Integracija umjetne inteligencije u sustave nacionalne sigurnosti: perspektive, izazovi i primjene u prevenciji terorizma

Bešlić, Matea

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department of Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:914417

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

INTEGRACIJA UMJETNE INTELIGENCIJE U SUSTAVE NACIONALNE SIGURNOSTI: PERSPEKTIVE, IZAZOVI I PRIMJENE U PREVENCIJI TERORIZMA

MATEA BEŠLIĆ

Split, rujan 2024.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

INTEGRACIJA UMJETNE INTELIGENCIJE U SUSTAVE NACIONALNE SIGURNOSTI: PERSPEKTIVE, IZAZOVI I PRIMJENE U PREVENCIJI TERORIZMA

MENTOR: doc. dr. sc. Tonći Prodan

KOMENTOR: izv. prof. dr. sc. Toni Perković

MATEA BEŠLIĆ

Matični broj studenta:

843/2022.

Split, rujan 2024.

Rad je izrađen u Sveučilišnom odjelu za forenzične znanosti Sveučilišta u Splitu pod nadzorom mentora doc. dr. sc. Tonćija Prodana i komentora izv. prof. dr. sc. Tonija Perkovića u razdoblju od svibnja do kolovoza 2024. godine.

Datum predaje diplomskog rada: 01. rujna 2024.

Datum prihvaćanja rada: 17. rujna 2024.

Datum usmenog polaganja: 23. rujna 2024.

Povjerenstvo: 1. prof. dr. sc. Josip Kasum

2. dr. sc. Marko Pilić

3. doc. dr. sc. Tonći Prodan

SADRŽAJ

1. UVOD

Suvremeni svijet suočen je s nizom sigurnosnih izazova koji su postali neizostavni dio svakodnevnog života, a jedan od najznačajnijih među njima je terorizam. Terorističke organizacije kontinuirano evoluiraju, koristeći nove tehnologije i taktike kako bi proširile svoj utjecaj i prijetile globalnoj sigurnosti. Globalizacija i napredak u komunikacijskim tehnologijama omogućili su terorističkim grupama operiranje nevjerojatnom brzinom i učinkovitošću, često ostajući korak ispred tradicionalnih sigurnosnih mehanizama. U tom kontekstu, države su primorane razvijati i prilagođavati svoje sigurnosne strategije kako bi mogle odgovoriti na ove kompleksne prijetnje.

Jedna od najvažnijih inovacija koja se pojavila u posljednjih nekoliko desetljeća je umjetna inteligencija (engl. *Artificial Intelligence* - UI), koja predstavlja ključni alat u unapređenju nacionalnih sigurnosnih sustava i sprječavanju terorističkih aktivnosti. Umjetna inteligencija, koja se definira kao sposobnost strojeva da oponašaju ljudske kognitivne funkcije poput učenja, zaključivanja i donošenja odluka, brzo se razvila od teorijskog koncepta do praktične primjene u raznim sektorima, uključujući nacionalnu sigurnost. Njezina primjena u sigurnosnim sustavima omogućava analizu velikih količina podataka, prepoznavanje obrazaca u ponašanju pojedinaca i grupa te predviđanje potencijalnih prijetnji na način koji je izvan dosega tradicionalnih metoda.

Napredni UI sustavi pružaju sigurnosnim agencijama mogućnost proaktivnog djelovanja, sprječavajući terorističke napade prije nego što se dogode. Primjerice, korištenjem umjetne inteligencije za analizu društvenih mreža, sigurnosne agencije mogu identificirati potencijalno radikalizirane pojedince i skupine te pravovremeno intervenirati. Međutim, integracija umjetne inteligencije u sustave nacionalne sigurnosti donosi i niz izazova koji ne mogu biti zanemareni. Etika i privatnost postaju ključne teme kada se radi o korištenju umjetne inteligencije u analizi podataka, jer prikupljanje i obrada osjetljivih informacija može dovesti do zloupotrebe i narušavanja ljudskih prava.

2. CILJ RADA

Kako bi se istražila uloga umjetne inteligencije (UI) u suvremenim sigurnosnim sustavima, s posebnim naglaskom na prevenciju terorizma, ovaj rad postavlja nekoliko ključnih ciljeva. Fokus je na procjeni tehnologija koje omogućuju primjenu UI u sustavima nacionalne sigurnosti, uz isticanje njihovih prednosti i potencijalnih rizika.

Ciljevi ovog rada su:

1. Identificirati i analizirati ključne tehnologije umjetne inteligencije: Pregledati i objasniti ključne tehnologije koje se koriste u sigurnosnim sustavima, kao što su strojno učenje, analiza velike količine podataka, obrada prirodnog jezika i prepoznavanje obrazaca.
2. Istražiti ulogu umjetne inteligencije u suvremenim sigurnosnim sustavima: Analizirati kako umjetna inteligencija doprinosi unapređenju nacionalne sigurnosti, s posebnim fokusom na prevenciju terorizma.
3. Procijeniti izazove masovne primjene umjetne inteligencije u sigurnosnim sustavima: Razmotriti potencijalne probleme koji se pojavljuju pri integraciji umjetne inteligencije u sustave nacionalne sigurnosti, s naglaskom na pitanja privatnosti i ljudskih prava.

Hipoteze koje se žele istražiti su:

H0: Primjena umjetne inteligencije značajno poboljšava učinkovitost sustava nacionalne sigurnosti u prepoznavanju i sprječavanju terorističkih prijetnji.

H1: Integracija umjetne inteligencije u sigurnosne sustave nosi značajan rizik narušavanja privatnosti i ljudskih prava, što zahtijeva razvoj strožih etičkih i pravnih okvira za njenu uporabu.

H2: Razvoj umjetne inteligencije specijalizirane za nacionalnu sigurnost može izazvati globalnu utrku u naoružanju UI tehnologijama, što može destabilizirati međunarodne odnose i povećati rizik od sukoba.

H3: Korištenje umjetne inteligencije u sigurnosnim sustavima može smanjiti potrebu za ljudskim nadzorom u određenim operacijama, ali istovremeno može povećati rizik od tehničkih pogrešaka s ozbiljnim posljedicama.

3. IZVORI PODATAKA I METODE

U ovom diplomskom radu, analizirana je primjena umjetne inteligencije (UI) u sustavima nacionalne sigurnosti, s posebnim naglaskom na prevenciju terorizma. Istraživanje se temelji na korištenju različitih izvora podataka i znanstvenih metoda kako bi se osigurala sveobuhvatna analiza postojećih trendova, tehnologija i pristupa u ovom području. Korištenje različitih izvora podataka i metoda omogućilo je multidisciplinarni pristup temi, a za potrebe istraživanja korišteni su sljedeći izvori podataka:

- Stručna literatura i znanstveni radovi: Rad se temelji na znanstvenim člancima, knjigama i pregledima literature iz područja UI, sigurnosnih studija i protuterorizma. Navedeni izvori pružaju uvid u ključne tehnologije i etička pitanja vezana uz primjenu UI.
- Izvještaji međunarodnih organizacija: Izvještaji NATO-a, UN-a, Europola i Instituta za ekonomiju i mir korišteni su za dobivanje empirijskih podataka o globalnim trendovima terorizma i sigurnosnim strategijama.
- *Online* resursi i alati: Online resursi korišteni su za definiranje ključnih pojmova i osiguranje kontekstualnog razumijevanja teme. Također, analiziran je „*Hatescape*", izvještaj specijaliziran za analizu ekstremističkog sadržaja na društvenim mrežama i drugim *online* platformama.
- Zakonodavne i strateške smjernice: Analizirani su zakonski i strateški dokumenti NATO-a, UN-a i Europola kako bi se razumjeli regulatorni okviri i etička pitanja povezana s upotrebom UI u sigurnosnim sustavima.

Korištene su znanstveno-istraživačke metode koje uključuju detaljan pregled relevantne literature, analizu i sintezu, induktivnu i deduktivnu metodu te metode deskripcije i kompilacije. Poseban fokus bio je na analizi velikih količina podataka (engl. *Big Data*), strojnog učenja, obrade prirodnog jezika i računalnog vida, kao i na njihovoj primjeni u identificiranju i predviđanju terorističkih prijetnji.

4. STRUKTURA RADA

Ovaj diplomski rad podijeljen je u nekoliko ključnih poglavlja koja zajedno čine cjelovitu analizu integracije umjetne inteligencije u sustave nacionalne sigurnosti, s posebnim naglaskom na prevenciju terorizma. Svako poglavlje fokusirano je na specifične aspekte teme, pružajući detaljan uvid u teorijske, tehničke i praktične elemente primjene umjetne inteligencije u području nacionalne sigurnosti.

U uvodnom dijelu rada, predstavljena je osnovna problematika i kontekst istraživanja. Definirani su ciljevi rada i hipoteze koje će biti analizirane u narednim poglavljima. U nastavku rada, definiraju se osnovni pojmovi te se objašnjava njihova povijesti i važnost u suvremenom kontekstu. U poglavlju „Tehnološka evolucija umjetne inteligencije" opisani su ključni koncepti umjetne inteligencije poput strojnog učenja, dubokog učenja, analize velike količine podataka i obrade prirodnog jezika. U sljedećem su poglavlju predstavljeni konkretni primjeri primjene umjetne inteligencije u prevenciji terorizma. Obrađene su metode analize podataka, prediktivne analitike, prepoznavanja obrazaca te identifikacije potencijalnih prijetnji. Primjena umjetne inteligencije, osim pozitivnih značajki, za sobom povlači i potencijalne negativne posljedice. U poglavlju „Opasnost masovne primjene umjetne inteligencije" razmatraju se pitanja privatnosti, ljudskih prava, te potencijalni rizici povezani s prikupljanjem i analizom osjetljivih podataka. U digitalnom dobu, društvene mreže postale su moćni alati za komunikaciju, mobilizaciju i širenje informacija, no, nažalost, i za nelegitimne svrhe. Jedna od najpopularnijih platformi koje terorističke skupine koriste za širenje svoje propagande, regrutaciju i koordinaciju je društvena mreža TikTok. U posljednjem dijelu rada, prikazani su rezultati istraživanja TikToka u svrhu detekcije ekstremističkog sadržaja te je predstavljena aplikacija za brzo pretraživanje i analizu TikTok sadržaja povezanog s terorističkim aktivnostima u svrhu sprječavanja istih.

5. REZULTATI I RASPRAVA

5.1. POJMOVI

5.1.1. Nacionalna sigurnost

Pojam „sigurnost“ ima duboke korijene u povijesti ljudskog društva, evoluciji jezika i razvoju civilizacija. U svom izvornom stoičkom značenju, izraz označava neuzdrmanost vanjskim događajima, odnosno bezbrižnost *(se-cura)* u smislu postizanja potpunog unutarnjeg mira.[1]

Pojam potječe iz latinskog jezika, ali se razvijao i proširivao kroz stoljeća, reflektirajući promjene u društvenim, političkim i tehnološkim kontekstima ljudske civilizacije. Koristi se u društvenim znanostima u različitim kontekstima, uključujući socijalnu, pravnu sigurnost pa sve do nacionalne sigurnosti. Sigurnost je jedan od osnovnih fenomena ljudskog društva kroz sve njegove faze razvoja. Bilo da se radi o sigurnosti pojedinca, države, skupine država ili međunarodne zajednice, cilj je uvijek zaštititi vrijednosti i stanje za koje se vjeruje da su od vitalnog značaja.[2]

U kontekstu nacionalne sigurnosti, sigurnost je bila ključna za opstanak i razvoj ljudskih zajednica od najranijih vremena, od osnovne zaštite pojedinaca do složenih sustava zaštite država i globalnih zajednica. U antičkim civilizacijama, kao što su Grčka i Rim, sigurnost se prvenstveno odnosila na vojnu obranu i zaštitu gradova-država od vanjskih napada. U srednjovjekovnoj Europi, sigurnost je često bila lokalizirana i ovisila o feudalnim gospodarima koji su pružali zaštitu svojim vazalima u zamjenu za lojalnost i službu. Moderno dobra i formiranje modernih nacionalnih država donijelo je potrebu za centraliziranom vojnom i policijskom silom kako bi se očuvala unutarnja stabilnost i obrana od vanjskih prijetnji. Industrijska revolucija donijela je nove dimenzije sigurnosti, uključujući ekonomsku sigurnost i zaštitu trgovačkih puteva. Revolucije i politički nemiri u 19. stoljeću u Europi potaknuli su razvoj sigurnosnih aparata unutar država za suzbijanje pobuna i održavanje reda. Dva svjetska rata drastično su proširila koncept nacionalne sigurnosti, uključujući strategije totalnog rata, civilne zaštite i obavještajne aktivnosti. U poslijeratnom periodu nastojalo se kolektivno upravljati sigurnosnim pitanjima i sprječavati sukobe osnivanjem Ujedinjenih naroda, NATO-a i drugih međunarodnih tijela. Pojam nacionalne

[1] sigurnost. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2024. Dostupno na: https://www.enciklopedija.hr/clanak/sigurnost (1.8.2024.).
[2] Tatalović, S., Bilandžić, M. (2005)., *Osnove nacionalne sigurnosti*. Zagreb, str. 23.

sigurnosti evoluirao je od osnovne zaštite teritorija i vojnog odvraćanja do sveobuhvatnog pristupa koji uključuje ekonomske, ekološke, zdravstvene i kibernetičke segmente.

