti protivnika čime se olakšava odabir i vrste hibridnih prijetnji koje će se koristiti na ciljanom području, sukladno kratkoročnim i/ili dugoročnim interesima i potrebama. Na društvenim mrežama i u širem informacijskom i medijskom prostoru ciljane publike više ne odlučuju kada će i hoće li se uključiti u sukob. One su u pozadini vidljivih sukoba u većoj ili manjoj mjeri uvijek uključene, a planeri hibridnih operacija odabiru koga će, kada i na kojem području uključiti u sukob po svom izboru.[560] Primjena hibridne inteligencije u hibridnim operacijama na društvenim mrežama omogućava konstantno prikupljanje i nadziranje podataka, stavova, mišljenja i podataka o promjenama u obrascima ponašanja shodno kojima se prilagođava i pospješuje daljnje djelovanje.

---

558 Usp. Akrap, 2011, str. 41.

559 Nissen Thomas, The Weaponization of Social Media, Royal Danish Defence College, NATO Strategic Communications Centre of Excellence, 2015. Dostupno na: https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media

560 Usp. Lipsey Richard, Network Warfare Operations: Unleashing the Potential, Center for Strategy and Technology, Air War College, Air University, SAD, 2005., Dostupno na: https://apps.dtic.mil/dtic/tr/fulltext/u2/a509649.pdf

6. HIBRIDNE OPERACIJE U HIBRIDNIM SUKOBIMA I HIBRIDNOM RATOVANJU

6.1. Američki i ruski pogled na nastanak hibridnih ratova i sukoba

Nastanak hibridnih sukoba dodatno će se prikazati kroz tumačenja SAD-a i Rusije o uzrocima njihovog nastanka te kroz prikaz utjecaja razvoja informacijsko-komunikacijskih sustava i računalnih tehnologija na transformaciju sukoba koji su se odvijali u kiber prostoru kao novoj bojišnici za ideje i ideologije i u kojima su društvene mreže postale ključni alati borbe, a informacije su postale snažna i učinkovita sredstva utjecaja.

Glavno polazište ruske vojne, akademske i političke elite jest da su SAD nakon završetka hladnog rata i sloma SSSR-a nastavile provoditi operacije utjecaja i psihološke operacije prema Rusiji „drugim načinima i sredstvima".[561] Za njih hladni rat nikad nije završio.[562] Propast SSSR-a vide kao posljedicu američkog „imperijalističkog" informacijskog rata.[563] Pod „drugim načinima i sredstvima" ruska vojna, akademska i politička elita misli na uvedenu doktrinu sukoba niskog intenziteta, na globalni informacijski prostor, informacijsko-komunikacijske sustave i računalne tehnologije na osnovi kojih je prvo nastao kiber prostor a naknadno i društvene mreže. Prema ruskom tumačenju, SAD su kiber prostor i nove informacijsko-komunikacijske sustave i računalne tehnologije iskoristile za nadogradnju nekonvencionalnog oblika ratovanja odnosno njegovu prilagodbu mogućnostima koje nude ovi sustavi i tehnologije. Prema ruskom gledištu, SAD su kiber prostor iskoristile za organiziranje prosvjeda, poticanje društvenih nemira i političkih prevrata u državama od interesa SAD-a.[564] Nastanak hibridnih sukoba iz ruskog diskursa promatra se kroz proces koji je poznat kao „obojane revolucije" koje su se nakon pada komunizma i sloma SSSR-a pojavile u novonastalim „tranzicijskim državama". Također smatraju da su, primjenom tehnologija koje koriste društvene mreže, procesi „obojanih revolucija" iz 1990-ih i 2000-tih dobili novu formu

561 Thomas L.Timothy, Russia's Reflexive Control Theory and the Military, Journal of Slavic Military Studies 17, 2004., str. 237.–256., dostupno na: https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

562 Kuzio Taras, Why Vladimir Putin is Angry with the West Understanding the Drivers of Russia's Information, Cyber and Hybrid War, Security Policy Working Paper, No. 7, Federal Academy for Security Policy, 2017., dostupno na: https://www.baks.bund.de/en/working-papers/2017/why-vladimir-putin-is-angry-with-the-west-understanding-the-drivers-of-russias

563 Rugge Fabio, Confronting an Axis of Cyber?, Istituto per gli Studi di Politica Internazionale, 2018., str. 39. Dostupno na https://www.ispionline.it/it/pubblicazione/confronting-axis-cyber-21458

564 Korybko Andrew, Hybrid Wars: The Indirect Adaptive Approach to regime Change, Moskva, 2018., dostupno na: https://1lib.nl/book/2801250/bdfe49?id=2801250&secret=bdfe49 str. 9., 34., 37., 45.,53.

kroz proces poznat kao „Arapsko proljeće“. „Obojane revolucije“ i „Arapsko proljeće“ ruska vojna, akademska i politička elitu promatra kao nastavak tradicionalnih operacija utjecaja i psiholoških operacija novim tehnologijama kroz kiber prostor, u kojima su SAD *mekanu moć* iskoristile u napadačke svrhe.[565] Primjena informacijsko-komunikacijskih sustava i računalnih tehnologija dio je nužne prilagodbe koju diktiraju tehnologije i prema njoj usvajanje novih mogućnosti radi ispunjavanja nacionalnih informacijskih strategija kroz kiber prostor kao novo bojište. Jedan od glavnih ciljeva SAD-a bio je pomoću informacijsko-komunikacijskih sustava i računalnih tehnologija kroz kiber prostor ciljanim publikama nametati ideje i ideologije o unipolarnom svjetskom poretku, nastaviti provoditi politiku dominacije punog spektra i ideje američkih geopolitičara i strategija.[566] Hibridni sukobi direktna su posljedica nastanka kiber prostora i informacijskih sukoba ideje unipolarnog svijeta SAD-a i ideje multipolarnog svijeta koju propagira Rusija te vezanih međusobno suprotstavljenih društvenih, političkih i sigurnosnih koncepata. Ruska istraživanja o uzrocima nastanka hibridnih sukoba i ratova navode kako je relativno jednostavno prepoznati na kojim područjima nastaju hibridni sukobi ukoliko se razumiju geoekonomski interesi ključnih aktera.[567] Jedan od načina kojim se pokreću hibridni sukobi, a po potrebi i ratovi kao krajnje rješenje, može se prepoznati u teoriji kaosa koju je američki general Steven Mann opisao u svom djelu 'Teorija kaosa i strateška misao'.

Vojne, političke i akademske elite SAD-a i država članica NATO saveza pojmom hibridnih sukoba i hibridnog ratovanja opisuju kombiniranje gospodarskih, diplomatskih i financijskih instrumenata hibridne moći, uz stalnu prijetnju vojnom silom, kojima Rusija nastoji narušiti provedbu politika EU-a, SAD-a i NATO saveza. U većem dijelu, uz iznimku borbe protiv terorizma, kontekst hibridnih sukoba, hibridnih operacija i hibridnih prijetnji povezuju s informacijskim sukobom SAD-a, NATO saveza i Rusije oko temeljnih političkih i ideoloških uvjerenja, vrijednosti i načela. U ovom kontekstu vrijedno je ponovno istaknuti teoriju ruskog teoretičara informacijskog ratovanja Dugina o sukobu euroatlantizma i euroazijanizma kao dva suprotstavljena modela.

565 Nye, 2019.

566 Korybko, 2018., str. 14.-18. Autor ističe ideje Zbigniewa Brzezinskog, Josefa Pilsudskog, Nicholasa Spykmana i Halforda Mackindera.

567 Usp. Ibid. str. 27.-28. i str 100.-101., Korybko A. The End of Pax Americana and the Rise of Multipolarity. Comparative Politics Russia, 2021., str. 67-173. https://doi.org/10.24411/2221-3279-2021-10013

Do šire upotrebe termina hibridnosti za opisivanje sukoba i ratovanja došlo je nakon ruske vojne intervencije u Gruziji 2008. i Ukrajini 2014. i 2015., u kojima je Rusija promijenila paradigmu planiranja i izvođenja vojnog djelovanja. U Gruziji je po prvi put iskoristila kiber prostor za pružanje neposredne potpore kinetičkim vojnim operacijama i za planiranje i izvođenje psiholoških operacija. Tada, tek godinu dana nakon što je nastao Facebook 2007., društvene mreže nisu imale zapaženiju ulogu. Međutim, kako je s vremenom njihova popularnost i globalni doseg rastao počele su se koristiti za izvođenje psiholoških operacija i kao vid potpore za izvršavanje kinetičkih (vojnih) operacija. Prikupljanje obavještajnih podatka o lokacijama, članovima postrojbi, izvođenje kiber operacija na brojnim svjetskim kriznim žarištima s vremenom je pokazalo da su društvene mreže postale neizostavan i učinkovit alat za planiranje i izvođenje kinetičke (vojne) i nekinetičke borbe (operacija utjecaja). Razmjeri učinaka društvenih mreža u „Arapskom proljeću“ i ruskoj intervenciji na Krimu u razmaku od samo par godina doveli su do redefiniranja hibridnog ratovanja. Jedan od razloga je bio što je moć društvenih mreža postala očita u postizanju strateških ciljeva. Pokazalo se da su društvene mreže (kao informacijsko-komunikacijski sustav osmišljen za umreženo, masovno i globalno komuniciranje primjenom tehnologija umjetne inteligencije koja na njima procesuira podatke o uvjerenjima, načelima i vrijednostima na automatizirani način) postale učinkoviti alati za postizanje ciljeva koji izlaze izvan komercijalnih okvira za koje su društvene mreže bile osmišljene. U Arapskom proljeću pokazale su moć u mobiliziranju i organiziranju društveno-političkih pokreta, aktivista i uličnih demonstracija sa strateškim posljedicama a to su u ovom slučaju bili politički i društveni prevrati. U ruskoj intervenciji na Krimu dodatno su pokazale moć u širenju dezinformacija, stvaranju informacijsko-psiholoških pritisaka i za izvođenje tehnoloških kiber napada sa strateškim posljedicama a to je u ovom slučaju bila aneksija Krima i stvaranje hibridnih prijetnji prema različitim ciljanim publikama kako u Ukrajini tako i izvan nje. U oba primjera društvene mreže pokazale su moć izvan konteksta i svrhe za koje su primarno bile osmišljene: širenje ideja i pomaganje ljudima u održavanju kontakata s prijateljima i obitelji. Do intervencije koja je rezultirala aneksijom Krima, u definicijama hibridnog ratovanja naglasak je bio na kombiniranju različitih elemenata kinetičke sile i tehnologija. Nakon Krima težište u definiciji hibridnog ratovanja stavljeno je na psihološke operacije i konvergenciju aktivnosti iz kiber prostora s kinetičkim djelovanjem u fizičkom prostoru kroz razne oblike političkog i/ili društvenog aktivizma te njihovo kombiniranje s nasilnim i manje nasilnim civilnim akterima, ovisno o potrebama napadača.

6.2. Općeniti pregled hibridnih operacija SAD-a i Rusije

Javno dostupne literature SAD i Rusiju identificiraju kao najvažnije državne aktere hibridnih sukoba i ratova. Postoje i drugi državni akteri koji imaju izgrađene vojne i informacijske sposobnosti strateškog planiranja i izvođenja hibridnih operacija, koji su također u nacionalne informacijske strategije integrirali nove tehnologije kao nove alate borbe za informacijsku nadmoć te imaju izgrađene kapacitete i mogućnosti održavanja stalne prijetnje kinetičkom silom.

Međusobne razlike u planiranju i izvođenju hibridnih operacija i hibridnih prijetnji promatramo kroz nekoliko razina: po različitim pristupima operacijama utjecaja i aktivnostima u kiber prostoru; po različitim pristupima u iskorištavanju društvenih mreža; po različitom opsegu iskorištavanja hibridne inteligencije za stvaranje dezinformacija; po vrstama i opsegu posredničkih aktera koje koriste te po trajanju samih operacija.

U razdobljima otvorenog rata i oružanih sukoba temeljna polazišta i pristupi planiranju i izvođenju psiholoških operacija između SAD-a i Rusije većim dijelom su podudarni. SAD i Rusija na gotovo sličan način gledaju na informacijsku nadmoć - kao sposobnost zaštite vlastitih informacija, uz istovremenu sposobnost projiciranja vlastitog utjecaja na protivničke informacije i informacijske sustave. Oba aktera informacijske operacije koriste u ofenzivne i defenzivne svrhe. Slične poglede imaju i u tumačenju obmane. Oba aktera slažu se da je obmana važan dio informacijskog ratovanja i srodnih operacija. Međutim, kod SAD-a obmana se veže isključivo za vojni kontekst psihološkog djelovanja, dok se kod Rusije obmana tumači *maskirovkom.* Maskirovka predstavlja neovisnu kategoriju operativne (borbene) podrške operacijama utjecaja koje se provode svakodnevno na svim razinama i izvan stanja rata ili sukoba.[568]

Dodatne razlike najočitije su u planiranju i izvođenju (prikrivenih) psiholoških operacija utjecaja u hibridnim sukobima kad se ova vrsta djelovanja smatra nelegitimnim načinom borbe. Usporedbom američkih hibridnih operacija u hibridnom ratu i ruskih hibridnih operacija u hibridnim sukobima, iako se radi o različitim kontekstima i potrebama, uočavaju se određene razlike i sličnosti u planiranju i izvođenju psiholoških operacija u načinima iskorištavanja društvenih mreža.

568 Heickerö, Roland, Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations, Swedish Defence Research Agency, 2010.

Glavni razlog različitim pristupima planiranju i izvođenju psiholoških operacija proizlazi iz različitih pristupa operacijama utjecaja. Rusija operacije utjecaja veže i za razdoblja izvan oružanih sukoba. Ovakav ruski pristup rezultat je shvaćanja prema kojem je Rusija stalna meta operacija utjecaja i informacijskih napadačkih aktivnosti SAD-a koje ugrožavaju njezin opstanak.[569] U ruskoj literaturi općenito se ne koristi pojam kiber prostor, osim kada se pozivaju na zapadnjačke ili druge strane izvore na tu temu. Umjesto toga koristi se termin informatizacija, konceptualizirajući time operacije utjecaja unutar kiber prostora kroz širi termin informacijskog rata (informatsionnaya voyna).[570] Prema ruskim stručnjacima, američki termin kiber prostor prvenstveno je tehnološki pojam, dok je ruski termin "informacijski prostor" koji promatraju u širim filozofskim i političkim značenjima. Prema ruskim tumačenjima, tehnologije su samo jedna od mnogih komponenti ovog prostora koju ne smatraju najvažnijom. Doktrina informacijske sigurnosti Ruske Federacije, na primjer, nijednom ne spominje riječ Internet. Za Rusiju se kroz informacijski prostor ujedno štite znanja i kultura nacije.[571] Od načina na koji definira kiber prostor do njegovog korištenja za stratešku upotrebu, očigledno je da Rusija na kiber prostor gleda drugačije od svojih zapadnih kolega. Kao što je James Wirtz primijetio: "Čini se da je Rusija, više od bilo kojeg drugog novonastalog aktera na kiber pozornici, osmislila način da ratovanje u kiber prostoru integrira u veliku strategiju u svrhu postizanja političkih ciljeva."[572]

Informacijski rat, kako taj izraz koriste ruski vojni teoretičari za opisivanje aktivnosti u kiber prostoru, holistički je koncept koji uključuje operacije računalnim mrežama, elektroničko ratovanje, psihološke operacije i informacijske operacije. Drugim riječima, kiber prostor je mehanizam koji omogućava nekoj zemlji da dominira informacijskim prostorom te se smatra domenom ratovanja za sebe.[573] Informacijsko okruženje prostor je u kojem se vode borbe za ideje, ideologije, identitete, za sustave vrijednosti, uvjerenja i načela. Napadačke aktivnosti u informacijskom okruženju imaju značajnu ulogu u ostvarivanju informacijske dominacije u

---

569 Cordey, 2019.; prema Blank, 2017.

570 Connell Michael i Vogler Sarah, Russia's Approach to Cyber Warfare, Center for Naval Analyses, 2016., str. 2.

571 Gady Franz-Stefan i Austin Greg, Russia, The United States, And Cyber Diplomacy, The EastWest Institute, 2010., str. 5., https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

572 Michael Connell i Sarah Vogler; prema James J. Wirtz, Cyber War and Strategic Culture: The Russian Integration of Cyber Power Into Grand Strategy, September 2016., dostupno na: https://apps.dtic.mil/sti/pdfs/AD1019062.pdf

573 Connell i Vogler, 2016., str. 2.-3.

svim fazama sukoba. Ova borba je unutar "informacijskog okruženja" vise manje stalna i beskrajna.[574] Ne poznaje granice, fizičke ili vremenske. Ovo je u oštroj suprotnosti sa zapadnim konceptom, a posebno konceptom SAD-a koji kiber prostor promatra kao zasebnu domenu, različito od informacijskog rata i povezanih psiholoških aspekata.[575] S obzirom na širi koncept informacijskog ratovanja, ruske operacija utjecaja u kiber prostoru imaju veću tendenciju da budu strateške i dugoročne prirode, a ne operativne ili taktičke.[576]

Ovakvo usmjerenje vidljivo je iz ruske informacijske politike kojom su definirana četiri središnja cilja: razvijanje sustava vrijednosti za rusko društvo; osiguravanje potpore državnim aktivnostima od domaćeg i međunarodnog javnog značaja (osiguravanje javne podrške državnoj politici); borba protiv destruktivnih ideologija, vjerskog ekstremizma i dezinformacija usmjerenih prema državnim politikama na nacionalnoj i međunarodnoj razini; suprotstavljanje poremećajima stabilnosti i sigurnosti te osiguravanje funkcioniranja nacionalne informacijske infrastrukture (uključujući vojne, tehnološke i političke aspekte).[577]

Evidentno je da kroz ruske hibridne operacije kiber napadi na KI-jeve i dezinformacijski napadi na um ciljanih publika predstavljaju jedinstveni operativni kontinuitet u cilju stvaranja konstantnih (24/7) informacijsko-psiholoških pritisaka u razdobljima rata i mira.[578] Uzimajući u obzir ruski pristup informacijskom ratu i kiber prostoru tj. informacijskom prostoru, evidentno je da Rusija u hibridnim operacijama na sveobuhvatniji način koristi sve tehnološke mogućnosti društvenih mreža u svrhu stvaranja cijelog spektra hibridnih prijetnji prema ciljanim publikama. Dezinformacijske kampanje na društvenim mrežama i sva raspoloživa tehnološka rješenja i mogućnosti za uobličavanje, ubrzavanje i anonimno automatizirano i masovno širenje dezinformacija u ruskim primjerima hibridnih operacija pokazale su se najiskoristivijima za uplitanje u unutarnje političke i izborne procese i produbljivanje društvenih i političkih podjela u ciljanim državama.

---

574 Timothy L. Thomas, Russian Information Warfare Theory: The Consequences of August 2008, in The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald, Ed. Stephen J. Blank and Richard Weitz, U.S. Army War College, Carlisle, Strategic Studies Institute, 2010, str. 266. Dostupno na https://www.jstor.org/stable/pdf/resrep12110.8.pdf

575 Connell i Vogler, 2015.

576 Ibid.

577 Gady i Austin, Russia, The United States, And Cyber Diplomacy, 2010., str. 5.

578 Rugge, 2018.

Iskorištavanjem svih dostupnih tehnoloških rješenja i mogućnosti koje nude društvene mreže za napadna informacijsko-psihološka djelovanja, psihološke operacije u kiber prostoru dobile su formu strateških informacijskih operacija za ostvarivanje vanjskopolitičkih ciljeva.

Društvene mreže Rusija koristi kako bi učinkovitije podrivala političku i društvenu koheziju NATO saveza (koji za Rusiju predstavlja simbol *tvrde moći* i prijetnju nacionalnoj sigurnosti), SAD-a, EU-a i njihov koncept liberalne demokracije.[579] Prema ovom načelu, Rusija hibridnim operacijama nastoji spriječiti širenje NATO saveza prema svojim granicama. U državama bivšeg sovjetskog prostora i državama od vlastitog interesa koje nisu članice NATO-a i EU-a, nastoji umanjiti atraktivnost u pristupanju njihovom članstvu i oslabiti političku moć, ugled i utjecaj lidera koji zagovaraju prozapadne i antiruske ideje i politike.[580] Cilj ovakvih operacija je nametnuti ideju multipolarnosti kao alternativu američkoj ideji unipolarnog svjetskog poretka.[581]

Načelnik stožera Oružanih snaga Ruske Federacije general Valerij Gerasimov, opisujući rusku doktrinu ratovanja nove generacije, istaknuo je presudnu ulogu asimetričnosti kiber prostora za umanjivanje protivničkog potencijala i presudnu ulogu nekinetičkih sredstava borbe u postizanju političkih i strateških ciljeva.[582] Najplastičniji primjeri koji savršeno oslikavaju Gerasimovljev koncept jesu hibridne operacije u kojima su društvene mreže postali učinkoviti i snažni alati borbe te imaju ključnu ulogu u planiranju i izvođenju čitavog spektra hibridnih prijetnji. Primjena ovog koncepta mogla se vidjeti prilikom vojne intervencije na Krimu, a potom i kroz uplitanja u demokratske političke i referendumske procese u SAD-u i pojedinim državama Europe. Perspektiva djelovanja bila je u skladu s Gerasimovljevim zapažanjem da će „u tekućoj revoluciji informacijske tehnologije, informacijski i psihološki rat uvelike biti temelj za pobjedu."[583]

U strategiji obrane SAD tijekom devedesetih godina 20. stoljeća pokrenuta je ideja da se novim tehnološkim i društvenim konceptima, među kojima je i široka primjena informacijskih i komunikacijskih tehnologija, omogući promjena odnosa između tradicionalno jasnih razlika

---

579 Usp. Nye, 2019. i Flore i autori, 2019.

580 Prema Izvješću Ministarstva vsnjkih poslova SAD-a. Usp. U.S. Department of State, Report to Congress on Efforts by the Russian Federation to Undermine Elections in Europe and Eurasia, Pursuant to the Countering America's Adversaries through Sanctions Act of 2017 (P.L. 11544), 2017.

581 Usp. Kuzio, 2017.

582 Akrap, 2019.

583 Connell i Vogler, 2015., str. 4; prema Chekinov i Bogdanov, The Nature and Content of a New-Generation.

War, Voyenna mysl [Military Thought in English Translation], No.4, 2013.

između ratnih sukoba i mirnodopskih razdoblja.[584] Ovu ideju posebno je predlagao rastući pokret pristaša neoliberalnih političkih rješenja u međunarodnim odnosima koja su bila dobro prihvaćena od strane svih predsjedničkih administracija u SAD.[585] „U tom periodu, primjena informacijsko-komunikacijskih tehnologija postala je privlačan izbor za široki krug donositelja odluka, stratega i stručnjaka. One su se mogle istovremeno upotrijebiti u cilju manifestacije *„mekane"* moći privlačenjem drugih nacija političkim idejama SAD-a, kroz primjenu javne diplomacije i širenje američke kulture u svijetu, kao i u cilju ostvarivanja *„tvrde"* moći, ostvarivanjem prvih destruktivnih vojnih operacija u kiber prostoru, odnosno intenzivnim razvojem špijunaže i nadzora svih građana u svijetu."[586]

U liberalno-demokratskim režimima, psihološke operacije utjecaja visoko su normalizirane i ograničene unutar relativno uskog operativnog opsega. Međutim, one su strogo zabranjene ili uvelike ograničene u vrijeme mira. Osim toga, upotreba propagande od strane vlade ili državnih agencija protiv vlastitog stanovništva ili naroda prijateljske strane države tradicionalno je smatrana neprihvatljivom u široj javnosti. Pravila angažmana su stoga visoko kodificirana i kontrolirana domaćim zakonima, kao što je američki Smith-Mundt zakon koji zabranjuje bilo kakav oblik utjecaja Pentagona na američke građane i novinske kuće. Demokratske su vlade općenito predane pridržavanju vladavine prava, zakona o odgovornosti vlasti i načela slobode govora.[587]

SAD vežu informacijski rat, psihološke operacije i obmanu isključivo za kinetičko (vojno) djelovanje odnosno za rat. Informacijske operacije javne diplomacije, bilo one javne ili tajne, ne vežu za termin informacijski rat, nego za stratešku komunikaciju[588], a operacije javne diplomacije nemaju atribuciju operacija utjecaja.[589] Terminom strateške komunikacije kod SAD-a i NATO saveza obuhvaćaju se informacijske operacije javne diplomacije (javne i nejavne), *mekana moć* i druge aktivnosti koje uključuju rad s informacijama sa svrhom

---

584 Arquilla John i Ronfeldt David, eds., In Athena's Camp, Preparing For Conflict in the Information Age, Rand Corporation, 1997. Dostupno na: https://www.rand.org/pubs/monograph_reports/MR880.html

585 Mladenović, 2016. Snažan utjecaj na američku vanjsku politiku imao je Joseph Nye autor koncepta „mekane" i „pametne" moći u međunarodnim odnosima. Nye je bio predsjedavajući Nacionalnog obavještajnog vijeća i pomoćnik državnog tajnika obrane za međunarodnu sigurnost u vremenu administracije Billa Clintona.

586 Mladenović, 2016.

587 Coredey, 2019., str. 26.

588 Cordey, 2019. i Cohen i Bar'el, 2017.

589 Heickerö, 2010.

stvaranja strateškog i političkog utjecaja na duža razdoblja izvan konteksta rata. Društvene mreže dio su usvojene strategije strateškog komuniciranja vladinih tijela, a metode vojne obmane i strateškog komuniciranja nisu nužno međusobno povezane.[590] U razdobljima rata i oružanih sukoba SAD hibridne operacije utjecaja u kiber prostoru vode putem službenih, diplomatskih, vojnih i vladinih informacijskih sustava. Jedinice specijalizirane za planiranje i izvođenje kiber operacija su pod ingerencijom Ministarstva vanjskih poslova i Ministarstva obrane SAD-a. Postoje slučajevi kiber operacija u kojima su sklapali ugovore s vanjskim izvođačima. Primjer je bila operacija Earnest Voice, astroturfing kampanja Cyber centra Centralnog zapovjedništva oružanih snaga SAD-a koju je razvila privatna tvrtka za web sigurnost, a cilj ove operacije bio je širenje proameričke propagande u informacijskom prostoru Pakistana, Afganistana i Iraka.[591]

„Slučaj SAD-a predstavlja karakterističan primjer kako su poslovi obrane i nacionalne sigurnosti u kiber prostoru postali isprepletani i funkcionalno povezani.“[592] „Obranom se bavi Ministarstvo obrane[593], vanjskim obavještajnim i tajnim operacijama bave se specijalizirane agencije poput CIA-e[594] (…), dok je praktična sposobnost za izvođenje operacija u kiber prostoru skoncentrirana u okviru Nacionalne obavještajne agencije.“[595] Prema izvješću RAND-a[596], u razdobljima rata SAD u Afganistanu i Iraku nisu stvarno razmatrale planiranje i izvođenje psiholoških operacija preko interneta ili su ih barem smatrale nedovoljno učinkovitima i neprikladnim protiv talibana, budući da je 2011. internet u obje zemlje koristilo svega 5% ukupne populacije.[597] Stratezi Ministarstva obrane SAD-a od 2003. javno govore o potrebi da se za poboljšanje raspona i učinkovitosti psiholoških operacija i propagande trebaju osloniti na sve mogućnosti koje pružaju internet i informacijske tehnologije. Iste godine Ministarstvo obrane SAD-a objavilo je Mapu informacijskih operacija – tzv. Rumsfeldov plan

590 Ibid.

591 Cordey, 2019., str 22., prema; Fielding & Cobain 2011. Operacija je izvedena na osnovi posebnog programa „internetske usluge u upravljanju osobama" kojeg je razvila DARPA. Na osnovi programa, hakeri američkih vojnih snaga mogli su upravljati do 10 zasebnih lažnih računa na društvenim mrežama.

592 Mladenović, 2016.

593 Eng. Department of Defense.

594 Eng. Central Intelligence Agency.

595 Mladenović, 2016., Eng. National Security Agency.

596 Munoz, Arturo. U.S. Military Information Operations in Afghanistan, RAND Corporation, Santa Monica, 2012.

597 Cordey, 2019., str. 24.; prema podacima Svjetske banke i Međunarodne telekomunikacijske unije, 2019.

za propagandu (Information Operations Roadmap – Rumsfeld's Roadmap to Propaganda, US DoD, 2003.)[598]. Taj dokument specificirano je imao za cilj da Ministarstvu obrane pruži plan za napredovanje informacijskih operacija kao temeljno vojne sposobnosti proširenjem i koordinacijom vojnih psiholoških operacija i operacija javne diplomacije. Iako u dostupnim zapadnim izvorima nema javno objavljenih relevantnih podataka o američkim hibridnim operacijama u hibridnim sukobima, pretpostavka je da ih SAD provodi sinergijom obavještajnih struktura, informacijskim operacijama javne diplomacije, financijskom potporom posredničkim gospodarskim organizacijama, vanjskim civilnim suradnicima i civilno-društvenim nevladinim organizacijama te medijskim operacijama posredstvom vladinih, nevladinih i privatnih medijskih organizacija.[599]

Nesumnjivo da kiber prostor i društvene mreže u američkim hibridnim operacijama i strateškoj komunikaciji imaju važnu ulogu i da ih se svestrano koristi za pospješivanje čitavog spektra djelatnosti. Kombiniranjem čitavog spektra informacijskog djelovanja i svih dostupnih instrumenata hibridne moći, SAD protiv Rusije djeluje na strateškoj razini u kiber prostoru i informacijskom prostoru ciljanih publika hibridnim instrumentima moći: ponajprije gospodarskim (kroz nametanje sankcija) i informacijskim (strateškom komunikacijom) nastoji umanjiti ruski vanjskopolitički i gospodarski utjecaj na lokalnim i regionalnim razinama na kojima SAD nastoji održati vlastiti geopolitički utjecaj. Prema ruskim tumačenjima, to podrazumijeva sprječavanje i/ili ometanje razvoja ruskih strateških međunarodnih projekata, primarno energetskih, SAD provodi principe liberalne demokracije, unipolarnog svijeta, strategiju dominacije punog spektra i širi savezništva za potrebe NATO saveza.
Iako se radi o međusobno različitim pristupima informacijskom ratovanju, ruske i američke hibridne operacije utjecaja imaju isti cilj: stvaraju hibridne prijetnje, ciljanim publikama nameću vlastitu volju i ostvaruju informacijsku nadmoć nad protivničkim korpusom javnog znanja. Pri tome koriste sve raspoložive mogućnosti koje nude društvene mreže.

Različiti pristupi ovise o različitim potrebama, kontekstima te o povijesno različitim pristupima informacijskom ratovanju. Evidentno je da se i u modelu strateškog komuniciranja i hibridnih operacija društvene mreže koriste kao učinkoviti alati u informacijskoj borbi u kiber prostoru u vidu potpore medijskim i psihološkim operacijama koje se vode preko tradicionalnih medija (tv, tiska, radija). Međusobno suprotstavljeni sustavi vrijednosti, uvjerenja i načela oko ideja

598 US DoD. Information Operations Roadmap., 2003.

599 Cohen i Bar'el, 2017.

unipolarnog i multipolarnog svijeta čine osnovu sukobljavanja u borbi za informacijsku nadmoć. Društvene mreže služe im kao novi instrumenti moći te snažni i učinkoviti alati pomoću kojih nastoje osigurati hegemoniju i dominaciju vlastitih ideja i ideologija.

Izdvajamo šest potvrđenih ruskih primjera i jedan potvrđeni primjer američkih hibridnih operacija koje su se, ovisno o strateškim i operativno-taktičkim ciljevima i potrebama, izvodile u različitim kontekstima i na različitim razinama iskorištavanja društvenih mreža za planiranje i izvođenje hibridnih prijetnji.

