UDK: 004.8: 323.28
Pregledni rad
18. V. 2024.

MARKO BANOŽIĆ*

UTJECAJ UMJETNE INTELIGENCIJE NA RAZVOJ TERORISTIČKIH ODNOSA S JAVNOŠĆU

SAŽETAK

Terorističke organizacije koriste strategije i aktivnosti odnosa s javnošću kako bi doprle do *mainstream* medija, a samim time i do javnosti. Zajednički su ciljevi suvremenoga terorizama i odnosa s javnošću privlačenje pažnje, prenošenje poruka i utjecaj na mišljenje. Vidljivo je da su pojedine terorističke organizacije, posebno Islamska država (IS), bile uspješno prilagođene digitalnomu okružju i stavile su komunikaciju na društvenim mrežama u središte svoje informacijske kampanje. Za koordinaciju svih službenih internetskih računa Islamske države bio je zadužen medijski centar *Al Hayat*. Vodili su ga visokoobrazovani tehnološki i komunikacijski stručnjaci koji su, između ostaloga, programirali aplikaciju *Dawn of Glad Tidings* koja omogućava prijenos informacija od vodstva preko boraca na bojištu pa sve do sljedbenika diljem svijeta. Zatim, *Al Hayat* zadužen je za provođenje *hashtag* kampanja na *Twitteru*. Komunikacijske platforme s omogućenom umjetnom inteligencijom (AI), uglavnom aplikacije za *chat*, moćni su alati za radikalizaciju. Posljednjih godina kroz primjenu umjetne inteligencije *Rocket.Chat* pojavio se kao vrlo pouzdana internetska komunikacijska platforma koju je 2018. godine usvojila Islamska država, a kasnije i Al-Qaeda, namijenjena za širenje propagande putem servera. Osim toga, terorističke organizacije iskorištavaju *deepfake* koji pokreće umjetna inteligencija za širenje propagande i novačenja. Sposobnost terorističkih organizacija da koriste algoritme umjetne inteligencije za procjenu golemih količina podataka najkritičnija je značajka terorizma potpomognuta umjetnom inteligencijom. U radu se na primjerima iz prakse pokazuje u kojoj se mjeri umjetna inteligencija koristi u terorističkim odnosima s javnošću i (protu)terorističkim djelovanjima.

Ključne riječi: terorističke organizacije, odnosi s javnošću, Islamska država, umjetna inteligencija (AI), teroristički odnosi s javnošću

* University of Mostar, Mostar, Bosnia and Herzegovina, markobanozic47@gmail.com

UVOD

Umjetna inteligencija je tijekom prošloga desetljeća doživjela revoluciju. Pojava terorizma potpomognuta umjetnom inteligencijom predstavlja značajan i rastući izazov nacionalnoj sigurnosti. Kako tehnologije umjetne inteligencije nastavljaju napredovati, terorističke organizacije sve više koriste ove alate za poboljšavanje svojih sposobnosti, prilagodbu svojih taktika, tehnika i procedura te propagiranje svojih ideologija. Predmet istraživanja predstavlja uporaba umjetne inteligencije u terorističkim odnosima s javnošću temeljena na primjerima iz prakse. Rezultati istraživanja definirat će ulogu i mjesto umjetne inteligencije u razvoju terorističkih odnosa s javnošću.

Glavna hipoteza:
H1: Umjetna inteligencija postala je novi komunikacijski kanal terorističkih organizacija.
Postavljena glavna hipoteza implicira više **pomoćnih hipoteza**:
H2: Terorističke organizacije imaju tendenciju ranoga usvajanja novih tehnologija iskorištavajući nove alate i platforme za promicanje svojih ciljeva.
H3: Komunikacijske platforme s omogućenom umjetnom inteligencijom, uglavnom aplikacije za *chat*, moćni su alati za teroriste koji žele radikalizirati i novačiti pojedince.
H4: Uporaba algoritama umjetne inteligencije za procjenu golemih količina podataka olakšava terorističkim organizacijama pripremanje terorističkoga akta.
H5: Napredni algoritmi dubinskoga učenja koji stječu sposobnost detaljne analize i oponašanja vizualnoga i slušnoga sadržaja omogućuju terorističkim organizacijama širenje dezinformacija.

U izradi ovoga rada korištene su sljedeće znanstvene metode: komparativno iščitavanje relevantne literature, komparativna analiza prethodnih istraživanja, teorijskih i praktičnih spoznaja o primjeni umjetne inteligencije u terorističkim odnosima s javnošću.