Danas, nacionalnu sigurnost kao pojam može se definirati kao stanje zaštite ključnih vrijednosti društva i njegovih institucija, očuvanje vitalnih nacionalnih interesa te integritet državnog teritorija i njenih struktura.[3]

5.1.2. Terorizam

Definiranje terorizma je zahtjevan zadatak zbog različitih perspektiva i konteksta u kojima se koristi. Izuzetno složeni društveni fenomen može se definirati kao pojam koji se koristi za opisivanje nasilnih akcija s ciljem postizanja određenih političkih, ideoloških, vjerskih ili društvenih ciljeva kroz upotrebu prisile i izazivanje straha. Ova definicija, iako u osnovi jednostavna, skriva složenost i raznolikost terorizma kao fenomena. U nastavku teksta su predstavljene neke definicije koje su široko prihvaćene i korištene u akademskim, pravnim i političkim krugovima.

Prema definiciji Hrvatske enciklopedije, terorizam je *"primjena oružanog i drugoga nasilja, najčešće protiv nedužnih osoba, radi ostvarenja političkog ili nekoga drugog cilja. Obilježava ga sustavnost u uporabi nasilja (ili prijetnji nasiljem), pretežno politička motivacija (borba za društvene promjene, politički utjecaj ili vlast), promišljen izbor izravnih žrtava te onih neizravnih (širenjem straha), kršenje ljudskih prava i dr. Određuje se i kao oblik političkog nasilja, metoda vojno-političke borbe i dr."*[4]

U svojoj knjizi „Sjeme zla", Mirko Bilandžić detaljno analizira fenomen terorizma i pruža preciznu definiciju koja reflektira složenost pojma. Prema Bilandžiću, terorizam se može definirati kao: *"Namjerno i sustavno korištenje ili prijetnja korištenjem nasilja od strane nedržavnih aktera s ciljem postizanja političkih, ideoloških, religijskih ili drugih ciljeva putem zastrašivanja šire javnosti ili utjecaja na vladine politike."*.[5] Njegova definicija terorizma obuhvaća namjernost i

[3] Hartland-Thunberg P. (1982). *National economic security: interdependence and vulnerability*. John F. Kennedy Institute, str. 50.
[4] terorizam. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2024. Dostupno na: https://www.enciklopedija.hr/clanak/terorizam (21.7.2024.).
[5] Bilandžić, M. (2010). *Sjeme zla – elementi sociologije terorizma*, Plejada, Zagreb, str. 14.

sistematičnost, upotrebu nasilja ili prijetnje nasiljem, ulogu nedržavnih aktera, specifične ciljeve, te strategiju zastrašivanja javnosti i utjecaja na vladine politike.

Brenda i James Lutz, istaknuti autori na polju proučavanja terorizma, u svojoj knjizi „*Global Terrorism"*, terorizam definiraju kao: *"Politički motivirano nasilje ili prijetnja nasiljem koje provode pojedinci, grupe, ili države, usmjereno prema nevladinim ciljevima, s namjerom da se izazove strah i utječe na publiku šire od neposrednih žrtava."*.[6] Prema Lutzovima, terorizam je definiran kao nasilje koje ima političke ciljeve, odnosno uključuje akcije koje su usmjerene na postizanje promjena u političkoj strukturi ili društvenim uvjetima. Osim stvarnog nasilja, terorizmom definiraju i prijetnje nasiljem koje mogu biti jednako učinkovite kao i stvarni napadi u stvaranju straha i nesigurnosti. Terorizam nije ograničen samo na nedržavne aktere. Pojedinci, grupe i čak države mogu koristiti terorističke taktike za postizanje svojih ciljeva. Osim toga, autori navode kako su terorističke akcije usmjerene prema ciljevima koji nisu direktno povezani s vladinim institucijama. Mete mogu uključivati civile, javne prostore, privatne objekte i druge nevladine ciljeve. Jedan od glavnih ciljeva terorizma je izazivanje straha među širom populacijom. Teroristički napadi su dizajnirani da stvore atmosferu nesigurnosti i panike. Terorizam je usmjeren na postizanje psihološkog učinka na publiku koja je šira od neposrednih žrtava napada. Cilj je utjecati na ponašanje i percepcije široke javnosti, vladinih institucija i međunarodne zajednice.

Ujedinjeni narodi nemaju jednu univerzalno prihvaćenu definiciju terorizma, ali je Generalna skupština UN-a u svojoj rezoluciji 49/60 (1994) dala opis koji se često koristi: *"Kaznena djela namjerno i sistematski usmjerena protiv nevinih civila s ciljem izazivanja straha i prisiljavanja vlade ili međunarodne organizacije na određene akcije."*.[7]

Europska unija definira terorizam u sklopu svoje Okvirne odluke Vijeća EU o borbi protiv terorizma (2002) kao *„kaznena djela namjerno počinjena zbog svoje prirode ili konteksta koja mogu ozbiljno naštetiti zemlji ili međunarodnoj organizaciji, s ciljem ozbiljnog zastrašivanja stanovništva ili nepropisnog prisiljavanja vlade ili međunarodne organizacije da izvrši ili se suzdrži od izvršenja bilo koje radnje."*.[8]

---

[6] Lutz, B., Lutz, J. (2008). *Global Terrorism*. Routledge, str. 9.
[7] Ujedinjeni narodi. (1994). Rezolucija 49/60, *Measures to eliminate international terrorism*. Generalna skupština. Dostupno na https://digitallibrary.un.org/record/172281?ln=en&v=pdf (21.7.2024.).
[8] Vijeće Europske unije. (2002). *Okvirna odluka Vijeća 2002/475/PUP o borbi protiv terorizma*. Dostupno na: https://eur-lex.europa.eu/eli/dec_framw/2002/475/oj (21.7.2024.).

Iako se definicije terorizma mogu razlikovati, one obično uključuju nekoliko zajedničkih elemenata: namjernu upotrebu nasilja, političke ili ideološke ciljeve, zastrašivanje šire javnosti i utjecaj na vladine politike.

5.1.3. Protuterorizam

Često se uz terorizam vezuju pojmovi protuterorizma i antiterorizma. Iako se navedena dva pojma često koriste kao sinonimi, postoje različite nijanse u kontekstu njihove primjene. Protuterorizam je prema Institutu za hrvatski jezik i jezikoslovlje istoznačnica protuterorističkim mjerama koje se definiraju kao *„mjere za sprječavanje terorističkoga čina ili odgovor na teroristički čin odnosno dokumentiranu prijetnju takvim činom"*.[9] Protuterorizam se odnosi na proaktivne, direktne i često vojne mjere usmjerene na suzbijanje i neutralizaciju terorističkih prijetnji. Takve aktivnosti, primjerice, uključuju sprječavanje novačenja, napade na terorističke centre za obuku, pronalaženje i zapljenu financijskih sredstava terorističkih organizacija te uhićenja i provođenje suđenja teroristima.

5.1.4. Antiterorizam

Za razliku od protuterorističkih mjera koje se fokusiraju na aktivno reagiranje i neutralizaciju aktivnih terorističkih prijetnji, antiterorističke mjere su uglavnom obrambenog ili pasivnog karaktera. Odnosno, antiteroristička djelatnost odnosi se na aktivnosti usmjerene na prevenciju terorističkih napada, poput otkrivanja, presretanja i sprječavanja prijetnji prije nego što dođe do napada. Takvi programi uključuju sustavne mjere za smanjenje vjerojatnosti terorističkih napada. U tom smislu, uvode se promjene koje, primjerice, poboljšavaju nadzor i ograničavaju pristup područjima s kojih bi teroristi mogli djelovati.[10] [11]

[9] protuterorističke mjere. Struna. Dostupno na: http://struna.ihjj.hr/naziv/protuteroristicke-mjere/49620/#naziv (21.7.2024.).
[10] Antiterorističke mjere. Struna. Dostupno na: http://struna.ihjj.hr/naziv/antiteroristicke-mjere/49619/#naziv (21.7.2024.).
[11] Šegvić, S. (2009). Antiterorizam u kontekstu borbe protiv organiziranog kriminala. *Zbornik radova Pravnog fakulteta u Splitu, 46*(4), str. 667.

5.1.5. Umjetna inteligencija

Pod pojmom inteligencije, najčešće se podrazumijeva sposobnost snalaženja u novim prilikama, sposobnost brzog razmišljanja, učenje iz iskustva te primjenu znanja.[12] David Wechsler, poznati američki psiholog koji je razvio nekoliko važnih testova inteligencije, definirao je inteligenciju kao *„zbirnu ili globalnu sposobnost pojedinca da djeluje svrhovito, da razmišlja racionalno i da se učinkovito nosi sa svojim okruženjem"*.[13] Kada se spominje pojam inteligencije, podrazumijeva se da je riječ o ljudskoj inteligenciji, stoga, kada je riječ o umjetnoj inteligenciji, zapravo se govori o umjetno stvorenoj inteligenciji koja imitira upravo inteligenciju čovjeka. Algoritmi poput neuronskih mreža dizajnirani su da oponašaju način na koji ljudski mozak obrađuje informacije. Na primjer, duboko učenje (engl. *Deep Learning*) tehnika je u umjetnoj inteligenciji koja se temelji na strukturama i funkcijama ljudskih neuronskih mreža.

Brojne su definicije umjetne inteligencije, međutim, može se primijetiti da se ista u svakoj zapravo opisuje kao sposobnost računala da radi ili misli kao čovjek. Prema definiciji Hrvatske enciklopedije, umjetna inteligencija (engl. *Artificial Intelligence* - UI) je *„dio računalstva koji se bavi razvojem sposobnosti računala da obavljaju zadaće za koje je potreban neki oblik inteligencije; također oznaka svojstva neživog sustava koji pokazuje inteligenciju (inteligentni sustav)."*[14] Odnosno, umjetna inteligencija je grana informatike koja se bavi razvojem računalnih sustava sposobnih za obavljanje zadataka koji obično zahtijevaju ljudsku inteligenciju. Ti zadaci uključuju učenje, zaključivanje, rješavanje problema, razumijevanje prirodnog jezika, prepoznavanje obrazaca, percepciju i donošenje odluka. UI može biti usmjerena na različite domene, od igara i robotike do medicinske dijagnostike i autonomnih vozila.

John McCarthy je često nazivan „ocem umjetne inteligencije" i igrao je ključnu ulogu u definiranju i razvoju ovog polja. McCarthy je prvi upotrijebio termin umjetna inteligencija 1956. godine na poznatoj Dartmouth konferenciji, koja se smatra rodnim mjestom modernog istraživanja ovog područja. Njegova definicija umjetne inteligencije bila je jednostavna, ali značajna: „*znanost i*

[12] inteligencija. Školski rječnik hrvatskog jezika. Dostupno na: https://rjecnik.hr/search.php?q=inteligencija (21.7.2024.)
[13] Wechsler, D. (1939). *The Measurement of Adult Intelligence*. Williams & Wilkins, str. 3.
[14] umjetna inteligencija. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2024. Dostupno na: https://enciklopedija.hr/clanak/umjetna-inteligencija (24.7.2024.).

inženjering stvaranja inteligentnih strojeva.“.[15] McCarthy je vidio umjetnu inteligenciju kao interdisciplinarno polje koje uključuje elemente znanosti (istraživanje, razumijevanje) i inženjeringa (izgradnja, primjena). Razvio je koncept računalnog dijeljenja vremena (engl. *timesharing*), koji je omogućio da više korisnika istovremeno koriste jedno računalo. Na taj je način značajno unaprijedio učinkovitost i pristup računalnim resursima. Radio je na formalizaciji znanja i razvoju algoritama za zaključivanje, što je osnova za mnoge moderne pristupe umjetnoj inteligenciji.

[15] McCarthy, J. (2007). *What is Artificial Intelligence?*. Dostupno na: http://www-formal.stanford.edu/jmc/whatisai.pdf (27.7.2024.).

5.2. SUVREMENI TERORIZAM U POSLJEDNIH 20 GODINA

Terorizam je u posljednjih dvadeset godina evoluirao kroz brojne promjene koje su redefinirale globalne sigurnosne izazove. Teroristički trendovi reflektiraju složenost i dinamičnost prijetnji koje predstavljaju terorističke organizacije, njihovi novi pristupi te promjene u međunarodnom odgovoru na terorizam. Za analizu terorističkih trendova korištena su izvješća Instituta za ekonomiju i mir (engl. *Institute for Economics and Peace*) - Globalni teroristički indeks (engl. *Global Terrorism Index* - GTI). GTI je sveobuhvatna studija koja analizira utjecaj terorizma za 162 zemlje koje pokrivaju 99,6 % svjetske populacije i, koristeći Globalnu bazu podataka o terorizmu (engl. *Global Terrorism Database* - GDT), rangira zemlje prema negativnom utjecaju terorizma.[16]

Od 2000. godine, prema Globalnom terorističkom indeksu, zabilježeno je nekoliko ključnih trendova u terorizmu: [17] [18]

- Značajan porast terorističkih napada
- Geografska koncentracija
- Promjena u prirodi terorizma
- Globalizacija terorističkih mreža

U nastavku je dan detaljniji pregled svakog od navedenih.

5.2.1. Značajan porast terorističkih napada

Od 2000. do 2011. godine, svake godine bilježi se postupan porast broja terorističkih napada. Iako se broj napada nije dramatično povećavao u svakoj godini, trend je bio jasan i konstantan. Porast je bio potaknut različitim faktorima, uključujući političku nestabilnost, regionalne sukobe i rast ekstremističkih ideologija.