Najplastičniji primjeri ruskih hibridnih operacija u hibridnom ratovanju bili su zabilježeni protiv Gruzije 2008. i Ukrajine 2014./2015. Najplastičniji primjer američkih hibridnih operacija utjecaja u hibridnom ratovanju zabilježen je protiv ISIL-a u Siriji 2015./2020.[600] Najbolji primjeri ruskih hibridnih operacija u hibridnim sukobima bili su protiv Estonije 2007., ponovno protiv Estonije te Latvije i Litve 2018./2019., SAD-a 2016., Francuske i Njemačke 2016./2017. te protiv Turske 2015./2016. Različita razina primjene društvenih mreža ovisila je o kontekstu zadanih operativno-taktičkih i strateških ciljeva hibridnih prijetnji.

U Estoniji je po prvi put upotrijebljen kiber prostor za napad na kritične infrastrukture u drugim državama, u Gruziji po prvi put za davanje potpore vojnim operacijama, a na primjeru Ukrajine društvene mreže su po prvi put korištene za pojačavanje učinaka svih hibridnih prijetnji i instrumenata hibridne moći u oružanom sukobu. Fokus operacija u Gruziji i Ukrajini bio je na umanjivanju ukupnih sposobnosti u suprotstavljanju vojnoj intervenciji. Na primjeru Ukrajine društvene mreže služile su za pojačavanje učinaka tradicionalnih operacija utjecaja i dezinformacijskih kampanja. Cilj djelovanja preko kiber prostora uz pomoć društvenih mreža bio je u učinkovitom stvaranju svih raspoloživih hibridnih prijetnji i oblika informacijsko-psiholoških pritisaka kao vida potpore vojnim, diplomatskim, gospodarskim instrumentima hibridne moći. Kontekst hibridnih operacija u Litvi, Estoniji i Latviji također je bio u stvaranju hibridnih prijetnji i davanju potpore ostalim instrumentima hibridne moći, međutim odvijale su se izvan konteksta oružanog sukoba i rata. Na primjeru Ukrajine i Gruzije jedno od najvažnijih pitanja bilo je sprječavanje širenja NATO-a na dogovorene zone utjecaja iz Jalte. Na primjeru

600 U ovu kategoriju operacija ubrajaju se i one koje su SAD i NATO savez izvodili tijekom rata na Kosovu 1998., u Afganistanu 2001. koje traju sve do danas te američke kiber operacije u Iraku od 2003. do 2011. Međutim, u njima društvene mreže nisu imale zapaženu ulogu. Na primjerima vojne intervencije na Kosovu, kao i na početku vojnih intervencija u Afganistanu i u Iraku, društvene mreže nisu postojale tako da primjeri ovih vojnih intervencija nisu predmet daljnjeg istraživanja.

hibridnih operacija protiv SAD-a 2016. tijekom kampanje za izbor Predsjednika SAD-a, Rusija je za stvaranje hibridnih prijetnji po prvi put opsežno koristila hibridnu inteligenciju za uobličavanje dezinformacija koje je širila preko društvenih mreža i preko njih stvarala učinkovite hibridne prijetnje koje su primarno bile usmjerene protiv američkog biračkog tijela. Ove operacije pokazale su se najuspješnijim ruskim tajnim operacijama utjecaja koje su izvedene protiv SAD-a.[601] Na primjeru Njemačke i Francuske ruske hibridne operacije bile su manjeg intenziteta te su se pokazale manje učinkovitim. Osim Gruzije i Ukrajine, ostale operacije odvijale su se izvan konteksta ratnog djelovanja, bile su primarno fokusirane na stvaranje prijetnji u razdobljima izbornih kampanja. Operacije u Turskoj nisu bile dio izbornih kampanja niti rata. Bile su složenijeg karaktera, s obzirom na njezin specifičan položaj sudjelovanja u ratu u Siriji, članstva u NATO-u te kao najvažnijeg ruskog energetskog partnera na području Crnog mora. Hibridne operacije SAD-a u Siriji bile su dio rata, društvene mreže koristile su se na višestruke načine za stvaranje samo dijela hibridnih prijetnji. U hibridnim operacijama u Siriji protiv ISIL-a, SAD je napustio korištenje službenih profila vladinih tijela na društvenim mrežama za planiranje i izvođenje vojnih psiholoških operacija u oružanom sukobu. Američke snage lažne račune na društvenim mrežama primarno su koristile radi sprječavanja regrutacije terorista i sprječavanja širenja terorističke propagande. Terorističke organizacije društvene mreže koristile su kao glavne alate za regrutaciju i za strateško komuniciranje, propagandu i mobilizaciju ciljanih publika za vlastite ideje i ideologije. Iz primjera ruskih hibridnih operacija na primjeru uplitanja u predsjedničke izbore u SAD-u 2016. i američkih hibridnih operacija u Siriji, iako se radi o različitom kontekstu, najočitija razlika je bila u opsegu primjene hibridnih prijetnji, u trajanju pripreme, ciljevima i opsegu informacijsko-psiholoških pritisaka. Američke hibridne operacije u Siriji bile su daleko kraće u pripremama i trajanju jer se naprosto radilo o *ad hoc* vojnoj intervenciji.

Ciljevi ruskih hibridnih operacija u SAD-u i EU-u bili su identični - stvaranje hibridnih prijetnji, a svrha društvenih mreža bila je pojačati hibridne prijetnje tijekom izbornih procesa. Izborni procesi i izborne kampanje pokazali su se razdobljima u kojima strani akter hibridnim operacijama može učinkovito pojačavati hibridne prijetnje i učinkovito iskorištavati društvene

601 Nye, 2019. Za ovu tvrdnju autor izdvaja izjavu bivšeg direktora NSA Michaela Haydena citiranog u Davis V. Gioe, Cyber Operations and useful fools: the approach of Russian hybrid intelligence, Intelligence and National Security. https://doi.org/10.1080/02684527.2018147934, prema kojem je Hayden izjavio "*I would not want to be in an American court of law and be forced to deny that I never did anything like that as director of NSA*" prema Suing Spies, The Economist, September 15, 2018, str. 29.

slabosti ciljanih publika. Društvene mreže u ovim razdobljima pokazale su učinkovitim alatima za stvaranje konstantnih (24/7) informacijskih i psiholoških pritisaka.[602] U razdobljima političkih kampanja i izbornih procesa, društvene slabosti najpogodnije su za produbljivanje podjela a volja i odluke ciljanih publika najpogodnije su za napade dezinformacijama i stvaranje informacijsko-psiholoških pritisaka sa svrhom (pre)oblikovanja njihovih uvjerenja, načela i vrijednosti u korist napadača, sve iz nekoliko razloga: tijekom izbornih procesa i kampanja u središtu javnog interesa su razne društvene i političke teme oko kojih se ciljane publike ujedinjuju i/ili se dijele; medijska pokrivenost tih tema preko tradicionalnih i netradicionalnih medija je najintenzivnija; u pravilu postoji visoka politička i društvena napetost, a aktivnosti ciljanih publika na društvenim mrežama tada su najizraženije te se radi o razdobljima kad ciljane publike donose odluke kojima određuju budućnost društva i države. Postojeće društvene slabosti tada su bolje iskoristive i tad kiber operacije predstavljaju glavnu hibridnu prijetnju društvu i demokratskim procesima.

Na primjeru izbora u Francuskoj i Njemačkoj pokazalo se da se tehnikom trolanja za učinkovitije širenje dezinformacija i propagande podjednako služe simpatizeri krajnje desnih i krajnje lijevih političkih stranaka.[603] U Francuskoj krajnje desne hakerske skupine koristile su ruske dezinformacijske sadržaje i razmjenjivale su taktike trolanja i dezinformiranja sa srodnim desničarskim hakerskim skupinama iz inozemstva.[604] U Francuskoj su mete hakerskih napada bili predsjednički kandidat Emmanuel Macron, kandidat La France Insoumise Jean-Luc Mélenchon, kandidat Socijalističke partije Benoît Hamon i kandidat Republikanske stranke François Fillon. U Njemačkoj je meta hakerskih napada bila Angela Merkel koja je branila snažne pozicije za nastavak sankcija protiv Rusije. Na izborima u Austriji i Nizozemskoj bilo je tek nekoliko zabilježenih slučajeva ciljanih dezinformacija protiv konkretnih kandidata, no ove države nisu o tome izvještavale u tolikoj mjeri kao Francuska i Njemačka. Rusija je, zbog službene optužbe administracije SAD-a i pripisivanja odgovornosti za uplitanje u netom završene predsjedničke izbore u SAD-u, opravdano privlačila najveću pažnju država EU-a.

602 Usp. Backes Oliver i Swab Andrew, Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States, Belfer Center for Science and International Affairs Harvard Kennedy School, 2019.

603 Baezner, Marie; Robin, Patrice, Hotspot Analysis: Cyber and Information Warfare in elections in Europe, 2017.

604 Usp. Cordey, 2019.

Međutim, to ne znači da i druge države i/ili nedržavni akteri nisu bili upleteni u destabiliziranje izbornih procesa na europskom tlu.[605]

Komparacijom ruskih hibridnih operacija u Europi i SAD-u vidljivo je da su korištene sve mogućnosti koje društvene mreže nude za stvaranje informacijsko-psiholoških pritisaka, od kiber napada na kritične infrastrukture do psiholoških operacija u kojima su se dezinformacije prilagođavale društvenim slabostima ciljanih publika. Međutim, s različitim intenzitetom napada prema različitim kritičnim infrastrukturama, različitim razinama pripreme, trajanju samih operacija i po opsegu korištenja hibridne inteligencije za stvaranje hibridnih prijetnji. Dezinformacije su u svim primjerima bile ključni čimbenik pomoću kojeg su svi uključeni akteri ciljanim publikama nastojali stvarati informacijsko-psihološke pritiske i pojačavati hibridne prijetnje. U primjeru SAD-a ruski kiber napadi na štićene informacijsko-komunikacijske sustave državnih institucija i političkih stranaka bili su daleko složeniji i agresivniji, dok su na tlu Europe bili slabije sofisticiranosti. Na oba kontinenta Rusija se prilagođavala političkom kontekstu i informacijskom okruženju te je kombinirala različite vrste hibridnih prijetnji, kao i različit intenzitet njihove primjene. Međutim, ciljevi su bili gotovo identični: stvaranje hibridnih prijetnji na operativno-taktičkoj i strateškoj razini, sve ovisno o potrebama i uočenim slabostima ciljanih publika koje su se prikupljale na društvenim mrežama na osnovu uvjerenja, načela i vrijednosti. Primjenom hibridne inteligencije za stvaranje dezinformacija i botova, trolova i astroturfing kampanja za njihovo ubrzavanje i širenje, dezinformacijama se pojačavao učinak i predstavljale su glavnu hibridnu prijetnju pomoću koje su se pojačavale ostale hibridne prijetnje i to ponajprije one koje su imale za cilj dodatno produbiti društvene, političke i ideološke podjele među ciljanim publikama. Cilj ovih operacija je bio postići informacijsku nadmoć nad korpusom znanja ciljanih publika. Najplastičniji primjer razlike između ruskih operacija na europskom i američkom kontinentu bio je u intenzitetu i troškovima. Troškovi operacija u SAD-u iznosili su oko 25 milijuna USD, dok su u Europi bili daleko niži.[606]

605 Usp. Baezner i Robin, 2017.

606 Nye, 2019.

6.3. Hibridne operacije i prijetnje kao dio hibridnog ratovanja - primjer hibridnih operacija Rusije u Ukrajini (2014/2015)

U hibridnom ratu u Ukrajini Rusija je koristila sve raspoložive instrumente hibridne moći i sve vrste hibridnih prijetnji. Primjer ruske intervencije ukazao je na moć hibridnih operacija za stvaranje hibridnih prijetnji. Sinergija kiber prostora, društvenih mreža, psiholoških operacija i instrumenata hibridne moći ovih čimbenika rezultirala je strateškom posljedicom – aneksijom Krima. Primjer Ukrajine bio je prvi primjer ruskog hibridnog ratovanja u kojem je društvene mreže koristila kao potporu kinetičkim vojnim operacijama i psihološkim operacijama. Ukrajina je bila primjer implementacije doktrine ratovanja nove generacije ruskog generala oružanih snaga Gerasimova. Asimetričnost kiber prostora iskorištena je pomoću društvenih mreža za stvaranje višestrukih i učinkovitih prijetnji i informacijsko-psiholoških pritisaka kroz kiber napade na kritične infrastrukture i psihološke operacije. U psihološkim operacijama društvene mreže, lažni računi, botovi, trolovi te strojno i automatizirano upravljane astroturfing kampanja koristilo se za stvaranje niza hibridnih prijetnji: povećavanje vidljivosti dezinformacija i strateških narativa s ruskih tradicionalnih medija, web portala i blogova.[607] Pozivi na promjenu politike i iniciranje prosvjeda ostvarivani su i najbolje su bili vidljivi kroz porast lažnih računa na Twitteru koji se podudarao s početkom procesa poznatog kao Euromaidan revolucija.[608] Trend povećanja registriranja lažnih računa na Twitteru zamijećen je i u rano proljeće 2014., pred sam početak oružane pobune na istoku Ukrajine.[609]

Najbitniju ulogu imale su automatizirane, masovne i optimizirane dezinformacije koje su se stvarale na društvenim mrežama i pomoću kojih je bilo moguće stvarati sve ostale hibridne prijetnje. Stvarao se izravan utjecaj na javno mnijenje, potkopavala se društvena kohezija, poticale su se podjele, izazivala se eskalacija društveno-političkih protesta, potkopavali su se suparnički politički programi, iskorištavala su se etnička i kulturna pitanja, isticale su se društvene slabosti, nastojalo se smanjiti povjerenje javnosti u rad vlade i vojske te potkopavati njihovu vjerodostojnost i legitimnost njihovih politika i operacija, širio se strah, panika, neizvjesnost. Preko društvenih mreža pružala se potpora vojnim operacijama na terenu, služile

---

607 Usp. Foxall Andrew, Putin's Cyberwar: Russia's Statecraft in the Fifth Domain, Policy Paper No. 9, Russia Studies Centre at the Henry Jackson Society, London, 2016. Dostupno na: http://henryjacksonsociety.org/wp-content/uploads/2018/06/Putins-Cyberwar.pdf

608 Svetoka, Sandra, Social media as a tool of Hybrid Warfare, Strategic Communications Centre of Exellence, NATO, Riga, 2016. Dostupno na: https://www.stratcomcoe.org/social-media-tool-hybrid-warfare

609 Ibid.

su za mobiliziranje vlastitih ciljanih publika i demobiliziranje protivničkih. Davala se informacijsko-psihološka podrška stvaranju separatističkih regija i jačanju separatističkih pokreta. Informacijsko-psihološkim pritiscima davala se potpora ostalim instrumentima hibridne moći, diplomatskim, vojnim i ekonomskim pritiscima.

Rusija je u hibridnim operacijama u Ukrajini dodatno primijenila ekonomsko-energetski instrument hibridne moći. To je Rusiji bilo potrebno budući da je Ukrajina bila važan čimbenik za tranzit i opskrbu europskog tržišta ruskim energentima. Ovakav paradigmatski zaokret u kombiniranju svih raspoloživih instrumenata moći kroz kiber prostor i uz pomoć društvenih mreža zapadne političke i vojne elite (primarno SAD-a i država članica NATO saveza) opisale su kao primjer ruskog hibridnog ratovanja. Iz ruskog kuta ove operacije promatrale su se kao obrambena strategija od američkih hibridnih aktivnosti strateškog karaktera i odgovor na američki „informacijski rat protiv Rusije".[610] Ruski zaokret opisan je doktrinom ratovanja generala Gerasimova koja podrazumijeva potrebu Rusije da snažnije iskoristi sva raspoloživa sredstva moći koja se mogu iskorištavati kroz kiber prostor kako bi se suprotstavila američkim hibridnim prijetnjama. Društvene mreže pokazale su se kao jedno od najučinkovitijih sredstava pomoću kojih je bilo moguće na najbolji način iskoristiti asimetričnost koju nudi kiber prostor i prednosti koje nude tehnologije društvenih mreža za masovnu, automatiziranu, optimiziranu i anonimnu diseminaciju dezinformacija i pomoću dezinformacija učinkovitije stvaranje hibridnih prijetnji iz kiber prostora. Ruski model hibridnog ratovanja pokazan na primjeru Ukrajine 2014. i 2015. dio je puno šireg strateškog pristupa u iskorištavanju svih prednosti informacijsko-komunikacijskih sustava i računalnih tehnologija u kiber prostoru kako bi se suprotstavila SAD-u i NATO savezu.[611] Njezin pristup opisuje se dijelom šireg koncepta nelinearnog ratovanja u kojem aktivnosti u kiber prostoru ne moraju nužno voditi brzoj pobjedi, već se baziraju na korištenju kiber prostora za stalna prilagođavanja napadačkog djelovanja. Kiber prostor i društvene mreže ovom pristupu nude gotovo savršene mogućnosti: anonimnost, neregulirano okruženje, brzinu i neposrednost koje su ojačane mogućnostima koje nude društvene mreže kroz prikupljanje potrebnih podataka i informacija na osnovi kojih je subverzivne mjere i informacijsko-psihološke pritiske, uz pomoć hibridne inteligencije moguće

610 Usp. Wither, James. Making Sense of Hybrid Warfare. Connections: The Quarterly Journal. 15., 2016., str. 73-87., dostupno na: https://www.researchgate.net/publication/301237833_Making_Sense_of_Hybrid_Warfare

611 Usp. Schnaufer, Tad A. II. Redefining Hybrid Warfare: Russia's Non-linear War against the West, Journal of Strategic Security 10, no. 1, str. 17-31., 2017. DOI: http://doi.org/10.5038/1944-0472.10.1.1538 Dostupno na: https://scholarcommons.usf.edu/jss/vol10/iss1/3

prilagođavati protivničkim slabostima, s ciljem umanjivanja njegove borbene spremnosti i narušavanja psihološke ravnoteže. Krajnji cilj je preko kiber prostora korištenjem svih raspoloživih mogućnosti koje nude informacijsko-komunikacijski sustavi i računalne tehnologije osigurati strateško djelovanje sa svrhom dugotrajnog slabljenja ukupne političke i vojne moći SAD-a i NATO saveza[612] kako bi onemogućila provedbu njihovih politika.

Glavni motiv bio je spriječiti pristupanje Ukrajine NATO savezu i zadržati Crnomorsku vojnu flotu na Krimu. Strateška logika hibridnih operacija bila je stvaranje višestrukih hibridnih prijetnji te narušavanje ukupne učinkovitosti upravljanja, donošenje brzih i adekvatnih protuodgovora. Primjer hibridnog rata u Ukrajini pokazao je da se društvene mreže mogu koristiti kao jedan od najučinkovitijih informacijskih instrumenata hibridne moći pomoću kojeg se mogu na djelotvoran način provoditi višestruke hibridne prijetnje. Pokazale su se učinkovitim alatom za ostvarivanje specifičnih taktičkih zadaća: stvaranje automatiziranih, anonimnih i masovnih dezinformacija sa svrhom stjecanja informacijske nadmoći i stvaranja informacijsko-psiholoških pritisaka na ciljane publike u Ukrajini i izvan nje. Pokazale su se učinkovitim alatom pomoću kojeg je ujedno moguće prilagođavati taktičko-operativno djelovanje, ovisno o ciljanim publikama i njihovim slabostima.

6.4. Hibridne operacije i prijetnje kao dio hibridnih sukoba – primjer ruskih hibridnih operacija i prijetnji prema Turskoj (u kontekstu rata u Ukrajini i u Siriji)

Ruske hibridne operacije i stvaranje hibridnih prijetnji prema Turskoj bile su dio geopolitičkog sukoba Rusije sa SAD-om i NATO savezom i dio nastojanja za održavanjem položaja Rusije kao ključnog aktera na širem području Crnog mora, istočnog Mediterana i Bliskog istoka. Kontekst hibridnih operacija u Turskoj bio je višeznačan i složeniji u izvedbama. Na kontekst i dinamiku ruskih hibridnih operacija i vrste hibridnih prijetnji koje je preko kiber prostora primjenjivala prema Turskoj utjecalo je nekoliko povezanih čimbenika. Turska je važna članica NATO saveza koja graniči s državama Bliskog istoka i Kavkaza (područjima koja obilježavaju stalne krize, hibridne prijetnje i oružani sukobi). Turska je sudionik oružanog posredničkog rata u Siriji u kojem je, na početku njegovog izbijanja, s Rusijom imala suprotstavljena gledišta spram vlasti u Siriji. Turska je Rusiji bila glavni partner u realizaciji novog ruskog energetskog pravca preko Crnog mora koji je za Rusiju važan iz geopolitičkih ekonomskih i vojnostrateških

612 Ibid.

razloga. Turska je Rusiji bila važan partner jer novim energetskim pravcem Rusija želi smanjiti geopolitički položaj Ukrajine kao ključne države za izvoz ruskog plina u Europu. Razlozi za smanjivanje geopolitičkog položaja Ukrajine su aspiracije SAD-a i Ukrajine za članstvom u NATO savezu. Navedeni čimbenici zahtijevali su rusku prilagodbu u primjeni hibridnih operacija i prijetnji geopolitičkom kontekstu i položaju Turske te je u njima bilo potrebno balansirati intenzitet i vrste hibridnih prijetnji kao i primjenu ekonomskih, diplomatskih i vojnih instrumenata hibridne moći. Uz diplomatske, informacijske i vojne instrumente hibridne moći važnu ulogu u ruskim hibridnim operacijama prema Turskoj, kao i na primjeru Ukrajine, imao je ekonomsko-energetski instrument moći.

Sinergijom svih instrumenata hibridne moći, kroz hibridne operacije i prijetnje, prema Turskoj i Ukrajini Rusija je nastojala realizirati ciljeve energetske politike te geopolitičke i geostrateške interese. U pozadini operacija prema Turskoj interesi su bili višestruki i povezani s hibridnim ratom u Ukrajini, aneksijom Krima i u suprotstavljanju interesima Turske u Siriji kako bi spriječila scenarij nasilnog rušenja vlasti koji su zagovarali SAD, članice NATO saveza i sunitske države Bliskog istoka. Cilj operacija i prijetnji usmjerenih prema Turskoj bio je podrivanje jedinstva NATO saveza, narušavanje kredibiliteta politika širenja NATO saveza na Ukrajinu i stjecanje naklonosti Turske kako bi pomoću Turske realizirala novi energetski pravac i time smanjila važnost Ukrajine za izvoz vlastitih energenata prema Europi. Glavni motiv bio je onemogućiti nastojanja Turske u svrgavanju vlasti u Siriji. Hibridnim prijetnjama i operacijama prema Turskoj Rusija je nastojala spriječiti razvoj „zapadnog“ energetskog pravca koji je Turska podržavala iz ekonomskih razloga. Radilo se o plinovodu koji je iz smjera Katara, preko Iraka i Sirije, trebao završiti u Turskoj kao krajnjoj točki za izvoz katarskog plina prema Europi čime bi Turska postala važno energetsko čvorište za opskrbu Europe katarskim plinom. Inicijativu je pokrenuo SAD kako bi ograničio ruski energetski utjecaj u Europi, a realizaciju plinovoda podržavale su pojedine članice EU-a, Turska i sunitske države na Bliskom istoku. Iz očitih razloga ovom projektu se protivila Rusija, a protivila se i Sirija jer je bio u koliziji s planovima Sirije da ona postane važno kopneno, pomorsko, energetsko i prometno čvorište Bliskog istoka i istočnog Mediterana.[613]

Zadržavanje Crnomorske vojne flote na Krimu Rusiji je bio važan preduvjet za održavanje njezine vojnopomorske nazočnosti na istočnom Mediteranu i u vojnim bazama u sirijskim

613 Sirija je 2009. pokrenula inicijativu pod nazivom „Strategija četiri mora“. Inicijativa je pokrenuta pred početak procesa poznatog kao „Arapsko proljeće“ koji je u Siriji rezultirao ratom. Kasnije tijekom rata u Siriji, sunitske države financirale su terorističke organizacije preko kojih su htjele srušiti sirijsku Vladu.

lukama kako bi mogla pružati operativnu taktičku i stratešku vojnu potporu Siriji. Pad vlasti u Siriji omogućio bi realizaciju novog zapadnog energetskog pravca koji bi ugrozio ruski energetski pravac preko Crnog mora koji je, na koncu, Rusija uspjela realizirati zajedno s Turskom. Primjeri jasno ukazuju na stratešku ulogu i moć hibridnih operacija i društvenih mreža kao učinkovitih sredstava za kombiniranje prijetnji i važnog informacijskog instrumenta hibridne moći kojim se osnažuju ostali instrumenti moći. Društvene mreže time su se pokazale kao učinkoviti alati u stvaranju informacijsko-psiholoških pritisaka koji mogu rezultirati potencijalnim strateškim posljedicama.[614] U ovom slučaju to je značilo zadržavanje na vlasti sirijske Vlade, smanjenje tranzita vlastitog plina preko Ukrajine i realiziranje vlastitog plinovoda preko Crnog mora radi opskrbe plinom EU-a.

6.5. Hibridne operacije i prijetnje kao dio hibridnog (posredničkog) rata u Siriji (2015. – 2020.) - primjer ISIL-a i SAD-a

Kiber prostor i društvene mreže tijekom Arapskog proljeća odigrale su veliku ulogu u širenju ideja i organiziranju demonstracija koje su rezultirale društveno-političkim prevratima u Tunisu, Libiji i Egiptu. Sirija je bila jedini primjer iz procesa „Arapskog proljeća“ u kojem su ulični prosvjedi i protuvladine demonstracije eskalirali u otvoreni posrednički rat. Prije Sirije nikad nije bila zabilježena toliko velika razina iskorištavanja kiber prostora i nikad nije bila zabilježena toliko opsežna upotreba društvenih mreža od strane svih aktera u zonama nekog sukoba.[615] Početak rata u Siriji koincidirao je s porastom korištenja računala u Siriji. Iznosio je 22,5%, dok je svega deset godina ranije bio na 0,2%.[616] Društvene mreže koristilo se za stvaranje brojnih hibridnih prijetnji. Dezinformacije i propaganda bile su ključne za učinkovito poticanje eskalacija društveno-političkih protesta, terorizma, nacionalnog i vjerskog ekstremizma; regrutirali su se teroristi; potenciralo se etnički motivirano nasilje i sektaško nasilje. Društvene mreže opsežno i učinkovito se koristilo za prikupljanje taktičkih obavještajnih podataka, mobiliziranje ciljanih publika, produbljivanje podjela i poticanje niza psiholoških čimbenika kako bi ciljane publike donosile odluke u korist napadača. Razumijevanje međunarodne dimenzije posredničkog rata u Siriji važno je za bolju kontekstualizaciju aktivnosti uključenih aktera (vanjskih, unutarnjih i posredničkih). U ratu u

614 Ovim primjerom dodatno je odgovoreno na 2. istraživačko pitanje.

615 Lynch, Freelon, Aday, 2014.

616 Baezner, Marie; Robin, Patrice, Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, 2017.

Siriji preko lokalnih vjerskih zajednica u početku su međusobno ratovali Iran i Libanon protiv Saudijske Arabije, Turske i Katara.[617] Kasnije je došlo do udvostručavanja snaga i odnosa. Preko ova dva bloka suprotstavljenih regionalnih država sukobljavali su se interesi glavnih hibridnih aktera SAD-a i Rusije. Posredničke hakerske grupe svi uključeni akteri koristili su društvene mreže vrlo opsežno za stvaranje konstantnih informacijsko-psiholoških pritisaka spram svih kategorija ciljanih publika. Kiber tehnološki napadi na informacijsko-komunikacijske sustave bili su nižeg i ograničenog ranga kvalitete. Međutim, ovakvi napadi preko kiber prostora bili su vrlo opsežni i provodile su ih visokim intenzitetom sve vrijeme trajanja rata sve uključene strane.

Kiber tehničkim napadima preko društvenih mreža narušavane su međusobne protivničke internetske usluge i infrastrukture, prikupljani su obavještajni podaci o pripadnicima, strukturama i položajima protivničkih snaga. Hakerske grupe većinom su koristile manje sofisticirane zlonamjerne programe dostupne na internetu. Kiber operacije tehnološkog utjecaja time su bile ograničene kvalitete, ali bile su vrlo opsežne i intenzivno su ih provodile čitavo vrijeme trajanja rata sve uključene strane. Hibridna inteligencija na društvenim mrežama bila je manje zastupljena za stvaranje dezinformacija. Automatiziranost poruka i informacija na društvenim mrežama primarno se koristila za učinkovitiju mobilizaciju i/ili demobilizaciju ciljanih publika te za širenje terorističke propagande i povezanih ideologija. Od svih društvenih mreža Facebook je najviše koristila provladina Sirijska elektronička vojska kao primarni alat u borbi za informacijsku nadmoć i služila se njime kao svojevrsnim centrom za odnose s javnošću u korist svojih sponzora.[618]

Za SAD je rat u Siriji označio novu paradigmu iskorištavanja društvenih mreža za planiranje i izvođenje kiber psiholoških operacija utjecaja u ratnim operacijama. Američkim hibridnim operacijama upravljao je Kiber centar za strateške protuterorističke komunikacije Ministarstva vanjskih poslova SAD-a. Prije preustroja, za svoje aktivnosti na društvenim mrežama koristio se službenim i stvarnim računima na društvenim mrežama. Primarni cilj američkih operacija preko društvenih mreža bio je u demobiliziranju i sprječavanju regrutacije terorista i suzbijanju širenja terorističke propagande. No, nakon njegovog preustroja do kojeg je došlo tijekom rata

617 Saudijska Arabija, Turska i Katar izravno su se protivile realizaciji inicijative sirijske Vlade „Strategija četiri mora“ a podržavale su razvoj inicijalno katarskog projekta plinovoda kojem je političku podršku davao SAD kao jedinoj alternativi koji je, po količinama plina iz neruskih izvora, trebao smanjiti ulogu ruskih dobavnih plinovodnih pravaca za EU.

618 Usp. Baezner i Robin, 2017.

u Siriji, preimenovao se u Kiber centar za globalna djelovanja, a operacije utjecaja nastavio je voditi lažnim računima na društvenim mrežama iz jednostavnog razloga što se na taj način postižu bolji rezultati u psihološkom djelovanju prema ciljanim publikama. Pretpostavka je da Kiber centar za globalna djelovanja Ministarstva vanjskih poslova SAD-a upravlja s nekoliko stotina lažnih računa na društvenim mrežama. Međutim, Rusija kroz „farme trolova“ poput spomenute „Agencije za istraživanje interneta“ vjerojatno upravlja znatno većim brojem lažnih računa. Iako je opseg korištenja lažnih profila američkog Kiber centra za globalna djelovanja relativno nedostupan, evidentno je da ovu mogućnost u hibridnim operacijama opsežno koriste i SAD i Rusija[619], ovisno o specifičnim operativno-taktičkim ili strateškim ciljevima i potrebama ispunjavanja ciljeva nacionalnih informacijskih strategija.

Od brojnih terorističkih organizacija koje su sudjelovale u ratu u Siriji, teroristička organizacija koja se najviše istaknula u planiranju i izvođenju hibridnih operacija bila je teroristička organizacija Islamska država Iraka i Levanta (ISIL) nazivana još i ISIS (Islamska država Iraka i Sirije) koja se smatrala najopasnijom, najbolje organiziranom i najdisciplinirani jom skupinom na Bliskom istoku, najbogatijom i financijski najbolje pokrivenom terorističkom organizacijom ikada te najtežom terorističkom prijetnjom do tada čiji cilj nije bio samo borba protiv Zapada, već uspostava i širenje Islamske države gotovo do Rima gdje je, prema njihovim prijetnjama, proklamirala uništenje prijestolnice katoličanstva.[620] Uz to što je bio teroristička organizacija, ISIL je pomoću društvenih mreža vješto regrutirao i mobilizirao ciljane publike te ih je kao sofisticirani obavještajni aparat koristio za prikupljanje podataka kojima je manipulirao kako u svojim redovima tako i u suparničkim grupama. ISIL je uz to bio propagandna, ideološka mašinerija koja je pomoću društvenih mreža vrlo učinkovito širila svoje ideje i ciljeve te pridobivala nove članove putem različitih sredstava i različitim mamcima. ISIL je fascinirao svojom dobrom organizacijom, ustrojstvom, dobro i taktički razrađenim načinima vladanja, uopće uspostavom vlasti, pridobivanjem novih članova i simpatizera. ISIL je bio primjer terorističke organizacije koja je društvene mreže iskoristila na daleko učinkovitiji način od bilo koje druge. U hibridnim operacijama ISIL se najviše oslanjao na društvenu mrežu Twitter.