TERORISTIČKI ODNOSI S JAVNOŠĆU

Odnos terorizma i medija najčešće se promatra kao simbiotski odnos koji se, s jedne strane, manifestira interesom terorističkih skupina za što većom prisutnošću u medijima radi postizanja što snažnijih medijskih učinaka, odnosno s druge strane, interesom medija za prenošenjem vijesti koje privlače pozornost javnosti. Teroristički akti oblici su specifičnih poruka kojima je cilj impresionirati određenu javnost ili na nju utjecati. U okviru komunikacije terorizam se koncipira kao nasilan jezik komunikacije. Terorističke organizacije, dosežući globalnu javnost pomoću masovnih medija, pokušavaju povećati svoje sposobnosti, i to publicitetom jer terorizam učinkovitije djeluje komunikacijom učinka nego razornim sadržajem. Teroristi i terorističke organizacije razvili su moderne sustave upravljanja medijima i počeli su koristiti većinu tehnika koje primjenjuju i stručnjaci odnosa s javnošću (Tomić, 2008: 251). Slijedom navedenoga možemo zaključiti da su zajednički ciljevi terorističkih odnosa s javnošću i odnosa s javnošću: privlačenje pažnje, prenošenje poruke i utjecaj na mišljenje.

INFORMACIJSKE KAMPANJE TERORISTIČKIH ORGANIZACIJA

Kada pišemo o informacijskim kampanjama terorističkih organizacija, bitno je istaknuti da je Hamas prva islamistička skupina koja je svoje ciljeve i ideologiju stavila na uvid široj javnosti objavljivanjem *Povelje* s 36 članaka 1998. godine. Kroz *Povelju* vješto se provlači temeljna poruka da je oslobađanje Palestine vjerska dužnost. Teroristička organizacija Hezbollah 2009. godine javnosti predstavlja *Manifest* koji obiluje protuameričkim porukama, dok Al-Qaeda 2010. godine pokreće časopis *Inspire* kojemu su ciljna skupina predani muslimanski vjernici, ali i nezadovoljnici te marginalizirane društvene skupine. U *Inspireu* važno mjesto imaju članci u kojima se objašnjavaju tehnike pravljenja eksploziva te se čitatelji potiču na vršenje terorističkih akata. No, od svih terorističkih organizacija Islamska država (IS) najuspješnije se prilagodila digitalnomu

okružju i stavila je komunikaciju na društvenim mrežama u središte svoje informacijske kampanje. Za koordinaciju svih službenih internetskih računa radikalnih islamista zadužen je medijski centar *Al Hayat*. Vode ga visokoobrazovani tehnološki i komunikacijski stručnjaci koji su, između ostaloga, programirali aplikaciju *Dawn of Glad Tidings* koja omogućava prijenos informacija od vodstva preko boraca na bojištu pa sve do sljedbenika diljem svijeta. Zatim, *Al Hayat* zadužen je za provođenje *hashtag* kampanja na *Twitteru*. Povrh toga, političkom satirom i internetskim izrugivanjem Zapadu džihadisti utječu na percepciju džihada kao *cool* pokreta te se zbližavaju s mladim i nezadovoljnim sljedbenicima diljem svijeta. Zadatak medijskoga centra *Al Hayat* kao i komunikacijskih stručnjaka jest stvaranje pozitivne slike o IS-u u medijima (kao organizaciji koja ispravlja nepravdu učinjenu prema muslimanima diljem svijeta) i na taj način privlačenje što većega broja sljedbenika i simpatizera. Za razliku od talibana koji su odbacili sve tehnološko, propaganda Islamske države jest *high-tech* operacija koju vode profesionalci, uključujući neke visokoobrazovane stručnjake sa Zapada. Kada su *Twitter* i *Facebook* preuzeli IS-ov video o odrubljivanju glave Jamesa Foleyja, unutar samo nekoliko sati tim za propagandu obnovio mu je pristup kroz mrežne stranice locirane u dijaspori. Jedan je od najuspješnijih pothvata IS-a aplikacija za *Twitter* na arapskome jeziku, nazvana *Zora radosnih vijesti* ili samo *Zora*. Aplikaciju, službeni proizvod IS-a, promovirali su njezini najveći korisnici reklamirajući je kao način da se održi korak s najnovijim vijestima o džihadističkoj skupini. Zatim je Islamska država tijekom Svjetskoga nogometnog prvenstva 2014. godine koristila *hashtagove* kao #Brazil2014, #ENG, #France i #WC2014. Ova taktika omogućila im je da dopru do milijuna pretraživanja na *Twitteru* u vezi sa Svjetskim prvenstvom, u nadi da će neki od čitatelja kliknuti na linkove s njihovih propagandnih materijala, posebno na video u kojemu britanski i australski džihadisti pokušavaju nagovoriti druge zapadnjačke muslimane da se pridruže njihovim redovima (Napoleoni, 2015: 76-77). Prema nekim podatcima, samo unutar IS-a početkom 2015. godine bilo je oko 25 000 registriranih *Twitter* adresa s kojih se tjedno, u prosjeku, slalo oko 200 000 poruka. Takva je komunikacija između fronte i populacijske baze pogodne za radikalizaciju i vrbovanje bez presedana u povijesti. Zbog toga većina sigurnosnih agencija još uvijek nije ni tehnološki ni stručno osposobljena pratiti i analizirati ovaj proces (Azinović, Jusić, 2015: 49-50).