Početkom 2000-ih, broj terorističkih napada bio je relativno stabilan, ali s nekoliko značajnih incidenata poput napada 11. rujna 2001. godine. Ovaj događaj izazvao je globalni „Rat protiv

[16] The Institute for Economics & Peace. (2014). *Global Terrorism Index 2014: Measuring and Understanding the Impact of Terrorism*. Dostupno na: https://www.economicsandpeace.org/wp-content/uploads/2023/12/GTI-2014-web.pdf (27.7.2024.).
[17] Isto
[18] The Institute for Economics & Peace. (2024). *Global Terrorism Index 2024.* Dostupno na: https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf (27.7.2024.).

terorizma“ i dramatično promijenio prirodu terorističkih aktivnosti. Invazija na Irak 2003. godine potaknula je nagli porast terorističkih aktivnosti, posebno u regiji Bliskog istoka. Sukobi u Iraku i Afganistanu postali su žarišta terorizma, s rastom broja napada svake godine.

U periodu od 2010. do 2013. godine, terorizam je doživio još jedan val rasta. Sukobi u Siriji i Iraku doprinijeli su porastu aktivnosti terorističkih grupa kao što su Islamska Država Iraka i Sirije (eng. *Islamic State of Iraq and Syria* - ISIS) i Al-Qaeda. U 2013. godini, zabilježeno je preko 10.000 terorističkih napada, što je povećanje od 44% u odnosu na 2012. godinu. Broj smrtnih slučajeva povezanih sa terorizmom dostigao je 17.958, što je povećanje od 61% u odnosu na prethodnu godinu.[19]

Period između 2014. i 2017. godine predstavlja vrhunac globalnog terorizma, s rekordnim brojem napada i smrtnih slučajeva. Pored Bliskog istoka, terorizam se proširio na Afriku, posebno u Nigeriji (Boko Haram) i Sahel regiji (JNIM i druge grupe). U 2014. godini, broj smrtnih slučajeva povezanih sa terorizmom porastao je na više od 32.000 što je bio gotovo trostruki porast u odnosu na 2011. godinu. Ukupan broj napada i smrtnih slučajeva od terorizma u 2015. godini dostigao je nove vrhunce, s tim da su Sirija, Irak, Afganistan, Pakistan i Nigerija činili više od 70% svih terorističkih aktivnosti. Od 2016. godine broj globalnih smrtnih slučajeva povezanih sa terorizmom počeo je opadati, ali je i dalje ostao na visokom nivou s obzirom na nove žarišne točke terorizma u Africi i Aziji. Sahel regija je postala novo globalno žarište terorizma, s dramatičnim porastom napada i smrtnih slučajeva. Broj smrtnih slučajeva u Sahelu porastao je za 2.860% od 2007. godine do 2023. godine.[20]

Iako su brojke smrtnih slučajeva i napada počele opadati nakon 2016. godine, prijetnja terorizma ostala je prisutna, a nova žarišta sukoba, posebno u Africi i Aziji, nastavila su poticati nasilje. Ovaj period pokazuje kako se terorizam prilagođava promjenama u globalnim okolnostima, te kako ostaje trajna prijetnja međunarodnoj sigurnosti, zahtijevajući stalnu pažnju i prilagodbu strategija borbe protiv terorizma.

[19] The Institute for Economics & Peace. (2014). *Global Terrorism Index 2014: Measuring and Understanding the Impact of Terrorism*. Dostupno na: https://www.economicsandpeace.org/wp-content/uploads/2023/12/GTI-2014-web.pdf (27.7.2024.).
[20] Isto

5.2.2. Geografska koncentracija

Globalna žarišta terorizma mijenjala su se i premještala od 2000. godine do danas. Tablica 1. prikazuje kako su se terorističke aktivnosti razvijale tokom posljednih 20-ak godina, koja područja su bila najviše pogođena i koje grupe su bile najaktivnije.

Tablica 1. Intenzitet terorističkih aktivnosti prema razdoblju

Razdoblje	Područja s najvišim intenzitetom	Glavne terorističke grupe
2000. – 2003.	Afganistan, Pakistan, Irak	Talibani, Al-Qaeda
2003. – 2010.	Irak, Somalija	Al-Qaeda, Al-Shabaab
2011. – 2014.	Sirija, Irak, Nigerija	ISIS, Boko Haram
2015. – 2017.	Bliski istok, Afrika, Europa	ISIS, Boko Haram, Al-Shabaab
2018. – danas	Afrika, Bliski istok	ISIS, Al-Shabaab, Talibani

Izvor: Autor prema GTI 2014 i GTI 2024

Početkom 2000-ih, Afganistan i Pakistan postale su ključne točke u borbi protiv terorizma, posebno nakon američke invazije na Afganistan 2001. godine. Navedena područja su bila centar aktivnosti talibana i Al-Qaede. Nakon invazije na Irak 2003. godine, isti je postao jedno od glavnih žarišta terorističkih aktivnosti. U isto vrijeme, Al-Shabaab je počeo jačati svoj utjecaj u Somaliji, postavši glavni akter terorizma u istočnoj Africi. Alžir je bio pogođen terorizmom zbog aktivnosti Naoružane islamske skupine (franc. *Groupe Islamique Armé* – GIA) koja je kasnije postala Al-Qaeda u Islamskom Magrebu (eng. *Al-Qa'ida in the Lands of the Islamic Maghreb* - AQIM)

Početkom sirijskog građanskog rata 2011. godine, Sirija je postala jedno od glavnih žarišta globalnog terorizma. Pojava ISIS-a u Siriji i Iraku dovela je do dramatičnog povećanja broja napada u regiji. Irak je ostao jedno od glavnih žarišta, s intenzivnim napadima koje je izvodio ISIS, posebno tijekom 2013. i 2014. godine kada je grupa osvojila velike teritorije. Tijekom razdoblja od 2011. do 2014. godine, Boko Harem se istaknuo kao dominantna teroristička grupa u zapadnoj Africi sprovodeći masovne napade, uključujući otmice, bombaške napade i masakre u sjeveroistočnoj Nigeriji. Također, Al-Shabaab je nastavio sa svojim napadima u Somaliji i proširio operacije u Keniji.

Period od 2015. do 2017. godine obilježen je dramatičnom ekspanzijom ISIS-a i njegovim kasnijim porazom, ali i širenjem terorizma u drugim dijelovima svijeta. Bliski istok, posebno Irak i Sirija, ostali su glavni epicentar terorističkih aktivnosti, dok su se nova žarišta pojavila u Africi,

posebno u Nigeriji, Somaliji, i Libiji. Europa je također postala meta velikih terorističkih napada, dok je Južna Azija i dalje trpjela kontinuirane napade od strane talibana i drugih ekstremističkih grupa.

Nakon 2018. godine, nastupile su značajne promijene u globalnom terorizmu. Iako je ISIS izgubio teritorijalnu kontrolu na Bliskom istoku, preostale ćelije nastavile su s gerilskim napadima. U Africi je nasilje eskaliralo i proširilo se na nova područja, posebno u Sahelu i Mozambiku, dok se Europa nastavila suočavati s manjim, pojedinačnim, ali ozbiljnim napadima. U Južnoj Aziji, talibani su se vratili u Afganistan s novom snagom, dok su se napadi u Pakistanu i Jugoistočnoj Aziji nastavili.

Geografska koncentracija terorističkih napada u posljednje četiri godine pokazuje jasno pomicanje fokusa ka Africi, posebno u području Sahela i Mozambika, dok su Bliski istok i Južna Azija zadržali svoje značajne uloge. Europa je zabilježila smanjenje intenziteta napada, ali je prijetnja ostala prisutna, posebno u urbanim sredinama. Jugoistočna Azija nastavila se suočavati s perzistentnim prijetnjama, ali s manjim intenzitetom u odnosu na prethodne godine.

5.2.3. Promjena u prirodi terorizma

U posljednjih 20-ak godina, priroda terorizma i ciljevi terorističkih napada su doživjeli značajne promjene reflektirajući širu dinamiku globalne politike, tehnologije i društvenih promjena. Ovo je razdoblje obilježeno prelaskom s centraliziranih, hijerarhijskih terorističkih organizacija na decentralizirane mreže i pojedince inspirirane radikalnim ideologijama.

Početak 2000-ih obilježen je aktivnostima Al-Qaede, kulminirajući napadima 11. rujna 2001. godine u Sjedinjenim Američkim Državama. Napadi Al-Qaede su pokazali visok nivo organizacije, planiranja i sofisticiranosti, s ciljem nanošenja masovnih žrtava i udara na simbole američke ekonomske, vojne i političke moći (World Trade Center, Pentagon). Glavni su ciljevi tada bili vojni i politički objekti, kao i simboli zapadne ekonomske moći. Al-Qaeda je ciljala i ambasade, vojne baze, i druge ključne infrastrukturne točke.

Uspon ISIS-a početkom 2010-ih predstavljao je novu fazu u prirodi terorizma. ISIS je proglasio kalifat na teritoriju Iraka i Sirije 2014. godine, i privukao desetke tisuća stranih boraca iz cijelog

svijeta. ISIS je ciljao ne samo vojne snage i vladine zgrade, već i civilnu populaciju u masovnim napadima, često usmjerenim na vjerske manjine, zapadne turiste i simbole kulturne baštine. Taktike su uključivale masovne pogubljenja, samoubilačke napade i otmice s ciljem podizanja globalnog straha.

Do kraja 2010-ih, ISIS je izgubio gotovo sve teritorijalne uporišta u Iraku i Siriji. Međutim, ostaci grupe i dalje su bili aktivni kroz gerilske napade i internacionalne terorističke operacije. Ciljevi su ostali uglavnom isti, ali s povećanim fokusom na destabilizaciju vlada u Africi i Aziji, gdje su slabije centralne vlasti omogućile veću slobodu djelovanja terorističkim grupama. Pojava i rast desničarskog ekstremizma, posebno u zapadnim zemljama, donijela je novu vrstu terorističkih prijetnji, usmjerenih na rasne, vjerske i političke protivnike.

Tehnološki napredak i globalne političke promjene u 2020-im godinama stvorile su novu dinamiku u terorizmu sa sve većim naglaskom na digitalne prijetnje i regionalne sukobe. Teroristički napadi su sveobuhvatniji i sofisticiraniji s naglaskom na raznovrsnost ciljeva. Od napada na civilne i vjerske zajednice, preko vojne i ekonomske infrastrukture do kibernetičkog terorizma, terorističke grupe su se prilagođavale novim izazovima i prilikama, koristeći ih za ostvarivanje svojih ciljeva. Njihove mete odražavale su šire društvene i političke tenzije, dok su napadi postajali sve nepredvidljiviji.

5.2.4. Globalizacija terorističkih mreža

Globalizacija terorističkih mreža od 2000. do 2024. godine bila je obilježena značajnim promjenama u prirodi, strukturi i operacijama terorističkih skupina. Jedan od ključnih segmenata globalizacije terorizma je pojava i širenje transnacionalnih terorističkih organizacija, poput Al-Qaede i kasnije Islamske države (IS). Navedene organizacije uspjele su izgraditi globalne mreže ćelija i pridruženih skupina, proširujući svoju prisutnost izvan tradicionalnih granica Bliskog istoka na Afriku, Aziju i čak dijelove Europe.

U nekim regijama, osobito u Sahelu, terorističke skupine su se počele baviti organiziranim kriminalom ili su se udruživale s kriminalnim organizacijama kako bi financirale svoje aktivnosti. Terorističke mreže postale su financijski neovisne zahvaljujući prihodima iz ilegalnih aktivnosti

poput trgovine drogom, krijumčarenja i otmica, što je dodatno kompliciralo napore u borbi protiv terorizma.

Terorističke skupine sve više koriste digitalne tehnologije i internet za regrutiranje, propagandu i planiranje napada. Navedeno omogućava terorističkim organizacijama dostizanje globalne publike, regrutiranje boraca iz različitih dijelova svijeta, te koordiniranje složenih napada na više kontinenata. Nakon velikog broja napada u zapadnim zemljama 2000-ih, došlo je do promjene fokusa s masovnih napada na takozvane vukove samotnjake i manje, lokalizirane napade, često inspirirane ili podržane putem *online* platformi. Također, mnoge zapadne zemlje usmjerile su resurse na prevenciju radikalizacije i deradikalizaciju, dok su istovremeno pojačale sigurnosne mjere.

Globalizacija je učinila terorizam fleksibilnijim, otpornijim i opasnijim, s kapacitetom da se brzo prilagodi promjenama u geopolitici i tehnologiji.

5.2.5. Korištenje modernih tehnologija

Korištenje tehnologije u terorističke svrhe predstavlja rastuću prijetnju u Europskoj uniji, kako je navedeno u Europolovom izvješću o terorizmu za 2023. godinu.[21] Teroristi i nasilni ekstremisti sve više koriste digitalne i tehnološke napretke za širenje propagande, regrutiranje novih članova, te koordinaciju aktivnosti, što ozbiljno ugrožava sigurnost unutar EU.