619 Usp. Cordey, 2019.

620 Usp. Radman, Lana, Psihologija terorizma Islamske države Iraka i Levanta, str. 1., Sveučilište u Zagrebu, Fakultet političkih znanosti, 2016. Dostupno na: https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg:122 (14.03.2017.).

Preko Twittera je regrutirao teroriste, širio terorističku propagandu, radikalizirao i indoktrinirao ciljane publike te je učinkovito homogenizirao sunite oko ideje kalifata. Twitter je koristio i za niz drugih potreba (npr. za financiranje, prikupljanje obavještajnih podataka i sl.). Međutim, za ove potrebe Twitter su koristile i druge terorističke organizacije i s njima povezane hakerske grupe. Specifičnost ISIL-a bila je u korištenju Twittera za uspostavljanje inicijalne komunikacije s potencijalnim teroristima, nakon koje bi daljnju regrutaciju, radikalizaciju i indoktrinaciju preusmjeravao na diskretnije i zatvorene mobilne komunikacijske aplikacije poput WhatsAppa i Telegrama te prema web stranicama koje su imale ograničeni pristup isključivo za potrebe radikalizacije terorista.[621] Twitter je tehnološkim rješenjima svim svojim korisnicima nudio tehničku i praktičnu jednostavnost u realizaciji ciljeva. Pružao je bolju kriptozaštitu, bio je prikladniji za otvorenu, anonimnu i šifriranu komunikaciju te je nudio jednostavniju mogućnost reaktiviranja ugašenih računa. Na Twitteru je ISIL imao najmanje 46.000 registriranih računa, ne brojeći lažne. Od ukupnog broja lažnih računa, 20% bilo je automatizirano i strojno upravljano.[622] Pomoću automatiziranog upravljanja mreže lažnih računa ISIL je koristio za regrutaciju i mobilizaciju te za povećavanje vidljivosti poruka i narativa stvarajući dojam o nepobjedivosti, sposobnosti i pobožnosti. Preko Twittera odvijala se glavna komunikacijska strategija koja je imala je za cilj dugoročnu transformaciju društva s potencijalnim strateškim učincima. Twitter je tvorničkim postavkama automatiziranih tehnologija koje su održavale njegove osnovne funkcije omogućio neprekidno ponavljanje desetak tisuća vjerskih sadržaja, jačanje i održavanje homogenosti te jednostavnost u prenošenju poruka i strateških narativa. Twitter je ISIL-u bio učinkovit alat za širenje ključnih narativa za ispunjavanje informacijske strategije: narativ brutalnosti služio je privlačenju pažnje na globalnoj razini, narativ utopizma za novačenje novih pristaša, narativ milosrđa za stjecanje povjerenja, a narativima kojima se propagiralo podnošenje žrtve, spremnost za rat i pripadnost vlastitim vrijednostima dodatno se motiviralo i mobiliziralo ciljane publike. Ključnu ulogu u regrutiranju mlađe generacije boraca imala je globalna dostupnost Twittera i drugih društvenih mreža preko pametnih telefona. Kratke tekstualne, video i audio poruke preko Twittera bile su daleko učinkovitije za regrutiranje boraca nego dugački monolozi Al Qaidinih vođa.[623]

---

621 Usp. NATO, 2016.

622 Berger J. M. i Morgan Jonathan, The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter, The Brookings Center for Middle East Policy. 2015, str. 7. Dostupno na: https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

623 NATO, 2016.

Društvene mreže u ratu u Siriji pokazale su se kao učinkovit alat u borbi za informacijsku nadmoć i učinkovit informacijski instrument hibridne moći kojim se informacijski prostor izlagao neprekidnim (24/7) informacijsko-psihološkim pritiscima te pojačavalo ostale instrumente hibridne moći (diplomatske, ekonomske i vojne) svih uključenih aktera.

6.6. Hibridni sukob SAD-a i Rusije - primjer ruskih hibridnih operacija i prijetnji tijekom predsjedničkih izbora u SAD-u (2016)

U historiografiji informacijskog ratovanja hibridne operacije izvedene tijekom američke izborne kampanje 2016. za predsjednika SAD-a bile su primjer najsloženije i najuspješnije (tajne) operacije utjecaja koju je Rusija izvela kroz kiber prostor pomoću društvenih mreža. Primjena hibridne inteligencije na društvenim mrežama za stvaranje dezinformacija, primjena svih raspoloživih tehnoloških rješenja za obradu i upravljanje podacima i informacijama koje na društvenim mrežama nude tehnologije umjetne inteligencije, hibridna inteligencija, automatizirano upravljanje mrežama lažnih računa, botovi, trolovi, astroturfing kampanje za planiranje i upravljanje psihološkim operacijama pokazali su moć za postizanje strateških ciljeva. Ovi primjeri hibridnih operacija podignuli su percepciju i svijest javnosti o moći društvenih mreža u psihološkim operacijama za stvaranje čitavog spektra hibridnih prijetnji usmjerenih na destabiliziranje političkih i izbornih procesa i postizanje informacijske nadmoći sa strateškim učincima. Ovi primjeri javnosti su neupitno pokazali da tehnološka nadmoć jednog aktera, u ovom slučaju SAD, ne predstavlja nužno veliku prednost, već da nadmoć u kiber prostoru postiže ona strana koja je kroz psihološke operacija sposobnija i učinkovitija u iskorištavanju svih raspoloživih prednosti koje nude kiber prostor i informacijsko-komunikacijske i računalne tehnologije koje koriste društvene mreže. Pokazali su javnosti moć tehnologija umjetne inteligencije i hibridne inteligencije na društvenim mrežama za planiranje i izvođenje kiber operacija utjecaja u hibridnom sukobu kao glavne hibridne prijetnje preko koje je bilo moguće na učinkovit način stvarati sve ostale hibridne prijetnje i ostvarivati stratešku logiku takvih prijetnji: stvarati izravan utjecaj na javno mnijenje, pogoršavati društvene podjele, poticati građanske nemire, uplitati se u izborni proces, smanjivati povjerenje američkih građana u nositelje vlasti, potkopavati upravljanje državnim funkcijama, poticati nasilni ekstremizam preko kiber prostora. Ključna hibridna prijetnja je bila stvaranje dezinformacija na društvenim mrežama te pomoću hibridne inteligencije prilagođavanje dezinformacija i strateških narativa društvenim slabostima američkog biračkog tijela na temelju njihovih uvjerenja, načela i vrijednosti. Ova mogućnost pokazala se učinkovitim načinom za

stvaranje konstantnih informacijsko-psiholoških pritisaka prema američkom biračkom tijelu kako bi se destabilizirao izborni proces.

U izbornim i političkim kampanjama Republikanska i Demokratska stranka u SAD-u godinama koriste Facebook i unajmljuju tvrtke specijalizirane za politički digitalni marketing koje, u tu svrhu, koriste usluge Facebooka u formi informacijskih operacija. Facebookove tehnike i metode za planiranje i izvođenje informacijskih operacija, za potrebe hibridnog rata u Siriji korištene su za stvaranje informacijsko-psiholoških pritisaka prema ciljanim publikama. Također ih je koristila i Rusija za potrebu uplitanja u izborne procese u Europi i u operacijama koje su bile usmjerene prema Turskoj. Međutim, u daleko manjem opsegu i sa slabijim razinama sofisticiranosti. Na primjeru hibridnog sukoba sa SAD-om i primjeru stvaranja hibridnih prijetnji prije, tijekom i nakon predsjedničke kampanje u SAD-u, informacijske operacije koje je osmislio Facebook i hibridnu inteligenciju Rusija je iskoristila na do tad najsloženiji način za planiranje i izvođenje psiholoških operacija. U ovim primjerima Rusija je pokazala sposobnost i umijeće u iskorištavanju hibridne inteligencije na društvenim mrežama. Primjenom hibridne inteligencije na društvenim mrežama, javno dostupne podatke i osobne preferencije američkih glasača iskoristila je za optimiziranje dezinformacija i na taj način dezinformacijama i manipuliranjem informacija na društvenim mrežama na učinkovit način iskoristila postojeće društvene slabosti SAD-a za vlastite političke ciljeve.

Uplitanje u izborne procese kao pojava i u kontekstu informacijskih sukoba kao i po prirodi ciljeva nije novi fenomen.[624] Radilo se o (tajnoj) psihološkoj operaciji utjecaja kojom je jedna strana drugoj strani nastojala destabilizirati izborni proces. Međutim, novost je bila u kiber prostoru preko kojeg su izvođene ove operacije, u metodologiji njihovog izvođenja, korištenim sredstvima, načinima i akterima koji su sudjelovali u njezinom izvođenju. Radilo se o (tajnoj) psihološkoj i specijalnoj operaciji. Nositelji ove operacije bile su ruske obavještajne strukture i s njima povezane i od strane države sponzorirane hakerske organizacije. Glavna sredstva bile su najpopularnije društvene mreže visokotehnoloških korporacija Facebook, Twitter i Google (YouTube). U operacijama se koristilo sve raspoložive mogućnosti koje ove korporacije nude

624 O povijesti uplitanja u međusobne izborne procese vidi više: Baezner i Patrice, 2017. i Walker Robert, Combating Strategic Weapons of Influence on Social Media, Naval Postgraduate School, Homeland Security Digital Library, SAD, 2019. Dostupno na: https://www.hsdl.org/?abstract&did=828243 Primjerice, 1968. Rusija je pomagala demokratskom kandidatu Hubertu Humphreyju da pobijedi na izborima protiv republikanskog i antikomunističkog kandidata Richarda Nixona. Također, primjer iz 1982. kada je ruska obavještajna služba protiv republikanskog kandidata Ronalda Reagana pokrenula dezinformacijsku kampanju u kojoj je prikazivan korumpiranim kandidatom američke obrambene industrije.

svojim korisnicima: lažni računi pojedinačni i grupni, automatizirani i strojno upravljani lažni računi, botovi, trolovi, memesi. Također, na društvenim mrežama korištena je hibridna inteligencija i sve druge tehnologije umjetne inteligencije koje obavljaju osnovne zadaće s podacima i informacijama na društvenim mrežama. Tehnologije umjetne inteligencije koje se primjenjuju na društvenim mrežama i podaci o uvjerenjima, načelima i vrijednostima američkih građana zloupotrebljavali su se za prepoznavanje društvenih slabosti američkog društva te su se isti ti podaci pomoću hibridne inteligencije koristili za planiranje i izvođenje psiholoških operacija u kojima su dezinformacije bile optimizirane prema navedenim slabostima te uvjerenjima, načelima i vrijednostima. Na ovaj način društvene mreže korištene su za stvaranje hibridnih prijetnji ovisno o potrebama.

Hibridne prijetnje koje su SAD i Rusija međusobno stvarale prema vlastitim ciljanim publikama kroz kiber prostor bile su dio međusobnih političkih napetosti i geopolitičkog sukoba. Eskalacija hibridnih prijetnji kroz kiber prostor bila je najvidljivija u periodu od početka procesa „Arapskog proljeća“ do njihove kulminacije u izbornoj 2016., kad su se odvijali izbori za novog američkog predsjednika.[625] Kad je SAD u okviru mandata UN-a započeo međunarodnu vojnu intervenciju u Libiji, novoizabrano rusko državno rukovodstvo nakon netom završenih izbora u Rusiji koncem 2011. i početkom 2012., optužilo je tadašnju državnu tajnicu SAD-a H. Clinton za poticanje i davanje potpore opoziciji u Rusiji za organiziranje antivladinih prosvjeda. Hibridne prijetnje su se nastavile i tijekom 2013., kad je ruski haker po imenu „Guccifer“ hakirao račun e-pošte Joea Podeste, bivšeg pomoćnika Billa Clintona. Sadržaj mailova naknadno je ciljano i isplanirano pušten u javnost u jeku predsjedničke kampanje 2016. protiv H. Clinton preko web poslužitelja WikiLeaks i DCLeaks. Sadržaj mailova javnosti je otkrio da je H. Clinton za vrijeme obnašanja dužnosti državne tajnice SAD-a privatni račun e-pošte koristila za razmjenu osjetljivih i tajnih podataka o vanjskopolitičkim pitanjima, što je bilo protivno odredbi saveznih zakona SAD-a.[626] Ovim činom ruski hakeri htjeli su ostvariti stratešku logiku: potkopati politički program kandidatkinje Demokratske stranke, utjecati na ponašanje biračkog tijela, diskreditirati vjerodostojnost i legitimnost politika te smanjiti povjerenje birača u nju kao kandidatkinju ove stranke kao nositelja aktualne vlasti. Tijekom 2014. zabilježen je niz kiber napada ruskih hakera na informacijsko-komunikacijske sustave Bijele kuće i Ministarstva vanjskih poslova SAD-a. U međuvremenu u Ukrajini je došlo

625 Usp. Baezner i Patrice, 2017.

626 Ibid.

do političkog prevrata i smjene dotadašnjeg proruskog rukovodstva Ukrajine, nakon čega je u Ukrajini uslijedio hibridni rat koji je rezultirao uspostavljanjem paralelnih neformalnih struktura vlasti i separatističkih regija s proruskim elementima na istoku Ukrajine i aneksijom Krima. Sve vrijeme sukoba SAD-a i Rusije, Ukrajina je bila poligon na kojem su obje zemlje kroz kiber prostor primjenjivale sve vrste hibridnih prijetnji. Ruski hakeri nastavili su s nizom kiber upada u informacijski sustav Pentagona i osobne elektroničke pošte američkih vojnih zapovjednika Središnjeg zapovjedništva oružanih snaga te u informacijske sustave Demokratske stranke.[627] Vrhunac ruskih hibridnih prijetnji odvijao se tijekom izborne 2016., kad je Rusija pokrenula najopsežnije dezinformacijske kampanje preko društvenih mreža. Iste godine zabilježeni su novi kiber napadi na servere Demokratske stranke i servere za registraciju glasača u saveznim državama. Ruski hakeri uspjeli su izvući korisničke podatke oko 200.000 američkih državljana iz saveznih država Arizona i Illinois. Iste godine, Rusija je na svom teritoriju prijavila otkrivanje zlonamjernog špijunskog programa na internetskim mrežama 20 različitih ruskih organizacija te je optužila SAD za pokroviteljstvo. SAD je optužio Rusiju za hakerske upade u servere Demokratske stranke i servere za registraciju glasača u saveznim državama, na što je Rusija odgovorila optužbama da je SAD politički i financijski davao podršku protuvladinim medijima i nevladinim organizacijama u Rusiji kako bi destabilizirao izbor novog ruskog predsjednika na izborima iz 2011./2012. Podrška antivladinim medijima i nevladinim organizacijama i demonstracijama koje su uslijedile diljem Rusije javnosti je bila poznata kao Snježna revolucija, a ruski mediji opisivali su je i povezivali s procesima Arapskog proljeća. Ubrzo je u Siriji izbio posrednički rat. Tijekom predizborne kampanje u SAD-u, kandidatkinja Demokratske stranke H. Clinton više puta isticala je ideju da Vijeće sigurnosti UN-a u zračnom teritoriju Sirije proglasi „Zonu zabrane letenja“, opciju koju su pojedini krugovi u SAD-u žestoko kritizirali zbog bojazni da bi to moglo dovesti do eskalacije sukoba s Rusijom.[628] Ruski kiber napadi na informacijsko-komunikacijske sustave Demokratske stranke koji su trajali sve vrijeme mogu se dovesti u kontekst s potencijalnim ruskim strahovima da bi izborom H. Clinton za Predsjednicu SAD-a u Siriji mogla biti uvedena navedena restrikcija UN-a poput one u Libiji koja je dijelom pridonijela svrgavanju libijskog vođe Ghaddafija. Rusija na sličan scenarij u slučaju Sirije nije htjela pristati zbog niza geopolitičkih,

627 Ibid., prema podacima Ministarstva za nacionalnu sigurnost i Saveznog ureda za istrage SAD-a. Iste godine UN-ova skupina vladinih stručnjaka, uključujući predstavništva 20 država, zajedno sa SAD-om i Rusijom, u kontekstu međunarodne sigurnosti objavila je izvješće o međunarodnim normama u području informacija i telekomunikacija (United Nations General Assembly, 2015).

628 Baezner i Patrice, 2017.

vojnostrateških geoekonomskih interesa na Bliskom istoku i istočnom Mediteranu.[629] Rusija je zapravo imala interes spriječiti dolazak na vlast demokratskog kandidata.[630] Prema podacima koje je objavila američka obavještajna zajednica, iza ruskih napora u pomaganju republikanskom kandidatu Donaldu Trumpu bio je i motiv osvete prema Demokratskoj stranci i H. Clinton zbog podrške koju su davali protuvladinim medijima, nevladinim organizacijama i opoziciji u Rusiji.[631] Naposljetku, nakon što je koncem 2016. demokratska kandidatkinja izgubila izbore, tadašnja vlada na odlasku službeno je optužila Rusiju da se uplitala u američki izborni proces i da je svojim aktivnostima u kiber prostoru i na društvenim mrežama pogodovala izboru Trumpa.

U učinkovitom stvaranju hibridnih prijetnji glavnu ulogu imali su tehnološki kiber napadi koji su se odvijali od početka Arapskog proljeća. Tehničkim kiber napadima na američke institucije ruski hakeri godinama su prikupljali podatke koje su naknadno, u izbornoj godini 2016., iskoristili za stvaranje učinkovitih dezinformacija. Prikupljene podatke može se kategorizirati prema dva kriterija. U prvoj kategoriji bili su podaci koji su se prikupljali iz informacijskih sustava i mreža državnih tijela koja su zadužena za upravljanje vanjskom i obrambenom politikom i izbornim procesima. U konkretnom primjeru radilo se o informacijsko-komunikacijskim sustavima Bijele kuće, američkog Ministarstva vanjskih poslova, Pentagona, Središnjeg zapovjedništva oružanih snaga, Nacionalne sigurnosne agencije i serverima s registrima glasača. U drugoj kategoriji bili su podaci koji su se prikupljali iz informacijskih sustava i mreža tijela Demokratske stranke: Nacionalnog Vijeća Demokratske stranke i Kongresnog izbornog vijeća. Političke stranke i njihovi informacijsko-komunikacijski sustavi posebno su zanimljive mete stranim obavještajnim službama jer političke stranke imaju pristup dokumentima o državnim politikama, a nemaju adekvatne i stroge mjere tehničke zaštite kao što imaju vladine institucije. Podaci američkih državnih, administrativnih, sigurnosnih, vojnih i političkih institucija iskorišteni su naknadno u dezinformacijskim kampanjama preko društvenih mreža u jeku predizborne i izborne kampanje.

---

629 Evan, Osnos; David, Remnick; Joshua, Yaffa; Annals of Diplomacy, Trump, Putin, and the New Cold War, What lay behind Russia's interference in the 2016. election—and what lies ahead?, March 6, 2017., https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war (05.08.2020)

630 Ibid.

631 Usp. Baezner i Patrice, 2017.

Uz vojne i civilne obavještajne strukture, nositelji dezinformacijskih kampanja bili su hakeri „Agencije za istraživanja interneta“ - ruske medijske korporacije sa sjedištem u Sankt Peterburgu, javnosti poznatije kao „farma trolova“.[632] Podijeljeni po timovima, pokrivali su različite teme iz američke unutarnje i vanjske politike. Svakodnevno su morali stvarati lažne profile, dezinformacije i komentirati zbivanja u SAD-u. Njihova misija bila je sudjelovati u „informacijskom ratu protiv SAD-a“ i općenito „širiti nepovjerenje prema kandidatima i političkom sustavu“.[633]

U hibridnim operacijama fokus nije bio na izazivanju tehnoloških poremećaja u glasačkim sustavima, kao na primjeru iz Ukrajine, niti u vidu napada za uskraćivanje usluga, niti su mete kiber napada bile kritične infrastrukture kako bi se izazivali poremećaji u gospodarskim djelatnostima kao što je bio primjer u Estoniji i u hibridnom ratu s Gruzijom i Ukrajinom. Fokus je bio na stvaranju dezinformacija na društvenim mrežama kako bi se dezinformacijama učinkovitije stvarao čitav niz drugih hibridnih prijetnji koje su bile primarno usmjerene na remećenje izbornog procesa, produbljivanje podjela, potenciranje društvenih nemira i izazivanje sumnji u pouzdanost te diskreditacija izbornih poruka američkim glasačima. Presudnu ulogu imali su lažni računi, automatizacija širenja dezinformacija i hibridna inteligencija pomoću koje su ruski hakeri dezinformacije prilagođavali uočenim slabostima i glasačkim preferencijama američkih državljana. Facebook se koristio za objavljivanje dezinformacijskih oglasa koji su bili sastavljeni na manipulativan način, tako da se dezinformacije nisu mogle prepoznati na vrijeme i time spriječiti njihov učinak. Neprepoznatljivost su postigli na način da su ih prilagođavali postojećim i različitim rascjepima u američkom društvu. Podaci koje su koristili bili su osobni stavovi i sklonosti te podaci, obavijesti, vijesti i informacije koje su bile javno dostupne iz američkih medija. Ovi podaci prikupljali su se godinama unaprijed te je, na osnovi njih, stvorena ogromna baza podataka o društvenim, klasnim i ideološkim podjelama po saveznim državama, o funkcioniranju američkog izbornog sustava i sl. Radilo se o klasičnom primjeru pripremne faze psiholoških operacija. Društvene mreže Facebook i Twitter i lažni profili u kombinaciji s primjenom hibridne inteligencije omogućili su učinkovitije produbljivanje postojećih podjela. Važnu novinu u pripremanju psiholoških operacija društvene mreže unijele su time da je bilo moguće

632 O ruskim „farmama trolova“ vidi pobliže: Sindelar Daisy, The Kremlin’s Troll Army, The Atlantic, 2014; Murdock Jason, What is the Internet Research Agency? Facebook Shuts Hundreds of Accounts Linked to Russian Troll Factory; Calamur Krishnadev, What is the Internet Research Agency?, The Atlantic, 2018.

633 Singer i Brooking, 2018.

godinama unaprijed graditi vjerodostojnost lažnih pojedinačnih i grupnih profila, stvarati sljedbenike i pomoću njih „legalizirati“ dezinformacije koje su se objavljivale u jeku izborne kampanje. Algoritmi Facebooka dodatno su rasplamsali javne rasprave na internetu o pitanjima imigracije, kontrole oružja, ali i druga otvorena pitanja iz američkog društva. Novina je bila i u mogućnostima da se stvarnim događajima pridaju dezinformacije koje su time dobivale na dodatnoj vjerodostojnosti. Primjer su bili sukobi policije s pripadnicima afroameričke zajednice. Botovima se dezinformacijama dodatno davala vjerodostojnost jer su omogućili njihovo automatizirano i masovno širenje. Na ovaj način su se učinkovito kroz društvene mreže i u širem medijskom prostoru pojačavale hibridne prijetnje. Stvaralo se okruženje javne nesigurnosti; isticali su se korupcijski skandali te kadrovske i političke odluke američke administracije; kandidati su se izlagali javnom sramoćenju; poticao se nacionalni, vjerski i politički ekstremizam; potencirala su se etnički motivirana djela nasilja i eskalacija društveno-političkih protesta; društvene, kulturne, vjerske i etničke skupine pozivalo se na promjene u dotadašnjim obrascima glasanja te ih se pozivalo na prosvjede. Pozivi preko Facebooka i Twittera, u kojima su botovi povećavali njihovu vidljivost, bili su očigledni primjeri koji su rezultirali upotrebom vatrenog oružja u Charlestonu u Južnoj Karolini, na koncertu u Las Vegasu u Nevadi, okupljanjem članova desničarske grupe Unite the Right u Charlottesvillu i povezano nasilje.[634] Ovi događaji o kojima su izvještavali američki mediji koristili su se za uobličavanje novih dezinformacija, a ciljane publike su bile radikalne skupine, nezadovoljnici socijalnom i ekonomskom situacijom i oporbeni društveni pokreti u cilju produbljivanja sukoba između manjina i ostatka stanovništva.[635] Strateški plan ruske dezinformacijske kampanje bio je potaknuti i pojačati nepovjerenje američkog društva u državne institucije i u izborni proces.[636] Psihološke operacije dizajnirane pomoću lažnih profila, automatiziranog sustava povratne sprege društvenih mreža i korištenjem hibridne inteligencije na društvenim mrežama bile su dodatno subverzivne, dvosmislene, bilo ih je teško pravovremeno identificirati te javno definirati i pripisati odgovornost. Cjelokupna namjera bila je nejasna i namjerno prikrivena.

Tijekom istrage koju su američka istražna tijela pokrenula nakon izbora, ni u jednom od dokumenata u kojima su istražna tijela opisala rusku metodologiju iskorištavanja lažnih računa za svoje aktivnosti nije bilo navedeno da je Rusija stvorila okruženje u koje je zasadila „sjeme

634 Walker Robert, Combating Strategic Weapons of Influence on Social Media, Naval Postgraduate School, Homeland Security Digital Library, SAD, 2019.

635 Ibid.

636 Nye, 2019.

podjela“.[637] Također, nisu izneseni statistički podaci i dokazi o izravnom učinku na konačni izborni rezultat. Društveno okruženje u SAD-u je od ranije bilo obilježeno rasizmom, ksenofobijom, netolerancijom, nasiljem, suprotstavljenim stavovima oko prava na nošenje oružja, kriminalom, homofobijom, islamofobijom i ekstremizmom.[638] Međutim, Rusija je hibridnim operacijama pomoću društvenih mreža, lažnim računima i primjenom hibridne inteligencije na društvenim mrežama uspjela trenutno utjecati na percepciju američkog biračkog tijela i na njihove obrasce ponašanja. Michael Hayden, bivši direktor Središnje obavještajne agencije SAD-a, navedeno je opisao na način da je Rusija pomoću društvenih mreža iskoristila postojeće napetosti u Sjedinjenim Državama, napominjući da „operacije utjecaja bile one prikrivene ili javne ne stvaraju podjele na terenu, nego ih pojačavaju".[639] Platforme društvenih mreža koje nude jeftinu i anonimnu mogućnost dosega milijuna ljudi pružile su jedinstvenu priliku za vođenje operacija koje nisu nove, ali su nove tehnologije koje na društvenim mrežama omogućavaju digitalne obmane.[640]

Ruske operacije bile su ogledni primjer kako su se društvene mreže, uvjerenja, načela i vrijednosti i hibridna inteligencija, kroz automatizaciju i optimizaciju izlaganja masovnim i anonimnim dezinformacijama, pomoću lažnih računa, botova i trolova, iskoristile za stjecanje informacijske nadmoći kroz tri osnovne taktike.

U prvoj taktici lažnim računima ruski hakeri su se američkim biračima predstavljali kao organizatori grupe od povjerenja. Jedan od takvih je bio lažni Twitter račun @Ten_GOP koji je sebe prozvao neslužbenim računom Republikanske stranke Tennesseeja sa sljedbom od 136.000 ljudi a to je, primjera radi, 10 puta više od broja službenih računa Republikanske stranke u Tennesseeju.[641] Njihovih 3.107 poruka bilo je ponovno tweetano 1.213.506 puta. Svaki ponovljeni tweet zatim se proširio na još nekoliko milijuna korisnika. Na dan izbora 2016. to je bio sedmi po redu najčešće retweetani račun na cijelom Twitteru.

Druga taktika bila je da su lažne račune i primijenjenu automatizaciju iskoristili kako bi se predstavili kao pouzdani izvor vijesti.[642] S naslovnom fotografijom američkog Ustava ruski

637 Walker, 2019, str. 45.

638 Ibid.

639 Ioffe Julia, The History of Russian Involvement in America’s Race Wars, The Atlantic, 2017. Dostupno na: https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/

640 Ghosh Dipayan i Scott Ben, #Digital Deceit:The Technologies behing precision propaganda on the Internet, 2018. Dostupno na: https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/

641 Singer i Brooking, 2018., str. 112

642 Ibid.

hakeri su se preko lažnog računa @tpartynews američkim biračima predstavljali kao središte konzervativnih pristaša pokreta Tea Party. Isti autori opisuju da su ruski hakeri na ovaj način mjesecima *gurali* protuimigrantske poruke u korist republikanskog kandidata, a slijedilo ih je i ponavljalo oko 22.000 korisnika Facebooka.