KOMUNIKACIJSKI KANALI TERORISTIČKIH ORGANIZACIJA

Internet – globalna mreža danas je najvažniji komunikacijski kanal terorističkih organizacija. Svjesne snage medija terorističke organizacije često vode i medijske kampanje. Prva internetska prijetnja zabilježena je 1999. godine kada su uredi za odnose s javnošću dvadesetak zemalja svijeta dobili elektroničku poruku koju je potpisala skupina časnika ruske raketne postrojbe, smještene u Kaluškoj oblasti, naoružane nuklearnim strateškim raketama. Primatelji poruke obaviješteni su da će časnici nezadovoljni svojim siromaštvom raketirati važne industrijske i vojne objekte zapadnih zemalja ako im njihove vlade ne isplate veliku svotu novca (Cyganov, 2004: 24). Edna Reid, Jialun Qin i Yilu Zhou u studiji *Collecting and Analyzing the Presence of Terrorist on the Web* detektiraju karakteristike interneta koje omogućavaju njegovu pogodnu instrumentalizaciju u ostvarivanju terorističkih ciljeva:

1. anonimnost komuniciranja
2. lak i jednostavan pristup
3. mala ili nepostojeća regulacija, cenzura ili neki drugi oblik vladavine kontrole
4. potencijalno ogromna publika koju predstavlja čitava svjetska populacija
5. brz protok informacija
6. gotovo nepostojeći troškovi održavanja i razvoja stranica i drugih oblika internetskih medija
7. multimedijalno okružje (mogućnost kombinacije teksta, slike, zvuka i videa, preuzimanje filmova, pjesama, knjiga, plakata i sl.)
8. mogućnost utjecanja na obilovanje izvještavanja klasičnih medija koji sve više koriste internet kao izvor svojih informacija (Reid, Zhou, 2005: 402-411).

Tonći Prodan, autor znanstvenoga članka *Internet, terorizam, protuterorizam*, objavljenoga u časopisu *Nacionalna sigurnost i budućnost* 2015. godine razlikuje *online* i *offline* (klasičnu, dosadašnju) radikalizaciju. Prema njemu, internet umreženim zainteresiranim pojedincima omogućava sljedeće:

1. informacije o izradi bombi, džihadistima, salafističkim publikacijama, Islamskoj državi, videouratke odrubljivanja glava i slično, omogućavajući im tako bržu i lakšu radikalizaciju, ali i pripremu za provođenje terorističkih napada bez uobičajene infrastrukture terorističke grupe
2. puno lakšu komunikaciju među ciljanim pojedincima i pronalazak istomišljenika diljem svijeta (Prodan, 2015: 16).

U zadnjih desetak i više godina značajan broj ljudi pridružio se džihadu upravo zbog snimki pogubljenja, konkretno dekapitacija. Zadnji primjer potkrepljuje navedene teze da se radi o „dobroj" propagandi, a dolazi s uhićenjima pripadnika raznih terorističkih ćelija u Europi i SAD-u. Snimke odrubljivanja glava nađene su u domovima gotovo svih uhićenih (Prodan, 2015: 117). Neke su terorističke grupe dizajnirale specijalne mrežne stranice za mlađu publiku, a propagandne poruke prenose se preko crtanih filmova i videoigara. Teroristi internetskim putem često upućuju i prijetnje te siju strah među populacijom. Takve prijetnje primio je i suosnivač *Twittera* Jack Dorsey, navodno zbog blokiranja korisničkih računa terorista i širenja njihove propagande. „Vaš virtualni rat prema nama izazvat će pravi, krvavi rat prema vama!" – prijetnja je upućena Jacku. Hamas je osmislio igricu naziva *The Conqueror* (osvajač). Ažurira se svakoga tjedna i dizajnirana je za djecu dok je Hezbollah razvio igru *Specijalne snage 1 i 2* koje emitiraju vojne misije protiv izraelske vojske. Na internetu su teroristi postavili i igricu *Noć Bushova uhićenja*, a cilj je uhićenje i ubijanje Busha, bivšega predsjednika SAD-a. Bitno je istaknuti ogroman broj korisnika raznih internetskih stranica u svijetu te je ovaj vid komunikacije, propagande i zastrašivanja iznimno bitan za terorističke organizacije. Pojavom interneta, a posebno WWW-a 1995. godine, informacija postaje doktrinarna kategorija te strateško sredstvo u izvršavanju postavljenih ciljeva i zadaća, posebno kroz nove teorije sukoba niskoga intenziteta, odnosno odvraćanja i sprječavanja eskaliranja kriznih situacija u ratna stanja, ali i stvaranja i upravljanja, namjerno izazvanim lokalnim krizama. Sukobi niskoga intenziteta u biti su borbe za ljudski um, a u toj su borbi psihološke operacije znatno važnije od vatrene moći (Akrap, 2011: 4).