Jedan od ključnih alata koji se koristi za radikalizaciju i regrutaciju su *gaming* platforme. Teroristi, posebno pristaše Islamske države (engl. *Islamic State* - IS), kreiraju grupe na platformama za komunikaciju u igrama gdje raspravljaju o različitim temama, uključujući medijske operacije, prevođenje propagandnog sadržaja i vjersku migraciju. Na desničarskoj sceni, ekstremisti koriste *gaming* platforme za stvaranje utopijskih zajednica unutar popularnih video igara, uključujući neo-nacističke rekreacije, antisemitizam i anti-LGBTQ+ teme. Cilj ovih aktivnosti je privući veću publiku, posebno mlađe simpatizere, te stvoriti osjećaj zajedništva kroz zajedničke hobije.

[21] Europol. (2023). *European Union Terrorism Situation and Trend Report 2023*. Publications Office of the European Union. Dostupno na: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat (2.8.2024.)

Šifrirane komunikacijske aplikacije također su ključan alat koji teroristi aktivno koriste. Funkcionalnosti *end-to-end* enkripcije takvih aplikacija omogućava teroristima sigurno komuniciranje unutar svojih zajednica, čime se otežava identifikacija i uklanjanje terorističkog sadržaja od strane sigurnosnih agencija.

U desničarskim ekstremističkim krugovima sve je vidljivija upotreba 3D printanja za izradu oružja. U Slovačkoj i Nizozemskoj, pojedinci povezani s desničarskim ekstremistima, uključujući i maloljetnike, uhićeni su zbog dijeljenja *online* uputa za izradu automatskog vatrenog oružja s dijelovima koji se mogu ispisati na 3D pisačima, kao i zbog posjedovanja 3D printanog oružja i dijelova za oružje.

Također, financijske tehnologije sve više utječu na financijske aktivnosti terorističkih i nasilnih ekstremističkih skupina. Za financiranje svojih aktivnosti teroristi koriste virtualne imovine, poput kriptovaluta, što im omogućava višu razinu anonimnosti.

Jedan od zanimljivih primjera korištenja novih tehnologija u terorističke svrhe je zabilježen u kolovozu 2022., kada je simpatizer Islamske države pokušao koristiti nezamjenjive tokene (eng. *non-fungible token* - NFT) kao novi način širenja propagande. Prvi prijavljeni slučajevi uključuju NFT-ove s prikazima zastave Islamske države i tekstovima koji hvale terorističku organizaciju za napade, kao i upute za izradu eksploziva. Ovi NFT-ovi su objavljeni na *online* tržištu, ali su ubrzo uklonjeni. Međutim, zbog nepromjenjivih tehnologija lanaca blokova (eng. *Blockchain)* na kojima su NFT-ovi zasnovani, oni ne mogu biti eliminirani, što ukazuje na novi izazov u borbi protiv terorizma.

U izvješću se, također, spominje kako se očekuje da će teroristi u budućnosti sve više koristiti tehnologije poput umjetne inteligencije. Teroristi mogu koristiti UI za poboljšanje efikasnosti propagande, ubrzanje radikalizacije putem interneta, te za daljinsko upravljanje vozilima i oružjem korištenim u napadima. Navedeni primjeri pokazuju kako se teroristi prilagođavaju i koriste najnovije tehnologije kako bi nastavili svoje aktivnosti, čime predstavljaju ozbiljan izazov za sigurnosne agencije i društvo u cjelini.[22]

[22] Europol. (2023). *European Union Terrorism Situation and Trend Report 2023*. Publications Office of the European Union. Dostupno na: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat (2.8.2024.)

5.3. TEHNOLŠKA EVOLUCIJA UMJETNE INTELIGENCIJE U POSLJEDNIH 20 GODINA

U posljednjih dvadeset godina umjetna inteligencija je doživjela izuzetnu transformaciju, prelazeći iz akademske sfere u široku primjenu u industriji i svakodnevnom životu. Ova evolucija može se promatrati kroz nekoliko ključnih razvojnih faza koje su omogućile UI tehnologijama da postanu integralni dio svakodnevnog života, poslovanja i znanstvenih istraživanja.

Tehnološki razvoj umjetne inteligencije u 2000-im godinama obilježen je značajnim ulaganjem u istraživanje i razvoj. Početna faza razvoja UI bila je vođena akademskim istraživanjem, a oko 2010. godine industrija je počela preuzimati ključnu ulogu. Ulaganja u UI tehnologije značajno su porasla što je omogućilo brzi napredak i komercijalizaciju mnogih aplikacija.[23]

5.3.1. „Big Data"

Razvoj umjetne inteligencije u 21. stoljeću bio je usko povezan s pojavom i razvojem tehnologije velike količine podataka (engl. *Big Data)*. Eksponencijalni rast količine podataka generiranih svakodnevno, u kombinaciji s napretkom u računalnoj snazi i algoritmima strojnog učenja, omogućio je umjetnoj inteligenciji da postigne nevjerojatne uspjehe u raznim industrijama. Pojam *Big Data* odnosi se na sve veće količine podataka koje su eksponencijalno rasle s pojavom interneta i interneta stvari (engl. *Internet of Things* - IoT). Međutim, *Big Data* ne obuhvaća samo volumen, odnosno količinu podataka koja se generira svakodnevno, već i brzinu kojom se ti podaci generiraju i obrađuju, raznolikost tipova podataka te vrijednost koju ti podaci donose u procesu donošenja odluka.[24]

Eksplozija podataka postala je očita početkom 2000-ih godina, kada su organizacije počele prikupljati ogromne količine podataka iz različitih izvora, uključujući društvene mreže, senzore, transakcijske sustave i druge digitalne platforme. Povijesno gledano, većina podataka bila je strukturirana, što znači da se mogla organizirati u tablice baza podataka. Međutim, s razvojem

[23] *Afrtificial Intelligence Index Report 2024*. Institute for Human-Centered AI, Stanford University. Dostupno na: https://aiindex.stanford.edu/report/ (15.8.2024.).
[24] Gandomi, A., Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), str. 138-139.

tehnologije i rastom digitalnih sadržaja, više od 80% elektroničkih podataka postalo je nestrukturirano. Nestrukturirani podaci odnose se na vrste podataka poput slika, videozapisa, glasovnih zapisa i drugih oblika koji se ne mogu lako kategorizirati ili analizirati tradicionalnim metodama.[25] Pojavila se potreba za razvojem naprednijih alata i tehnika za obradu i analizu nestrukturiranih podataka. Razvoj *Big Data* tehnologija omogućio je prikupljanje, pohranu i obradu ogromnih količina podataka iz različitih izvora. Zahvaljujući navedenom, omogućeno je stvaranje inteligentnih sustava koji mogu analizirati podatke, prepoznati obrasce i donositi odluke temeljene na kontekstu. Kombinacija *Big Data* analitike i algoritama za strojno učenje dodatno je ubrzala razvoj sofisticiranih UI sustava.

5.3.2. Duboko učenje

Faza dubokog učenja, koja je započela krajem 2000-ih, predstavlja jednu od najznačajnijih prekretnica u razvoju umjetne inteligencije. Duboko učenje vrsta je strojnog učenja koje koristi višeslojne neuronske mreže za analizu podataka. Razvoj ovog područja postao je iznimno važan zbog porasta računalne snage i dostupnosti velikih skupova podataka. Navedene mreže mogu naučiti složene obrasce u podacima, što je dovelo do napretka u područjima kao što su računalni vid, prepoznavanje govora i obrada prirodnog jezika. Algoritmi dubokog učenja kao što su konvolucijske neuronske mreže (engl. *Convolutional Neural Network* - CNN) i rekurentne neuronske mreže (engl. *Recurrent Neural Network* - RNN), postali su ključni alati u mnogim primjenama, od autonomnih vozila do medicine.[26]

Jedan od ključnih čimbenika koji je omogućio eksploziju dubokog učenja je razvoj grafičkih procesora (engl. *Graphics Processing Unit* - GPU) i specijaliziranih hardverskih akceleratora. GPU-ovi omogućuju paralelnu obradu velikih količina podataka, što je ubrzalo obuku dubokih neuronskih mreža.

[25] *Big data analytics: What it is and why it matters*. SAS. Dostupno na: https://www.sas.com/en_us/insights/analytics/big-data-analytics.html (15.8.2024.)
[26] Cena, J. (2024). *Exploring the Evolution of Artificial Intelligence: From Early Concepts to Modern Applications*. Artificial Life.

5.3.3. Obrada prirodnog jezika

Obrada prirodnog jezika (engl. *Natural Language Processing* - NLP) doživjela je revoluciju zahvaljujući razvoju modela temeljenih na takozvanim transformer arhitekturama koje omogućuju paralelnu obradu podataka i učinkovito učenje dugoročnih zavisnosti u tekstu. Ovi modeli koriste duboke neuronske mreže za analizu i generiranje prirodnog jezika, omogućujući preciznije i kontekstualno razumijevanje teksta. Kao rezultat, ostvaren je značajan napredak u zadacima poput automatskog prevođenja, analize sentimenta, prepoznavanja entiteta i generiranja teksta. NLP se koristi u širokom spektru aplikacija, od pametnih pomoćnika do složenih analitičkih sustava.[27]

Jedan od najznačajnijih modela u području obrade prirodnog jezika je Googleov projekt „BERT“ koji značajno poboljšava sposobnost tražilice da razumije upite na prirodnom jeziku. BERT je napredni UI sustav koji koristi dvosmjerno duboko učenje za prepoznavanje i razumijevanje teksta razmatrajući kontekst svake riječi u rečenici u odnosu na druge. Isti omogućuje Googleu preciznije tumačenje konteksta i značenja riječi te daje relevantnije rezultate pretraživanja.[28]

Ključni napredak u polju obrade prirodnog teksta je generativni unaprijed obučeni transformator (engl. *Generative Pre-trained Transformer* - *GPT*). Zajedno s arhitekturama poput BERT-a, GPT modeli su revolucionirali NLP zadatke. Zahvaljujući svojoj sposobnosti korištenja dubokog učenja na velikim korpusima teksta, gore navedeni modeli mogu s izuzetnom preciznošću stvoriti kontekstualne reprezentacije riječi i rečenica koje se koriste za izvršavanje različitih zadataka, kao što su analiza sentimenta, prepoznavanje entiteta, automatski prijevod, odgovaranje na pitanja i generiranja teksta.[29]

5.3.4. Računalni vid

Računalni vid, kao jedna od ključnih komponenti UI, doživio je značajan napredak zahvaljujući tehnikama dubokog učenja, posebno kroz razvoj CNN-a. Tehnologije konvolucijskih neuronskih

[27] Cena, J. (2024). *Exploring the Evolution of Artificial Intelligence: From Early Concepts to Modern Applications*. Artificial Life.
[28] Schwarz, B. (2019). *Welcome BERT: Google's latest search algorithm to better understand natural language*. Search Engine Land. Dostupno na: https://searchengineland.com/welcome-bert-google-artificial-intelligence-for-understanding-search-queries-323976 (15.8.2024.)
[29] Cena, J. (2024). *Exploring the Evolution of Artificial Intelligence: From Early Concepts to Modern Applications*. Artificial Life.

mreža omogućuje strojevima da prepoznaju i klasificiraju objekte na slikama i videozapisima što je dovelo do primjene u autonomnim vozilima, medicinskom snimanju i sustavima nadzora. Primjena UI u računalnom vidu otvara nove mogućnosti za automatizaciju i analizu vizualnih podataka u realnom vremenu. Osim CNN-a, generativne mreže kao što su generativne kontradiktorne mreže (engl. *Generative Adversarial Networks* - GAN) omogućile su stvaranje realističnih slika i videozapisa otvarajući nove mogućnosti u kreativnim industrijama, kao i u području sintetičkih podataka za treniranje drugih UI sustava.[30] Još neke primjene računalnog vida dane su u tablici 2.