Konačno, treća taktika je bila da su se lažnim računima predstavili kao osobe od povjerenja: kao baka, radnik sa Srednjeg Zapada, odlikovani ratni veteran koji su objavljivali svoje emocionalne iskaze o tekućim događajima, kao i preporuke za koga glasati.[643] Lažni računi predstavljali su se na razne načine - od desno orijentiranih pristaša pokreta Tea Party do lijevo orijentiranih Crnih aktivista; one na ljevici nagovarali su da „izaberu mir i glasaju za Jill Stein, poručujući glasačima kako treba vjerovati da to nije bačeni glas. Navodni afričko-američki organizator Crnih aktivista zapravo je bio jedan od ruskih hakera sa sjedištem u Sankt Peterburgu u Rusiji čije su objave na Facebooku bile podijeljene 103.8 milijuna puta prije nego što mu je Facebook zatvorio lažni račun nakon predsjedničkih izbora.[644]

Ruski hakeri zapravo su slijedili klasične hladnoratovske *aktivne mjere* izlažući američke glasače dezinformacijskim sadržajima prema korisničkim preferencijama tijekom izborne godine koristeći obje ekstremne strane američke političke scene za vlastite potrebe.[645] Odabrani odbor za obavještajne poslove Senata Sjedinjenih Država[646] rusku strategiju *aktivnih mjera* na društvenim mrežama opisao je kroz pet ključnih ciljeva ruske dezinformacijske strategije, kroz ruske vanjskopolitičke ciljeve koje u radu opisujemo kroz hibridne prijetnje: za potkopavanje povjerenja građana u demokratsko upravljanje; poticanje i pogoršavanje podjela i političkih pukotina; narušavanje povjerenja između građana i izabranih dužnosnika i njihovih institucija; populariziranje programa ruske politike među stranim stanovništvom i stvaranje općeg nepovjerenja u glavne izvore informacija. Kako su tehnologije društvenih mreža u novom digitaliziranom okuženju omogućile zamagljivanje granica između činjenica i fikcije, postalo je moguće na nove učinkovitije načine ostvarivati dobro poznate metode aktivnih mjera i operacija utjecaja.[647]

---

643 Ibid.

644 Ibid., str. 113.

645 Ibid., str. 112.

646 Select Committee on Intelligence of the United States Senate.

647 Usp. Stoica, Aurelian. From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment, 2020. Dostupno na: https://www.researchgate.net/publication/341541149_From_Social_Influence_to_Cyber_Influence_The_Role_of_New_Technologies_in_the_Influence_Operations_Conducted_in_the_Digital_Environment

Nakon intenzivnih aktivnosti u izbornoj godini otkrivena je pozadina lažnog Twitter računa #Ujedinite desnicu (engl.#UniteTheRight) preko kojeg su se organizirali prosvjedi na krajnjoj desnici, a što je kulminiralo ubojstvom u Virginiji u Charlotesvilleu. Također je otkriveno da je ključni račun koji je širio mržnju započinjao sa svojim aktivnostima svaki dan u 8.00 sati po moskovskom vremenu. Shvativši da su otkrili lažni račun, istražene su aktivnosti na tom računu prije protesta u Charlotesvillu. Utvrđeno je da je tijekom 4 godine s tog lažnog računa dnevno objavljivano oko 100 tweetova, sveukupno više od 130.000. Isprva, glavni je fokus bio na potpori jednoj britanskoj stranci krajnje desnice. Zatim se prebacio na jačanje ruske strane u ukrajinskom sukobu da bi se potom okrenuo zagovaranju Brexita i na kraju potpori kandidaturi republikanskog kandidata na američkim predsjedničkim izborima. Nakon što su predsjednički izbori u SAD-u završili, ruski hakeri su se okrenuli prema prosvjedima ekstremističkih organizacija.[648] Pomoću mreže lažnih računa dodatno su stvarali podjele. Na Twitteru su uspjeli oformiti mrežu od barem 60.000 lažnih računa u jednoj mreži botova preko kojih su iskrivljavali američki politički dijalog[649]. Samo na Twitteru istraživači su otkrili da je od oko 400.000 bot računa koji su se borili da utječu na rezultat predsjedničkih izbora u SAD-u, dvije trećine bilo u korist republikanskog kandidata s kojih su se ponekad slale pozitivne poruke o njihovom izabranom kandidatu, dok bi u drugim slučajevima postajali agresivniji u izričaju i porukama.[650] Mreže botova protiv demokratske predsjedničke kandidatkinje aktivno su tražile hashtagove za Clinton, preplavljujući ih neprijateljskim političkim napadima. Približavanjem dana izbora, botovi u korist republikanskog kandidata povećali su se u broju i u volumenu te su nadmašili glasove u korist demokratskog kandidata u omjeru 5 prema 1.[651]

U mnogim plaćenim objavama Facebooku i Twitteru isticali su rasnu i društvenu nepravdu. Kako bi maksimizirali neslaganja i suprotstavljanja preko lažnih profila stvarali su objave kojima su unosili dodatne podjele tako što su kroz plaćene oglase povećavali vidljivost njihovih međusobno suprotstavljenih stavova. U nekima su promovirali solidarnost između manjinskih skupina, u drugima su pozivali na rasnu jednakost, a u nekima su isticali policijsku brutalnost prema manjinskim skupinama. U nekim objavama manjinske skupine poticali su na sabotiranje izbora. Istodobno, u drugim objavama nudili su potpuno drugačiju perspektivu o pitanjima rasne i društvene (ne)jednakosti. Tako su u nekima podržavali provođenje zakona i kritizirali

---

648 Singer i Brooking, 2018., str. 112.

649 Ibid., str 138-139.

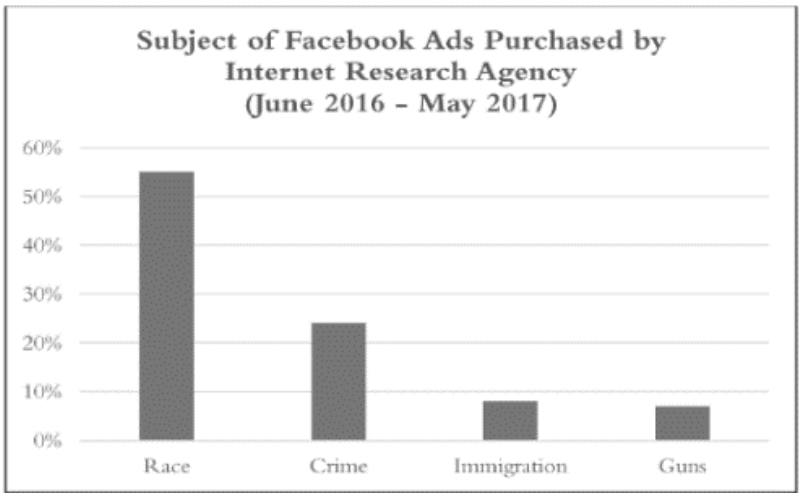
650 Ibid. str. 143.

651 Ibid.

one koji su dovodili u pitanje integritet policajaca, u nekima su omalovažavali liberalni pokret Crnački životi vrijede[652], a u nekim još ekstremnijim podržavali su bijele nacionalističke skupine pozivima na nasilje prema crnačkim zajednicama. Na jednak način iskorištavali su i druga društvena i klasna pitanja koja su bila izvorišta postojećih društvenih i političkih podjela, kao što su pitanja imigracije, LGBT prava, kontrole oružja i religije. Radilo se o sofisticiranoj i dobro koordiniranoj informacijskoj kampanji koja je osmišljena kako bi se dodatno poticale hibridne prijetnje.[653]

Neke od objava bile su u izravnoj vezi s predsjedničkim izborima ili predsjedničkim kandidatima. Međutim, mnoge objave bile su diskretne te im se nije mogla olako pripisati namjera uplitanja u izbornu kampanju. U takvim objavama podjele su se produbljivale oko problematike kriminala, imigracije, prava na nošenje oružja na način da su se ovim temama izlagale obje strane suprotstavljenog ideološkog spektra.

Tablica 1. Grafički prikaz tema koje su ruski hakeri koristili tijekom kampanje za izbor predsjednika SAD-a 2016. za stvaranje hibridnih prijetnji prema ciljanim publikama preko Facebooka (podaci se odnose za razdoblje od lipnja 2016. do svibnja 2017.)



Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str.193.

652 engl. Black Lives Matter (BLM).

653 Usp. Aceves J. William, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019. Dostupno na: https://repository.law.umich.edu/mjrl/vol24/iss2/2

Iz Tablice 1. proizlazi da su hakeri ruske „Agencije za istraživanje interneta“ Facebook koristili za stvaranje nekoliko hibridnih prijetnji: stvaranje izravnog utjecaja na javno mnijenje, pogoršavanje društvenih podjela, agitiranje i poticanje građanskih nemira, smanjenje povjerenja ciljanih publika u nositelje vlasti, uplitanje u izborni proces, potkopavanje upravljanja i državnih funkcija u pojedinim saveznim državama SAD-a. Iz Tablice 1. vidljivo je da se najviše koristila rasna problematika. Rasna problematika koristila se u 55% objava, tema kriminaliteta bila je na drugom mjestu s oko 23% objava, na trećem mjestu s oko 8% objava koristile su se teme imigracije, a na četvrtom mjestu s ukupno oko 6% objava prava američkih državljana na korištenje i upotrebu vatrenog oružja. Strateška logika objava bila je stvaranje informacijskih i psiholoških pritisaka, širenje dezinformacija, podržavanje i promicanje polarizacije političkih rasprava radi potkopavanja političkih programa američkih političkih stranaka i predsjedničkih kandidata, iskorištavanje etničkih, vjerskih i kulturnih identiteta američkih glasača radi potkopavanja društvene kohezije, organiziranje prosvjeda i povećanje rizika od radikalizacije i eskalacije nasilja.

Zoran primjer najuspješnijeg lažnog računa na Facebooku po broju isporuka i ostvarenih pregleda[654] bio je pod nazivom „Podrži značku”. Lažni profil kreiran je u jeku predsjedničke kampanje u listopadu 2016., ostvario je 1.334.544 isporuka i 73.063 pregleda. Preko ovog lažnog profila ciljane publike bili su pojedinci u dobi između 20 i 65+ godina koji žive u SAD-u, sa sklonostima i interesom prema Facebook grupama u kojima se zagovara dostojanstvo američkih policajaca. Kako bi manipulirali ovom kategorijom ciljanih publika na Facebooku, ruski hakeri otvorili su i druge lažne Facebook grupne profile pod nazivom „Podrži snage reda“[655], „Tanka plava linija“[656], „Memorijalna stranica poginulom policajcu“[657], „Ujedinjene udovice policajaca“[658], „Nacionalno udruženje supruga policajaca“[659] i „Heroji iza značke“[660].

654 Facebook razlikuje isporučene i objavljene oglase. Broj isporučenih objava određuje trenutak kada ga Facebook isporuči pojedinačnom i/ili grupnom korisniku. To ne garantira da je objava pregledana. Broj isporuka otkriva stvarni doseg prema kojem se vidi da je neki oglas pregledan. Vidi pobliže: Facebook Business, The Value of Viewed Impressions, uvid ostvaren 28.08.2020, https://www.facebook.com/business/news/viewed-impressions.

655 engl. Support Law Enforcement.

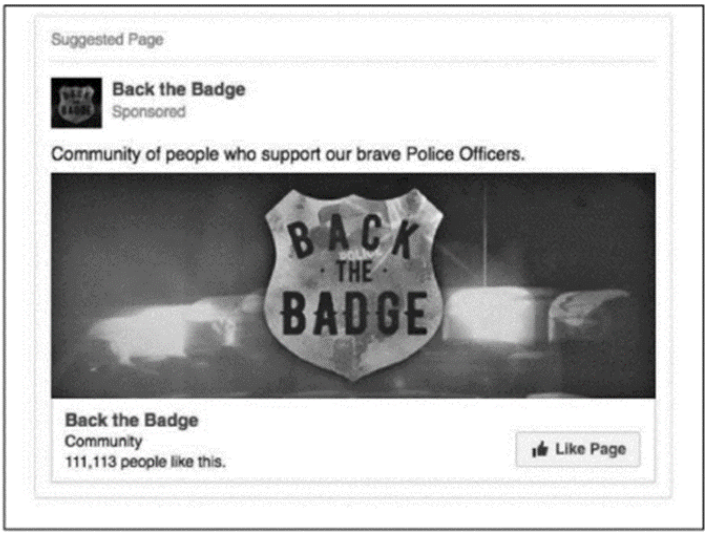
656 engl. The Thin Blue Line.

657 engl. Officer Down Memorial Page.

658 engl. Police Wives United.

659 engl. National Police Wives Association.

660 engl. Heroes Behind the Badge.



Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str.194.

Slika 29. Izgled lažnog Facebook grupnog profila „Podrži značku“.

Jedan od uspješnijih lažnih grupnih profila po broju pojavljivanja i pregleda isporučenih objava/oglasa kojim se produbljivala podjela po rasnoj problematici bio je lažni grupni profil „Crna pitanja“. Kreiran je u srpnju 2015., više od godinu dana prije same predsjedničke kampanje.[661] Ciljane publike bili su pojedinci između 18 i 65 godina, s prebivalištem u SAD-u i sa sklonostima i interesima prema Facebook grupama koje su okupljale zagovornike dostojanstva crnačke populacije. U svrhu produbljivanja podjela na ovu temu, ruski hakeri registrirali su i druge lažne Facebook grupne profile pod nazivom „Martin Luther King, Jr.“, „Pokret za civilna prava afričkih Amerikanaca“[662], „Afrička američka povijest“[663], „Malcolm X“, „HuffPost Crni glasovi“[664] i „Afrički Amerikanac“[665].

661 Autor se poziva na arhivu oglašavanja preko DM: U.S.HOUSE OF REPRESENTATIVES, PERMANENT SELECT COMMON INTELLIGENCE,

https://drive.google.com/open?id=1yxQ7-T_5aWvfMaIOMjrFOFjmP2PNQfVm.

662 engl. African American Civil Rights Movement.

663 engl. African American history.

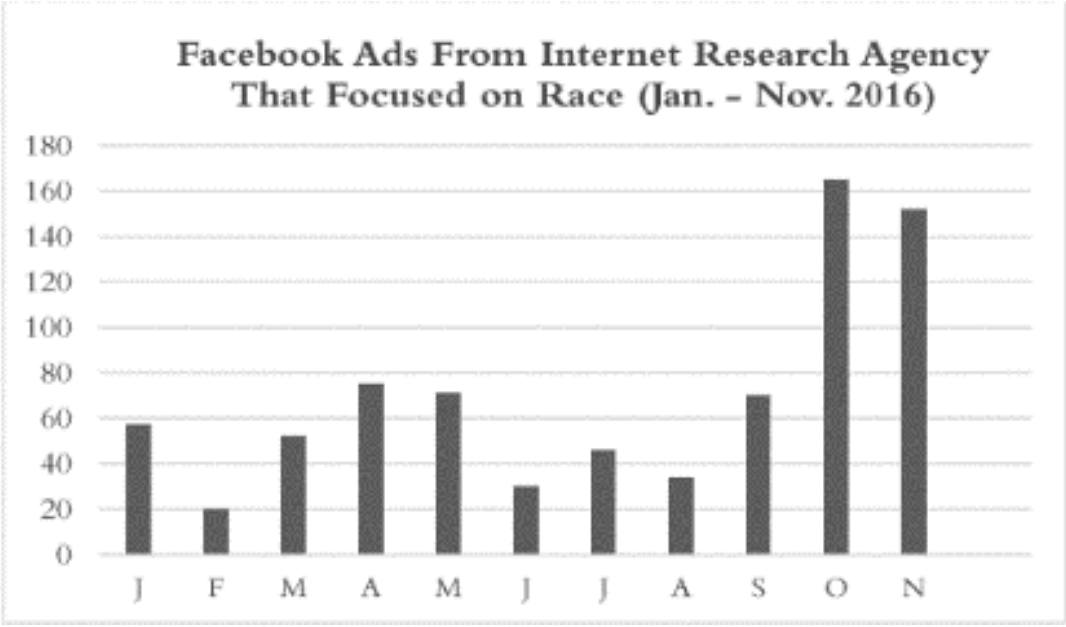
664 engl. HuffPost Black Voices.

665 engl. African American.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str.195.

Slika 30. Izgled lažnog Facebook grupnog profila „Crna pitanja“.

Tablica 2. Grafički prikaz trenda porasta rasno intoniranih oglasa koji su objavljivani posredstvom lažnih profila na Facebooku, za razdoblje od siječnja do studenoga 2016.



Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 195.

Iz podataka prikazanih u Tablici 2. nedvosmisleno proizlazi da je količina informacijskih sadržaja koji su bili usredotočeni na podizanje rasnih pitanja i tenzija tijekom izbornog ciklusa varirala na mjesečnoj razini. Iz predloženog prikaza proizlazi da se količina takvih sadržaja u razdoblju od lipnja 2015. do prosinca 2015. kretala od 20 do 70 mjesečno. Sve do rujna 2016. broj objava bio je relativno stalan s manjim oscilacijama. Međutim, kako se približavao vrhunac predsjedničke kampanje, broj objava drastično je povećan u listopadu i studenome 2016.

The True Story of 'Rights' in the United States

American Imperialism–It's War, Struggle, Racism!

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str.186.

Slika 31. Ilustracija plakata kojima je sovjetska vlada iskorištavala rasnu problematiku u SAD-u za širenje ideja komunizma.

Slikom 31. želi se pokazati da rasna problematika koju su hakeri ruske Agencije za istraživanje interneta koristili za stvaranje hibridnih prijetnji tijekom izborne kampanje za predsjednika

SAD-a 2016. nije bila nova ruska taktika. Slikom se želi pokazati da se rasna problematika koristila u operacijama utjecaja još iz vremena bivšeg SSSR-a iz 1919., kada su tadašnji čelnici SSSR-a prepoznali da rasna nejednakost u SAD-u pruža priliku za promicanje i širenje ideja komunizma. Tada su se za kritiziranje propusta američke unutarnje politike koristili tiskani mediji, a vizualne slike u obliku plakata bile su važan dio propagandnih kampanja. Tema rasizma bila je dominantna u mnogim kampanjama iz tog doba. Rasna problematika bila je aktualna i korisna i za stvaranje hibridnih prijetnji u izbornoj godini 2016. Za isticanje i stvaranje podjela na Facebooku aktivno najviše su se koristili rasno intonirani grupni lažni profili: „Crni aktivisti“[666], Afričko Kraljevstvo“[667] i „Probuđeni Crnci“[668]. Povjerenje među afroameričkim biračkim tijelom gradilo se time što ih se privlačilo u članstvo kroz slogane i pozive na borbu za crno dostojanstvo, objavama domoljubnog i šaljivog sadržaja, kao i temama iz popularne kulture. Međutim, kako su se približavali izbori, ruski hakeri su ih, kako se radi o tradicionalnim glasačima Demokratske stranke, personaliziranim izlaganjem (dez)informcijskim sadržajima u formi oglasa nastojali odvratiti od izlaska na izbore.[669] Unutar svake lažne Facebook grupe prilagođenim objavama prema korisničkim preferencijama jačala se homogenost unutar grupe ili između više grupa s jednakim uvjerenjima, vrijednostima i načelima. No, istodobno se između grupa sa suprotnim vrijednostima, uvjerenjima i načelima objavama koje su u sebi imale elemente dezinformacije pojačavala međusobna netrpeljivost. Na jednak način poticao se strah od džihadizma, homofobije te podjele oko zakona i prava na nošenje vatrenog oružja.[670] Na jednak način lažni profili i automatski sustav povratne sprege doprinijeli su dodatnim podjelama oko policijskih intervencija. U tu svrhu ruski hakeri koristili su pojedinačne račune pod lažnim nazivima *Watch.the.Police, Being Patriotic, USA_Gunslinger, Angry Eagle*.[671] Američka obavještajna zajednica potvrdila je da se radilo o svakodnevnim temama koje su prisutne u američkim medijima i američkom društvu.

666 engl. Blacktivist.

667 engl. AfroKingdom.

668 engl. Woke Blacks.

669 Walker, 2019.

670 Vilmer i autori, 2018. Autori za detaljniji uvid o ruskom uplitanju u američku izbornu kampanju 2016. upućuju na na Borisa Toucasa, L’Affaire russe: la démocratie américaine ébranlée, IFRI Research Paper, Potomac Papers, 32, December 2017.

671 Walker, 2019.

Tablica 3. Grafički prikaz dosega rasno intoniranih oglasa po ostvarenom broju dijeljenja i ostvarenih interakcija pomoću lažnih profila na Facebooku prema različitim kategorijama načela, uvjerenja i vrijednosti ciljanih publika.[672]

Nazivi lažnih Facebook profila	**Facebook URL**	**Ukupni broj ostvarenih podjela**	**Ukupni broj ostvarenih interakcija**
Crni aktivisti	/Blackactivist	103,767,792	6,182,835
Srce Texasa	/Txrebels	102,950,151	3,453,143
Ujedinjeni muslimani Amerike	/MuslimAmerica	71,355,895	2,128,875
Biti domoljub	/Patriototus	51,139,860	4,438,745
Sigurne granice	/Secured.Borders	5,600,136	1,592,771
Ujedinjeni LGBT	/Lgtbun	5,187,494	1,262,386

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 197.

Iz Tablice 3. prepoznaje se da su, tijekom izborne kampanje za Predsjednika SAD-a 2016., najveći broj međusobnih interakcija unutar vlastitih zajednica ostvarile zajednice koje po načelima, uvjerenjima i vrijednostima predstavljaju međusobno suprotstavljene kategorije ciljanih publika: Srce Texasa, Biti Domoljub i Sigurne granice (koje zagovaraju smanjivanje prava manjinskim skupinama i protive se ilegalnim migracijama) nasuprot zajednica koji zagovaraju povećavanje prava manjina i ilegalne migracije (Ujedinjeni LGBT), koje zagovaraju veća vjerska prava islamskim zajednicama u SAD-u (Ujedinjeni muslimani Amerike) i zajednica koje se bore za snažnije poštivanje prava crnačke populacije (Crni aktivisti). Navedeni brojevi o ostvarenim međusobnim interakcijama unutar vlastitih zajednica nedvosmisleno upućuju da je cilj lažnih objava hakera ruske Agencije za istraživanje interneta bio unutarnja mobilizacija svake pojedinačne zajednice čime su se ujedno pospješivale dodatne podjele između zajednica sa suprotstavljenim načelima, uvjerenjima i vrijednostima. Na ovaj način pospješivalo se stvaranje niza hibridnih prijetnji: stvarao se izravan utjecaj na javno mnijenje, pogoršavale su se društvene podjele, pozivalo se na građanske nemire, uplitalo se u izborni proces, smanjivalo se povjerenje u nositelje vlasti, potkopavalo se upravljanje državnih funkcija u pojedinim saveznim državama, poticao se nasilni ekstremizam te se pospješivalo ostvarivanje strateške logike za svaku navedenu hibridnu prijetnju.

672 Pod interakcijama na društvenim mrežama podrazumijeva se komentiranje, davanje oznaka sviđanja ili nesviđanja na određene informacijske sadržaje i njihovo prosljeđivanje drugim korisnicima društvenih mreža.

Osim što su bile masovne, automatizirane i anonimne, (dez)informacije su bile dodatno neprimjetne jer su objave na društvenim mrežama bile optimizirane prema uvjerenjima, načelima i vrijednostima američkih birača. Prema ovom kriteriju optimizirane dezinformacije mogle su se podijeliti prema nekoliko kategorija[673] kojima su se njihovi stvaratelji vodili prilikom planiranja. Prvu kategoriju činile su objave s elementima satire ili parodije[674] u kojima nije bilo namjere da izazovu štetu, ali je u njima bila namjera prevare. Drugu kategoriju činile su objave s namjerom da zbunjuju i obmanjuju[675] kojima se željelo uobličiti željeni kontekst neke teme, događaja ili osobe. Treću kategoriju činile su objave s varljivim sadržajima u kojima se autor predstavljao originalnim i autentičnim sadržajima[676]. Četvrtu kategoriju činile su objave s fabriciranim sadržajima[677] koji su bili 100% lažni, s namjerom da prevare i nanesu štetu. Petu kategoriju činile su objave s lažnim poveznicama[678] u kojima naslovi ili vizualni sadržaji nisu podržavali sadržaj prema kojem se usmjeravala pozornost. Šestu kategoriju činile su objave s lažnim kontekstima[679] u kojima se originalni sadržaj neke informacije ili vijesti iz medija dijelio zajedno s dezinformacijom. Sedmu kategoriju činile su objave s manipulativnim sadržajima[680] u kojima se manipuliralo nekom originalnom viješću, informacijom ili fotografijom s namjerom prevare.

Preko Twittera ruski hakeri uspjeli su generirati na milijune objava. Utvrđeno je približno 2.752 lažna profila preko kojih je objavljeno oko 131.000 poruka.[681] Uz to, identificirano je približno 36.000 lažnih profila s aktivnostima koje su bile vezane uz predsjedničke izbore. Preko njih je na vrhuncu izborne kampanje objavljeno oko 1,4 milijuna objava. Matematički gledano ove objave na Twitteru ostvarile su približno ukupno 288 milijuna pojavljivanja. Twitter je dodatno iskorišten za stvaranje hibridnih prijetnji među američkim građanima, a prednjačile su objave

673 Wardle Claire, Fake News: It's Complicated, First Draft, 2017, dostupno na: https://firstdraftnews.org/fake-news-complicated/

674 engl. Satire or Parody.

675 engl. Misleading Content.

676 engl. Imposter Content.

677 engl. Fabricated Content.

678 engl. False Connection.

679 engl. False Context.

680 engl. Manipulated Content.

681 Aceves, 2019. Isti autor se poziva na dokument Russian Investigative Task Force Hearing with Social Media Companies Before the H. Permanent Select Comm. on Intelligence, 116th Cong. 11, 2017. (statement of Sean J. Edgett, Acting General Counsel, Twitter, Inc.)

na temu rasnih podjela koje su iskorištene na do tada nezabilježen način.[682] Google je prijavio najmanji broj aktivnosti povezanih s ruskom propagandnom kampanjom. Identificirao je samo dva računa za koja se činilo da su dio ruske dezinformacijske kampanje, što su Googleovi dužnosnici objasnili time da je razlog tomu najvjerojatnije činjenica da su te aktivnosti bile ograničene zbog različitih Googleovih zaštitnih mjera koje su uvedene uoči izbora i činjenice da svoje proizvode nije prepustio personaliziranom ciljanju koje su preferirali ruski hakeri.[683]

Prema optužnici Ministarstva pravosuđa SAD-a protiv ruske „Agencije za istraživanje interneta“, za još dva entiteta te trinaest ruskih državljana navodi se da su se lažnim profilima američkih osoba na društvenim mrežama predstavljali kao američki građani, da su upravljali lažnim stranicama i lažnim grupnim profilima kako bi privlačili pozornost američkih građana na vlastite objave. Optuženi su da su preko lažnih profila na društvenim mrežama poticali podjele oko političkih i društvenih pitanja, da su lažno prikazivali da račune na društvenim mrežama kontroliraju američki aktivisti a u stvarnosti su ih kontrolirali optuženi. Optuženi su da su ukradenim identitetima stvarnih američkih osoba preko lažnih profila pod kontrolom ruske Agencije za istraživanje interneta objavljivali oglase kojima su ometali američki politički sustav, uključujući i predsjedničke izbore 2016.[684] Optuženi su za organiziranje političkih skupova unutar SAD-a i da su se pri tom predstavljali kao američki entiteti i osobe, bez otkrivanja ruskog identiteta i pripadnosti Agenciji za istraživanje interneta te da su na taj način neke političke kandidate promovirali, a neke omalovažili i da su lažno se predstavljajući komunicirali s nesvjesnim pojedincima povezanim s kampanjom republikanskog kandidata i drugim političkim aktivistima kako bi koordinirali političke aktivnosti.[685] Američka optužnica identificirala je nekoliko ključnih momenata. Veliki broj plaćenih objava Facebooku odnosio se na političke stranačke kandidate i u većini njih se republikanskog kandidata predstavljalo u pozitivnom svjetlu, dok se demokratskog kandidata predstavljalo u negativnom svjetlu. No, isto tako, istaknuto je da se dio objava uopće nije odnosio ni na kandidate niti na izbore, već na isticanje niza pitanja društvene problematike. U optužnici se objašnjava da su nekim objavama

682 Ibid. dokument Russian Investigative Task Force Hearing with Social Media Companies Before the H. Permanent Select Comm. on Intelligence, 116th Cong. 11 (2017) (statement of Rep. K. Michael Conaway).

683 Ibid., dokument Russian Investigative Task Force Hearing with Social Media Companies Before the H. Permanent Select Comm. on Intelligence, 116th Cong. 11 (2017) (statement of Kent Walker, Senior Vice President and General Counsel, Google).

684 Ibid. dokument Indictment at 20-23, United States v. Internet Research Agency, No. 18-cr00032-DLF (D.D.C. Feb. 16, 2018), 2018 WL 91477 [hereinafter IRA Indictment].

685 Ibid.

ruski hakeri imali za cilj utjecati na konzervativne glasače i da su u tu svrhu koristili lažne profile „Sigurne granice“, „Stop Invaziji stranaca“ i „Ujedinjeni Jug“ , „Srce Teksasa“, da su se lažnim profilima pod nazivom „Probuđeni Crnci“, „Crni aktivisti“, „Ujedinjeni Muslimani Amerike“ i „Ujedinjeni američki domoroci“ preko kojih su (dez)informacijama nastojali utjecati na odluke manjinskih skupina. Stalni odbor za obavještajne poslove Doma[686] naknadno je objavio detaljno izvješće prema kojem je ruska dezinformacijska kampanja koristila više platformi, uključujući Facebook, Twitter, Instagram i Google, da su objave generirane u svrhu "promoviranja političkih i društvenih poruka kojima su se izazivale podjele kroz ideološki spektar…". Potom je Senatski odbor za obavještajne poslove izdao preliminarno izvješće u kojem se navodi da je istraga razotkrila "daleko opsežnije napore Rusije da manipulira medijima kako bi se posijao razdor i uplitalo u izbore 2016. i u američko društvo".[687] U naknadno objavljena dva izvješća[688] Senatski odbor za obavještajne poslove objavio je detaljnu forenzičku analizu podataka kojom je ojačan zaključak da su napori Rusije bili koordinirani, sustavni i da su nastojali dodatno produbiti podjele američke javnosti.[689] Primijetili su, na primjer, da je ruska dezinformacijska kampanja potaknula „afroameričke glasače da bojkotiraju izbore ili da slijede pogrešne postupke glasanja 2016., da je među meksičko-američkim i latinoameričkim biračima nastojala stvoriti osjećaj nepovjerenja u američke institucije“, da je potaknula „da ekstremno desno orijentirani birači budu dodatno suprotstavljeni" i da je širila „senzacionalističke, zavjereničke i druge oblike bezvrijednih političkih vijesti i dezinformacija na glasače širom političkog spektra".[690]

Slikama 29. i 30. te slikama od 32. do 46. želi se prikazati izgled i sadržaj lažnih profila na Facebooku koji su bili predmet istraga Senatskog odbora za obavještajne poslove SAD-a koji

---

686 engl. House Permanent Select Committee on Intelligence. Ibid., dokument: H. PERMANENT SELECT COMM.ON INTELLIGENCE, 116TH CONG., REP.ON RUSSIA'SACTIVE MEASURES (2018),

https://intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf. [hereinafter HPSCI Report].

687 Ibid., dokument: S. SELECT COMM.ON INTELLIGENCE, 116TH CONG., INITIAL FINDINGS OF INTELLIGENCE COMMUNITY ASSESSMENT (2018),

https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf

688 Ibid., dokument: STAFF OF S. SELECT COMM. ON INTELLIGENCE, 115TH CONG., NEW REPORTS SHED LIGHT ON INTERNET RESEARCH AGENCY'S SOCIAL MEDIA TACTICS (2018).

689 Ibid., dokument: RENEE DIRESTA ET AL., NEW KNOWLEDGE, THE TACTICS AND TROPES OF THE INTERNET RESEARCH AGENCY (2018); PHILIP N. HOWARD ET AL., COMPUTATIONAL PROPAGANDA RESEARCH PROJECT, THE IRA, SOCIAL MEDIA AND POLITICAL POLARIZATION IN THE UNITED STATES, 2012-2018 (2018).

690 Ibid.

su se dovodili u kontekst ruskih objava na Facebooku tijekom izborne kampanje za izbor Predsjednika SAD-a. Logički smisao stvaranja lažnih profila bio je stvaranje sljedbenika lažnih profila posredstvom kojih su ruski hakeri pomoću Facebooka stvarali niz hibridnih prijetnji. Osnovna zamisao prijetnji bila je u produbljivanju podjela između pojedinih kategorija ciljanih publika automatiziranom diseminacijom sadržaja koji su odgovarali načelima, uvjerenjima i vrijednostima koje su zagovarale međusobno suprotstavljene zajednice konzervativnog, crnačkog i manjinskog dijela glasačkog tijela SAD-a. Ujedno, logički smisao prijetnji bio je u jačanju homogenosti unutar navedenih zajednica i njihovoj mobilizaciji kako bi se na što učinkovitiji način ostvarila strateška logika svake pojedine prijetnje.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 32. Izgled lažnog Facebook grupnog profila „Sigurne granice“.

Izvor: Robert Walker, Combating Strategic Weapons of Influence on Social Media, 2019., str. 52.

Slika 33. Sadržaj objavljen na grupnom lažnom profilu „Sigurne granice“.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 34. Izgled lažnog Facebook grupnog profila „Ujedinjeni Jug“.

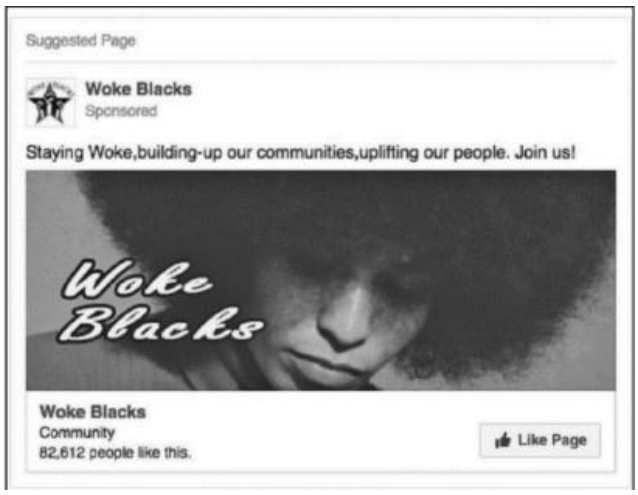
Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 35. Izgled lažnog Facebook grupnog profila „Stop Invaziji“.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 36. Izgled lažnog Facebook grupnog profila „Srce Teksasa“.