Televizija – zbog svoga učinka slike i tona teroristi različitim kanalima sve više dostavljaju materijale TV postajama u uvjerenju da će se njihova poruka prenijeti domaćoj i međunarodnoj javnosti. Za globalni terorizam posebno značenje imaju satelitske televizijske postaje i programi. Većina islamističkih skupina, uključujući i Al-Qaedu, na Bliskome istoku služi se dostupnim kanalima prema katarskoj televiziji *Al Jazeeri*. Druga važna televizijska postaja na ovome dijelu svijeta jest *Al Arabiya* sa sjedištem u Dubaiju. Američki ministar obrane Donald Ramsfeld izjavio je da su *Al Jazeera* i *Al Arabiya* najpopularnije televizijske stanice u Iraku i one se žestoko protive koalicijskim snagama. Da bi neutralizirao utjecaj televizija koje su redovito objavljivale poruke Sadama Huseina i Osame bin Ladena, američki ministar obrane najavio je početak emitiranja američkoga satelitskog programa u Iraku. Nakon terorističkoga napada Melvida Jašarevića na Veleposlanstvo SAD-a u Bosni i Hercegovini i na domaćoj *Federalnoj televiziji* dogodila se ekskluzivna objava videoporuke terorista. Al-Qaeda, talibani i somalski Al-Shabab razvili su medijske produkcijske kuće da bi poslali svoje internetske poruke visoko standardizirane proizvodnje. Tri su glavne terorističke medijske organizacije: *Al-Sahab (the Clouds)*, *Global Islamic Media Front (GIMF)* i *Al Fajr*. U tim medijskim kućama sadržaji se prevode na engleski, njemački i francuski, a snimke su iznimno kvalitetne (Prodan, 2015: 119).

Agencije – zbog svoje tehničke organizacije i načina rada novinske agencije također su postale dobar kanal distribucije informacija terorističkih organizacija. Posebno su teroristima zanimljive velike svjetske agencije koje servisiraju sve važnije globalne i nacionalne medijske kuće. Među nji-

ma najzanimljiviji su *AP*, *Reuters*, *AFP* i dr.
Tisak – terorističke skupine uspješno razvijaju sustav upravljanja medijima i postupno počinju koristiti sofisticirane tehnike komuniciranja. Poznato je da je Irska Republikanska Armija (IRA) tiskala i svoje novine *An Phoblacht*, a IS redovno je tiskala svoje magazine *Rumiyah* i *Dabiq*. Pored navedenih, teroristi često upućuju poruke i pomoću londonskoga ureda arapskoga lista *Al-Quds* i londonskoga lista *Ashharq Al-Awsat*.

Tu su i drugi kanali poput kurira, telefona, *face to face* komunikacije, e-adrese, faks poruke, videosnimke, SIM kartice za mobilne telefone, USB vanjske memorije, teklića, dostavljača, satelitskoga telefon, komunikacije šifriranim porukama elektroničke pošte i SMS tekstualnim porukama (Prodan, 2015: 124).

Teroristi se čak služe i kodiranjem podataka u okviru grafičkih ili zvučnih *fileova* ne narušavajući njihovu strukturu, pa čak ne mijenjajući ni njihovu dužinu. Tako kodirane informacije može pročitati samo onaj tko zna da takav file nosi informaciju i posjeduje odgovarajući ključ. *Mrtve javke* u današnjemu digitalnom vremenu predstavljaju način na koji jedna osoba šalje drugoj osobi poruke preko interneta, ali ne pritiskujući tipku „pošalji" (engl. *send*). Primatelju poruke dostupni su podatci za prijavljivanje na internet na račun pošiljatelja, tako da može vidjeti poruku. Profesori iz BiH Vlado Azinović i Muhamed Jusić u istraživačkome radu pod nazivom *Novi zov rata u Siriji i bosanskohercegovački kontingent stranih boraca* došli su do saznanja da je *face to face* komunikacija na prvome mjestu načina radikalizacije bosanskohercegovačkih građana dok internet te već uspostavljene veze održava. Proces radikalizacije i vrbovanja obično se odvija u privatnosti domova i u alternativnim strukturama u kojima se obavlja vjerska aktivnost bez znanja i odobrenja Islamske zajednice u Bosni i Hercegovini. Neke od ovih ilegalnih ili paralelnih mikrozajednica (paradžemata ili paramesdžida) smatraju se središtima ideološke radikalizacije i vrbovanja za iseljenja u Siriju i Irak (Azinović, Jusić, 2015: 13).