Tablica 2. Primjene računalnog vida

Primjena	**Primjeri**
Detekcija objekata	Samovozeća vozila, sustavi za sigurnost i nadzor
Klasifikacija slika	Analiza medicinskih slika, filtriranje sadržaja na internetu
Segmentacija slika	Medicinska dijagnostika, analize u autonomnim vozilima
Praćenje objekata u videozapisima	Sustavi za nadzor, analize ponašanja potrošača
Generiranje realističnih slika	Umjetnička kreacija, izrada lažiranih (engl. *Deepfake)* videa

Izvor: Autor prema Cena, J. (2024)

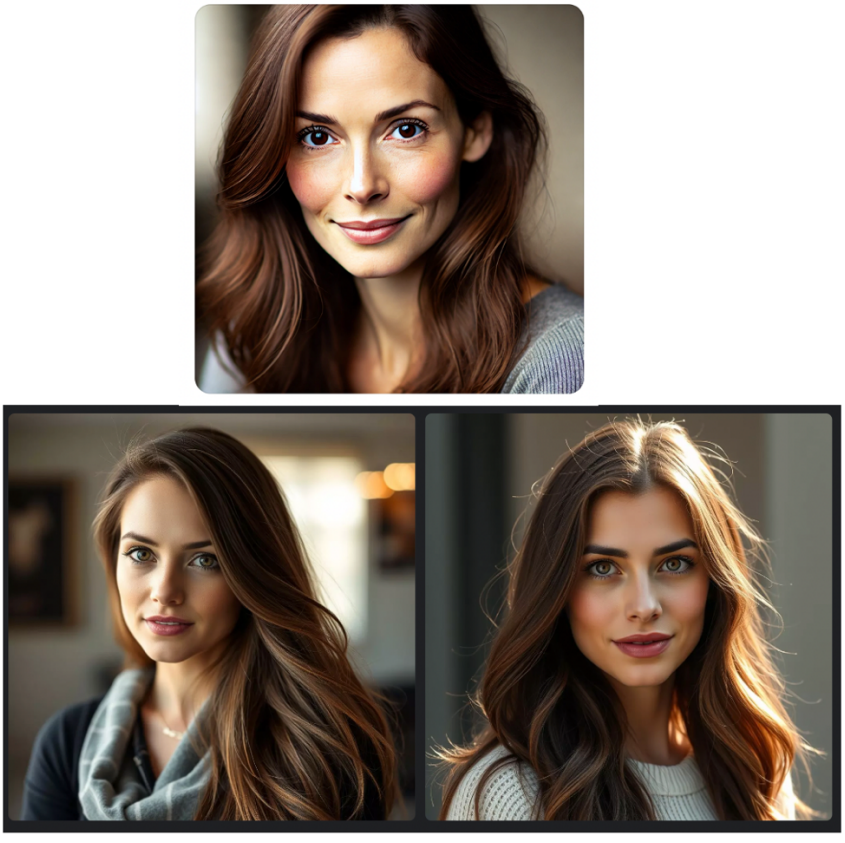
Značajan iskorak u području računalnog vida postignut je predstavljanjem CNN modela pod nazivom „AlexNet“. AlexNet je 2012. godine osvojio prestižno natjecanje u prepoznavanju vizualnih objekata, poznato kao „*ImageNet Large Scale Visual Recognition Challenge*“ (ILSVRC). AlexNet je postigao izvanredne rezultate u prepoznavanju slika, nadmašivši sve dotadašnje tradicionalne pristupe strojnom učenju i računalnom vidu te je pritom smanjio stopu pogreške gotovo u pola u odnosu na prethodno najbolje metode. Uspjeh AlexNet-a izazvao je golem interes za duboke neuronske mreže, ne samo unutar znanstvene zajednice, već i u industriji, čime su se otvorili novi putevi za primjenu dubokog učenja u različitim područjima.[31] [32]

[30] Cena, J. (2024). *Exploring the Evolution of Artificial Intelligence: From Early Concepts to Modern Applications*. Artificial Life.
[31] LeCun, Y., Bengio, Y., Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), str. 440.
[32] Alom, M. Z. et al. (2018). *The history began from AlexNet: A comprehensive survey on deep learning approaches.*

5.3.5. Generativni modeli

Generativni modeli omogućavaju strojevima stvaranje novih podataka koji nalikuju postojećim, što predstavljaju jedno od najzanimljivijih područja u suvremenoj umjetnoj inteligenciji. Tehnologija generativnih modela nije samo napredak u analizi podataka, već i korak prema razvoju strojeva koji mogu stvarati originalne sadržaje, poput slika, glazbe i teksta.

Jedna od ključnih primjena navedenih modela je u stvaranju realističnih slika što je postalo moguće s razvojem tehnologija kao što su generativne kontradiktorne mreže (engl. *Generative Adversarial Networks* - GAN) i varijacijski autokoderi (engl. *Variational Autoencoders* - VAE). GAN i VAE su dva ključna modela koja se koriste za generiranje podataka, ali imaju različite prednosti i primjene. GAN se često koristi za generiranje visoko kvalitetnih slika, dok se VAE koristi u situacijama gdje je važna kontrola nad varijabilnošću generiranih podataka. Slika 1. prikazuje generiranje UI fotografije uz pomoć ChatGPT i getimg.ai generatora.



Slika 1. Generiranje fotografije uz pomoć ChatGPT-a (gore) i getimg.ai (dolje)

Izvor: Autor

Postupak izrade fotografije započeo je definiranjem osnovnih karakteristika subjekta, u ovom slučaju žene u tridesetim godinama smeđe kose i smeđih očiju, a rezultate možete vidjeti gore.

Kako generativni modeli postaju sve sofisticiraniji, postavlja se pitanje etičkih implikacija njihove upotrebe. Na primjer, generativni modeli mogu biti korišteni za stvaranje lažnih slika ili videozapisa (engl. *Deepfake*), što može imati ozbiljne posljedice za društvo. S druge strane, ovi modeli imaju veliki potencijal za pozitivne primjene u personalizaciji sadržaja, unapređenju kreativnih industrija, pa čak i u obrazovanju. U budućnosti, generativni modeli bi mogli igrati ključnu ulogu u razvoju opće umjetne inteligencije. Isti ne samo da uče klasificirati ili prepoznati uzorke u podacima, već uče i kako generirati nove podatke koji su slični onima na kojima su trenirani, uključujući kreiranje slika, sintezu govora, proizvodnju glazbe i druge kreativne zadatke. Na ovaj se način približava vrijeme stvaranja strojeva koji posjeduju kreativnost sličnu ljudskoj. Generativno učenje moglo bi postati temelj za razvoj inteligentnih sustava sposobnih za samostalno učenje i prilagođavanje u dinamičnim okruženjima.

David Foster u svojoj knjizi *„Generative Deep Learning“* ističe kako je diskriminativno modeliranje dugo vremena dominiralo napretkom u strojnom učenju. Diskriminativno modeliranje je bilo popularnije jer je u većini slučajeva lakše riješiti diskriminativne probleme nego generativne. Na primjer, lakše je trenirati model da prepozna je li slika djelo Van Gogha nego generirati potpuno novu sliku u stilu Van Gogha. Međutim, s razvojem tehnologija strojnog učenja, ograničenja i poteškoće u generativnom modeliranju postupno su se smanjivale. U posljednjih deset godina, značajan napredak u ovom području postignut je zahvaljujući novim primjenama strojnog učenja na generativne zadatke. Autor napominje da su neki od najzanimljivijih napredaka u ovom razdoblju ostvareni upravo u generativnom modeliranju, posebno u generiranju slika lica. Generativno modeliranje počelo je privlačiti sve veću pažnju zbog svoje potencijalne primjene u industriji. Iako je diskriminativno modeliranje bilo primjenjivo na mnoge praktične probleme, poput medicinske dijagnostike, gdje je korisno imati model koji može predvidjeti prisutnost bolesti, generativno modeliranje sada počinje nalaziti primjenu u specifičnim poslovnim problemima. Na primjer, danas postoje API-ji koji omogućuju generiranje originalnih blogova na određenu temu ili proizvodnju različitih slika proizvoda u bilo kojem željenom okruženju.

Generativni modeli omogućuju strojevima razvijanje dubljeg razumijevanja podataka, čime otvaraju nove mogućnosti za istraživanje i primjenu umjetne inteligencije u raznim područjima. [33]

5.3.6. Umjetna opća inteligencija

Umjetna opća inteligencija (engl. *Artificial General Intelligence* - UOI) predstavlja sljedeći korak u razvoju umjetne inteligencije, s ciljem da računalni sustavi postignu sposobnosti slične ljudskom umu u različitim područjima. Dok su trenutne UI tehnologije, poznate kao usko specijalizirane UI (engl. *Narrow AI*), usmjerene na izvršavanje specifičnih zadataka s visokim stupnjem učinkovitosti, UOI ima za cilj razviti strojeve koji mogu razumjeti, učiti i izvoditi bilo koji intelektualni zadatak koji je u stanju obavljati ljudsko biće.

UOI se razlikuje od uske UI po svojoj sposobnosti autonomnog funkcioniranja, učenja u općim okvirima i prilagođavanja različitim situacijama, što joj omogućava da donosi odluke i poduzima radnje bez stalnog nadzora čovjeka. Fleksibilnost i autonomnost omogućavaju UOI-u učinkovito prilagođavanje složenim i dinamičnim okruženjima.

Razvoj UOI-a zahtijeva interdisciplinarnu suradnju, koja obuhvaća područja kao što su računalne znanosti, kognitivna psihologija, neurologija i filozofija. Za postizanje UOI-a, istraživači moraju razumjeti osnovne principe ljudske spoznaje i replicirati te procese u računalima, uz istovremeno unapređenje računalnih kapaciteta UI sustava.[34]

[33] Foster, D. (2023). *Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play* (2nd ed.). O'Reilly Media.
[34] Latif, E., et al. (2023). *Artificial General Intelligence (AGI) for Education*. AI4STEM Education Center, University of Georgia, str. 2-4.

5.4. UMJETNA INTELIGENCIJA KAO ALAT BORBE PROTIV TERORIZMA

U proteklih nekoliko desetljeća, svijet se suočio s rastućim prijetnjama terorizma koje su postale sve inovativnije i raširenije. Terorističke skupine su se razvile u smjeru u kojem planiraju i izvode napade koristeći nove tehnologije, internet i društvene medije za širenje svoje ideologije i koordinaciju svojih aktivnosti. Nacionalne sigurnosne agencije okrenule su se novim alatima i tehnologijama kako bi učinkovito odgovorile na novonastale prijetnje. Među njima, umjetna inteligencija se istaknula kao ključni alat za analizu podataka, predikciju prijetnji i poboljšanje operativne učinkovitosti.

UI, s naglaskom na strojno učenje i duboko učenje, omogućila je razvoj naprednih sustava koji mogu analizirati velike količine podataka u stvarnom vremenu, prepoznati obrasce koji bi mogli ukazivati na terorističke aktivnosti i automatski reagirati na prijetnje. Ovo poglavlje istražuje povijest razvoja UI -a u kontekstu nacionalne sigurnosti, te analizira kako se ova tehnologija koristi u borbi protiv terorizma.

5.4.1. Kratka povijest primjene UI u nacionalnoj sigurnosti

Primjena umjetne inteligencije u nacionalnoj sigurnosti ima svoje korijene u sredini 20. stoljeća, kada su računalne tehnologije počele igrati važnu ulogu u vojnim i obavještajnim operacijama. Tijekom hladnog rata, Sjedinjene Američke Države i njihovi saveznici suočili su se s potrebom za naprednim alatima koji bi im omogućili učinkovito upravljanje sve složenijim sigurnosnim izazovima. U tom kontekstu, Agencija za napredna obrambena istraživanja (engl. *Defense Advanced Research Projects Agency* - DARPA) bila je jedna od ključnih institucija koja je pokrenula istraživanje i razvoj UI-a za vojne i sigurnosne svrhe.[35]

Rane UI tehnologije bile su primitivne u usporedbi s današnjim standardima, ali su pružile temelje za buduće napretke. Fokus je bio na razvoju sustava koji bi mogli pomoći u analizi obavještajnih podataka, automatizaciji određenih vojnih procesa i podršci u donošenju odluka na strateškoj razini. Takvi sustavi bili su posebno korisni za kodiranje i dešifriranje komunikacija, analizu

[35] Whitlock, C., Strickland, F. (2023). *Winning the National Security AI Competition: A Practical Guide for Government and Industry Leaders*. Apress, str. 209

velikih količina podataka iz različitih izvora te za simulaciju i modeliranje različitih scenarija u vojnom kontekstu. Tijekom 1980-ih i 1990-ih godina, razvoj računalnih tehnologija i algoritama strojnog učenja omogućio je znatno širu primjenu UI tehnologija u nacionalnoj sigurnosti. U tom razdoblju, UI je počeo igrati ključnu ulogu u obradi i analizi velikih skupova podataka, što je bilo od vitalne važnosti za obavještajne agencije koje su se suočavale s velikim količinama informacija iz različitih izvora.

Jedan od primjera primjene UI u to vrijeme bila je automatska analiza satelitskih snimaka.[36] Ovi sustavi omogućili su obavještajnim službama bržu i precizniju identifikaciju objekata i aktivnosti na terenu, što je bilo ključno za nadzor nad potencijalnim prijetnjama i planiranje vojnih operacija. Uz to, UI je korišten za simulacije vojnih scenarija, što je omogućilo optimizaciju strategija i procjenu mogućih ishoda različitih vojnih intervencija.

U ovom razdoblju također je došlo do razvoja prvih prediktivnih sustava koji su koristili UI za analizu povijesnih podataka i predviđanje budućih prijetnji. Navedeni sustavi su omogućili obavještajnim agencijama da unaprijed prepoznaju obrasce ponašanja koji bi mogli ukazivati na potencijalne sigurnosne rizike, čime su povećali sposobnost proaktivnog djelovanja. [37]

5.4.2. Primjena umjetne inteligencije u analizi podataka

Jedan od glavnih izazova s kojima se sigurnosne agencije suočavaju u borbi protiv terorizma jest obrada ogromnih količina podataka prikupljenih iz različitih izvora. Tradicionalne metode analize podataka često su nedostatne zbog količine i složenosti informacija koje treba obraditi. Umjetna inteligencija nudi inovativne pristupe koji omogućuju učinkovitiju analizu podataka.