Slikama 32. do 36. prikazan je izgled lažnih profila na Facebooku pod nazivom „Sigurne granice“, „Ujedinjeni Jug“, „Stop Invaziji“ i „Srce Texasa“ na kojima su ruski hakeri stvarali i širili objave koje su bile prilagođene načelima i vrijednostima spomenutih zajednica na način da su zagovarali borbu protiv ilegalnih migracija i zatvaranje granica, na osnovu kojih su stvarali hibridne prijetnje produbljivanje društvenih podjela i nastojali ostvariti stratešku logiku takve prijetnje: iskorištavanje etničkih i kulturnih identiteta radi potkopavanja društvene kohezije.



Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 37. Izgled lažnog Facebook grupnog profila „Probuđeni Crnci“.

Izvor: Robert Walker, Combating Strategic Weapons of Influence on Social Media, 2019., str. 52.

Slika 38. Sadržaj objavljen na grupnom profilu „Probuđeni crnci“.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 39. Izgled lažnog Facebook grupnog profila „Crni aktivisti“.

Slikama 37., 38., 39. želi se ukazati na izgled lažnih profila „Probuđeni crnci“ i „Crni aktivisti“ pomoću kojih su ruski hakeri stvarali i širili objave kako bi stvarali hibridne prijetnje produbljivanja društvenih podjela i mobilizirali crnačku populaciju za vlastite ciljeve.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 40. Izgled lažnog Facebook grupnog profila „Ujedinjeni Muslimani Amerike“.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str. 241. – 249.

Slika 41. Izgled lažnog Facebook grupnog profila „Ujedinjeni američki domoroci“.

Slikama 40. i 41. prikazan je izgled i sadržaj lažnih profila „Ujedinjeni Muslimani Amerike“ i „Ujedinjeni američki domorodci“ kojima su ruski hakeri stvarali sljedbenike objava kojima su za vlastite potrebe mobilizirali ciljane publike među islamskim vjernicima i indijanskim plemenima. Objavama se stvaralo hibridne prijetnje produbljivanja društvenih podjela pri čemu su se za potkopavanje društvene kohezije iskorištavali rasni, vjerski, etnički i kulturni identiteti različitih kategorija ciljanih publika.

Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States 2019., str. 199.

Slika 42. Izgled lažnih profila na Instagramu koje su ruski hakeri koristili u mobilizaciji ciljanih publika u cilju organiziranja uličnih skupova suprotstavljenih skupina.

Slika 42. prikazuje izgled lažnih profila na Instagramu koje su ruski hakeri koristili u mobilizaciji ciljanih publika kako bi organizirali ulični skup međusobno suprotstavljenih skupina oko rasnih pitanja. Skup je organiziran kao odgovor na performans kojim je na poluvremenu Super Bowla američka glazbena zvijezda Beyoncé ukazala na ideje crnačkog Facebook pokreta „Crnački životi vrijede“ koja je okupljala crnačku populaciju lijevo-liberalnih pogleda. Jedan skup nazvan je „Protestni skup za Beyoncé“ koji je privukao korisnike Instagrama koji zagovaraju ideje pokreta „Crnački životi vrijede“ protiv bijele supremacije, a drugi je nazvan "Prosvjedni skup protiv Beyoncé" kojim se pozivalo na prosvjede protiv pokreta „Crnački životi vrijede“. Ruski hakeri pomoću spomenuta dva odvojena lažna profila na Instagramu uspješno su organizirali okupljanje suprotstavljenih skupina na adresi sjedišta Nacionalne nogometne lige, 345 Park Avenue, u New Yorku. Za vrijeme održavanja skupa nisu zabilježeni sukobi i nasilje, no ovaj primjer nije bio izoliran događaj.

Pomoću lažnih profila botova, trolova i hashtagova preko Facebooka uspješno je organiziran stvarni sukob između dvije suprotstavljene grupe demonstranta oko gradnje džamije u Houstonu između članova lažne Facebook grupe „Srce Texasa“ i „Ujedinjeni muslimani

Amerike“. U svrhu mobiliziranja preko spomenutih lažnih stranica prikazivani su video sadržaji sa stvarnim prizorima nasilja između crnačke i bjelačke populacije.[691] Time su se dodatno stvarale društvene podjele i ostvarivala njihova strateška logika.

Izvor: Nadler, Crain, Donovan, Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech, 2018., str. 31.

Slika 43. Izgled i sadržaj objave preko lažnog Facebook grupnog profila „Biti domoljub “.

Slikom 43. želi se prikazati izgled i sadržaj objave preko lažnog Facebook grupnog profila „Biti domoljub “ koja je okupljala zagovornike dostojanstva policije. Logika ove objave bio je evocirati stvarni napad na policiju, ali na način da se stvarni događaj prema pripadniku policije lažno povezao s članovima stvarne Facebook grupe „Crni životi vrijede“. Za ovaj oblik dezinformacije i stvaranje hibridne prijetnje produbljivanja podjela između crnačke populacije, pripadnika policije i njihovih simpatizera iskorišten je stvarni događaj iz američkih medija.

691 Nye, 2019.

Objavljivanje rezultata istrage dovelo je do dodatnih kontroverzi, podjela i nemogućnosti ostvarivanja konstruktivnog javnog dijaloga u američkom društvu budući da su različiti pogledi na izvješća i nalaze obavještajnih službi izazivali dodatne rascjepe po političkim linijama.[692]

Izvor: Walker Robert, Combating Strategic Weapons of Influence on Social Media, 2019.

Slika 44. Izgled i sadržaj objave preko lažnog Facebook profila #Anonymus.

Izvor: Walker Robert, Combating Strategic Weapons of Influence on Social Media, 2019., str. 41.

Slika 45. Izgled i sadržaj objave preko lažnog Facebook profila „Jenna Abrams".

692 Walker, 2019.

Tag you bro... The Great Meme War is not over! Let's asseble here. americaneagle

Izvor: Walker Robert, Combating Strategic Weapons of Influence on Social Media, 2019., str. 100.

Slika 46. Izgled i sadržaj objave preko lažnog Facebook profila „Ljuti Orao“.

Slikama 44., 45. i 46. prikazane su objave ruskih hakera kojima su nakon objave rezultata Senatskog odbora SAD-a za obavještajne poslove dodatno produbili podjele između američkih građana na način da su plaćenim objavama preko lažnih profila „Anonymous News“, „Jenna Abrams“ i „Angry Eagle“ nastojali diskreditirati obavještajnu zajednicu SAD-a. Prikazanim objavama hakeri ruske Agencije za istraživanje interneta dodatno su u korpusu javnog znanja ciljanih publika među američkim građanima stvarali hibridne prijetnje: pogoršavali su društvene podjele, nastojali su smanjiti povjerenje američkih građana u u nositelje vlasti, potkopavati funkcije državnih tijela SAD-a.

Ruska „Agencija za istraživanje interneta“ nije izmislila dezinformacije niti je bila prva organizacija koja se koristila logičkim zabludama za stjecanje strateške informacijske prednosti.[693] I druge države, uključujući i SAD, kroz povijest pomoću propagande pokušavale su utjecati na ciljane publike u drugim državama kako bi ostvarile vlastite političke interese. Međutim, ono u čemu se Rusija istaknula u hibridnim operacijama protiv SAD-a jest vještina iskorištavanja prednosti kiber prostora i svih mogućnosti koje nude društvene mreže za

693 Walker, 2019.

planiranje i izvođenje učinkovitih psiholoških operacija, kroz znanje i vještinu iskorištavanja hibridne inteligencije i osobnih podataka korisnika društvenih mreža za uobličavanje dezinformacija i za stvaranje hibridnih prijetnji. Dezinformacijama je jačala vjerodostojnost time što je koristila istinite događaje koje su na društvenim mrežama objavljivali američki mediji i građani. Takve događaje kombinirala je s lažnim sadržajima i tako stvarala učinkovitije dezinformacije. Pomoću botova i trolova dezinformacije je učinkovito širila u informacijski i medijski prostor SAD-a, istodobno slabeći američke kontra narative. Prikazani primjeri lažnih Facebook profila (pojedinačnih i grupnih) na Twitteru i Instagramu i plaćenih objava pokazuju kako se u planskoj i dobro pripremljenoj hibridnoj operaciji društvene mreže na učinkovit način mogu koristiti za stvaranje informacijske nadmoći i hibridnih prijetnji s mogućim strateškim posljedicama.

Tehnologije umjetne inteligencije koje koristi Facebook Rusiji su omogućile anonimnost djelovanja, a primjena hibridne inteligencije omogućila je stvaranje učinkovitih dezinformacija koje su bile prilagođene preferencijama američkih građana. Facebook je ruskim hakerima omogućio optimizaciju troškova i ulaganje u one dezinformacije za koje su ciljane publike pokazale najveći angažman i interes.[694] Ruski hakeri iskoristili su sve što Facebook, Twitter, Instagram i YouTube koriste za poslovne ideje i potrebe. Dezinformacijama su uspjeli mobilizirati simpatizere i zagovornike različitih političkih, rasnih, ideoloških, religijskih i drugih spornih društvenih tematika, a plaćenim objavama isticali su njihove krajnosti. Time su postigli dvostruki učinak. Uspjeli su stvarati hibridne prijetnje, a dezinformacijama stvarati autentičnost i vjerodostojnost.

SAD nisu predvidjele tamnu stranu tehnološke revolucije.[695] Tehnologije koje su razvile i usavršile američke tehnološke korporacije Rusija je iskoristila kao nove instrumente moći za stvaranje hibridnih prijetnji i potkopavanje američkog koncepta liberalne demokracije.[696] Cilj hibridnih operacija u SAD-u bio je urušiti povjerenje američkog biračkog tijela u vodeće medije, državne institucije i u sam politički poredak. Ključna stavka u ovim operacijama bila

694 O načinu djelovanja ruskih hakera detaljnije vidi: DiResta i autori, The Tactics & Tropes of the Internet Research Agency, 2018 i Senatski Odbor za obavještajnu službu (engl. Senate Select Committee on Intelligence) i Ured direktora za nacionalnu sigurnost (engl. Office of the Director of National Intelligence), Background to Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution, Washington, DC: National Intelligence Council, 2017, str. 2–4. Dostupno na https://permanent.access.gpo.gov/gpo76345/ICA_2017_01.pdf.

695 Walker, Shanthi, Jessica, 2020.

696 Nye, 2019.

je da se u većini plaćenih objava na društvenim mrežama nije mogla pripisati klasifikacija govora mržnje. Cilj ovih operacija imao je širi strateški kontekst: stvarati informacijsko-psihološke pritiske da je predsjednik države izabran pod utjecajem vanjskog aktera, izazvati sumnju u sposobnost državnog vodstva, razvijati opći osjećaj nepovjerenja u državne institucije i maknuti fokus SAD-a s država istočne Europe te time oslabiti američke vanjskopolitičke pozicije radi ostvarivanja vlastitih vanjskopolitičkih i geoekonomskih interesa u ovom dijelu Europe.[697]

U ovom poglavlju, primjerima hibridnih operacija koje su SAD-a i Rusija primjenjivale na različitim geografskim područjima, dodatno je potvrđena glavna hipoteza da se umjetna inteligencija koju koriste društvene mreže, neovisno radi li se o kontekstima hibridnih sukoba ili hibridnog ratovanja, koristi za preoblikovanje korpusa javnog znanja ciljane publike i za stjecanje informacijske nadmoći. Ovim poglavljem potvrdno je odgovoreno na treće istraživačko pitanje na način da je prikazano da se trenutno sve tri najpopularnije društvene mreže, Facebook, YouTube i Twitter, svaka zbog svojih specifičnosti, koriste kao učinkoviti alati utjecaja u ostvarivanju specifičnih ciljeva, bez obzira na prostorna i vremenska ograničenja.

697 Cohen i Bar'el, 2017.

7. NOVI OBRASCI PREVENCIJE I OBRANE OD HIBRIDNIH PRIJETNJI

Zloupotreba osobnih i grupnih uvjerenja, načela i vrijednosti korisnika društvenih mreža i tehnologija umjetne inteligencije na društvenim mrežama za planiranje i izvođenje psiholoških operacija pomoću učinkovitih dezinformacija postala je politički i sigurnosni problem koji predstavlja ozbiljnu prijetnju demokratskim procesima, pravnom poretku, nacionalnoj i međunarodnoj sigurnosti. Različiti akteri (državni, nedržavni, korporacije) ovu mogućnost koriste za ostvarivanje političkih ciljeva, nacionalnih informacijskih strategija i stvaranje hibridnih prijetnji. Komercijalni imperativi kojima se rukovode vlasnici društvenih mreža i nedovoljna politička usmjerenost država da adekvatnije reguliraju digitalni prostor novim normama, rezultirali su pojavom hibridnih operacija utjecaja u kiber prostoru u kojima se zlouporaba društvenih mreža koristi za učinkovito stjecanje informacijske nadmoći nad korpusom javnog znanja ciljanih publika u svrhu njegovog (pre)oblikovanja prema napadačevim potrebama. S obzirom na nepostojanje spomenutih pravila i normi kao i na mogućnosti zlouporabe kiber prostora i društvenih mreža u akademskoj i sigurnosnoj zajednici pojavio se interes o potrebi jačanja svijesti za definiranjem pravila sukobljavanja i ratovanja, odnosno ponašanja u kiber prostoru. „Ta pravila trebaju i smiju odrediti samo subjekti međunarodnog prava, a ne tvrtke i korporacije koje taj prostor pokušavaju monopolizirati.“[698]

Nedovoljnim reguliranjem etičkih i moralnih pravila pri upotrebi tehnologija umjetne inteligencije na društvenim mrežama otvorene su mogućnosti njihove zloupotrebe. Umjetna inteligencija na društvenim mrežama zloupotrebljava se u unutarnjim i vanjskim političkim borbama, stvorene su negativne implikacije na organizaciju i sadržaj korpusa javnog znanja. Posljedično, došlo je do negativnog reflektiranja njihove zlouporabe na političku i društvenu stabilnost. Selektivna izloženost samo određenom skupu podataka, obavijesti i informacija, izvršene podjele prema uvjerenjima, načelima i vrijednostima i mogućnosti njihovog (pre)oblikovanja u skladu s potrebama vlasnika društvenih mreža otvaraju neviđene mogućnosti stvaranja dezinformacija i hibridnih prijetnji i na taj način preko kiber prostora ostvarivanja zacrtanih političkih ciljeva. Pomoću dezinformacija koje su postale vjerodostojnije i snažnije u učincima, moguće je jednostavnije (pre)oblikovati uvjerenja, načela i vrijednosti, utjecati na mišljenja i odluke ciljanih publika u vlastitu korist. Posljedično, preko kiber prostora moguće je jednostavnije pokretati destabilizacijske procese u različitim kontekstima željenog

698 Akrap, 2019.

djelovanja informacijskog napadača (društvenim, političkim i sigurnosnim). Izvršenom podjelom korisnika društvenih mreža prema uvjerenjima, načelima i vrijednostima primjenom tehnologija umjetne inteligencije njihova uvjerenja, načela i vrijednosti moguće je (pre)oblikovati prema interesima napadača, sukladno ciljevima informacijskih strategija i radi učinkovitijeg ostvarivanja strateške logike hibridnih prijetnji. Primjerice, nekom političkom akteru tijekom izborne kampanje moguće je povećati ili smanjiti popularnost, mobilizirati ili demobilizirati dio biračkog tijela te na taj način posredno utjecati na ishode izbora za političke interese i potrebe hibridnih aktera. Na jednak način mobiliziraju se pristaše nasilnih, radikalnih, terorističkih organizacija, potiču se demonstracije, propagira se nasilje i terorizam. Algoritmi preporuka i rangiranja (dez)informacije koje sadrže radikalne i ekstremne stavove čine vidljivijima i vjerodostojnijima, što ne mora odgovarati stvarnom stanju. Ovakva stanja moguće je potencirati psihološkim operacijama pomoću društvenih mreža, odnosno stvarati željenu percepciju o zbilji koja ne mora biti utemeljena na objektivnom i činjeničnom znanju. Činjenica je da tehnologije umjetne inteligencije na društvenim mrežama ne prepoznaju objektivno točan i istinit podatak, obavijest ili informaciju, već je njihova zadaća da usmjere pozornost korisnika društvenih mreža prema onim sadržajima koji su u skladu s osobnim i/ili grupnim preferencijama korisnika. Na ovaj način došlo je do dekonstrukcije korpusa javnog znanja i narušavanja temeljnih postulata informacijske znanosti: potiče se stvaranje dezinformacija. U prvi plan, kad je to nekome u interesu, dolaze dezinformacije na osnovi kojih u stvarnom svijetu nastaju društvene, sigurnosne i političke krize. Pogoduje se narušavanju temeljnih ljudskih i društvenih normi kao što su transparentnost i zaštita ljudskih prava.

Stvaranje podatkovnog i digitalnog suvereniteta i zaštita osobnih podataka pohranjenih na serverima vlasnika društvenih mreža nameću se kao logična rješenja za otklanjanje i ublažavanje nastalog problema dezinformacija. Nedovoljan interes vlasnika društvenih mreža zbog ekonomskih razloga da iz vlastitog poslovanja otklone tehnološka rješenja koja omogućavaju zloupotrebu njihovih platformi predstavlja dodatni problem. Postojeća programska rješenja algoritama preporuka i rangiranja sadržaja i postavki umjetne inteligencije na društvenim mrežama potrebno je zamijeniti rješenjima koja neće pogodovati stvaranju hibridnih prijetnji.

Prepoznavanje, odvraćanje i otklanjanje štetnih posljedica prijetnji iz kiber prostora koje nastaju zloupotrebom umjetne inteligencije koje koriste društvene mreže jedna je od glavnih tema koje se izučavaju unutar strateških studija i obavještajnih studija te izazova s kojima se suočava akademska i sigurnosna zajednica. Neophodno je razvijati sveobuhvatni odgovor te

razumijevanje implikacija zlouporabe hibridne inteligencije u kontekstu stvaranja dezinformacija i drugih vrsta hibridnih prijetnji te hibridnih sukoba i ratova. Nove informacijske strategije trebale bi biti nositelji ovakvog razumijevanja, a pomoću njih bi države izgradile adekvatne mehanizme prevencije i obrane i otklonile štetne posljedice za demokratski i društveni poredak. Mehanizmi prevencije, odvraćanja i obrane trebali bi se temeljiti na izgradnji otpornosti ukupnog društva prema informacijskim i psihološkim pritiscima vanjskih aktera. Jedan od preduvjeta da bi se to ostvarilo jest u podizanju svjesnosti političke, akademske zajednice, civilnog društva i medija o snazi zloupotrebe hibridne inteligencije i tehnologija koje primjenjuju društvene mreže na organizaciju korpusa javnog znanja i koje će, ukoliko ne budu adekvatno regulirane, imati dodatan snažni subverzivni učinak na političke i društvene procese u godinama koje dolaze.

Umjetna inteligencija razvija se mnogo brže nego što se donose regulative potrebne kako bi se smanjio rizik od njene zlouporabe.[699] Primjena umjetne inteligencije na društvenim mrežama za planiranje i izvođenje psiholoških operacija i u njima stvaranje učinkovitih dezinformacija i povezanih prijetnji, u značajnoj mjeri podigla je rizike koji sve većem broju država predstavljaju sigurnosne i političke probleme. Iz RAND-ovog istraživanja[700] moguće je izdvojiti tri kategorije rizika koje mogu proizaći na osnovi zlouporaba umjetne inteligencije koju koriste društvene mreže.

Glavne kategorije rizika su:

- Etički i pravni:
- primjena prava u međunarodnim oružanim sukobima;
- moralna odgovornost;
- ljudsko dostojanstvo;
- poštivanje ljudskih prava i privatnosti.

699 Artificial Intelligence and National Security, Federation of American Scientist, 2020. Dostupno na: https://fas.org/sgp/crs/natsec/R45178.pdf.

700 Usp. Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, Derek Grossman, Military Applications of Artificial Intelligence, Ethical Concerns in an Uncertain World, RAND Corporation, 2020., str. 29-40., https://www.rand.org/pubs/research_reports/RR3139-1.html

- Operativno-taktički:
- povjerenje u medije i u pouzdanost činjenica;
- zloupotreba osobnih podataka građana;
- dezinformacije;
- hibridne operacije;
- hibridne prijetnje.
- Strateški:
- neprimjetnost, anonimnost;
- upravljanje eskalacijom međunarodnih sporova/sukoba
- strateška stabilnost;
- informacijska nadmoć;
- (pre)oblikovanje korpusa javnog znanja.

Dosadašnja nedovoljna regulacija primjene umjetne inteligencije na društvenim mrežama omogućila je zloupotrebe i štetne utjecaje po političku, društvenu i sigurnosnu stabilnost na taktičkim i strateškim razinama. Iskustva država iz različitih formi međunarodnih sukoba posljednjih desetak godina jasno pokazuju da su različiti i brojni akteri razvili sposobnosti da tehnologije umjetne inteligencije koje na društvenim mrežama služe za planiranje i izvođenje informacijskih operacija za marketinške svrhe zloupotrebljavaju za vlastite ciljeve sa strateškim posljedicama po političke i društvene procese u domicilnim državama. Evidentno je da su društvene mreže zbog nedovoljnih pravila i ograničavanja zloupotrebe tehnologija umjetne inteligencije postale snažni i učinkoviti alati utjecaja s mogućim strateškim posljedicama na organizaciju javnog znanja i stjecanje informacijske nadmoći. Tehnologijama umjetne inteligencije kroz automatizirane, masovne, anonimne dezinformacije društvene mreže dobile su snagu „oružja“ pomoću kojih je na učinkovit način preko kiber prostora moguće učinkovito ostvarivati različite forme strateških ciljeva: od narušavanja funkcionalnosti gospodarskih i informacijsko-komunikacijskih infrastruktura do preoblikovanja korpusa javnog znanja ciljanih publika za političke interese. U hibridnim sukobima tehnologije umjetne inteligencije evidentno su doprinijele razvijanju mogućnosti da određene aktivnosti u kiber prostoru ostanu ispod praga ratnih djelovanja. Dominacija informacijama i razumijevanje moći informacija kroz povećanje njihove brzine, preciznosti i učinkovitosti odlučujući je čimbenik u korištenju informacija kao učinkovitog i djelotvornog sredstva za stvaranje novih formi prijetnji, informacijske nadmoći i (pre)oblikovanja korpusa javnog znanja preko kiber prostora. U hibridnim sukobima umjetna inteligencija je nositelj ove evolucije. Ona može oponašati

ponašanja, utjecati na njih i mijenjati ih u skladu s napadačevim potrebama, čime (pre)oblikuje društvene i ekonomske učinke hibridnih sukoba.[701] Međunarodnim sigurnosnim čimbenicima, civilnim i vojnim donositeljima odluka na nacionalnim razinama nužna je potreba unapređivati strategije i koncepte kako bi proširili znanja o zlouporabama hibridne inteligencije u hibridnim sukobima i hibridnom ratovanju. To bi trebalo uključivati procjenu gdje postojeća obuka, taktike, tehnike i procedure dopuštaju njezinu učinkovitu upotrebu. Što je najvažnije, u sektoru obrane i sigurnosno-obavještajne zajednice nužno je graditi sveobuhvatne kapacitete i razvijati nove inicijative u kojima će se ukazivati na snagu i mogućnosti umjetne inteligencije u svim aspektima njezine primjene, a naročito u onima u kojima je različiti akteri (državni i nedržavni) u međunarodnim sukobima zlouporabljuju za stvaranje učinkovitih dezinformacija i hibridnih prijetnji korpusima javnog znanja iz kiber prostora. Ova činjenica nameće se sama po sebi kako bi se bolje predvidjeli učinci primjene različitih sustava i sposobnosti umjetne inteligencije ali i njezine zloupotrebe s obzirom na prednosti koje nudi za postizanje taktičkih, operativnih i strateških ciljeva. Kao što je nedavna studija američkog RAND-a naglasila: različiti akteri će sve više iskorištavati prilike i mogućnosti u kiber prostoru, ne samo za širenje dezinformacija, sebi sklone narative ili za nanošenje fizičke štete različitim vrstama kritičnih infrastruktura, već i za nanošenje štete bazama na kojima su pohranjeni „osobni podaci građana i funkcionalnosti algoritama o kojima će u sve većoj mjeri ovisiti moderna društva."[702] Detaljna analitika baza podataka, ciljana propaganda i jeftini, uvjerljivi lažni videozapisi predstavljat će snažne načine pomoću kojih će se manipulirati javnim mnijenjem u dosad nezamislivim razmjerima. Umjetna inteligencija zloupotrebljavat će se za 'hiperpersonalizirano ciljanje utjecajem'[703] kojim će se nastojati ostvarivati politički, vojni i geopolitički ciljevi. 'Hiperpersonalizirano ciljanje" dezinformacijama bit će po niskoj cijeni dostupno državnim i nedržavnim akterima.[704]

U svrhu prevencije, obrane i odvraćanja od prijetnji koje dolaze iz kiber prostora na osnovu zlouporabe tehnologija umjetne inteligencije predlažemo izradu nove nacionalne informacijske strategije i nudimo preporuke kojima bi se obuhvatila odgovarajuća paradigma obrane od

701 Thiele, 2020., str. 6.

702 Usp. Mazarr i sur., 2019.

703 engl. 'hyper-personalized influence targeting'.

704 Usp. The European Centre of Excellence for Countering Hybrid Threats, HYBRID COE EXPERT POOL MEETING ON CYBER, The future of cyberspace and hybrid threats, Hybrid CoE, Trend Report 6, 2021.

hibridnih prijetnji. Izrada nacionalne informacijske strategije podrazumijeva dva ključna koraka:

1) Izradu modela ranog prepoznavanja i upozoravanja prema kojem se može relevantno i vjerodostojno utvrditi da će se neka ciljana publika naći ili se već nalazi pod informacijsko-psihološkim pritiscima i napadima dezinformacijama s ciljem trajnog ili što dužeg utjecaja na promjenu sadržaja, vrijednosti i organizacije njezinog javnog prostora znanja;
2) Potrebu uvođenja podatkovnog i digitalnog suvereniteta na nacionalnoj i međunarodnoj razini, unutar kojeg bi se uspostavila bolja pravila ponašanja i otklonile mogućnosti zloupotrebe osobnih podataka građana na društvenim mrežama i zloupotrebe tehnologija umjetne inteligencije za planiranje i izvođenje hibridnih operacija.

Nacionalna informacijska strategija s osnovnim preporukama trebala bi pouzdano izvršavati tri ključne aktivnosti: „rano uočavanje i prepoznavanje nadolazećeg napada, nedvojbeno identificiranje napadača, omogućavanje primjerenog protudjelovanja s obzirom na upotrijebljena sredstva i na njihov intenzitet u odnosu na planirane učinke.“[705] Glavna područja zaštite i prevencije odnosila bi se na tri ključna područja: jačanje kiber sigurnosti, jačanje zaštite nacionalnih KI-jeva te nacionalnog i međunarodnog podatkovnog prostora. Da bi mehanizmi odvraćanja i ublažavanja štitili i aktivno provodili učinkovitu obranu od mogućih štetnih posljedica, potrebno je razumjeti moć algoritama i drugih tehnologija umjetne inteligencije koje se zloupotrebljavaju kroz hibridnu inteligenciju i koriste se na društvenim mrežama u realizaciji hibridnih prijetnji; shvatiti potencijalne rizike i složenosti hibridnih operacija te prilagoditi postojeće propise i standarde.

7.1. Izrada nacionalne informacijske strategije

Stvaranje novih formi prijetnji iz kiber prostora pomoću tehnologija umjetne inteligencije koje koriste društvene mreže izvan uobičajenog ciklusa rata i ratovanja zamaglilo je stvarne namjere i ciljeve njihovih planera i izvoditelja. Pred države i institucije ova činjenica nametnula je potrebu za novim pristupom u odvraćanju takvih prijetnji i za izgradnju prilagodljivih i učinkovitih mehanizama koji bi bili u stanju pravovremeno prepoznati takve prijetnje.

705 Akrap, 2019., str. 46.

Postavlja se pitanje kako u doba globalizacije i digitalizacije informacijskog društva[706] izgraditi nove adekvatne mehanizme prilagođene novim, složenijim sigurnosnim izazovima 21. stoljeća? Iskustva država daju dovoljno pokazatelja da informacijsko-komunikacijski sustavi više nisu sustavi za širenje istine i točnih podataka. Osnovna pretpostavka izgradnje adekvatnih mehanizama je razumijevanje da je ključ operacija utjecaja u kiber prostoru i prijetnji koje iz njih nastaju postala hibridna inteligencija, odnosno mogućnosti zlouporabe algoritama i drugih tehnologija umjetne inteligencije za stvaranje učinkovitih dezinformacija i drugih različitih formi prijetnji radi ostvarivanja političkih ciljeva. Zloupotreba hibridne inteligencije za uobličavanje korisničkih podataka (načela, uvjerenja i vrijednosti) u dezinformacije i za učinkovitije iskorištavanje slabosti ciljanog političkog ili društvenog sustava postala je neupitna mogućnost. Tehnologije su postale alati pomoću kojih je u kiber prostoru na učinkovit način moguće iskorištavati različita načela, uvjerenja i vrijednosti: sklonosti pojedinaca ili grupa radikalnim ili ekstremističkim uvjerenjima, terorističkim organizacijama i nasilnim organizacijama; postojeće društvene, političke, kulturne, identitetske i ideološke podjele; klasnu nejednakost, rasne, vjerske te međuetničke napetosti; nedostatak političke suglasnosti političkih elita o budućnosti društva, korupciju, neučinkovitost državnih institucija u provođenju zakona; nedostatak prirodnih resursa i ovisnost o stranim državama itd. Jednako tako, hibridnom inteligencijom na društvenim mrežama moguće je iskorištavati i nesposobnost državnih tijela u predviđanju, suočavanju, izgradnji otpora i prilagođavanju i oporavku od sigurnosnih izazova i kriznih stanja te nedostatak ili nepostojanje društvene otpornosti na hibridne prijetnje. Tehnologije društvenih mreža, hibridne prijetnje i hibridne operacije u sinergiji s hibridnom inteligencijom donose nove paradigme napada i stvaranja okolnosti kojima se pogoduje nastajanju takvih prijetnji. Problemi dezinformacija čine se ključnim i zahtijevaju uvođenje nove informacijske strategije s osnovnom zadaćom odvraćanja i obrane od dezinformacija i hibridnih prijetnji koje se dezinformacijama dodatno osnažuju i pospješuju.

706 Naziv informacijsko društvo, od poč. 1990-ih upotrebljava se u dokumentima Europske unije za označivanje suvremenoga društva, koje svoj gospodarski, znanstveni i kulturni razvoj zasniva na uvođenju i širenju računalne i telekomunikacijske tehnologije te stvaranju, obradbi i prijenosu informacija kao temelju za rast produktivnosti društva. Osnovne smjernice razvoja informacijskoga društva predočene su u tzv. Bangemannovu izvještaju, što ga je Europsko vijeće prihvatilo 1994. Dostupno na: informacijsko društvo.

Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021., (7. 9. 2022.), <http://www.enciklopedija.hr/Natuknica.aspx?ID=27411>.