UMJETNA INTELIGENCIJA I SUVREMENI TERORIZAM

Otac računarstva John Von Neumann (1903. – 1957.) izjavio je da računala nikada neće dosegnuti ni jednu osobinu inteligencije. Nije trebalo dugo da Neumann shvati da je pogriješio. Već tridesetih godina 20. stoljeća pojavljuju se složeniji elektromehanički strojevi za automatsku obradu podataka koji se smatraju pretečom umjetne inteligencije, a njezin pravi početak nastao je na znanstvenoj konferenciji *Dartmounth* u američkome Hanoveru 1956. godine. Autor pojma John McCarthy opisao je umjetnu inteligenciju kao znanstvenu disciplinu koja se bavi osmišljavanjem „računalnih sustava čije se ponašanje može tumačiti kao inteligentno" (Prister, 2019: 71). U akademskim krugovima koristi se još niz definicija umjetne inteligencije (engl. *artificial intelligence* – AI) s nastojanjem da obuhvate sva istraživanja vezana za problematiku prenošenja svojstava biološke inteligencije stroju, prije svega računalu, s ciljem da tada takvo računalo može rješavati probleme i kompleksne zadatke, koje najčešće nazivamo problemski zadatci, koje klasični programi ne mogu riješiti ili mogu riješiti, ali uz velike napore poput dugoga vremena trajanja izvođenja programa te velikih troškova za pisanje i implementiranje programa (Stipaničev, Šerić, Braović, 2021: 13). Alan Mathison Turing, britanski matematičar, kriptograf i računalni teoretičar, objavio je 1950. godine provokativan članak koji je i do danas ostao predmetom žučnih stručnih rasprava i polemika. Naime, on u članku *Računalni strojevi i inteligencija* izravno navodi: „Predlažem da razmotrimo pitanje: 'Mogu li strojevi misliti?'" (Prister, 2019: 69). Primjena umjetne inteligencije u odnosima s javnošću moguća je kao i u drugim područjima društvene zbilje prvenstveno zato što ona može pomoći preciznije, brže i lakše ciljati stratešku javnost i postići veću interaktivnost i pozornost medija. Praktičarima u odnosima s javnošću umjetna inteligencija pomaže pretvoriti govor u tekst, prevesti audiodatoteke i tekstualne datoteke na više jezika, pratiti autentičnosti videozapisa, analizu sentimenta, stvaranje sadržaja putem alata za pisanje, što sve skupa čini odnose s javnošću učinkovitijim (Tomić,

Volarić, Obradović, 2022: 9). Pojava terorizma potpomognuta umjetnom inteligencijom predstavlja značajan i rastući izazov nacionalnoj sigurnosti. Kako tehnologije umjetne inteligencije nastavljaju napredovati, terorističke organizacije sve više koriste ove alate za poboljšavanje svojih sposobnosti, prilagodbu svojih taktika, tehnika i procedura i propagiranje svojih ideologija. Sposobnost terorističkih organizacija da koriste algoritme umjetne inteligencije za procjenu golemih količina podataka predstavlja opasnost za izvršenje terorističkoga napada identificiranjem mogućih ciljeva.

UMJETNA INTELIGENCIJA KAO NOVI KOMUNIKACIJSKI KANAL TERORISTIČKIH ORGANIZACIJA

Na primjeru Islamske države vidjeli smo da terorističke organizacije imaju tendenciju ranoga usvajanja novih tehnologija iskorištavajući nove alate i platforme za promicanje svojih ciljeva. Za svoje potrebe koriste se svim funkcijama masovnih medija, što je dokaz da su prepoznale važnost i ulogu masovnih medija u suvremenome društvu te da modele i tehnike komuniciranja uključuju u strategije svoga djelovanja radi postizanja što većega utjecaja na učinke koje masovno komuniciranje ima na društvo u cjelini. U posljednjemu desetljeću umjetna inteligencija doživjela je revoluciju i njezine su prednosti terorističke organizacije objeručke prihvatile. U nastavku rada predstavit će se alati umjetne inteligencije koji se koriste u terorističkim djelovanjima.