5.4.2.1. Analiza podataka s društvenih mreža (SOCMINT)

Društvene mreže postale su jedno od glavnih sredstava komunikacije i širenja informacija, uključujući i one povezane s terorizmom. Sigurnosne agencije koriste UI za praćenje i analizu

[36] Whitlock, C., Strickland, F. (2023). *Winning the National Security AI Competition: A Practical Guide for Government and Industry Leaders*. Apress, str. 85.
[37] Montasari, R. (2022). The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights. *Artificial Intelligence and National Security*. Springer, str. 180.

komunikacija na društvenim mrežama (engl. *Social Media Intelligence* - SOCMINT) kako bi identificirale potencijalno radikalizirane pojedince i grupe. Algoritmi strojnog učenja mogu prepoznati obrasce u jeziku, frazama i slikama koje ukazuju na ekstremističke sklonosti. Na primjer, određeni izrazi, simboli ili *hashtagovi* mogu signalizirati povezanost s terorističkim organizacijama. Osim toga, UI može automatski pratiti promjene u ponašanju korisnika na društvenim mrežama, kao što su iznenadne promjene u interesima ili učestalo sudjelovanje u raspravama vezanim za nasilne ideologije. Dobiveni podaci mogu se koristiti za izradu profiliranja pojedinaca koji bi mogli predstavljati prijetnju, što omogućuje sigurnosnim agencijama da na vrijeme poduzmu odgovarajuće mjere.[38]

Korisnici društvenih mreža često nesvjesno odaju informacije koje bi inače nerado podijelili, posebno s organima reda, što čini SOCMINT izuzetno učinkovitim alatom za prepoznavanje potencijalnih prijetnji. SOCMINT se već koristi u različitim fazama imigracijskih procedura, posebno u kontekstu vizne obrade.[39] Na primjer, informacije s društvenih mreža mogu otkriti ekstremističke stavove, kriminalnu prošlost ili druge čimbenike koji bi mogli dovesti do odbijanja vize. Korištenje ovih tehnika u procesu imigracije pomaže u otkrivanju pojedinaca sklonih nasilnom ekstremizmu ili onih koji imaju namjeru prekršiti uvjete vize.

Međutim, implementacija SOCMINT-a u imigracijske procedure nosi i određene rizike i izazove. Najveći problem predstavlja verifikacija identiteta na mreži, s obzirom na to da korisnici često koriste pseudonime ili lažne profile. Također, jezične i kulturološke barijere mogu otežati pravilno tumačenje objava na društvenim mrežama.

5.4.2.2. Otvoreni izvori informacija (OSINT)

Pored društvenih mreža, UI se također koristi za analizu podataka iz otvorenih izvora (eng. *Open Source Intelligence* - OSINT), kao što su vijesti, blogovi, forumi i druge *online* platforme. Ovi izvori često sadrže vrijedne informacije koje mogu pomoći u prepoznavanju i sprječavanju

[38] National Cyber Crime Research & Innovation Centre. (2021). *Manual on Social Media Intelligence (SOCMINT) for Law Enforcement Agencies*. Bureau of Police Research & Development, Ministry of Home Affairs, Government of India.
[39] Lewulis, Piotr. (2024). Social Media Intelligence as a Tool for Immigration and National Security Purposes. *Internal Security Review*. ResearchGate, str. 407-408.

terorističkih prijetnji. Jedna od ključnih prednosti OSINT-a je pristup velikom broju javno dostupnih podataka, uključujući informacije s interneta, društvenih mreža, medija i raznih baza podataka. Ove informacije mogu biti iznimno korisne za analizu terorističkih prijetnji i identificiranje potencijalnih terorista. Posebno se ističe važnost korištenja znanstvenih baza podataka koje sadrže informacije o terorističkim napadima, kao i platformi koje omogućuju praćenje *online* aktivnosti povezanih s terorizmom.

Andrić, u svom radu, naglašava da su teroristi vrlo vješti u korištenju suvremenih tehnologija, uključujući šifriranu komunikaciju i kibernetičke napade, što dodatno komplicira borbu protiv terorizma. Kako bi se potencijalne prijetnje prepoznale na vrijeme, za nacionalne sigurnosne agencije, ključno je korištenje sofisticiranih alata za analizu podataka. Jedan od primjera takvih alata je platforma TANGELS, koja koristi tehnologije umjetne inteligencije za automatsko pretraživanje i analizu podataka s interneta, uključujući duboki i površinski *web*.[40]

5.4.2.3. Prikupljanje i analiza velike količine podataka („Big Data“)

UI omogućava sigurnosnim agencijama obradu velike količine podataka iz različitih izvora u stvarnom vremenu. Zahvaljujući naprednim algoritmima za prepoznavanje obrazaca i anomalija u podacima, agencije mogu otkriti i prevenirati terorističke aktivnosti. Na primjer, UI može analizirati transakcije na bankovnim računima, obrasce putovanja ili komunikacijske podatke kako bi se identificirale sumnjive aktivnosti koje bi mogle ukazivati na planiranje terorističkog napada.[41]

Jedan od glavnih aspekata primjene UI u borbi protiv terorizma unutar NATO-a jest analiza podataka prikupljenih s raznih senzora i nadzornih sistema. Umjetna inteligencija može brzo obraditi ogromne količine informacija, otkrivajući uzorke i anomalije koje bi mogle ukazivati na terorističke aktivnosti. Navedeno je posebno važno u kontekstu prepoznavanja i neutralizacije improviziranih eksplozivnih naprava (engl. *Improvised Explosive Devices* - IED), koji predstavljaju značajnu prijetnju vojnicima i civilima u sukobima diljem svijeta. Osim za prepoznavanja i neutralizacije IED-a, UI također igra važnu ulogu u obrani od bespilotnih letjelica

[40] Andrić, J., Terzić, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. *International Journal of Information and Operations Management Education*, 17(1), str. 6-9.
[41] Akilli, E. (2024). *Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics, and Privacy*. SETA, str. 3.

koje terorističke grupe sve češće koriste za izviđanje, prikupljanje informacija, pa čak i za napade. NATO koristi UI za razvoj sustava koji mogu identificirati, pratiti i neutralizirati ove prijetnje u realnom vremenu.[42]

5.4.3. Prediktivna analitika u prevenciji terorističkih napada

Prediktivna analitika je još jedno područje u kojem UI igra ključnu ulogu u borbi protiv terorizma. Korištenjem povijesnih podataka o prethodnim terorističkim aktivnostima, UI modeli mogu identificirati obrasce koji ukazuju na povećani rizik od budućih napada. Koristeći napredne tehnike analize podataka ovi modeli mogu predvidjeti gdje i kada bi se mogli dogoditi napadi, omogućavajući sigurnosnim agencijama proaktivno djelovanje.

5.4.3.1. Prediktivni modeli

Primjena umjetne inteligencije nije ograničena samo na tehnologiju detekcije i neutralizacije prijetnji. Ista je, također, ključna u unaprjeđenju strategija za obranu kritične infrastrukture, kao što su energetski resursi, komunikacijske mreže i transportni sustavi. UI omogućuje preciznije modeliranje potencijalnih napada i razvoj učinkovitih protumjera, što je posebno važno u urbanim sredinama, gdje teroristički napadi mogu imati katastrofalne posljedice.[43]

Prediktivni modeli UI koriste se za analizu širokog spektra podataka, uključujući povijesne podatke o terorističkim napadima, društveno-političke uvjete, geografske informacije i druge varijable koje mogu utjecati na pojavu terorizma. Ovi modeli omogućuju sigurnosnim agencijama identificiranje visoko rizične lokacije i vremenske okvire, što im pomaže u raspoređivanju resursa na najugroženija područja.

Korištenjem podataka o komunikaciji, financijskim transakcijama, kretanjima osoba i ponašanjima na društvenim mrežama, UI modeli mogu prepoznati obrasce koji se ne bi lako uočili tradicionalnim metodama analize. Ovi obrasci omogućavaju stvaranje prediktivnih modela koji pomažu u identificiranju potencijalnih prijetnji prije nego što se dogode. Na primjer, kako navodi

[42] Countering Terrorism. NATO. Dostupno na: https://www.nato.int/cps/en/natohq/topics_77646.htm (5.8.2024.)
[43] Isto

Akili, UI može analizirati povijesne podatke o prethodnim terorističkim napadima, uključujući vrijeme, mjesto, metode i motive napada, i stvoriti prediktivne modele. Isti zatim mogu predložiti vjerojatnost novih napada na temelju sličnosti s prethodnim incidentima ili identificiranih obrazaca u ponašanju pojedinaca ili grupa.[44]

5.4.3.2. Identifikacija ranjivih skupina

Prediktivna analitika također može pomoći u identifikaciji ranjivih skupina koje su podložne radikalizaciji. Korištenjem podataka o demografiji, društvenim i ekonomskim uvjetima, UI modeli mogu prepoznati skupine ljudi koji su podložniji utjecaju terorističkih ideologija.[45] Sigurnosne agencije i vlade na taj način mogu poduzeti preventivne mjere, poput obrazovnih programa ili socijalnih inicijativa, kako bi spriječili radikalizaciju u zajednicama.

Sustavi za detekciju anomalija pokretani UI tehnologijom igraju ključnu ulogu u prepoznavanju neobičnih obrazaca u financijskim transakcijama, putovanjima i *online* komunikacijama. Ovi sustavi su dizajnirani za identifikaciju odstupanja od normalnog ponašanja koja mogu ukazivati na pripremu terorističkih aktivnosti. Na primjer, neuobičajeno velike transakcije na računima, neobični obrasci putovanja ili sumnjive *online* aktivnosti mogu biti označene kao potencijalne prijetnje.

Jedna od ključnih prednosti UI u ovom kontekstu je sposobnost obrade velikih količina podataka u stvarnom vremenu, što omogućuje brzu reakciju na potencijalne prijetnje. Međutim, ova tehnologija također postavlja izazove u smislu smanjenja broja lažno pozitivnih rezultata, kao i održavanja privatnosti pojedinaca.[46]

[44] Akilli, E. (2024). *Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics, and Privacy*. SETA, str. 2.
[45] Montasari, R. (2022). The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights. *Artificial Intelligence and National Security*. Springer, str. 33-34.
[46] McKendrick, K. (2019). *Artificial Intelligence Prediction and Counterterrorism*. International Security Department, Chatham House, str. 12.

5.4.4. Uklanjanje terorističkog sadržaja s interneta

Internet je postao glavno sredstvo za širenje terorističke propagande i radikalizaciju pojedinaca. Terorističke organizacije koriste društvene mreže, blogove i druge *online* platforme kako bi promovirale svoje ideologije, regrutirale nove članove i planirale napade. UI se koristi za automatsko otkrivanje i uklanjanje terorističkog sadržaja s navedenih platformi, što je ključni korak u sprječavanju širenja nasilnih ideologija.[47]

UI koristi napredne algoritme za prepoznavanje terorističkog sadržaja na internetu. Ovi algoritmi analiziraju tekstualne, vizualne i video sadržaje kako bi identificirali ključne riječi, fraze i slike koje su povezane s terorizmom. UI tehnologije, poput modela za obradu prirodnog jezika i konvolucijskih neuronskih mreža mogu prepoznati nasilne videozapise ili slike koje prikazuju terorističke napade, kao i tekstove koji promoviraju nasilje ili mržnju.

Akili naglašava da je učinkovitost ovih alata usko povezana s njihovom sposobnošću razumijevanja konteksta i nijanse sadržaja, čime se smanjuje vjerojatnost pogrešne cenzure legitimnog sadržaja dok se točno prepoznaju stvarne prijetnje. UI tehnologije su značajno ubrzale proces otkrivanja i uklanjanja terorističkog sadržaja s interneta, a zahvaljujući naprednom algoritamskom pristupu, sadržaji povezani s terorizmom mogu biti otkriveni i uklonjeni unutar 15 do 20 minuta od trenutka kada su postavljeni na mrežu.[48] Vrijeme reakcije je od iznimne važnosti s obzirom na brzinu kojom se sadržaj može širiti na društvenim mrežama.

Unatoč navedenim prednostima, implementacija ovih tehnologija suočava se s izazovima, uključujući ograničenja podataka i različite metode koje teroristi koriste za prikrivanje svojih aktivnosti. Identifikacija obrazaca među različitim skupovima podataka, kao i složenost podataka, može otežati točnost algoritama, što zahtijeva kontinuirano usavršavanje i prilagodbu ovih sustava kako bi bili što učinkovitiji u prepoznavanju i uklanjanju terorističkog sadržaja s interneta. Također, terorističke organizacije se neprestano prilagođavaju i mijenjaju načine i platforme za objavu ekstremističkog sadržaja i planiranje terorističkih aktivnosti kako bi umanjile vjerojatnost otkrivanja.

[47] Akilli, E. (2024). *Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics, and Privacy*. SETA, str. 4.
[48] Isto, str. 4.

5.4.5. Tehnologija prepoznavanja lica

Tehnologija prepoznavanja lica postala je jedno od najkontroverznijih oruđa u borbi protiv terorizma. Integrirana s UI sustavima, ista omogućava sigurnosnim agencijama identifikaciju i praćenje osumnjičenih terorista u stvarnom vremenu, koristeći nadzorne kamere postavljene na javnim mjestima.

Navedena tehnologija prepoznavanja lica temelji se na naprednim algoritmima koji analiziraju i uspoređuju lica s postojećim bazama podataka kako bi se utvrdio identitet pojedinaca. Ista omogućava skeniranje lica u masi i uspoređuje ih s bazama podataka koje sadrže slike poznatih ili osumnjičenih terorista. Na primjer, kamere s integriranom UI mogu u stvarnom vremenu prepoznati lica i povezati ih s osobama koje su u bazi podataka, čime se omogućuje brza identifikacija potencijalnih prijetnji.[49] Primjena prepoznavanja lica posebno je korisna na mjestima s velikim brojem ljudi, poput zračnih luka, željezničkih stanica i velikih događaja.