Informacijska strategija na nacionalnoj razini nužna je iz nekoliko ključnih razloga:

- „primarni cilj svih budućih neprijateljskih aktivnosti bit će nastojanje napadača da stvori stanje informacijske nadmoći“ u informacijsko-komunikacijskom prostoru“[707];
- „kako bi se taj cilj ostvario, napadač će napadati tri ključne kritične infrastrukture (nacionalne i međunarodne): informacijsko-komunikacijsku (uključujući kiber prostor), energetsku, vodno-prehrambenu“[708];
- „najučinkovitije sredstvo za ostvarivanje stanja informacijske nadmoći jest stjecanje nadmoći u kiber prostoru“[709];
- „pravila sukobljavanja i ratovanja u kiber prostoru ne postoje, što znači da nema metoda, radnji, ciljeva i sredstava koji su zabranjeni. Ne postoji međunarodno prihvaćen sustav ni organiziranost nadzora i kontrole nad procesima i aktivnostima u tom prostoru. Time se znatno otežava organiziranje učinkovitih obrambenih mjera, posebno na pasivnoj preventivnoj razini“[710];
- „budući napadi bit će hibridne naravi. U njima će prednjačiti uporaba nekinetičkih sredstava (operacije utjecaja, informacijske i medijske operacije, uporaba različitih politika kao izvora prijetnji), dok će se kinetička ubojita sredstva (vojna, oružana) upotrebljavati tek kad se iscrpe sve mogućnosti primjene nekinetičkih metoda i modela napada. Dodatna prednost tih napada je jednostavnija mogućnost njihovog učinkovitog poricanja, odnosno otežano identificiranje stvarnog napadača i njegovih namjera“[711];
- „ako se želi biti učinkovit u pripremi, planiranju, vođenju i nadzoru hibridnih prijetnji i hibridnih operacija, nužna je upotreba sposobnosti izvještajno-sigurnosnog sustava, i to u svim fazama djelovanja. Budući da se djelovanjem izvještajno-sigurnosnog sustava na prikupljanju i obradi nužnih podataka prijetnje mogu lakše uočiti, potrebno je njegovo aktivno sudjelovanje u fazama ranog otkrivanja i u stvaranju uvjeta za postupanja u učinkovitoj preventivnoj aktivnoj obrani.“[712]
- međunarodni sukobi postali su multimodalni i odvijaju se konstantno (24/7) i kad nema otvorenog oružanog sukoba, ali ima stalnog političkog sukobljavanja;

---

707 Akrap, 2019., str. 43.-44.

708 Ibid.

709 Ibid.

710 Ibid.

711 Ibid.

712 Ibid.

- zlouporabe tehnologija i sustava koji umrežavaju komunikacijske procese na globalnoj razini, koji razmjenjuju i umrežavaju podatke, obavijesti, ideje, mišljenja, stavove, načela, uvjerenja, vrijednosti, dominantni su nositelji informacijsko-psiholoških pritiska a njihova zlouporaba je suptilna i teže pravodobno uočljiva;
- informacijsko-komunikacijski pritisci izvode se psihološkim operacijama kroz kiber prostor, a moć umjetne inteligencije u stvaranju dezinformacija postala je neupitna i očigledna;
- psihološke operacije odvijaju se konstantno u pozadini glavnih i vidljivih događaja. Različiti oblici sukoba više se neće moći kategorizirati pod konvencionalne ili nepravilne, državne ili nedržavne sukobe.

Postalo je očigledno da pomoću tehnologija društvenih mreža planeri operacija utjecaja u kiber prostoru dobivaju potrebne referentne točke o društvenim, institucionalnim i političkim slabostima ciljanih publika prema kojima se primjenom hibridne inteligencije prilagođavaju dezinformacije i informacijsko-psihološki pritisci kroz ostale vidove prijetnji kojima nastoje otežati protudjelovanja. Bez adekvatne regulacije, zlouporaba hibridne inteligencije pogađa cjelokupno društvo, predstavlja glavnu prijetnju organizaciji korpusa javnog znanja i pogoduje narušavanju sigurnosti i otpornosti društva na mogućnost konstantnog izlaganja dezinformacijama. Vlasnici društvenih mreža tehnologije umjetne inteligencije razvijaju i upravljaju njima. Međutim, to zahtijeva bolju regulaciju i adekvatnu primjenu standardiziranih pravila, etičkih i moralnih normi kojima bi se pridonijelo sprječavanju zlouporaba umjetne inteligencije za stvaranje učinkovitih prijetnji iz kiber prostora.

Primjeri planiranja i izvođenja hibridnih operacija u primjerima hibridnog ratovanja i hibridnih sukoba jasno ukazuju da su društvene mreže bile ključan čimbenik pomoću kojeg su se stvarale hibridne prijetnje. Hibridne operacije postale su učinkovita metoda kojom preko kiber prostora akter s većim umijećem u iskorištavanju hibridne inteligencije i društvenih mreža može podrivati kulturne i identitetske simbole, sustav vrijednosti, uvjerenja i načela ciljanih publika za vlastite potrebe, bez obzira radi li se o ratu ili miru. Evidentno je da su time društvene mreže postale alati utjecaja pomoću kojih je postalo moguće iskorištavati postojeće slabosti ciljanih publika protiv njih samih s potencijalnim strateškim posljedicama.

Rastuća zlouporaba društvenih mreža za stvaranje hibridnih prijetnji iz kiber prostora jasno ukazuje na potrebu novog obrasca protudjelovanja sa svrhom njihovog pravovremenog prepoznavanja, prevencije, odvraćanja i ublažavanja potencijalnih štetnih posljedica. Osnovne

zadaće nove informacijske strategije stoga bi trebale biti usmjerene na razvijanje odgovarajućih mehanizama i sustava protumjera kako bi se na vrijeme prepoznale prijetnje, nositelji prijetnji te unaprijed pripremili protuodgovori i protumjere. Nacionalna informacijska strategija kao strateški koncept sigurnosti zahtijevala bi sinkronizaciju i prilagodbu prijetnjama iz kiber prostora s tri osnovna polazišta:

- na osnovi boljeg razumijevanja i kontekstualizacije operacija utjecaja koje se planiraju i izvode u kiber prostoru pomoću umjetne inteligencije koju koriste društvene mreže i hibridnih prijetnji koje iz ovakvih operacija proizlaze iz kiber prostora;
- izrade smjernica za izgradnju nacionalnih sposobnosti za poboljšavanje sigurnosti i povećavanja spremnosti u stvaranju protumjera izgradnjom modela ranog upozoravanja i prepoznavanja;
- na uspostavi okvira za postizanje podatkovnog i digitalnog suvereniteta na nacionalnoj i međunarodnoj razini.

Drugim riječima, mehanizmi kojima bi se odvraćale prijetnje koje proizlaze iz hibridnih operacija zahtijevali bi jednako takve hibridne odgovore i strategije. Opravdanje za formiranje hibridne protustrategije tj. obrane u vidu prevencije i otklanjanja štetnih posljedica hibridnih prijetnji kao rezultat hibridnih operacija pronalazimo u nekoliko ključnih razloga:

- Hibridne operacije utjecaja planiraju se i izvode primarno u kiber prostoru sa svrhom stvaranja prijetnji iz kiber prostora u pravilu u razdobljima mira;
- Takve prijetnje i operacije utjecaja manifestiraju se neprimjetnim dezinformacijama i drugim oblicima informacijsko-psiholoških pritisaka pomoću društvenih mreža konstantno i u pozadini vidljivih događaja. Osobni podaci građana s društvenih mreža neometano i neprimjetno se zloupotrebljavaju sa svrhom preoblikovanja sustava vrijednosti, uvjerenja i načela napadnutog društva. Cilj ovakvih prijetnji i operacija je kratkoročno ili dugoročno promijeniti organizaciju njegovog korpusa javnog znanja, manipulirati njegovim pamćenjem, sužavati pamćenje na dezinformacije i na skup informacijskih sadržaja od interesa napadača;
- Kiber prostor je idealan za planiranje i upravljanje sukoba u kojem različiti akteri (državni, nedržavni i korporacije) mogu neometano planirati i izvoditi psihološke operacije pomoću učinkovitih dezinformacija.

Nacionalnom informacijskom strategijom doprinijelo bi se uspostavi hibridne obrane kao strateškog pristupa u prevenciji, suprotstavljanju i odvraćanju prijetnji i pravovremenog prepoznavanja ciljeva i nositelja operacija utjecaja iz kiber prostora u kojima društvene mreže

različiti akteri zlouporabljuju za ostvarivanje političkih ciljeva. Hibridna obrana podrazumijevala bi primjenu prilagodljivih i sveobuhvatnih načina za prepoznavanje hibridnih prijetnji. Obrana bi trebala biti koncipirana na prilagodljive načine kao što se društvene slabosti, na prilagodljive načine kroz kiber prostor, koriste za stvaranje hibridnih prijetnji. Hibridna obrana podrazumijevala bi holistički pristup u prepoznavanju vlastitih društvenih slabosti i stvaranja otpornosti na hibridne prijetnje u čijem se planiranju i izvođenju takve slabosti iskorištavaju. Izgradnja hibridne obrane podrazumijevala bi podizanje percepcije u društvu i kod donositelja političkih odluka o procesima u kojima određene situacije u kiber prostoru, pomoću tehnologija umjetne inteligencije i primjenom anonimnih operacija utjecaja, mogu prerasti u jednu ili više formi hibridnih prijetnji. Podizanjem percepcije izgradnja hibridne obrana sa strateške razine omogućila bi učinkovita i koordinirana višesložna i višesektorska protudjelovanja spram hibridnih prijetnji. O mogućnostima zloupotreba tehnologija umjetne inteligencije na društvenim mrežama za političke ciljeve šira javnost i društvo kao korisnici usluga društvenih mreža nemaju dovoljno jasnu i široku sliku. Procesi prepoznavanja i razlikovanja istine od neistine u prostoru javnog znanja „ne smiju biti oslonjeni isključivo na algoritme i umjetnu inteligenciju“[713].

Nedovoljna reguliranost „tvorničkih“ postavki tehnologija umjetne inteligencije očito je omogućila njihovu zlouporabu u učinkovitijim performansama automatiziranog i anonimnog stvaranja hibridnih prijetnji i učinkovitijem nametanju volje na procese razmišljanja i donošenje odluka od interesa napadača. Zlouporabe „tvorničkih„ postavki naročito su se pokazale pogubnima u razdobljima izvan konteksta rata u izbornim procesima kad su uvjerenja, načela i vrijednosti ciljanih publika najizloženija dezinformacijama. U ovim razdobljima ciljane publike su najranjivije i najpodložnije dezinformacijama i vanjskom utjecaju iza kojeg su skriveni politički interesi: produbljivanje društvenih i političkih podjela i potenciranje društvene i političke nestabilnosti. Opisani primjeri iz zadnjeg desetljeća dovoljno su upozorenje o potrebi stvaranja konceptualnog okvira nove nacionalne informacijske strategije kojom bi se se trebalo na vrijeme prepoznati i prevenirati takve forme prijetnji. Evidentno je potrebno bolje reguliranje i uvođenje pravila u upotrebi algoritama i drugih tehnologija umjetne inteligencije u prikupljanju, pohrani i obradi podataka, obavijesti i informacija na društvenim mrežama. Nužne promjene doprinijele bi umanjivanju mogućnosti njihove zlouporabe za sve suptilnije i anonimne digitalizirane oblike dezinformacijskih kampanja. Dezinformacijske kampanje su

713 Ibid., str. 45.

ključni čimbenici kojima se u operacijama utjecaja u kiber prostoru pospješuju ostale hibridne prijetnje i zbog čijeg snažnijeg učinka operacije utjecaja u kiber prostoru ostvaruju bolju učinkovitost. Svrha hibridne obrane bila bi usmjerena na osvještavanje političkih elita o primjeni hibridnih taktika i važnosti otklanjanja čimbenika koji doprinose društvenim slabostima koje su -kako smo pokazali- planerima i izvoditeljima operacija utjecaja u kiber prostoru od najveće vrijednosti u njihovom planiranju i provođenju. Razumijevanje novih alata i njihovih taktičkih mogućnosti koje se u kiber prostoru ostvaruju primjenom hibridne inteligencije i otklanjanje vlastitih slabosti od ključne su važnosti. Primarne mete hibridnih operacija i prijetnji koje je potrebno štititi su: društvo u cjelini, korpus javnog znanja, društveni i politički demokratski poredak.

Zadaća hibridne obrane kroz novu informacijsku strategiju je prevencija, obrana i otklanjanje potencijalnih štetnih posljedica. Zbog snažnih kratkoročnih ili dugoročnih posljedica hibridnih prijetnji i operacija po organizaciju korpusa javnog znanja sa strateško-političke razine nužno je ukazati na tri bitna smjera budućeg djelovanja u rješavanju nastalih problema:

- na trenutne nedostatke nereguliranosti kiber prostora i zlouporabe tehnologija društvenih mreža te na nepostojanje ustaljenih pravila;
- na nužan zaokret mjerodavnih državnih struktura i tijela da na vrijeme mogu prepoznati, uspješno spriječiti ili odvratiti prijetnje koje se na učinkovit način mogu stvarati u kiber prostoru: državni prevrati, vanjska uplitanja u izborne kampanje, unutarnje političke i društvene procese, produbljivanje političkih, društvenih i sigurnosnih kriza;
- na potrebu razvijanja nacionalnog i međunarodnog sustava protumjera kako bi se pravovremeno mogle identificirati vlastite ranjivosti, vanjske prijetnje i njihovi nositelji s pripremljenim protuodgovorima i protumjerama.

Izgradnja hibridne obrane postala je nužnost zbog gotovo neograničenih mogućnost planiranja, stvaranja i širenja kriza kroz kiber prostor u stvarni svijet. Nova informacijska strategija doprinijela bi jačanju ukupne sigurnosti društva, društvene otpornosti, identificiranju vlastitih slabosti na svim razinama društva, uključujući ljude, procese, tehnologiju i podatke. Od naročitog interesa je zaštita sustava upravljanja i vođenja koji predstavlja ključ (ne)uspješnog (ne)funkcioniranja i (ne)djelovanja. „Najranjiviji dijelovi svakog sustava i procesa jesu ljudi,

zbog čega je njihovoj sigurnosti, stalnom procesu obrazovanja, obučavanja i usavršavanja te razvoju ukupne društvene sigurnosne kulture potrebno posvetiti posebnu i trajnu pozornost.“[714]

7.2. Izgradnja modela ranog prepoznavanja i upozoravanja

Kao osnovi korak u informacijskoj strategiji odnosno izgradnji mehanizma protumjera, predlažemo izgradnju modela prepoznavanja i ranog upozoravanja da se na vrijeme može relevantno i vjerodostojno utvrditi da će se neka ciljana publika naći ili se već nalazi pod informacijskim napadom s ciljem trajnog ili što dužeg utjecaja na promjenu sadržaja, vrijednosti i organizacije prostora javnoga znanja. Ovim modelom doprinijelo bi se izgradnji sustava hibridne obrane, višoj razini sigurnosti društva i njegovoj ukupnoj otpornosti na prijetnje iz kiber prostora. Ujedno bi se podignula svijest korisnika društvenih mreža o karakteru operacija utjecaja koje se planiraju i izvode iz kiber prostora, formi prijetnji koje stvaraju te bi se ukazalo na potrebu uvođenja adekvatnijih regulatornih okvira kojima bi se onemogućila ili barem ograničila zlouporaba hibridne inteligencije na društvenim mrežama za planiranje, stvaranje i izvođenje prijetnji iz kiber prostora. Modelom ranog prepoznavanja i upozoravanja podignula bi se percepcija o složenoj prirodi hibridnih sukoba i moći hibridne inteligencije za stvaranje prijetnji poput produbljivanja podjela, poticanja na radikalizam, ekstremizam ili na terorizam. Evidentno je da svi korisnici digitaliziranog prostora javnog znanja i društvenih mreža mogu biti izloženi dezinformacijama i konstantnim informacijsko-psihološkim pritiscima u manjoj ili većoj mjeri.

Izgradnja modela prepoznavanja i ranog upozoravanja suočava se s tri glavna izazova:

- Prvi je već spomenuta činjenica da u kiber prostoru nema zabranjenih metoda, radnji, ciljeva i sredstava te ne postoje pravila sukobljavanja i ratovanja, ne postoji međunarodno prihvaćen sustav niti organiziranost kontrole nad procesima i aktivnostima u tom prostoru;
- Drugi izazov predstavlja snažan komercijalni interes vlasnika društvenih mreža da ne otklone glavne uzroke koji dezinformacijama na društvenim mrežama daju tako snažan učinak. Pri tome mislimo na lažne profile koji dezinformacijama i njihovim autorima daju anonimnost. Potrebno je otkloniti mogućnosti zloupotrebe osobnih podataka korisnika društvenih mreža da se prema njima uobličavaju dezinformacije. Bolja

714 Ibid.

regulacija i uspostavljanje adekvatnih regulatornih okvira kojima bi se ograničila zloupotreba umjetne inteligencije jedan je od ključnih zaokreta. Posljedično, otklonili bi se negativni učinci dezinformacija na organizaciju javnog znanja.

- Treći izazov predstavlja činjenica da su planeri i provoditelji operacija utjecaja u kiber prostoru u pravilu sigurnosno-obavještajne strukture zbog čega je karakter hibridnih operacija dodatno prikriven i teže uočljiv.

Evidentna je potreba da državne politike donesu nove koncepte prevencije, obrane i otklanjanja potencijalnih štetnih posljedica i da uvedu dodatna pravila i norme odgovornosti u kiber prostoru i na društvenim mrežama. „Države kao subjekt međunarodnog prava imaju vodeću ulogu u procesima ranog prepoznavanja i reakcije na hibridne prijetnje. Međutim, ne trebaju se ustručavati od toga da u određenom trenutku i na određeno razdoblje drugim sektorima (privatnom, javnom, akademskom), ako je u danom trenutku i procesu to najbolje rješenje, prepuste dio odgovornosti, zadržavajući pri tome snažnu sastavnicu nadzora nad djelovanjem zajedničkog tima. Suradnja mora biti obvezna za sve dionike tog procesa.“[715]

Društvene mreže osmišljene su za komercijalne svrhe, kao medij i kao informacijsko-komunikacijsko sredstvo koriste se za ostvarivanje legitimnih ciljeva u političkim i izbornim kampanjama kako bi se na učinkovitiji način biračkom tijelu privukla pažnja na vlastite informacijske sadržaje. Evidentno je da se koriste u operacijama utjecaja u kiber prostoru za prikriveno političko djelovanje, stvaranje učinkovitih dezinformacija u korpusu javnog znanja ciljanih publika i drugih formi prijetnji kako bi se preko kiber prostora na učinkovit način destabilizirali politički, društveni, sigurnosni procesi u drugim državama, ovisno o vlastitim potrebama. Poticanje podjela u ciljanim društvima, ekstremizma, radikalizma i terorizma i stvaranje dugoročne političke i društvene i sigurnosne destabilizacije -ovisno o krajnjem cilju- može eskalirati u svrgavanje postojećih struktura vlasti pa i rat kao krajnje rješenje međunarodnih sporova. Primjer su bile hibridne operacije u Europi, SAD-u, Ukrajini i u Siriji. Prema međunarodnom pravu nekoj državi može se suditi samo ako se potvrdi njezina odgovornost u kršenju suvereniteta druge države. Adresiranje nečije odgovornosti u kiber prostoru još uvijek se nalazi u pravnom vakuumu. „Subjekt međunarodnog prava (država, relevantna međunarodna organizacija) mora preuzeti svoju zakonodavnu ulogu i propisati jasna i obvezujuća pravila ponašanja u kiber prostoru te pravila, načine i metode kažnjavanja uočenih

715 Ibid., str. 46.

i prepoznatih nedopuštenih aktivnosti u kiber prostoru, bez obzira na to tko ih je počinio.“[716] To dakako iziskuje složenije odgovore jer je utvrđivanje odgovornosti otežano. Operacije utjecaja u kiber prostoru u pravilu su tajne, provode ih obavještajne državne strukture i često ostaju neotkrivene, naročito kad se provode na strateškoj razini. Provjeravanje i nadziranje sljedivosti dezinformacijskih kampanja, ciljeva i njihovih autora otežava njihova masovnost, automatiziranost i anonimnost. Ovom vrstom operacija ciljanim publikama se iz kiber prostora u njihovom korpusu javnog znanja nude fragmentirane informacije bez utvrđenog činjeničnog sadržaja ili prepoznatljivog izvora, pripremljene i uobličene na osnovi njihovih uvjerenja, načela i vrijednosti. Njihovoj neprimjetnosti doprinijela je sinergija „tvorničkih“ postavki algoritama, umjetne inteligencije i lažnih profila. Činjenica da su ove vrste operacija utjecaja s ovakvim mogućnostima u pravilu tajne i da ih koriste sigurnosno-obavještajne strukture stvara snažne psihološke i subverzivne učinke po ostvarivanje ciljeva. Obavještajnim službama i agencijama ove činjenice i mogućnosti dodatno osiguravaju prikrivenost, a napadnutim državama otežavaju adekvatno praćenje stvarnih namjera i ciljeva informacijskog napadača.

Model ranog prepoznavanja promatramo kroz a) fazu pripreme; b) fazu uočavanja informacijskog napada i c) fazu odvraćanja mogućih posljedica.

a) Faza pripreme

Faza pripreme podrazumijeva političku potporu mjerodavnim državnim tijelima koja će biti zadužena za stvaranje odgovora i protumjera: osvještavanje i podizanje percepcije potencijalnih ciljanih publika o svim aspektima hibridnih prijetnji i operacija utjecaja u kiber prostoru (tko ih provodi, kako ih provodi i s kojim ciljevima). To podrazumijeva „trajno sigurnosno osposobljavanje, obučavanje i obrazovanje ljudi uključenih u pojedine procese zaštite kritičnih infrastruktura koje su prva meta napada hibridne naravi svih budućih napadača“ [717].

b) Faza uočavanja informacijskog napada

Faza uočavanja informacijskog napada podrazumijeva uočavanje tendencija planskog i usmjerenog stvaranja informacijsko-psiholoških pritisaka prema ciljanim publikama. U ovoj fazi potrebno je prepoznati kroz koje je instrumente *mekane moći* država-napadač prisutna u

716 Ibid., str. 45.

717 Ibid.

napadnutoj državi, potrebno je uključiti političku, diplomatsku, medijsku i informacijsku potporu sa svrhom osvještavanja i podizanja percepcije o izloženosti napadu.

c) Faza odvraćanja mogućih posljedica

Faza odvraćanja podrazumijeva provedbu utvrđenih ciljeva iz prethodnih faza te primjenu odgovarajućih protumjera, uz stalnu potrebu prilagođavanja trenutnom stanju. U ovoj fazi od najveće vrijednosti bi bilo utvrditi izvor napada odnosno planera i izvoditelja dezinformacija.

Prepoznavanje dezinformacija u kiber prostoru nije jednostavno iz tri razloga. Napad je u pravilu anoniman, izvodi se pomoću pojedinačnih i/ili grupnih lažnih profila, u napadačkim taktikama primjenjuju se različite taktike koje su prilagođene danim okolnostima, društvenim slabostima ciljanih publika i samim potrebama napadača. Treći je razlog da napade u pravilu provode obavještajne strukture. Kroz sve tri faze odvraćanja potrebno je razvijati jednako prilagodljive sposobnosti i protuodgovore.

Predložene faze trebale bi integrirati aktivnosti države, javnog, privatnog i akademskog sektora i standardizirati te definirati aktivnu obranu i odvraćanje napada kroz štićenje pojedinih sektora KI-jeva. Funkcionalnim održavanjem KI-jeva gradi se povjerenje stanovništva i medija u institucije te se na taj način doprinosi suzbijanju hibridnih prijetnji i operacija. „Potrebno je stalno ulaganje materijalnih i ljudskih resursa u kiber, tehničku i fizičku zaštitu KI-jeva – kako na nacionalnoj, tako i na međunarodnoj razini – te integriranje tih zaštita s obzirom na integriranost i visoku međuovisnost KI-jeva, u cilju njihove zaštite od mogućih napadača, kao i njihova brzog i učinkovitog oporavka nakon izlaganja pojedinom sigurnosnom riziku, ulaganje u pojedinačnu i opću sigurnost.“[718]

Model ranog prepoznavanja i upozoravanja time bi bio primarno usmjeren na prevenciju vanjskog utjecaja na ključna područja: zaštitu informacijsko-komunikacijske infrastrukture, kiber sigurnost[719] i otklanjanje nasilnog ekstremizma i radikalizma u društvu.

718 Ibid., str. 45.

719 Kiber sigurnost čini sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kiber prostoru.

7.3. Nositelji modela ranog prepoznavanja i upozoravanja

Suprotstavljanje prijetnjama koje se planiraju i izvode iz kiber prostora na Zapadu uglavnom je vezano za vojnu perspektivu djelovanja mjerodavnih vojnih struktura. Međutim, glavnina takvih prijetnji ne odvija se u okolnostima klasičnog oružanog sukoba. Hibridne prijetnje društvenoj i političkoj stabilnosti odvijaju se u razdobljima mira, kriza i poraća kad se hibridnim operacijama planski i sustavno potiču političke, društvene i sigurnosne krize izvan konteksta rata. U hibridnim operacijama do najvećeg izražaja dolazi nevojna i nekonvencionalna priroda informacijsko-psiholoških pritisaka. Kako ovakva forma prijetnje nije vojne naravi, glavni nositelji protuodgovora i protumjera trebale biti civilne komponente: policijska, sigurnosno-obavještajna, civilna pravosudna tijela, akademska zajednica i civilno društvo. Hibridnost u aktivnom napadu uključuje mnoštvo aktera i raznolikost fizičkih i digitalnih oblika utjecaja. Model ranog prepoznavanja i upozoravanja trebao bi uključiti jednako tako višeslojne institucionalne napore i aktere: standardne modele informacijske sigurnosti, nacionalne civilne komponente, akademsku i stručnu javnost, tehnološke tvrtke, posredničke institucije i nevladin sektor. Dakako, nezaobilazni sudionik u ovom modelu je cjelokupno društvo kojem bi mjerodavna tijela trebala podići svjesnost o mogućnostima zloupotrebe algoritama i tehnologija umjetne inteligencije u prikupljanju, pohrani i obradi njihovih uvjerenja, načela i vrijednosti na društvenim mrežama. Stoga je izgradnja mehanizama otpornosti na negativne učinke zlouporaba hibridne inteligencije na društvenim mrežama postala evidentna potreba.

Središnju ulogu u provedbi nacionalne informacijske strategije imaju glavni nositelji takve strategije: državna tijela i nacionalni sigurnosno-obavještajni sustavi.

Državna tijela u prvom redu odgovorna su za održavanje stabilnosti gospodarskog, političkog i društvenog poretka, zadužena su za sigurno i neometano funkcioniranje informacijsko-komunikacijskih infrastruktura i funkcija koje društvo, politički i društveni poredak čine sigurnim, stabilnim i otpornim na hibridne prijetnje te su odgovorna za otklanjanje kritičnih društvenih slabosti. Uloga nacionalnih sigurnosno-obavještajnih sustava u provođenju informacijskih strategija i protuodgovora na hibridne prijetnje i operacije nameće se sama po sebi. Zadaća stranih sigurnosno-obavještajnih sustava je prikupljanje taktičkih podataka i informacija o ciljanim publikama kako bi na mogli diseminirati dezinformacije u cilju da se na što učinkovitiji način iskoriste slabosti ciljanih publika. U tom kontekstu, zadaća ovih sustava je u kiber prostoru planirati i izvoditi operacije utjecaja na osnovi utvrđenih kritičnih slabosti u uvjerenjima, načelima i vrijednostima ciljane publike te, shodno njima, isporučiti

dezinformacije kojima se potiče niz ostalih vrsta prijetnji. Strani sigurnosno-obavještajni sustavi određuju kategorije ciljanih publika koje će se izlagati opisanim konstantnim informacijsko-psihološkim pritiscima. Nacionalni sigurnosno-obavještajni sustavi u kontekstu prevencije i obrane od vanjskog djelovanja preko kiber prostora imaju presudnu ulogu. Njihova uloga je u jačanju nacionalne i nadnacionalne razine prevencije, u podizanju razine svjesnosti situacije te procjenjivanju rizika i otpornosti vlastitog društva ili sustava. Po prirodi obavljanja zadaća nacionalni sigurnosno-obavještajni sustavi raspolažu kapacitetima, sredstvima i specifičnim znanjima u prepoznavanju modaliteta djelovanja stranih sigurnosno-obavještajnih sustava u kiber prostoru. Razumijevanje, prepoznavanje, suzbijanje i otklanjanje štetnih učinaka hibridnih prijetnji i hibridnih operacija smatramo potrebnim kako bi se postigla optimalna integracija funkcija, aktivnosti i zadaća tijela koja, u skladu sa svojim nadležnostima, sudjeluju u aktivnostima i zadaćama procesa upravljanja sigurnosnim rizicima, od istraživanja i razumijevanja hibridnih operacija i prijetnji, procjene rizika do preventivnih mjera sigurnosne zaštite i odgovora u slučaju njihove realizacije, uključujući i aktivnosti i zadaće procesa upravljanja u kriznim stanjima. Hibridne prijetnje i operacije kroz tehnološke i dezinformacijske napade iz kiber prostora predstavljaju oblike informacijsko-psihološke agresije i one jesu glavne prijetnje društvu i nacionalnim politikama. Zlouporabama hibridne inteligencije na društvenim mrežama koje prikupljaju podatke o društvenim slabostima, ciljane publike su postale ranjivije i izloženije anonimnim, masovnim i automatiziranim informacijsko-psihološkim pritiscima s potencijalnim strateškim posljedicama. U dogledno vrijeme, kako se budu dodatno razvijale, tehnologije umjetne inteligencije na društvenim mrežama nesumnjivo će se koristiti za nove forme dezinformacija. Prema dosadašnjim iskustvima u hibridnim sukobima, ukoliko se upotreba informacijsko-komunikacijskih infrastruktura i tehnologija umjetne inteligencije adekvatno ne regulira one će se nastaviti zloupotrebljavati za sve suptilnije i realnije dezinformacije.

7.4. Preporuke

U sklopu izgradnje koncepta hibridne obrane i nacionalne informacijske strategije kroz model ranog prepoznavanja i upozoravanja postoji nekoliko osnovnih pretpostavki i preporuka na osnovu kojih će se mjerodavna tijela učinkovitije pripremiti za suprotstavljanje prijetnjama i operacijama utjecaja u kiber prostoru:

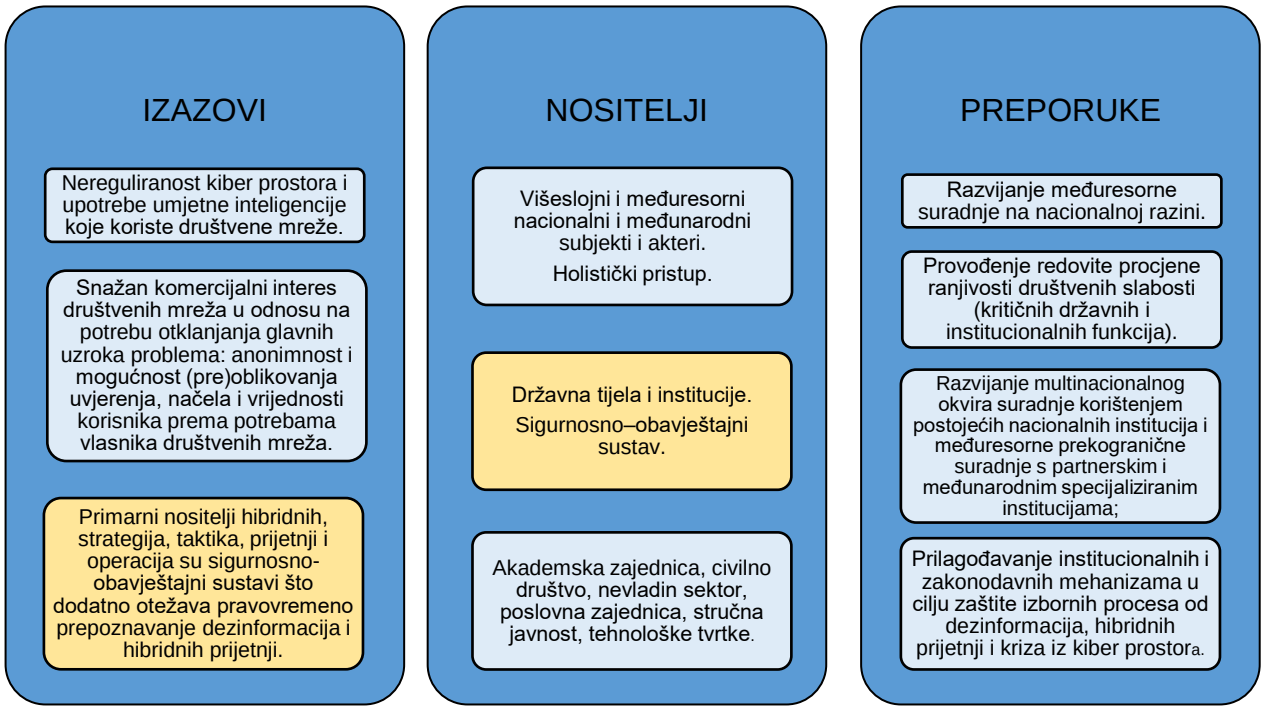
1) Razvijanje međuresorne suradnje na nacionalnoj razini. To podrazumijeva dodatno razvijanje suradnje i programa osvještavanja kojim bi se takve aktivnosti na učinkovitiji način

koordinirale između nositelja državne vlasti, mjerodavnih državnih tijela, sigurnosno-obavještajne zajednice, akademske i poslovne zajednice, civilnog društva, medija i pojedinaca. Ova preporuka podrazumijeva razvijanje adekvatnih politika, smjernica i stručnih analiza o zloupotrebama hibridne inteligencije na društvenim mrežama u kojima se načela, uvjerenja i vrijednosti zloupotrebljavaju za kreiranje prijetnji i planiranje i izvođenje operacija utjecaja iz kiber prostora. Međusobna koordinacija na nacionalnoj razini poboljšala bi pripremljenost i otpornost vladinih tijela i cjelokupnog društva te učinkovito provođenje ciljeva nove informacijske strategije.