Deepfake i dezinformiranje

Deepfake stvara i manipulira video, audio ili slike proizvedene metodama dubokoga učenja i tehnike koje se čine stvarnima. *Lip-sync*, *puppetmaster* i *face swap* neke su od tehnika koje se koriste za sintetički video, sliku i govor generacija (Ahmad, Ali, Ahahzad, 2022: 807). Terorističke organizacije koriste *deepfake* koji pokreće umjetna inteligencija i tehnike generiranja sadržaja za širenje propagande, novačenja i širenja dezinformacija. *Deepfakeovi* prvenstveno se stvaraju naprednim algoritmima dubinskoga učenja te navedeni algoritmi stječu sposobnost detaljne analize i oponašanja vizualnoga i slušnoga sadržaja, čime se omogućuje stvaranje zapanjujuće realističnih krivotvorina. Priroda dezinformacija u svojoj se biti kroz povijest nije naročito mijenjala. Dezinformacija je bila i ostala sredstvo manipulacije koje je, s obzirom na dostupne kanale komuniciranja, korišteno u svrhu pokoravanja, nanošenja štete ili ostvarivanja drugih interesa manipulatora. Pojavom društvenih mreža nestao je monopol nad masovnim komuniciranjem. Kanali masovnoga komuniciranja dostupni su pojedincu, skupinama, organizacijama i to bez regulacije kakva je izgrađena u demokratskim društvima u odnosu na klasične masmedije. Ono što danas dezinformacijski proces stavlja u prvi plan jest dostupnost kanala diseminacije, njihova preciznost i učinkovitost, naročito kroz društvene mreže (Popovac, 2020: 73). Širenjem dezinformacija i izmišljenoga vizualnog sadržaja terorističke organizacije imaju za cilj poticanje radikalizacije među ciljanom publikom. Godine 2022. ukrajinska televizijska novinska kuća *Ukrajiana 24* tvrdila je da su njezin prijenos uživo i mrežna stranica bili hakirani, a tijekom hakiranja prikazan je kiron koji lažno navodi da se Ukrajina predala. Osim toga, internetom je kružila lažna snimka ukrajinskoga predsjednika Zelenskoga, u kojoj on naizgled poziva Ukrajince da se predaju (https://nypost.com/2022/03/17/deepfake-video-shows-volodymyr-zelensky-telling-ukrainians-to-surrender/, 4. 11. 2023. godine). Ti scenariji pokazuju kako tehnologija *deepfakes* može širiti dezinformacije i izazvati zabunu tijekom oružanih ratova ili geopolitičkih kriza. Napretkom ove tehnologije *audio-deepfakeovi* također su postali značajan izazov. Teroristi mogu oponašati glasove legitimnih osoba koristeći tehnologiju sinteze govora, također poznatu kao *TEXT TO SPEECH*. Kreatori mogu utjecati na ljude i prevariti ih sa zlom namjerom stvaranja uvjerljivih audioporuka koje zvuče poput glasa žrtve. Dubinu komunikacijske krize koja je vrhunac doživjela inflacijom lažnih vijesti prepoznala je i Europska komisija koja naglašava važnost samoregulacije. Istodobno, tehnološki divovi i digitalne platforme poku-

šavaju dati svoj doprinos u razvoju automatiziranih (*fact-check*) sustava vođenih umjetnom inteligencijom, koji bi trebali olakšati novinarima, urednicima, ali i korisnicima prepoznavanje društveno štetnih komunikacijskih formi (Grmuša, Prelog, 2020: 62).

Platforme za *chat* s umjetnom inteligencijom

Komunikacijske platforme s omogućenom umjetnom inteligencijom, uglavnom aplikacije za *chat*, imaju potencijal biti moćni alati za teroriste koji žele radikalizirati i novačiti pojedince. Koristeći algoritme umjetne inteligencije, ove platforme mogu poslati prilagođenu poruku koja zadovoljava interese i ranjivosti potencijalnih novaka. Automatizirani i ustrajni angažman putem *CHATBOTA* može potaknuti osjećaj pripadnosti unutar ekstremističkih mreža. Prednosti korištenja *chatbota* za terorističke skupine jesu: anonimnost, višejezična sposobnost i, samim time, doseg globalne publike. *Rocket.chat* vrlo je pouzdana internetska komunikacijska platforma koju je usvojila Islamska država u prosincu 2018. godine, a kasnije i Al-Qaida. Ova platforma olakšava šifrirane razgovore između terorističkih skupina i njihovih pristaša, omogućujući širenje propagande putem servera.

Dronovi

Korištenje bespilotnih letjelica moguće je promatrati s različitih sigurnosnih aspekata. Potencijalna sigurnosna ugroza može biti nenamjerna – primjerice uslijed nestručna i nepažljiva rukovanja bespilotnom letjelicom – te namjerna kada korisnik bespilotnu letjelicu koristi s izravnom namjerom počinjenja kaznenoga djela kao što je, primjerice, napad na određenu štićenu osobu ili teroristički napad (Gržin, Marić, 2018: 147). Razvoj bespilotnih letjelica pružio je terorističkim organizacijama novi alat za vođenje asimetričnoga rata. Prednosti su dronova:

1. omogućavanje izviđanja, nadzora i prikupljanja informacija
2. mogu se naoružati
3. obilaženje tradicionalnih sigurnosnih mjera i pokretanje napada iz neočekivanih kutova
4. mali resursi.

Hezbollah, militantna organizacija koja podržava Iran, poznata je po širokoj upotrebi bespilotnih letjelica. Njihov program bespilotnih letjelica s vremenom je rastao te sada imaju flotu bespilotnih letjelica, koja se sastoji od bespilotnih letjelica iranske proizvodnje, primjerice Ababil i Mirsad 1, kao i vlastitih vrsta. HAMAS je palestinska militantna organizacija koja ima dugogodišnju stratešku suradnju s Hezbolahom i Iranom, koja se proširila na područje tehnologije. Godine 2021. Hamas je objavio video samoubilačke letjelice *SHEHAB* koja nosi streljivo s ugrađenim bojevim glavama. No, Izraelska obrambena služba tvrdila je da njihov sustav *Iron Dome Rocker Defense* (IDRD) uspješno presreće veliku većinu nadolazećih raketa koje predstavljaju prijetnju izraelskim gradovima. Po sličnim obrascima Islamska država počela je koristiti bespilotne letjelice 2013. godine. Tehnologija rojevih bespilotnih letjelica, nekad prikazivana kao znanstvena fantastika, sada je surova stvarnost koja bi mogla promijeniti lice ratovanja. Rojevi napada dronova mogu dovesti do masovnih žrtava i razaranja širokih razmjera. Početkom 2018. godine dogodio se prvi napad bespilotnih letjelica u povijesti na ruske snage stacionirane u Siriji. Roj od 13 bespilotnih letjelica natovarenih bombama napao je ruske snage, sedam dronova presrela je i uništila ruska obrana, dok je preostalih šest uspješno prizemljeno. Iako nije bilo žrtava niti značajne štete, incident je skrenuo pozornost na potencijalnu prijetnju koju predstavljaju rojevi dronova u rukama nedržavnih aktera.