Uz prepoznavanje lica, tehnologija obrade slike također igra ključnu ulogu u otkrivanju prijetnji. Ista može identificirati i analizirati objekte na slikama ili videozapisima. Na primjer, UI sustavi sada mogu prepoznati oružje u javnim prostorima, kao što su škole, aerodromi ili korporativni kampusi. Algoritmi mogu analizirati videozapise sa sigurnosnih kamera kako bi otkrili potencijalno opasne objekte, kao što su pištolji ili noževi, i odmah upozoriti sigurnosno osoblje.[50]

Navedene tehnologije se često oslanjaju na postojeće mreže kamera u velikim javnim prostorima. Na primjer, kada sustav prepozna oružje u videu, prvo ga označava kao sumnjiv objekt, a zatim brzo podiže nivo upozorenja ako je potrebno. Sigurnosni službenici mogu dobiti obavijest na svoje mobilne uređaje zajedno sa slikom na kojoj je detaljno prikazano oružje i identificirana sumnjiva osoba. Ovaj proces omogućuje brzo donošenje odluka o tome hoće li se aktivirati hitne službe ili se upozorenje može odbaciti kao lažna uzbuna.[51]

[49] Akilli, E. (2024). *Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics, and Privacy*. SETA, str. 2-3.
[50] Isto, str. 2-3.
[51] Isto, str. 2-3.

5.5. OPASNOST MASOVNE PRIMJENE UMJETNE INTELIGENCIJE

Uvođenje umjetne inteligencije u različite aspekte društva donosi neosporne koristi, ali također otvara vrata brojnim izazovima i rizicima koji zahtijevaju pažljivo razmatranje. Kako UI tehnologije postaju sve prisutnije, raste zabrinutost zbog njihovog potencijala narušavanja temeljnih ljudska prava, privatnosti i etičkih normi. Masovna primjena UI u područjima poput nacionalne sigurnosti, nadzora i manipulacije informacijama ne samo da može ugroziti individualne slobode, već može destabilizirati i globalne geopolitičke odnose. U daljnjem tekstu razmatraju se ključne opasnosti povezane s masovnom primjenom umjetne inteligencije, uključujući etičke dileme, prijetnje privatnosti, manipulaciju informacijama i geopolitičke implikacije. Ove teme postaju sve relevantnije kako UI postaje neizbježan alat u oblikovanju budućnosti društava širom svijeta.

5.5.1. Etika i pristranost

Primjena UI u borbi protiv terorizma neizbježno otvara pitanja o etičnosti takvih postupaka. Sigurnosne agencije koriste UI kako bi prikupile i analizirale podatke, često bez znanja ili pristanka pojedinaca, što može dovesti do ozbiljnih kršenja privatnosti i drugih osnovnih prava. Na primjer, masovno nadziranje društvenih mreža može se smatrati oblikom špijuniranja, posebno ako se provodi bez odgovarajuće pravne regulative.

Etnička profiliranja i diskriminacija također su veliki rizici kod primjene UI tehnologija. Algoritmi strojnog učenja često se treniraju na povijesnim podacima koji mogu biti pristrani, što znači da UI sustavi mogu donositi odluke koje su pristrane prema određenim skupinama. Pristranost može rezultirati neproporcionalnim nadzorom ili sumnjom na određene etničke ili vjerske skupine, što dodatno pogoršava društvene nejednakosti. Postoji rizik da upotreba UI u nadzoru i praćenju bude zloupotrijebljena za ciljanje pojedinaca ili grupa na temelju njihovih uvjerenja, političkih stavova, religijskih opredjeljenja ili drugih osobnih karakteristika. U ovim situacijama, može se dodatno narušiti povjerenje građana u državne institucije i sustave za provođenje zakona, te potkopati osnovna ljudska prava.

Kako bi se izbjegle ove etičke dileme, potrebno je uspostaviti jasne smjernice i pravne okvire koji će regulirati upotrebu UI u sigurnosnim kontekstima. To uključuje transparentnost u korištenju tehnologije, osiguravanje odgovornosti za eventualne zloupotrebe i promicanje jednakosti i nediskriminacije u svim aspektima borbe protiv terorizma.

5.5.2. Privatnost

Primjena umjetne inteligencije, također, izaziva ozbiljne zabrinutosti u vezi s privatnošću i građanskim slobodama. UI omogućava prikupljanje i analizu velikih količina podataka, uključujući osobne informacije, društvene interakcije i obrasce ponašanja, što može dovesti do značajnih povreda privatnosti.

Zabrinutost proizlazi iz mogućnosti da nevini pojedinci budu označeni kao potencijalne prijetnje na temelju algoritama koji analiziraju njihove *online* aktivnosti. Algoritmi mogu pogrešno identificirati nekoga kao sumnjivog, što može dovesti do neopravdanog nadzora, praćenja ili čak pravnih posljedica. To izaziva ozbiljna pitanja o pravu na privatnost, posebno u društvima koja se temelje na liberalno-demokratskim vrijednostima. Zloupotreba ovih tehnologija u represivne svrhe mogla bi dovesti do erozije demokratskih sloboda i stvaranja nadzornog društva u kojem su građani stalno pod paskom.[52]

Postoji rizik da tehnologija prepoznavanja lica bude korištena za profiliranje određenih etničkih ili vjerskih skupina, što može dovesti do diskriminacije i nepravde. Stoga je ključno osigurati da se ova tehnologija koristi u skladu s etičkim smjernicama i pravnim standardima, kako bi se zaštitila prava pojedinaca dok se istovremeno osigurava javna sigurnost.[53]

Kako navodi Montasari, jedan od većih rizika predstavlja takozvani kumulativni rizik intruzije, gdje se interakcijom automatiziranih sustava stvara mreža povezanih sustava za prikupljanje podataka, koja može rezultirati većim narušavanjem privatnosti nego kada su ti sustavi izolirani.

[52] Ganor, B. (2021). Artificial or Human: A New Era of Counterterrorism Intelligence? *Studies in Conflict and Terrorism,* str. 605–624.
International terrorism and Social threats of artificial intelligence - Yaser Esmailzadeh
[53] Cataleta, M. S. (2020). *Humane Artificial Intelligence: The Fragility of Human Rights Facing AI*. East-West Center.

Uređaji temeljeni na internetu stvari (engl. *Internet-of-Things* - IoT), poput Apple Siri i Amazon Alexa, prikupljaju velike količine osobnih podataka, što izaziva ozbiljne zabrinutosti. Tako dobiveni podaci koriste se za profiliranje korisnika, a postoji opasnost da prikupljeni podaci postanu dostupni trećim stranama, čime se dodatno narušava privatnost.[54]

Emocionalna UI, koja se koristi za prepoznavanje i analizu emocija korisnika putem biometrijskih podataka, dodatno komplicira problem privatnosti. Problem nastaje kada podaci prikupljeni profiliranjem postanu dostupni trećim stranama ili se koriste za donošenje odluka u područjima kao što su osiguranje ili sigurnost.[55]

Posebno je problematičan paradoks između želje korisnika za personaliziranim uslugama i potrebe za zaštitom njihove privatnosti. Ovaj paradoks je posebno ilustriran u slučaju skandala s Cambridge Analyticom, gdje su podaci korisnika Facebooka neovlašteno korišteni za političko oglašavanje. Ovaj skandal pokazuje kako podaci prikupljeni za jednu svrhu mogu biti zloupotrijebljeni, što dovodi do ozbiljnih posljedica po privatnost korisnika, ali i po demokratske procese.[56]

5.5.3. Manipulacija informacijama i psihološki rat

UI tehnologije omogućuju stvaranje lažnih vijesti i *deepfake* sadržaja koji se mogu koristiti za manipulaciju javnim mnijenjem i destabilizaciju društava. Korištenje UI u psihološkom ratovanju može narušiti povjerenje u institucije i medije, te izazvati društvene sukobe. Dugoročne posljedice ovakvih strategija uključuju smanjenje društvene kohezije i potencijalno poticanje unutarnjih nemira u ciljnim zemljama.

Russell, kao jedan od ozbiljnih rizika masovne primjene umjetne inteligencije, ističe mogućnost zloupotrebe iste. UI bi mogao biti korišten od strane zlonamjernih aktera, poput autoritarnih vlada ili kriminalnih organizacija, za nadzor, manipulaciju informacija, ili čak za provođenje ratnih operacija s minimalnim ljudskim uključivanjem. Takva primjena umjetne inteligencije mogla bi

[54] Montasari, R. (2023). *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. Springer Nature Switzerland AG, str. 72-73
[55] Isto, str. 73.
[56] Isto, str. 76.

destabilizirati društva i ugroziti globalnu sigurnost, stvarajući nove oblike prijetnji koje dosad nisu postojale.[57]

Esmailzadeh upozorava na ozbiljnu prijetnju manipulacijom informacijama kroz upotrebu umjetne inteligencije (UI), posebno u kontekstu širenja propagande i dezinformacija.[58] Algoritmi UI mogu se koristiti za analizu društvenih mreža i drugih *online* platformi kako bi identificirali pojedince koji su najosjetljiviji na ekstremističke poruke. Zatim, ove osobe mogu biti ciljano izložene personaliziranom sadržaju koji pojačava njihove radikalne stavove i potiče ih na nasilne aktivnosti.

Jedna od glavnih opasnosti koje Esmailzadeh ističe je mogućnost da terorističke grupe koriste UI za stvaranje i širenje propagande i dezinformacija na velikoj skali, koristeći UI-pokretane botove i algoritme za automatsko generiranje i distribuciju sadržaja. Ove kampanje mogu biti dizajnirane kako bi ciljale specifične demografske grupe, manipulirale javnim mnijenjem i širile lažne ili obmanjujuće informacije.[59]

Poseban izazov predstavlja činjenica da UI može prilagoditi i optimizirati propagandu u realnom vremenu, temeljem reakcija korisnika, čime se povećava njezina učinkovitost i doseg. Sposobnost manipulacije informacijama pomoću UI predstavlja značajnu prijetnju globalnoj sigurnosti i društvenoj stabilnosti, te zahtijeva razvoj novih strategija i tehnologija za otkrivanje i suzbijanje UI-generirane propagande i dezinformacija.

5.5.4. Geopolitičke implikacije

Razvoj umjetne inteligencije donosi sa sobom značajne geopolitičke posljedice koje imaju potencijal preoblikovati globalne odnose moći i međunarodnu sigurnost. Kako napredak u UI i robotici postaje sve prisutniji, stručnjaci upozoravaju na mogućnost pojave nove velike sile u ovom području. Države koje prednjače u razvoju i primjeni UI tehnologija mogle bi steći stratešku prednost nad svojim suparnicima, što bi moglo dovesti do nove faze geopolitičkog natjecanja.

[57] Russell, S. (2019). *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking, str. 112-115.
[58] Esmailzadeh, Y., & Motaghi, E. (2024). International terrorism and social threats of artificial intelligence. *Journal of Globalization Studies*, 15(1), str. 172-173.
[59] Isto, str. 174.

Nova geopolitika umjetne inteligencije može utjecati na dinamiku globalnih odnosa moći, jer dominacija u UI postaje ključni faktor u oblikovanju međunarodne politike i ekonomije.

Jedna od najvažnijih implikacija razvoja umjetne inteligencije je njen utjecaj na vojne operacije i oružane sukobe. UI tehnologije omogućavaju razvoj autonomnih oružanih sustava, sofisticirane analize podataka za planiranje vojnih operacija i mogućnost provođenja preciznih napada s minimalnim ljudskim uplitanjem. Tehnološke inovacije redefinirat će karakteristike ratovanja, čime će se promijeniti i strategije država u vođenju vojnih operacija. Sve navedeno će imati duboke strateške posljedice za globalnu sigurnost, jer će UI tehnologije i koncepti u ratovanju postati sve važniji u budućim sukobima.

Promjene koje donosi UI također će imati utjecaj na međunarodne saveze i političke odnose. Kako države prilagođavaju svoje strategije da bi se nosile s novim tehnološkim izazovima, geopolitička dinamika bit će značajno promijenjena. Osim toga, UI će igrati ključnu ulogu u oblikovanju budućih konflikata, ekonomskih odnosa i globalne politike.

U konačnici, razvoj umjetne inteligencije donosi sa sobom ne samo tehnološke inovacije već i značajne geopolitičke promjene koje će oblikovati globalnu sigurnost i odnose moći u nadolazećim desetljećima.

5.6. STUDIJA SLUČAJA („CASE STUDY“) – ANALIZA DRUŠTVENE MREŽE TIKTOK

Društvene mreže postale su sastavni dio svakodnevnog života, omogućujući ljudima širom svijeta povezivanje, dijeljenje informacija i komunikaciju na dosad neviđene načine. Međutim, uz brojne prednosti koje donose, društvene mreže također postaju alat koji terorističke skupine koriste za svoje zlonamjerne aktivnosti. TikTok, kao jedna od najpopularnijih platformi među mlađom populacijom, sve češće privlači pažnju zbog potencijala za zloupotrebu u terorističke svrhe. Njegova masovna popularnost, jednostavnost u kreiranju sadržaja te algoritmi koji omogućuju viralnost videozapisa čine ga posebno pogodnim za širenje ekstremističkih ideologija, regrutaciju novih članova, pa čak i organizaciju napada. Unatoč naporima platforme da spriječi zloupotrebe, terorističke skupine pronašle su načine kako iskoristiti TikTok za promicanje svojih ciljeva, često prikrivajući svoj sadržaj kroz popularne trendove i *meme* kulturu, čime dodatno povećavaju doseg svojih poruka i otežavaju njihovo prepoznavanje.