2) Provođenje redovite procjene ranjivosti kritičnih društvenih, institucionalnih i političkih funkcija i slabosti. Svrha ovih procjena bila bi pravovremeno prepoznavanje i ublažavanje te otklanjanje uzroka koji pogoduju stvaranju hibridnih prijetnji. Vanjskom akteru time bi bile smanjene mogućnosti stvaranja prijetnji, iskorištavanja slabosti i ograničila bi se učinkovitost hibridnih operacija, informacijsko-psiholoških pritisaka i dezinformacija. Redovite procjene ranjivosti i slabosti bitan su preduvjet i podrazumijevaju izradu političko-strateških analiza s ciljem identifikacije i otklanjanja vlastitih društvenih slabosti. Model ranog prepoznavanja i upozoravanja u ovom dijelu trebao bi osigurati prepoznavanje kritičnih slabosti društva i razvijanje njegove otpornosti na vanjske prijetnje. Razumijevanje na koje načine se hibridna inteligencija zloupotrebljava na društvenim mrežama u planiranju i izvođenju prijetnji i operacija utjecaja za učinkovitije iskorištavanje opisanih slabosti predstavlja dodatnu vrijednost u odvraćanju napadnih informacijskih operacija (psiholoških operacija). Opisana metodologija planiranja i izvođenja hibridnih operacija iz kiber prostora daje koristan odgovor. Odgovori na osnovi sinkroniziranih i sustavnih analiza i procjena vlastitih društvenih slabosti i formi vanjskih prijetnji iz kiber prostora trebali bi doprinijeti pravovremenom otkrivanju dezinformacijskih kampanja koje kratkoročno ili dugoročno mogu imati štetne posljedice po organizaciju korpusa javnog znanja.

3) Razvoj multinacionalnog okvira suradnje korištenjem postojećih nacionalnih institucija i međuresorne prekogranične suradnje s partnerskim i međunarodnim specijaliziranim institucijama. Ova preporuka podrazumijeva razmjenu praksi i iskustava te međunarodnu koordinaciju, uspostavljanje mehanizama suradnje te razmjenu podataka i informacija s vlasnicima društvenih mreža, koordiniranje politika, sprječavanje ili otklanjanje mogućnosti zloupotreba umjetne inteligencije koju koriste društvene mreže.

4) Prilagođavanje institucionalnih i zakonodavnih mehanizama u cilju zaštite izbornih procesa od dezinformacija i hibridnih prijetnji iz kiber prostora.



Slika 47. Izgradnja modela prepoznavanja i ranog upozoravanja.

Slikom 47. žele se prikazati ključni izazovi, glavni nositelji i glavne preporuke u izgradnji modela prepoznavanja i ranog upozoravanja u sklopu novog koncepta prevencije i obrane od hibridnih prijetnji u kiber prostoru. Slikom se želi dodatno naglasiti ključna uloga državnih tijela i institucija sa središnjom ulogom nacionalnog sigurnosno-obavještajnog sustava. Razlog njegove središnje uloge je u tome što su primarni nositelji hibridnih strategija, taktika, prijetnji i operacija sigurnosno-obavještajni sustavi stranih država.

7.5. Potreba za izgradnjom modela digitalne i podatkovne suverenosti

„Jedan od neophodnih odgovora je u mehanizmima stvaranja, oblikovanja te očuvanja podatkovnog i digitalnog suvereniteta država (i međudržavnih integracijskih zajednica) na temelju kojeg bi, kao što utvrđuju suverenitet unutar vlastitih fizičkih granica, izgradili suverenitet i u vlastitom digitalnom prostoru unutar kojeg bi se uspostavila bolja pravila ponašanja.“[720] Jedan od pozitivnih pomaka u tom pravcu predstavljaju Berlinska deklaracija

720 Mlinac, Akrap, Lasić-Lazić, 2020.

koju su države članice EU-a usvojile u prosincu 2020. i Europska podatkovna strategija (Rezolucija 2020/2217(INI)) koju je Europski parlament usvojio 2021. „Digitalna transformacija podrazumijeva sudjelovanje čitavog društva u digitalnom prostoru, poštivanje temeljnih prava i demokratskih vrijednosti, jačanje međusobnog povjerenja, podizanje razine digitalne pismenosti i stvaranje sustava umjetne inteligencije koji će poticati otpornost i održivost na temeljnim vrijednostima i interesima ljudi i javnog sektora. Izgradnja ovakvih mehanizama ima za cilj jačati politike digitalnog suvereniteta kojima će države jačati vlastite sposobnosti u digitalnom prostoru za pružanje, primanje i razmjenu usluga radi učinkovitog međusobnog djelovanja.“[721]

Sa stajališta organizacije znanja možemo reći da je podatkovni suverenitet jedan od generičkih koncepata u novoj mapi javnog znanja. Generički pojmovi funkcioniraju kao predodžbene sheme za organizaciju poruka, motivaciju publike i prepoznavanje aktera u javnoj komunikaciji.[722] „One su žarišne točke sustava poruka i tvore čvorne točke mape znanja jedne zajednice koja dijeli iste vrijednosti, ima zajedničke interese te stvara i rabi ista znanja u ostvarivanju svojih ciljeva.“[723] „Odgovornost informacijske znanosti za javno znanje u informacijskom prostoru može biti prvenstveno u izradi standarda i alata za oblikovanje i upravljanje javnim znanjem kako bi se osigurao čisti informacijski prostor, dostupnost objektivnih informacija i ravnopravnost u razmjeni znanja.“[724]

„Temeljna načela na kojima treba graditi nacionalni i međudržavni podatkovni i digitalni suverenitet počivaju na promoviranju, očuvanju i razvijanju načela demokracije i slobode govora; na razvijanju transparentnosti i zaštiti ljudskih prava; sprječavanju monopola, cenzure i širenja dezinformacija te na uspostavljanju mehanizama odgovornosti za nešto što je napisano, objavljeno i podijeljeno, pri čemu javni interes treba biti ispred privatnih i korporativnih interesa.“[725]

„U tom cilju zadaća nacionalnih vlada i multinacionalnih organizacija treba biti uspostava sigurnih i pouzdanih mehanizama kojima bi se definirala pravila ponašanja i kojima bi se

721 Ibid.

722 Tuđman, Miroslav. Suverenitet ili izolacija: skica za istraživanje informacijskih strategija i predodžbenih shema u javnome znanju, 2007.

723 Ibid.

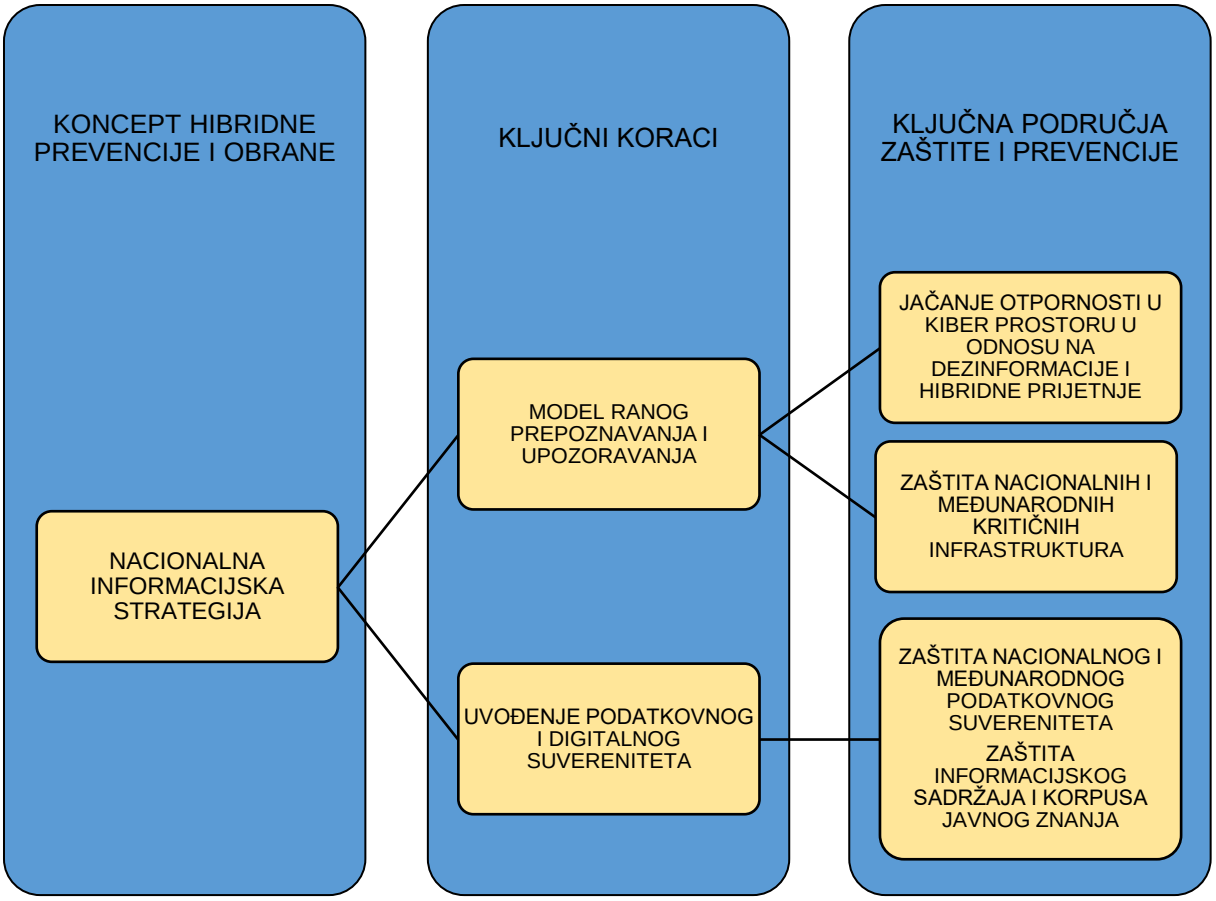
724 Mlinac, Akrap, Lasić-Lazić, 2020.

725 Ibid.

uspostavili zakoni koji bi vrijedili za ponašanje u kiber svijetu. Ovi mehanizmi trebali bi pridonijeti izgradnji učinkovite, sigurne, pouzdane, obnovljive i otporne kritične informacijsko-komunikacijske infrastrukture; daljnjem istraživanju, razvoju i provedbi temeljnih načela te razvijanju sposobnosti reagiranja na različite prijetnje. Temeljna načela nacionalnog i međudržavnog podatkovnog i digitalnog suvereniteta trebaju počivati i na sustavima umjetne inteligencije, ali ne na način da su algoritmi, programi i umjetna inteligencija donositelji odluka nego da se njihove prednosti i kvalitete iskorištavaju kao preporuke o kojima će konačne odluke donositi društvo. Jedno od temeljnih načela koja bi trebala osigurati provedbu podatkovnog i digitalnog suvereniteta počiva na transparentnoj interakciji, koordinaciji i zajedničkom radu državnih i međunarodnih institucija s privatnim, javnim i akademskim sektorom. Takvim pristupom mogu se i trebaju spriječiti sve one aktivnosti velikih tehnoloških kompanija koje teže preuzimanju dijelova suvereniteta koji imaju države i međudržavne organizacije. Države i međudržavne organizacije moraju biti čimbenici koji će određivati „pravila ponašanja i djelovanja“, a ne da tehnološke tvrtke same sebi definiraju pravila te same prate, nadziru i kontroliraju tu primjenu. Takvo ponašanje velikih tehnoloških tvrtki koje teže ka preuzimanju dijela suvereniteta može se tumačiti kao moderni tehnološki neo-imperijalizam.“[726]

Izrada nove nacionalne informacijske strategije kroz predloženi koncept hibridne obrane, te modele ranog prepoznavanja i upozoravanja i uspostavljanja digitalne i podatkovne suverenosti, stvorila bi preduvjete za bolje razumijevanje hibridnih prijetnji i hibridnih operacija koje je potrebno poduzeti radi pravovremenog prepoznavanja i otklanjanja štetnih posljedica. Nova nacionalna informacijska strategija treba počivati na moralnim načelima i temeljnim načelima slobode, javnosti i povjerenja te na pristupu točnim informacijama kao temeljnom ljudskom pravu. Temeljna svrha nacionalne informacijske strategije predstavljala bi protuodgovor na hibridne prijetnje i hibridne operacije. Ujedno bi predstavljala doprinos u izradi standarda i sredstava za oblikovanje i upravljanje javnim znanjem kako bi se osigurao čisti informacijski prostor, dostupnost objektivnih informacija i ravnopravnost u razmjeni znanja.

726 Ibid.



Slika 48. Novi obrasci prevencije i obrane od hibridnih prijetnji u kiber prostoru.

Slikom 48. u novom obrascu prevencije i obrane od hibridnih prijetnji želi se naglasiti središnja uloga Nacionalne informacijske strategije kroz uvođenje modela ranog prepoznavanja i upozoravanja te podatkovnog i digitalnog suvereniteta s ključnim područjima zaštite i prevencije i obrane od hibridnih prijetnji. Također, slikom se dodatno žele naglasiti ciljevi novog koncepta obrane i prevencije:

- podizanje svijesti o štetnim posljedicama zloupotrebe hibridne inteligencije na društvenim mrežama na organizaciju korpusa javnog znanja;
- podizanje svijesti o moći društvenih mreža kao taktičkih i učinkovitih alata za planiranje i izvođenje hibridnih operacija, realizaciju hibridnih strategija i taktika, te za stvaranje hibridnih prijetnji s potencijalnim strateškim posljedicama na korpuse javnog znanja ciljanih publika: osiguravanje napadačeve informacijske nadmoći;
- razvijanje povjerenja u institucije, društvo i državu, institucionalne sposobnosti;
- razvijanje medijske, digitalne i znanstvene pismenosti; promoviranje, očuvanje i razvijanje načela demokracije i slobode govora, transparentnosti i zaštite ljudskih prava;

- sprječavanje monopola, cenzure i širenja dezinformacija te uspostavljanje mehanizama odgovornosti za nešto što je napisano, objavljeno i podijeljeno.

Činjenica je da u kiber prostoru zloupotreba algoritama i drugih tehnologija umjetne inteligencije kroz prikupljanje, obradu i (pre)oblikovanje uvjerenja, načela i vrijednosti na društvenim mrežama imaju snažnu negativnu primjenu u fizičkom prostoru sa stvarnim učincima i posljedicama na društvene, političke, kulturološke i druge vrste identiteta koje su od interesa napadača. Neadekvatna reguliranost kiber prostora i društvenih mreža predstavljaju jedne od ključnih razloga zbog čega se glavnina psiholoških operacija planira i izvodi u kiber prostoru pomoću društvenih mreža. Prikupljanje taktičkih informacija i njihovo (pre)oblikovanje prema potrebama napadača kroz kiber prostor s posljedicama na fizički prostor u realnom vremenu tehnološki je omogućila višedimenzionalnost umjetne inteligencije i struktura prostora u kojem se potrebne informacije prikupljaju, pohranjuju i obrađuju. Primjena i zloupotreba hibridne inteligencije u operacijama utjecaja u kiber prostoru dodatno je ukazala na međusobnu neodvojivost podataka, njihove elektromagnetne prirode, kiber prostora kao elektromagnetnog okruženja te stvarnih događaja u fizičkom prostoru. Ovoj činjenici u svrhu izgradnje adekvatne informacijske strategije potrebno je prilagoditi političko-strateško razumijevanje uzroka i posljedica. Jedna od zadaća nove nacionalne informacijske strategije bila bi ukazati na ovu neospornu činjenicu. Najbolji primjer toga su tehnološki napadi na kritične infrastrukture iz kiber prostora. Aktivni napadi odvijaju se kroz kiber prostor, a štetne posljedice očituju se u fizičkom prostoru s mogućim taktičkim i strateškim posljedicama. U hibridnim operacijama konvergencija fizičkog i kiber prostora do izražaja dolazi i kroz djelovanje dezinformacija s daleko pogubnijim učincima na organizaciju korpusa javnog znanja. Činjenica je da su države, društva, zajednice i pojedinci globalizacijom društvenih mreža postali ovisniji o kiber prostoru i da su, proporcionalno, postali ranjiviji i izloženiji dezinformacijama i hibridnim prijetnjama koje se stvaraju na osnovi društvene slabosti odnosno podataka o njihovim uvjerenjima, načelima i vrijednostima. Mogućnost njihove zlouporabe u psihološkim operacijama postala je ključna mogućnost za učinkovito nametanje napadačeve volje i preoblikovanje korpusa javnog znanja prema potrebama napadača. U hibridnim operacijama tehnološki napadi predstavljaju pripremne radnje koje imaju potpornu ulogu u prikupljanju podataka bitnih za planiranje dezinformacija temeljem kojih se pospješuju učinci hibridnih prijetnji. Zbog ove činjenice bilo bi potrebno da nova nacionalna informacijska strategija obuhvati novu paradigmu napadačkog djelovanja koja se koristi u hibridnim operacijama. Kiber prostor je pogrešno promatrati prostorom koji se iskorištava isključivo za

izazivanje tehnoloških napada na kritične infrastrukture te bi bilo pogrešno zadržati se samo na razini njegove tehnološke zaštite. Stoga bi bilo potrebno da se izgradnji nove nacionalne informacijske strategije pristupi iz psihološke odnosno kognitivne perspektive kiber prostora. Nova informacijska strategija trebala bi počivati na zaštiti kulturnih, nacionalnih i drugih identitetskih simbola, nacionalnih vrijednosti, uvjerenja i načela. Primjeri hibridnih operacija dovoljno pokazuju da su prijetnje kognitivnoj domeni (razmišljanju i donošenju odluka) ciljanih publika daleko veća opasnost od tehnoloških napada na kritične infrastrukture. Dezinformacijskim kampanjama koje se izvode kroz operacije utjecaja u kiber prostoru pomoću društvenih mreža iskorištavaju se kognitivne pristranosti, usložnjavaju se prijetnje i povećavaju rizici te generiraju potencijalne krize. U tom kontekstu mehanizme aktivne prevencije, obrane, odvraćanja i zaštite nacionalnih i međunarodnih kritičnih infrastruktura bilo bi potrebno proširiti i uskladiti s mehanizmima aktivne prevencije, obrane i odvraćanja od hibridnih prijetnji kulturnim, nacionalnim i drugim identitetskim simbolima.

Nacionalna informacijska strategija trebala bi doprinijeti izgradnji ukupne otpornosti društva na dezinformacije i potencijalna krizna stanja koja proizlaze iz kiber prostora. Kako je informacija pokretač nacionalne moći u aktivnom napadu ona je ujedno pokretač moći u aktivnoj prevenciji, obrani i odvraćanju. U primjeru aktivne prevencije, obrane i odvraćanja moć informacije proizlazila bi iz sinergije nacionalnih, međunarodnih i informacijskih mjera i protuodgovora. Izvan konteksta oružanih sukoba hibridne prijetnje i operacije planiraju se i izvode sa svrhom generiranja kriza na osnovi iskorištavanja društvenih slabosti u strateškim uporišnim točkama (kulturne, ideološke i identitetske slabosti i ranjivosti) o kojima ovisi politička, društvena i sigurnosna stabilnost ciljane publike. U razdobljima mira, kriza i poraća ove uporišne kritične točke konstantno se napadaju dezinformacijama, različitim formama hibridnih prijetnji i ostalim instrumentima hibridne moći, primarno ekonomskim i financijskim, kako bi se korpus javnog znanja ciljanih publika preoblikovao prema potrebama napadača. Najosjetljivije i najslabije su države s većim stupnjem unutarnjih poteškoća u upravljanju, sa slabim državnim strukturama, s većim unutarnjim podjelama te s većim stupnjem korupcije. Slabosti društva, kulturni, nacionalni i drugi identitetski simboli, temeljni sustav njihovih vrijednosti, uvjerenja i načela jesu mete sustavnih i koordiniranih napada dezinformacijama. Primarna zadaća nacionalne informacijske strategije bila bi zaštita upravo ovih kritičnih identitetskih simbola, gradila bi društvenu otpornost na vanjske utjecaje, osigurala bi primjenu potrebnih mjera prevencije i doprinijela bi izgradnji unutarnje društvene i političke kohezije. Neke od zadaća informacijske strategije bile bi: prepoznavanje uzroka kriznih stanja,

ukazivanje na njih u svrhu otklanjanja, razvijanje povjerenja u institucije, jačanje svjesnosti društva i države o potrebi adekvatnije regulacije umjetne inteligencije na društvenim mrežama i sprječavanja zlouporaba hibridne inteligencije, razvijanje institucionalnih sposobnosti, medijske, digitalne i znanstvene pismenosti.

8. ZAKLJUČAK

Društvene mreže postale su snažni i učinkoviti taktički alati za stjecanje učinaka sa strateškim posljedicama: stjecanje informacijske nadmoći i (pre)oblikovanje korpusa javnog znanja ciljanih publika prema potrebi napadača. Dezinformacije i hibridne prijetnje koje se stvaraju pomoću društvenih mreža postale su glavne prijetnje koje proizlaze iz kiber prostora. Društvene mreže i tehnologije umjetne inteligencije u kiber prostoru postale su novi instrumenti moći u kiber prostoru i glavni taktički alati za stvaranje učinkovitih dezinformacija iz kojih proizlazi niz štetnih utjecaja na oblikovanje korpusa javnog znanja. U hibridnim sukobima koriste se za postizanje informacijske nadmoći. Društvene mreže jesu dominantni snažni i učinkoviti alati utjecaja za vođenje strateških informacijskih operacija utjecaja.

Istraživanjem je potvrđeno da je glavna meta hibridnih prijetnji postao korpus javnog znanja ciljanih publika. Time je odgovoreno na drugo istraživačko pitanje. Pokazano je da je izostanak nužnih pravila kojima bi se ograničila zloupotreba tehnologija umjetne inteligencije na društvenim mrežama doveo do novih formi psiholoških operacija, njihove učinkovitije operacionalizacije na taktičkim, operativnim i strateškim razinama. Psihološke operacije u kiber prostoru pomoću društvenih mreža i primjenom hibridne inteligencije time su postale hibridne i učinkovitije. Automatizirani sustav povratne sprege na društvenim mrežama pogoduje širenju dezinformacija, a hibridna inteligencija optimizira dezinformacije i poboljšava procese utjecaja. Nastale hibridne operacije time su postale dominanta metoda ispunjavanja ciljeva nacionalnih informacijskih strategija koje imaju za cilj stvarati globalnu informacijsku dominaciju. Opisanim primjerima pokazano je da se hibridne operacije odvijaju konstantno iza vidljivih događaja u stvarnom svijetu i da je takvim pritiscima izložen cjelokupni korpus javnog znanja ciljanih publika. Primjerima hibridnih operacija pokazano je da se u njihovom provođenju bilježi pojačan intenzitet djelovanja stranih sigurnosno-obavještajnih sustava koji zloupotrebljavaju društvene mreže kako bi prepoznali društvene slabosti i predviđali buduća ponašanja ciljanih publika, sukladno kojima dezinformacije prilagođavaju operativno-taktičkim i strateškim ciljevima kako bi pospješili hibridne prijetnje.

Evidentno je da su društvene mreže postale dominantan taktički informacijski instrument hibridne moći sa strateškim posljedicama kojim državni akteri djelovanjem stranih sigurnosno-obavještajnih sustava u rješavanju međunarodnih sporova pojačavaju učinak i određuju uspjeh ostalih instrumenata hibridne moći (političkih, diplomatskih, ekonomskih, vojnih itd). Time je ujedno odgovoreno na treće istraživačko pitanje jer je istraživanje pokazalo da svi akteri na

svim geografskim područjima sukobljavanja koriste trenutno najpopularnije društvene mreže (YouTube, Twitter i Facebook) za stvaranje učinkovitih dezinformacija i hibridnih prijetnji prema svim kategorijama ciljanih publika, ovisno o potrebama, ciljevima i okolnostima.

Shodno tome, umjetna inteligencija na društvenim mrežama ne smije dobiti preveliku moć odnosno autoritet u donošenju odluka, poglavito na političko-strateškoj razini. Onaj tko ima pristup, kontrolu i nadzor nad umjetnom inteligencijom na društvenim mrežama u poziciji je da kontekstualizira i interpretira njezine rezultate. Nadzor, kontrola, upravljanje i kontekstualiziranje ciljeva koji se žele postići njezinom primjenom stoga su od ključne važnosti.

Radom se pokazalo da su društvene mreže u virtualnom svijetu stvorile niz negativnih posljedica na organizaciju znanja iz kojih su u stvarnom svijetu nastali stvarni politički, društveni i sigurnosni problemi koji dugoročno predstavljaju ozbiljan sigurnosni rizik za političku i društvenu stabilnost, za demokratske procese te za organizaciju znanja.

Namjera istraživanja je donositeljima političkih odluka povećati percepciju o nužnosti jačanja politika kojima će se u kiber prostoru spriječiti zloupotrebe tehnologija umjetne inteligencije i društvenih mreža za stvaranje dezinformacija i hibridnih prijetnji, koje će doprinijeti izgradnji mehanizama za uspostavu digitalne i podatkovne suverenosti te koje će, u konačnici, doprinijeti otklanjanju štetnih posljedica dezinformacija na korpus javnog znanja.

POPIS SLIKA

POPIS TABLICA

LITERATURA:

1. A Multinational Capability Development Campaign project (MCDC) Countering Hybrid Warfare Project: Countering Hybrid Warfare, 2019.
2. Aceves, J. W., *Virtual Hatred: How Russia Tried to Start a Race War in the United States*, 2019. URL: https://repository.law.umich.edu/mjrl/vol24/iss2/2
3. Affaya, N. M., *The Arab Spring: Breaking the chains of authoritarianism and postponed democracy*, Contemporary Arab Affairs, 2011. URL: https://caus.org.lb/wp-content/uploads/2021/10/The-Arab-Spring-breaking-the-chains-of-authoritarianism.pdf
4. Akrap, G., *Informacijske strategije i oblikovanje javnoga znanja*, National security and the future, str. 77-151., 2009., URL: https://hrcak.srce.hr/80639
5. Akrap, G. *Informacijske strategije i operacije u oblikovanju javnog znanja*, Sveučilište u Zagrebu Filozofski fakultet, Zagreb, 2011.
6. Akrap, G. *Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura*, *Strategos*, 2019. URL: https://hrcak.srce.hr/231009
7. Akrap, G; Mandić I., *Why Security Science*, Security Science Journal, Vol. 1 No. 2, 2020. URL: https://zagrebsecurityforum.com/securitysciencejournal/id/4163
8. Američko Ministarstvo domovinske sigurnosti, Korištenje društvenih medija za poboljšanu situacijsku svijest i podršku u odlučivanju, 2014. URL:https://www.dhs.gov/publication/using-social-media-enhanced-situational-awareness-decision-support
9. Arquilla, J. i Ronfeldt F. D., The Advent of Netwar, RAND, 1996., URL: http://www.rand.org/pubs/monograph_reports/MR789.html
10. Arquilla, J. i Ronfeldt F. D. (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, 1997. URL: https://www.rand.org/pubs/monograph_reports/MR880.html
11. Arquilla, J. i Ronfeldt D., *The Advent of Netwar (Revisited), Networks and Netwars: The Future of Terror, Crime, and Militancy,* RAND, 2001. URL: https://www.rand.org/pubs/monograph_reports/MR1382.html
12. *Artificial Intelligence and National Security*, Federation of American Scientist, November 10, 2020., URL: https://fas.org/sgp/crs/natsec/R45178.pdf (28.05. 2019.)

13. Berchane, N. i N., *Artificial Intelligence, Machine Learning, and Deep Learning: Same context, Different concepts*, Master Intelligence Economique et Stratégies Compétitives, 2018., Dostupno na: https://master-iesc-angers.com/artificial-intelligence-machine-learning-and-deep-learning-same-context-different-concepts/ (17.02.2022.).
14. Assa, H., *Infuencing Public Opinion u The Cognitive Campaign*, Strategic and Intelligence Perspectives in Yossi Kuperwasser i David Siman-Tov, Editors, The Institute for National Security Studies, Tel Aviv, 2019. Dostupno na https://www.inss.org.il/publication/the-cognitive-campaign-strategic-and-intelligence-perspectives/ (15.08.2020).
15. Atkinson, C. *Hybrid Warfare and Societal Resilience: Implications for Democratic Governance*, Information & Security: An International Journal 39, no. 1, 2018, str. 63-76., URL: http://dx.doi.org/10.11610/isij.3906
16. Backes, O. i Swab, A., *Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States*, Belfer Center for Science and International Affairs Harvard Kennedy School, 2019. URL: https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states (20.01. 2021.)
17. Baezner, M.; Robin, P., *Hotspot Analysis:The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict*, October 2017, Center for Security Studies, ETH Zürich. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf
18. Baezner, M.; Robin, P., *Hotspot Analysis: Cyber and Information Warfare in elections in Europe*, December 2017, Center for Security Studies (CSS), ETH Zürich. URL:https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf
19. Bakshy, E.; Messing, S.; Adamic, L., *Exposure to ideologically diverse news and opinion on Facebook*, Science, New York, May 2015., URL:https://www.researchgate.net/publication/276067921_Political_science_Exposure_to_ideologically_diverse_news_and_opinion_on_Facebook
20. Berger J. M.; Morgan J., *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*, The Brookings Center for Middle East Policy, 2015., URL:https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

21. Bergh A., *Social network centric warfare – understanding influence operations in social media*, Norwegian Defence Research Establishment, 2019. URL:https://www.ffi.no/en/publications-archive/social-network-centric-warfare-understanding-influence-operations-in-social-media
22. Berkovsky, S.; Kaptein, M.; Zancanaro, M. *Adaptivity and personalization in persuasive technologies in Proceedings of the International Workshop on Personalization in Persuasive Technology*, 11th International Conference on Persuasive Technology, Salzburg, Austria, 2016, str. 13-25,. URL: http://ceur-ws.org/Vol-1582/17Kaptein.pdf
23. Bienvenue E.; Rogers Z.; Troath S.; *Cognitive Warfare: The Fight We've Got*, 2019.,URL:https://www.cove.org.au/adaptation/article-cognitive-warfare-the-fight-weve-got/
24. Bouchrika I., *What Is The Fourth Industrial Revolution: Risks, Benefits & Responses*, 2021., URL: https://research.com/careers/what-is-the-fourth-industrial-revolution
25. Brangetto, P.; Veendendaal, M., *A Influence Cyber Operations: the Use of Cyberattacks in Support of Influence Operations*, 8th International Conference on Cyber Conflict, Tallinn, Cooperative Cyber Defence Centre of Excellence, NATO, 2016., URL: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf (16.08.2021.)
26. Brzica N., *Hibridni ratovi i suvremeni sukobi*, Fakultet političkih znanosti, Zagreb, 2018.,URL:https://www.fpzg.unizg.hr/_download/repository/Doktorki_rad_Nikola_Brzica.pdf (20.01.2021.)
27. Burnore N., *Social Media Applications for Unconventional Warfare*, U.S. Army Command and General Staff College, Homeland Security Digital Library, SAD, 2013., URL: https://www.hsdl.org/?abstract&did=761246 (26.03.2020.)
28. Calamur K., *What is the Internet Research Agency?*, The Atlantic, 2018., URL:https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/ (25.07.2020.)
29. Castells M., *Mreže revolta i nade, društveni pokreti u doba interneta*, JP Službeni glasnik, 2018.
30. Connell M.; Vogler S., *Russia's Approach to Cyber Warfare*, Center for Naval Analyses, 2016., URL: https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf (17.02.2019.)