UMJETNA INTELIGENCIJA I PROTUTERORISTIČKO DJELOVANJE

Umjetna inteligencija potrebna je u odgovoru na terorizam jer su količina i raznolikost informacija potrebnih za rješavanje terorizma previše složene i raznolike da bi ih obradio i analizirao ljudski um bez pomoći. Neki su od alata umjetne inteligencije koji se koriste u suvremenom svijetu:

a) **SKYNET** američke Agencije za nacionalnu sigurnost 2015. godine odnosi se na prikupljanje podataka putem algoritma strojnoga učenja pakistanske mobilne mreže koja je sadržavala 55 milijuna korisnika u svrhu predviđanja potencijalnih terorista.
b) **RADAR-iTE** – njemački savezni policijski ured uvodi nacionalni alat za procjenu rizika od terorizma koji uključuje prisluškivanje unutar i izvan domova, nadzor telekomunikacija, elektronički nadzor prebivališta ili preventivni pritvor.
c) **DEXTER** – NATO je razvio prototip tehnologije za suzbijanje prijetnji od vatrenoga oružja i eksploziva u masovnim javnim prostorima poput podzemnih željeznica, zračnih luka i dr. Sustav identificira pojedince koje nose oružje i eksploziv među pješacima.
d) **MediFor i SemaFor –** Agencija za napredne obrambene istraživačke projekte (DARPA) uložila je velika sredstva u tehnologije detekcije kroz dva preklapajuća programa: medijska forenzika (MediFor) i semantička forenzika (SemaFor), čiji je cilj pomoću algoritama osmišljavati napredne tehnologije za otkrivanje lažnih medija, slika i videozapisa.

Kina i Indija su, primjerice, kriminalizirale korištenje *deepfakea* u kriminalne svrhe. Između ostaloga, u protuterorističke svrhe koriste se i nadzorne kamere vođene umjetnom inteligencijom.

ZAKLJUČAK

Predviđanje budućih zločina država diljem svijeta smatra se ključnim sredstvom za učinkovitu prevenciju terorizma. Korištenje umjetne inteligencije za predviđanje terorizma dio je prelaska s reaktivnoga na preventivni pristup borbi protiv terorizma. Komparativnim iščitavanjem relevantne literature, komparativnom analizom prethodnih istraživanja, teorijskih i praktičnih spoznaja o primjeni umjetne inteligencije u terorističkim odnosima s javnošću potvrđene su postavljene hipoteze. Na primjeru prilagodbe Islamske države digitalnomu okružju i postavljanjem komunikacije na društvenim mrežama u središte svoje informacijske kampanje potvrđena je prva pomoćna hipoteza (H2) koja glasi da terorističke organizacije imaju tendenciju ranoga usvajanja novih tehnologija iskorištavajući nove alate i platforme za promicanje svojih ciljeva. Druga pomoćna hipoteza (H3), koja glasi da su komunikacijske platforme s omogućenom umjetnom inteligencijom uglavnom aplikacije za *chat*, moćni alati za teroriste koji žele radikalizirati i novačiti pojedince, potvrđuje se činjenicom da terorističkim organizacijama ovakve platforme omogućuju anonimnost, višejezičnu sposobnost i, samim time, doseg globalne publike. Treća pomoćna hipoteza (H4), koja glasi da uporaba algoritama umjetne inteligencije za procjenu golemih količina podataka olakšava terorističkim organizacijama pripremanje terorističkoga akta, potvrđuje se spoznajom da grane umjetne inteligencije strojno i duboko učenje omogućuju filtar i selekciju ogromnih količina podataka u znatno kraćemu vremenu, čime je terorističkim organizacijama olakšana priprema terorističkoga akta. Korištenje *deepfakea* u svrhu širenja dezinformacija u potpunosti potvrđuje četvrtu pomoćnu hipotezu (H5), da napredni algoritmi dubinskoga učenja koji stječu sposobnost detaljne analize i oponašanja vizualnoga i slušnoga sadržaja omogućuju terorističkim organizacijama širenje dezinformacija. Korištenje alata umjetne inteligencije, primjerice *deepfake*, *Tex To Speech*, *AI chatbot*, *Rocket.chat*, bespilotnih zračnih sustava, tzv. dronova u terorističke svrhe, u potpunosti potvrđuje glavnu hipotezu (H1), da je umjetna inteligencija postala novi komunikacijski kanal terorističkih organizacija. Ostvarivanje zajedničkih ciljeva terorističkih odnosa s javnošću i odnosa s javnošću promatrani kroz privlačenje pažnje, prenošenje poruka i utjecaj na mišljenje definitivno se primjenjuju i putem alata umjetne inteligencije. Ono najbitnije što razdvaja terorističke odnose s javnošću i odnose s javnošću jest društvena odgovornost praktičara i društvena korisnost cilja. U budućnosti ćemo svjedočiti svojevrsnoj utrci terorističkih organizacija i sigurnosnih agencija u primjeni umjetne inteligencije u terorističke svrhe, odnosno definiranju zakonodavstva koje bi spriječilo ili barem ublažilo takve devijacije te implementiralo alate umjetne inteligencije u svrhu unapređenja sigurnosti.