31. Cohen D.; Bar'el O., *The Use of Cyberwarfare in Influence Operation*, Blavatnik Interdisciplinary Cyber Research Cente, Tel Aviv University, 2017., https://icrc.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf (11.01.2021.)
32. Cordey, S., *Cyber Influence Operations: An Overview and Comparative Analysis*, Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich, 2019., URL:https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf (19.09.2020)
33. Čotić, D., *Uloga osobnih i demografskih čimbenika u namjeru online kupovine kod potrošača*, Sveučilište u Splitu, Ekonomski fakultet, 2021., str. 22., URL: https://urn.nsk.hr/urn:nbn:hr:124:213833, (29.05.2022).
34. Crnčić, S., *Umjetna inteligencija u poslovanju*, Diplomski rad, Sveučilište Sjever, 2020., URL: https://urn.nsk.hr/urn:nbn:hr:122:847217 (11.08.2021.)
35. Čehulić Lidija, Euroatlantizam, Politička kultura, Zagreb, 2003.
36. Davis N., *5 ways of understanding the Fourth Industrial Revolution*, World Economic Forum, 2015., URL: https://www.weforum.org/agenda/2015/11/5-ways-of-understanding-the-fourth-industrial-revolution/ (17.2.2022.).
37. Danyk Y.; Zborovska O., *Development and Implementation of a new Concept of Crisis situation syndrome: Syndrome of a Hybrid War*, Eureka, Health Sciences, Number 6, 2018., URL: http://eu-jr.eu/health/article/view/797 (15.01.2020.)
38. DiResta R.; Shaffer K.; Ruppel B.; Sullivan D.; Matney R.; Fox R.; Albright J.; Johnson B., *The Tactics & Tropes of the Internet Research Agency*, New Knowledge, 2018, URL: https://digitalcommons.unl.edu/senatedocs/2/ (18.02.2020.)
39. Europsko Vijeće, Vijeće Europske unije, Priopćenje za medije, 10. prosinca 2019.: Countering hybrid threats: Council calls for enhanced common action. URL: https://www.consilium.europa.eu/hr/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/
40. Egel D.; Robinson E.; Cleveland T. C.; Oates C.; *AI and Irregular Warfare: An Evolution, Not a Revolution*, War on the Rocks, October 31, 2019., URL: https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/ (23.02.2020).

41. Fabien M., *AI in Military Enabling Applications*, CSS Analyses in Security Policy, No. 251, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf (28.09.2020.)

42. Facebook, *Optimizing your Facebook campaign objective*, AdEspresso, URL: https://adespresso.com/guides/facebook-ads-optimization/campaign-objective/ (10.07. 2020.

43. Facebook, *Information Operations and Facebook*, 2017., URL: https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf (13,03.2019.)

44. Flore, M.; Balahur-Dobrescu, A.; Podavini, A.; Verile, M., *Understanding Citizens` Vulnerabilities to Disinformation and Data-Driven Propaganda*, Publications Office of the European Union, Luxembourg, 2019., URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC116009 (11.09.2020.)

45. Forrest, E. M.; Benjamin, B.; Andrew, J. L.; Mark, A.; Christian, C.; Kelly, K.; Derek, G.; *Military Applications of Artificial Intelligence, Ethical Concerns in an Uncertain World*, RAND Corporation, 2020., str. 29-40., https://www.rand.org/pubs/research_reports/RR3139-1.html (21.09.2021.)

46. Foxall A., *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*, Policy Paper No. 9, Russia Studies Centre at the Henry Jackson Society, London, 2016., URL:http://henryjacksonsociety.org/wp-content/uploads/2018/06/Putins-Cyberwar.pdf (07.06.2019.).

47. Fredheim R., NATO Strategic Communications Centre of Exellence, Robotrolling 2, 2017., URL: https://www.stratcomcoe.org/robotrolling-20172 (29.04.2021.)

48. Fridman O., *The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political and Public Discourse*, Defence Strategic Communications, The official journal of the NATO Strategic Communications Centre of Excellence, Volume 2, 2017., str. 61 – 86., URL: https://www.stratcomcoe.org/ofer-fridman-russian-perspectiveon-information-warfare-conceptual-roots-and-politicisation-russian (5.8.2020.)

49. Gady F.S., Austin G., *Russia, The United States, And Cyber Diplomacy*, The EastWest Institute, 2010. str. 5., URL: https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf (04.09.2017.)

50. Gerasimov V., *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, US Army Press, Military Review, January-February 2016., str. 23-29. URL:https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (14.02.2017.)

51. Ghosh D., Scott B., *#Digital Deceit:The Technologies behing precision propaganda on the Internet*, 2018., URL: https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/ (23.07.2019.)

52. Giannopoulos G., Smith H., Theocharidou M., *The landscape of Hybrid Threats: A conceptual model*, 2021., URL: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/ (22.06.2021.)

53. Gonçalves, C. P., *Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats*., 2019. URL: https://www.intechopen.com/chapters/68561 (14.02.2021)

54. Giesea Jeff, *It's Time To Embrace Memetic Warfare*, NATO Strategic Communications Centre of Excellence, Riga, 2017.

URL:https://www.act.nato.int/images/stories/media/doclibrary/open201705-memetic1.pdf (29.04.2021.)

55. Gonzáles-Cabanás, J.; Cuevas Á.; Cuevas, R.; López-Fernández J.; García D., *Unique on Facebook: Formulation and Evidence of (Nano)targeting Individual Users with non-PII Data*, 2021., str.1. URL: https://arxiv.org/abs/2110.06636 (16.02.2022.)

56. Graves C., Matz S., *What Marketers Should Know About Personality-Based Marketing*, Harvard Business Review, 2018., URL: https://hbr.org/2018/05/what-marketers-should-know-about-personality-based-marketing (02.05.2020)

57. Howard N. P., Ganesh B., Liotsiou D., *The IRA, Social Media and Political Polarization in the United States: 2012-2018*, Oxford University, Oxford, UK, 2018. URL: : https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report.pdf (17.08.2020.)

58. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, dostupno na: https://www.enciklopedija.hr/

59. Ioffe J., *The History of Russian Involvement in America's Race Wars*, The Atlantic, 2017., URL: https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/ (15.03.2019.).

60. Joint Publication 3-13, 2014, *Information Operations*, dostupno na: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, (30.04.2019.).

61. Joint Concepts - Operating in the Information Environment.Pdf, URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf (31.12.2020.)

62. Kumar R., *Potential impact of Artificial Intelligence on future strategies*, King's College London, 2021., URL: https://www.researchgate.net/publication/350022050_Potential_impact_of_Artificial_Intelligence_on_future_strategies (17.06.2022.)

63. Kaput M., *The AI Terms Cheat Sheet [Easy Explainer of AI Terminology]*, Marketing Artificial Intelligence Institute, 2021., URL:https://www.marketingaiinstitute.com/blog/the-marketers-guide-to-artificial-intelligence-terminology?_ga=2.91286621.636606009.1634325315-126872872.1634325315 (02.01.2022.)

64. Kaput M., *Facebook AI: An Honest Assessment*, Marketing Artificial Intelligence Institute, 2021, URL: https://www.marketingaiinstitute.com/blog/how-facebook-uses-artificial-intelligence-and-what-it-means-for-marketers, (10.01.2022.)

65. Kerbusch P., Keijser B., Selmar S., *Roles of AI and Simulation for Military Decision Making*,2018., URL:https://pdfs.semanticscholar.org/885b/182170db541d48ca7f0380bc0447ce56c9ae.pdf. (22.03.2021.)

66. Kiesler J., *A Next Generation National Information Operations Strategy and Architecture*, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2021., URL: https://www.belfercenter.org/publication/next-generation-national-information-operations-strategy-and-architecture#footnote-045 (03.02.2022.)

67. Kohlbacher F., *The Use of Qualitative Content Analysis in Case Study Research*, Volume 7, No. 1, Art. 21., 2006., dostupno na http://www.qualitative-research.net/index.php/fqs/article/view/75/153#g332
68. Korybko, A., Haddad, H., *Chaos Theory, Global Systemic Change, and Hybrid Wars* // Comparative Politics Russia, 2016, No.4, str. 25-35. URL: DOI: 10.18611/2221-3279-2016-7-4(25)-25-25 (22.12.2019.)
69. Korybko A., *Hybrid Wars: The Indirect Adaptive Approach to regime Change*, Moskva, 2018., URL: https://1lib.nl/book/2801250/bdfe49?id=2801250&secret=bdfe49 (11.05.2019.)
70. Kosinski M.; Stillwell D.; Graepel T., *Digital records of behavior expose personal traits*, Proceedings of the National Academy of Sciences, 2013., URL: https://www.pnas.org/content/110/15/5802 (20.04.2019.)
71. Kreiss, D., *Micro-targeting, the quantified persuasion*. Internet Policy Review, 6(4), 2017., URL: https://doi.org/10.14763/2017.4.774 (14.03.2020.)
72. Kuzio T., D'anieri P., *The Sources of Russia's Great Power Politics*, E-International Relations, Bristol, England 2018. URL: https://www.e-ir.info/publication/the-sources-of-russias-great-power-politics-ukraine-and-the-challenge-to-the-european-order/ (15.06.2020.)
73. Kuzio T., *Why Vladimir Putin is Angry with the West Understanding the Drivers of Russia's Information*, Cyber and Hybrid War, Security Policy Working Paper, No. 7, Federal Academy for Security Policy, 2017. URL: https://www.baks.bund.de/en/working-papers/2017/why-vladimir-putin-is-angry-with-the-west-understanding-the-drivers-of-russias (22.09.2020.)
74. Langworthy Stacy, Power Dynamics in an Era of Big Data, London School of Economics and Political Science, 2019. URL: http://www.lse.ac.uk/ideas/publications/updates/big-data
75. Lipsey A. R., *Network Warfare Operations: Unleashing the Potential*, Center for Strategy and Technology Air War College, Air University, SAD, 2005., URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a509649.pdf (13.07.2018.)
76. Liddell H., *The Strategy of Indirect Approach*, Internet Archive, 1954., URL: https://archive.org/stream/strategyofindire035126mbp/strategyofindire035126mbp_djvu.tx (25.07.2020.)
77. Lind S. W., *Understanding Fourth Generation War*, Homeland Security Digital Library, 2004., URL: https://www.hsdl.org/?view&did=482203 (16.02.2019.)

78. Lind S. W.; Nightengale K.; Schmitt F. J.; Sutton W. J.; Wilson I. G., *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette,1989, str. 22-26, URL: https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html (25.11.2021.).
79. Lin H., Kerr J., *On Cyber-Enabled Information/Influence Warfare and Manipulation*, Center for International Security and Cooperation, Stanford, SAD, 2017., URL: https://cisac.fsi.stanford.edu/publication/cyber-enabled-informationinfluence-warfare-and-manipulation (25.01.2021.)
80. Leonova O., *Sharp Power – the New Technology of Influence in a Global World*, World Economy and International Relations, Moskva, 2019., URL: https://www.imemo.ru/en/jour/meimo/index.php?page_id=685&id=9020&at=a&pid (11.03.2020.)
81. Lynch M., Freelon D., Aday S., *Syria's Socially Mediated Civil War*, Institute of Peace, United States 2014. URL: https://www.usip.org/publications/2014/01/syrias-socially-mediated-civil-war (24.03.2020.)
82. Harhoff D.; Heumann S.; Berlin N.J.; Lorenz P., *Outline for a German Strategy for Artificial Intelligence*, July 2018, str. 6., URL: https://www.ip.mpg.de/fileadmin/ipmpg/content/aktuelles/Outline_for_a_German_Artificial_Intelligence_Strategy.pdf (25.03.2022.)
83. Hartmann K., Giles K., *The Next Generation of Cyber-Enabled Information Warfare*, Cooperative Cyber Defence Centre of Excellence, NATO, 2020. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_13_Hartmann_Giles.pdf (23.01.2022.)
84. Heap B., Hansen P., Gill M., *Strategic Communications Hybrid Threats Toolkit*, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, NATO Strategic Communications Centre of Excellence, Riga, 2021., URL: https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213 (14.02.2022.)
85. Henriksen E. E., *Big data, microtargeting, and governmentality in cybertimes, The case of the Facebook-Cambridge Analytica data scandal*, Master thesis in political science, Department of Political Science University of Oslo, 2019. Dostupno na: https://www.duo.uio.no/handle/10852/69743 (23.05.2020)
86. Heickerö Roland, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency, 2020.

87. Hofmann, J., *Mediated democracy – Linking digital technology to political agency*. Internet Policy Review, 2019., URL: https://doi.org/10.14763/2019.2.1416 (12.02.2021.)
88. Hutchinson William, *Influence Operations: Action and Attitude*, 2010. URL; https://ro.ecu.edu.au/isw/33/ (11.02.2021.)
89. Mann, S. R., *Chaos Theory in Strategic Thought* // Parametes, 1992. Dostupno na: https://archive.org/stream/1992Mann/1992+mann_djvu.txt (11.06.2021)
90. Matz S., Netzter, O., *Using Big Data as a Window into Consumers' Psychology, Current Opinion in Behavioral Sciences*, 2017., str. 7-12. URL: https://www.sciencedirect.com/science/article/pii/S2352154617300566. (15.04. 2019.).
91. Markotić K., *Umjetna inteligencija (AI) - Sve što trebate znati*, MachineDesk, 2021., URL:https://www.machine-desk.com/industrija-4-0/umjetna-inteligencija-ai (19.02.2022.)
92. Markopoulos, P., Kaptein, M. C., Ruyter de, B. E. R., Aarts, E. H. L., *Personalizing persuasive technologies: explicit and implicit personalization using persuasion profiles*. International Journal of Human Computer Studies, 2015, str. 38-51. URL: https://www.semanticscholar.org/paper/Personalizing-persuasive-technologies%3A-Explicit-and-Kaptein-Markopoulos/5f7351d1c71bac1f4bd0e18bb7eb94f817dc4908#citing-papers (14.19.2021.)
93. Mazarr J. M.; Bauer R. M.; Casey A.; Heintz S.A.; Matthews J. L., *The Emerging Risk of Virtual Societal Warfare, Social Manipulation in a Changing Information Environment*, RAND Corporation, SAD, 2019. URL: https://www.rand.org/pubs/research_reports/RR2714.html (19.09.2020.)
94. Roselle, L., Miskimmon, A., O'Loughlin, B., *Strategic narrative: A means to understand soft power*, Sage Journals, 2014. Dostupno na: (PDF) Strategic narrative: A new means to understand soft power (researchgate.net) (19.09.2021.)
95. Normak Magnus, How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks, The European Centre of Excellence for Countering Hybrid Threats, 2019. https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_15_Non-state-Actors.pdf

96. Mladenović D., *Multidisciplinarni aspekti kiber ratovanja*, Fakultet organizacijskih znanosti, Sveučilište Beograd, 2016., URL:https://uvidok.rcub.bg.ac.rs/bitstream/handle/123456789/1248/Doktorat.pdf (17.05.2020.)
97. Murdock J., *What is the Internet Research Agency? Facebook Shuts Hundreds of Accounts Linked to Russian Troll Factory*, Newsweek, 2018, URL: https://www.newsweek.com/what-internet-research-agency-facebook-shuts-hundreds-accounts-linked-russia-870889;
98. Munoz, A., *U.S. Military Information Operations in Afghanistan*, RAND Corporation, SAD,2012., URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1060.pdf (18.07.2019.)
99. Millicent A., *AI at the US Department of Homeland Security – Current Projects*", 2019, https://emerj.com/ai-sector-overviews/artificial-intelligence-homeland-security/ (22.07.2021.)
100. Nadler, A., Crain, M., Donovan, J., *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech*, Data & Society Research Institute, SAD, Report, 2018., URL: https://datasociety.net/library/weaponizing-the-digital-influence-machine/ (20.2.2020.)
101. Nadler, A., McGuigan, L., *An impulse to exploit: the behavioral turn in data-driven marketing*. Critical Studies in Media Communication. 2017., str. 1-15. URL: https://www.researchgate.net/publication/320535625_An_impulse_to_exploit_the_behavioral_turn_in_data-driven_marketing (25.03.2020.)
102. Nemeth, W. J., *Future war and Chechnya: a case for hybrid warfare*, Monterey, California. Naval Postgraduate School, 2002., URL: https://calhoun.nps.edu/handle/10945/5865 (29.05.2020.)
103. Neudert M.L., Nahema M., *Polarisation and the use of technology in political campaigns and communication*, European Parliamentary Research Service, Brussels, 2019. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf (17.08.2021.)
104. Nestoras A., *Political Warfare: Competition in the Cyber Era*, Policy Brief, The Wilfried Martens Centre for European Studies, Brussels, 2019. URL:

https://martenscentre.eu/publications/political-warfare-competition-cyber-era (20.03.2020.)

105. Nissen T., *The Weaponization of Social Media*, Royal Danish Defence College, NATO Strategic Communications Centre of Excellence, 2015. URL: https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media (28.04.2019)

106. Normak M., *How States Use Non-State Actors*: *A Modus Operandi for Covert State Subversion and Malign Networks*. The European Centre of Excellence for Countering Hybrid Threats. 2019., URL: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-15-how-states-use-non-state-actors-a-modus-operandi-for-covert-state-subversion-and-malign-networks/ (09.04.2020.)

107. Nye J., *Protecting Democracy in an Era of Cyber Information War*, Belfer Center for Science and International Affairs, Harvard Kennedy School, SAD, 2019., URL: https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war (18.09.2021.)

108. Nye J., The Future of Power, Public Affairs, New York 2011.

109. Oates, S., *The easy weaponization of social media: why profit has trumped security for U.S. companies*. Digi War 1, 2020., str., 117–122, URL: https://doi.org/10.1057/s42984-020-00012-z (11.12.2020.)

110. Office of the Director of National Intelligence, "*Assessing Russian Activities and Intentions in Recent US Elections*," January 2017., URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf (17.04.2020.)

111. Orttung, R., Walker, C., *Russia's International Media Poisons Minds*, Moscow Times, 2014, URL: https://themoscowtimes.com/articles/russias-international-media-poisons-minds-40194 (16.02.2020.).

112. Osnos, E., Remnick, D., Yaffa, J., *Trump, Putin, and the New Cold War, What lay behind Russia's interference in the 2016. election—and what lies ahead?*, March 6, 2017., URL: https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war (05.08.2020)

113. Paikowsky Deganit i Matania Eviatar, *Influence Operations in Cyber: Characteristics and Insights*; The Cognitive Campaign: Strategic and Intelligence Perspectives Yossi Kuperwasser and David Siman-Tov, Editors, The Institute for National Security Studies,

Tel Aviv, 2019., URL: https://www.inss.org.il/publication/the-cognitive-campaign-strategic-and-intelligence-perspectives/ (15.08.2020).

114. Papakyriakopoulos, O.; Hegelich, S.; Shahrezaye, M.; Serrano Medina, J. C., *Social media and microtargeting: Political data processing and the consequences for Germany*, Big Data & Society, Research Article, 2018., URL: https://journals.sagepub.com/doi/full/10.1177/2053951718811844#_i26 (18.09.2020.)

115. Pescetelli, N., *A Brief Taxonomy of Hybrid Intelligence*, Forecasting 3, MDPI, 2021., str. 633-643, URL: https://doi.org/10.3390/forecast3030039 (17.02.2022.)

116. Pomerantsev, P., i Weiss, M., T*he Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, New York, 2014., URL: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

117. Putica M., *Umjetna inteligencija: Dvojbe suvremenog razvoja*, Filozofski fakultet, Sveučilište Mostar, Hum, vol. 13, br. 20, 2018, str. 198-213. URL: https://hrcak.srce.hr/219733. (19.03.2022.)

118. Svetoka S., *Social media as a tool of Hybrid Warfare*, NATO Strategic Communications Centre of Exellence, Riga, 2016. URL: https://www.stratcomcoe.org/social-media-tool-hybrid-warfare (29.04.2021.)

119. Radman, Lana, Psihologija terorizma Islamske države Iraka i Levanta, Sveučilište u Zagrebu, Fakultet političkih znanosti, 2016. Dostupno na: https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg:122 (14.03.2017.).

120. Rand, W., *The Weaponization of Information, The Need for Cognitive Security*, RAND Corp., 2017., URL; https://www.rand.org/pubs/testimonies/CT473.html; (19.04.2019.)

121. Rugge F., *Mind Hacking Information Warafre In The Cyber Age*, Istituto per gli Studi di Politica Internazionale, Milano, Analysis No. 319, 2018., URL: https://www.ispionline.it/sites/default/files/pubblicazioni/analisi319_rugge_11.01.2018_2.pdf (19.05.2019.)

122. *Robotic Process Automation, RPA in Advertising* | Social Media, Data Management, SEO, April 30, 2021. URL: https://www.robomotion.io/blog/rpa-in-advertising-social-media-data-management-seo/ (20.03.2022.)

123. Saslow Alec, *Artificial Intelligence Plays a Critical Role Fueling Online Disinformation*, 2021., URL: https://decode.org/news/artificial-intelligence-plays-a-critical-role-fueling-online-disinformation/ (10.01.2022.)

124. Schnaufer, T. A., *Redefining Hybrid Warfare: Russia's Non-linear War against the West*, Journal of Strategic Security 10, no. 1, str. 17-31., 2017. URL: https://scholarcommons.usf.edu/jss/vol10/iss1/3 (25.06.2019.)

125. Schmidt E., Work R., *In Search of Ideas: The National Security Commission on Artificial Intelligence Wants You*, War on the Rocks, 2019, URL: https://warontherocks.com/2019/07/in-search-of-ideas-the-national-security-commission-on-artificial-intelligence-wants-you/ (11.03.2020.)

126. Schwab, K. "*The Fourth Industrial Revolution.*" Encyclopedia Britannica, March 23, 2021. URL: https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734. (21.03.2022.)

127. Senate Select Committee on Intelligence and Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution*, Washington, DC: National Intelligence Council, 2017, str. 2–4. URL: https://permanent.access.gpo.gov/gpo76345/ICA_2017_ 01.pdf (11.11.2020.)

128. Siboni Gabi, *The First Cognitive War*, in Strategic Survey for Israel 2016-2017, eds. Anat Kurz i Shlomo Brom, Institute for National Security Studies, Tel Aviv, 2016, URL: https://www.inss.org.il/publication/first-cognitivewar/.(11.02.2020.)

129. Singer W.P. i Brooking T. Emerson, *LikeWar: The Weaponization of Social Media*, 2018.

130. Sindelar D., *The Kremlin's Troll Army*, The Atlantic, 2014, URL: https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/ (15.02.2021.)

131. Stoica, A., *From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment*, 2020., URL: https://www.researchgate.net/publication/341541149_From_Social_Influence_to_Cyber_Influence_The_Role_of_New_Technologies_in_the_Influence_Operations_Conducted_in_the_Digital_Environment (19.09.2020.)

132. Thomas L.T., *Russia's Reflexive Control Theory and the Military*, Journal of Slavic Military Studies 17, 2004. str. 237–256., URL: https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf (11.03.2020.)

133. Thiele, R., *Artificial Intelligence –A key enabler of hybrid warfare*, Hybrid Center of Excellence, Working Paper 6, 2020. URL: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-6-artificial-intelligence-a-key-enabler-of-hybrid-warfare/ (22.02.2022.)

134. Thiele, R., Schmid, J., *Hybrid Warfare – Orchestrating the Technology Revolution*, The Institute for Strategic, Political, Security and Economic Consultancy, No. 663,2020. URL: https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf (21.02.2022.)

135. The European Centre of Excellence for Countering Hybrid Threats, *The future of cyberspace and hybrid threats*, Hybrid CoE Trend Report 6, 2021. URL: https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210407_Hybrid_CoE_Trend_Report_6_The_future_of_cyberspace_and_hybrid_threats_WEB.pdf (25.03.2022.)

136. Timothy L. T., *Russian Information Warfare Theory: The Consequences of August 2008*, in The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald, Ed. Stephen J. Blank and Richard Weitz, U.S. Army War College, Carlisle, Strategic Studies Institute, 2010., URL: https://www.jstor.org/stable/pdf/resrep12110.8.pdf (17.06.2020.)

137. Tuđman, M., *Suverenitet ili izolacija: skica za istraživanje informacijskih strategija i predodžbenih shema u javnome znanju,* 2007., URL: https://www.researchgate.net/publication/281099563_Suverenitet_ili_izolacija_skica_za_istrazivanje_informacijskih_strategija_i_predodzbenih_shema_u_javnome_znanju/citation/download (28.02.2021.)

138. Tuđman, M., *Informacijsko ratište i informacijska znanost*, Hrvatska sveučilišna naklada, Zagreb, 2008.

139. Tuđman, M., '*Informacijske operacije i mediji ili kako osigurati informacijsku superiornost*', National security and the future, 10(3-4). URL: https://hrcak.srce.hr/80565 (09.12.2021.)

140. Tuđman, M., *Dezinformacija*. Zbornik u čast Petru Strčiću, Povijesno društvo Rijeka. 2012.,str.205-219,URL: https://www.researchgate.net/publication/281626713_Dezinformacija (11.03.2022.)
141. Tuđman, M., *Programiranje istine*, Hrvatska sveučilišna naklada, Zagreb, 2013.
142. Tufecki Z., *We're Building a Dystopia Just to Make People Click on Ads*, Ted Talk, 2017., URL:https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads (05.07.2021.)
143. Underwood K., *Cognitive Warfare Will Be Deciding Factor in Battle*, SIGNAL Magazine, 2015., URL: https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle (05.07.2021.)
144. US DoD, *Information Operations Roadmap*, 2003., URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Information_Operations_Roadmap_30_October_2003.pdf (17.07.2020.)
145. Yanakiev, Y.; Dimov, P.; Bachvarov, D., *Conceptualizing The Role of Societal Resilience In Countering Hybrid Warfare*, Information & Security: An International Journal, 2018, str. 77-89, URL: https://doi.org/10.11610/isij.3907 (23.04.2020.)
146. Youyou, W.; Kosinski, M.; Stillwell, D., *Computer-Based Personality Judgments Are More Accurate Than Those Made By Humans*, Proceedings of the National Academy of Sciences of the United States of America 112, no. 4, 2015, URL: https://www.pnas.org/content/112/4/1036 (27.06.2019.)
147. Van Niekerk, B., Manoj, M., *Social Media and Information Conflict*, International Journal of Communication 7, 2013. str. 1162–1184., URL: https://ijoc.org/index.php/ijoc/article/view/1658, (05.11.2019.)
148. Vilmer, J.-B.J.; Escorcia, A., Guillaume, M., Herrera, J., *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, Paris, 2018., URL: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (18.03.2019.)
149. Vujić, J., *Rat svjetova, Euroazijanizam protiv atlantizma*, Zagreb, 2012.
150. Walker, R., *Combating Strategic Weapons of Influence on Social Media*, Naval Postgraduate School, Homeland Security Digital Library, SAD, 2019. URL: https://www.hsdl.org/?abstract&did=828243 (11.11.2020.)

151. Walker, C., Ludwig, J., *From 'Soft Power' to 'Sharp Power', Rising Authoritarian Influence in the Democratic World*, National Endowment for Democracy, 2017. URL: https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf (13.04.2020.)
152. Walker, C., Kalathil, S., Ludwig, J., *The Cutting Edge of Sharp Power*, Journal of Democracy Volume 31, Number 1, National Endowment for Democracy and Johns Hopkins University Press, 2020. URL: https://www.ned.org/wp-content/uploads/2020/01/Cutting-Edge-Sharp-Power-Walker-Kalathil-Ludwig.pdf (08.09.2020.)
153. Wardle, C., *Fake News: It's Complicated*, First Draft, 2017, URL: https://firstdraftnews.org/fake-news-complicated/ (18.02.2021.)
154. We are Social, 2020., https://wearesocial.com/digital-2022
155. Van der Aalst, W.M.P., *Hybrid Intelligence: to automate or not to automate, that is the question*, International Journal of Information Systems and Project Management, 2021., URL: https://www.sciencesphere.org/ijispm/archive/ijispm-090201.pdf (11.09.2021.)
156. Wither, J., *Making Sense of Hybrid Warfare*. Connections: The Quarterly Journal. 15. 2016, str. 73-87., URL: https://www.researchgate.net/publication/301237833_Making_Sense_of_Hybrid_Warfare (18.05.2021.)
157. Zakon RH o kritičnim infrastrukturama, URL: www.nn.hr (11.08.2021.)

ŽIVOTOPIS AUTORA

Autor je rođen 24. listopada 1977. u Splitu, Hrvatska. Osnovnu školu završio je u Starom Gradu na Hvaru. Srednju školu smjer opća gimnazija upisao je i pohađao u Jelsi na Hvaru. Zbog preseljenja srednju školu istog smjera završio je u Krku na otoku Krku. Prvu godinu studija na Pravnom fakultetu Sveučilišta u Rijeci upisao je u akademskoj godini 1996./1997. Studij prava diplomirao je na Pravnom fakultetu Sveučilišta u Splitu u akademskoj godini 2003./2004. nakon čega je, iste godine, na istom sveučilištu, upisao sveučilišni poslijediplomski studij smjer Pomorsko pravo i međunarodno pravo mora. Godine 2006. zaposlio se u Ministarstvu vanjskih poslova i europskih integracija Republike Hrvatske (danas Ministarstvo vanjskih i europskih poslova). Državni stručni ispit položio je 2007. nakon čega se zapošljava u Ministarstvu unutarnjih poslova RH. Magistrirao je 2012. na temu „Maksimalno širenje granica epikontinentalnih pojaseva Arktičkih država i energetska bogatstva Arktičkog oceana“ čime je iz područja društvenih znanosti stekao akademski naziv magistar pravnih znanosti. U akademskoj godini 2015./2016. upisao je doktorski studij na Odsjeku za informacijske i komunikacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu.

Autor je i koautor znanstvenih radova iz područja informacijskih i komunikacijskih znanosti:

1. Nikola Mlinac, Gordan Akrap, Jadranka Lasić-Lazić: Novi oblici manipuliranja u digitaliziranom prostoru javnog znanja i potreba za uspostavom digitalnog i podatkovnog suvereniteta//National security and the future, Vol. 21, No.3, 2020.
2. Političke i sigurnosne dimenzije korištenja društvenih mreža u suvremenom informacijskom prostoru //National security and the future, Vol.17, No. 3, 2016., str. 31-44.
3. Nikola Mlinac, Dario Malnar, Sigurnosno-obavještajna komponenta zaštite kritične nacionalne energetske infrastrukture Republike Hrvatske, 7. Međunarodna znanstveno-stručna konferencija Dani kriznog upravljanja, Velika Gorica, Hrvatska, Zbornik radova 2014., str.1007. – 1021.