LITERATURA

Ahmad, W., Ali, I. (2022) „ResVit: A Framework for Feepfake Videos Detection“, in: *International journal of electrical an computer engineering systems*, 13, 9, Josip Juraj Strossmayer University of Osijek.

Akrap, G. (2011) *Specijalni rat 1*, Večernji list, Zagreb.

Azinović, V., Jusić, M. (2015) *Zov rata u Siriji i bosanskohercegovački kontigent stranih boraca, Atlantska inicijativa*, Sarajevo.

Cyganov, V. (2004) „Media-terorizm”, in: *Terorizm i sredstva massovnoj informaciyi*, Nika-Centr, Kijev.

Grmuša, M., Prelog, L. (2020) „Uloga novih tehnologija u borbi protiv lažnih vijesti – iskustva i izazovi hrvatskih medijskih organizacija“, *Medijske studije*, 11, 22, Zagreb.

Gržin, M., Marić, A. (2018) „Pravna regulacija bespilotnih letjelica i mjere sprječavanja zlouporabe u Republici Hrvatskoj s policijskog aspekta”, *Policija i sigurnost*, 27, 1, Zagreb.

Miller, J. R. (2022) Deepfake video of Zelensky telling Ukrainians to surrender removed from social platforms, New York Post, https://nypost.com/2022/03/17/deepfake-video-shows-volodymyr-zelensky-telling-ukrainians-to-surrender/ (4. 11. 2023.).

Popovac, J. (2020) „Dezinformacije u digitalnom dobu: Borba za istinu”, *Medijska istraživanja*, Zagreb.

Prister, V. (2019) „Umjetna inteligencija”, *Media, Culture and Public Relations*, 10, 1, Zagreb.

Prodan, T. (2015) *Internet, terorizam, protuterorizam*, Nacionalna sigurnost i budućnost, Zagreb.

Reid, E., Qin, J., Zhou, Y. (2005) *Collecting and Analyzing the Presence of Terrorist on the Web,* Intelligence Security Informatics, International Conference, Atlanta.

Stipaničev, D., Šerić, Lj., Braović, M. (2021) *Uvod u umjetnu inteligenciju*, Fakultet elektrotehnike, strojarstva I brodogradnje, Split.

Tomić, Z. (2016) *Odnosi s javnošću*, Teorija i praksa, Zagreb, Sarajevo – Synopsis.

Tomić, Z., Volarić, T., Obradović, Đ. (2022) „Umjetna inteligencija u odnosima s javnošću“, *South Eastern European Journal of Communication*, Sveučilište u Mostaru, 4, 2, Mostar.

THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON THE DEVELOPMENT OF TERRORIST PUBLIC RELATIONS

ABSTRACT

Terrorist organizations use public relations strategies and activities to reach the mainstream media and thus the public. The common goals of contemporary terrorism and public relations are to attract attention, convey messages and influence opinion. It is evident that some terrorist organizations, especially the Islamic State (IS), have been successfully adapted to the digital environment and have placed communication on social networks at the center of their information campaign. The Al Hayat media center was in charge of coordinating all the official Internet accounts of the Islamic State. It was led by highly educated technological and communication experts, who, among other things, programmed the "Dawn of Glad Tidings" application, which enables the transmission of information from the leadership through the fighters on the battlefield to followers all over the world. Next, Al Hayat is in charge of conducting hashtag campaigns on Twitter. Artificial intelligence (AI)-enabled communication platforms, mainly chat apps, are powerful tools for radicalization. In recent years, through the application of artificial intelligence (AI), "Rocket.Chat" has emerged as a very reliable online communication platform adopted by the Islamic State in 2018, and later by Al-Qaeda, intended for spreading propaganda through servers. In addition, terrorist organizations exploit deepfakes powered by artificial intelligence to spread propaganda and recruitment. The ability of terrorist organizations to use AI algorithms to assess vast amounts of data is the most critical feature of AI-assisted terrorism. The paper shows examples from practice to what extent artificial intelligence is used in terrorist relations with the public and (counter)terrorist activities.

Keywords: terrorist organizations, public relations, Islamic State, artificial intelligence (AI), terrorist public relations.