5.6.1. TikTok analiza

Ciarán O’Connor u svojom izvješću *„Hatescape: An In-Depth Analysis of Extremism and Hate Speech on TikTok”* pruža sveobuhvatan uvid u način na koji se ekstremističke ideologije i govor mržnje šire na jednoj od najpopularnijih društvenih platformi današnjice, TikToku. O'Connorov izvještaj, temeljen na istraživanju provedenom tijekom tri mjeseca, analizirao je više od tisuću videozapisa kako bi se razumjela dinamika širenja mržnje i ekstremizma na platformi. U istraživanju su identificirani ključni načini na koje se TikTok koristi za promoviranje tzv. nadmoći bijelaca (engl. *White supremacy*), podršku terorističkim organizacijama te negiranje povijesnih događaja poput holokausta.[60]

[60] O’Connor, C. (2021). *Hatescape: An in-depth analysis of extremism and hate speech on TikTok*. Institute for Strategic Dialogue. Dostupno na: https://www.isdglobal.org/isd-publications/hatescape-an-in-depth-analysis-of-extremism-and-hate-speech-on-tiktok/ (3.8.2024.)

5.6.1.1. Alat za širenje mržnje

TikTok je platforma koja je privukla stotine milijuna korisnika širom svijeta, zahvaljujući svojoj jednostavnosti korištenja i mogućnosti za stvaranje i dijeljenje kratkih videozapisa. No, kako izvještaj pokazuje, ta ista platforma pruža prostor i onima koji žele širiti mržnju i ekstremizam. Autori izvještaja identificirali su 312 videozapisa koji promiču nadmoć bijelaca, što čini 30% analiziranog uzorka. Ti videozapisi često koriste teorije zavjere kao što su takozvana „velika zamjena“ i „bijeli genocid“ kako bi opravdali svoje stavove. Prema navedenim teorijama zavjere, bijelci su namjerno zamijenjeni drugim rasama kroz migracije i demografske promjene, što je ideologija koja je poslužila kao motivacija za brojne terorističke napade, uključujući napad na džamije u Christchurchu 2019. godine.

Jedna od ključnih točaka izvještaja jest analiza kako TikTokove funkcije, poput „duetiranja“, „hashtagova“, te video efekata, mogu biti korištene za širenje mržnje. Na primjer, funkcija „duet“ omogućuje korisnicima kreiranje videozapisa koji se pojavljuju uz već postojeći sadržaj, što se može koristiti za ciljanje i napadanje drugih korisnika na temelju njihovih zaštićenih osobina kao što su rasa, religija ili spolna orijentacija. U izvještaju se također navodi da ekstremisti koriste popularne *hashtagove* kao što su #fyp i #foryou kako bi proširili doseg svojih videozapisa i došli do šire publike.

Negiranje holokausta i širenje antisemitizma predstavljaju još jedan ozbiljan problem na TikToku. U istraživanju je identificirano 26 videozapisa koji negiraju postojanje holokausta ili koriste kodirane reference kako bi promovirali antisemitizam. Detektirani videozapisi variraju od onih koji izravno negiraju da se holokaust ikada dogodio, do onih koji koriste zagonetne kodove i simbole kako bi zaobišli algoritme za prepoznavanje mržnje na TikToku. Zabrinjavajuća je činjenica da ovakav tip sadržaja i dalje pronalaze put do publike, što ukazuje na potrebu za strožim nadzorom i moderiranjem sadržaja na platformi.

5.6.1.2. Glorifikacija ekstremista i terorista

Izvještaj, također, otkriva zabrinjavajuće visoku razinu podrške ekstremistima i teroristima na TikToku. Od 1.030 analiziranih videozapisa, 246 (24%) veliča ili promovira pojedince i organizacije povezane s ekstremizmom i terorizmom. Među najčešće spominjanim osobama su

Adolf Hitler, Ratko Mladić i Brenton Tarrant, napadač iz Christchurcha. U izvještaju se ističe da je posebno alarmantno što je velik broj videozapisa koji podržavaju Tarranta i dalje dostupan na platformi, unatoč TikTokovim pravilima protiv promicanja nasilnog ekstremizma.

Sadržaji povezani s ISIS-om također su prisutni na TikToku. Istraživači su identificirali videozapise koji sadrže propagandni materijal spomenute terorističke organizacije, uključujući snimke egzekucija i napada automobilima bombama. Videozapisi ne samo da glorificiraju nasilje, već također služe kao alat za regrutiranje novih članova i širenje njihove ideologije.

5.6.1.3. Neadekvatno uklanjanje sadržaja

Iako TikTok ima pravila i smjernice protiv promicanja mržnje i ekstremizma, izvještaj pokazuje da uklanjanje sadržaja nije dosljedno. Samo 18,5% videozapisa u uzorku uklonjeno je do kraja istraživanja, dok je preostalih 81,5% i dalje bilo dostupno na platformi u trenutku pisanja izvještaja. Podaci ukazuju na ozbiljne propuste u provedbi TikTokovih pravila i naglašava potrebu za poboljšanjem mehanizama moderiranja sadržaja.

Izvještaj *„Hatescape“* jasno pokazuje da TikTok, unatoč svojim naporima, nije uspio u potpunosti suzbiti širenje ekstremizma i govora mržnje na svojoj platformi. Dok je TikTok popularan među mladima zbog svoje kreativnosti i mogućnosti za izražavanje, ta ista platforma također služi kao alat za one koji žele širiti mržnju i ekstremizam. Potrebne su strože mjere nadzora i uklanjanja sadržaja, kao i veća transparentnost i odgovornost platforme u borbi protiv ovih štetnih pojava. Izvještaj poziva na hitne akcije kako bi se spriječilo daljnje širenje mržnje i osiguralo sigurnije okruženje za sve korisnike.

5.6.2. Aplikacija za analizu i detekciju terorističkog sadržaja na TikToku

Iako većina sadržaja na TikTok platformi ima zabavni karakter, porast broja korisnika donosi i povećan rizik od zloupotrebe platforme za širenje opasnog i nepoželjnog sadržaja, uključujući terorističke poruke i propagandu. S obzirom na ovu rastuću prijetnju, postala je očita potreba za alatom koji bi omogućio praćenje i analizu ove popularne društvene mreže kako bi se detektirao i uklonio teroristički sadržaj.

Aplikacija, razvijena kao alat za analizu i detekciju terorističkog sadržaja na TikToku, omogućuje korisnicima brzo pretraživanje i analizu videozapisa temeljenih na određenim *hashtagovima*, pružajući detaljne informacije koje pomažu u procjeni rizika i identifikaciji nepoželjnog sadržaja. Aplikacija koristi službeni TikTok API te je izrađena u Python programskom jeziku koristeći Streamlit *framework*, što omogućuje intuitivno i jednostavno sučelje za korisnike.

5.6.2.1. Funkcionalnosti aplikacije

1. Pretraga po *hashtagovima*

Jedna od glavnih funkcionalnosti aplikacije jest mogućnost pretraživanja sadržaja na TikToku putem specifičnih *hashtagova*. *Hashtagovi* su ključni element TikToka jer omogućuju grupiranje sadržaja oko određenih tema ili trendova. Korisnici aplikacije mogu unijeti određeni *hashtag* koji žele analizirati, a aplikacija će zatim pretražiti TikTok bazu podataka i dohvatiti sve videozapise koji su povezani s tim *hashtagom*.

Navedena funkcionalnost omogućuje brzu i učinkovitu analizu velikog broja videozapisa, što je posebno važno u situacijama kada je potrebno brzo reagirati na potencijalnu prijetnju. Pretraga po *hashtagovima* omogućuje korisnicima usmjeravanje svojih napora na specifične teme ili trendove koji su povezani s terorističkim sadržajem, što povećava efikasnost analize. Kao rezultat pretrage po određenom *hashtagu*, aplikacija prikazuje videozapise koji su objavljeni u posljednjih mjesec dana, sortirane po broju pregleda. Rezultate koje aplikacija daje za pretraživanje po *hashtagu* „palestine“ mogu se vidjeti na slici ispod.

Korisničko ime	Link na video	Broj pregleda	Broj lajkova	Broj komentara	Broj dijeljenja	Hashtagovi	Opis videa	Država
aymen_sahli11	https://www.tiktok.com/@aymen_sahli11/video/7404990513675291910	2386	12	1	0	love, like, messi, viral, foryou, ronaldo, palestine, lafar, minhadupla, ي…	#love #حبيض_ايمن #palestine #viral #CapCut #MinhaDupla #ي, #foryou …	DZ
fear.allah_quran	https://www.tiktok.com/@fear.allah_quran/video/7404998502125784…	2022	417	4	6	islam, palestine, fypシ゚, fupシ	Palestine ya Allah #fupシ #fypシ゚#islam #palestine	GB
km...love80	https://www.tiktok.com/@km...love80/video/7404987203975154962	1948	370	0	22	khan, palestine, fouryou, capcut	#CapCut #khan #fouryou #palestine @✌Pakhtoon😈🔥 @Kashif khan	PK
zlynnnnnn._	https://www.tiktok.com/@zlynnnnnn._/video/7404995954979491090	1943	15	0	0	viralvideo, fyp, palestine, fypage, tiktokshop, capcut, fypシviral, perfu…	yer sebab benda ni kena borong kalau beli satu tak pernah cukup ya #…	MY
johanjohari76	https://www.tiktok.com/@johanjohari76/video/7404999091719048455	1565	194	12	40	red, beach, mentalhealth, palestine, kata, choi, motivasi, katakata, tik…	#motivasi #motivasihidup #mentalhealth #palestine #kata #katakata …	SG
_faith_in_allah_	https://www.tiktok.com/@_faith_in_allah_/video/7405003717738614…	1305	157	0	10	shorts, viral, tiktok, quran, dua, fy, allah, fyp, islam, palestine, palstine	Dua for palestine #fyp #fy #shorts #tiktok #quran #islam #palstine #vir…	NL
wahrany2paris	https://www.tiktok.com/@wahrany2paris/video/7404984994940128544	1069	293	12	5	gaza, palestine	#palestine #gaza	FR
lis_11.09	https://www.tiktok.com/@lis_11.09/video/7404985502752951584	1064	21	0	0	freepalestine, bruxelles, palestine, bosniangirl, erinnerung, freesyria, …	Maybe…#CapCut #helpafghanistan #afghanistan🇦🇫 #freeafghanistan …	DE
wahrany2paris	https://www.tiktok.com/@wahrany2paris/video/7404988669234351392	1021	157	9	3	chicago, usa, gaza, palestine	#chicago #usa #palestine #gaza	FR

Slika 2. Rezultati TikTok pretrage po hashtagu "palestine"

Izvor: Autor

Slika 2. prikazuje podatke o videozapisima koji su objavljeni posljednjih mjesec dana (na dan 22. kolovoza 2024.) s *hashtagom* „palestine“ te su sortirani po broju pregleda. Na slici se može vidjeti devet videozapisa s najvećim brojem pregleda, dok se ostali mogu pregledati vertikalnim *scrollom*.

2. Detaljna analiza videozapisa

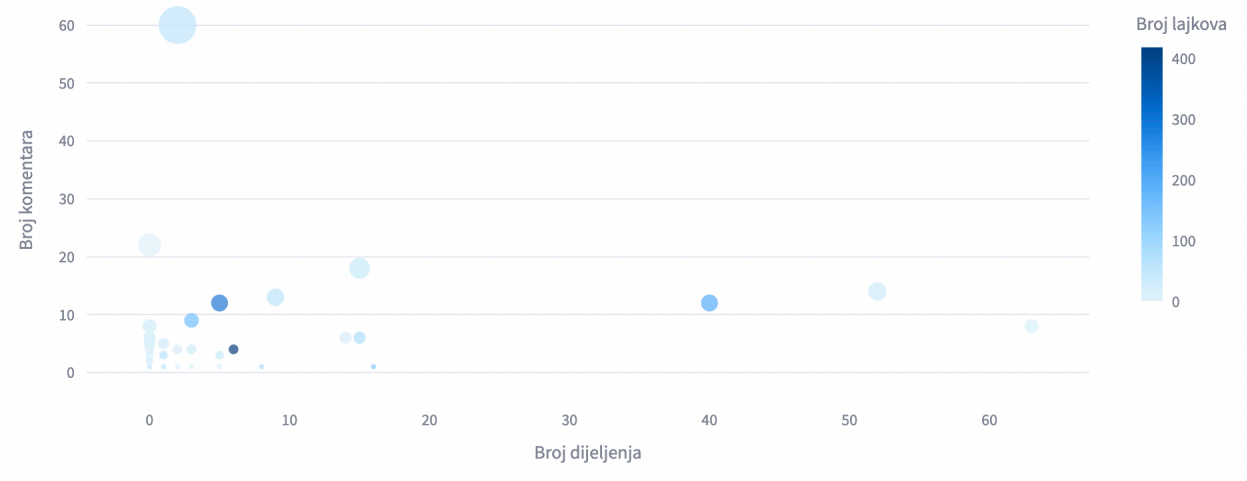
Kada aplikacija pronađe videozapise povezane s traženim *hashtagom*, korisniku se prikazuju detaljne informacije o svakom videozapisu:

- Korisničko ime: Aplikacija prikazuje korisničko ime autora videozapisa što može pomoći u identifikaciji potencijalnog izvora terorističkog sadržaja ili organizacija koje stoje iza širenja takvog sadržaja.
- Link na video: Omogućena je poveznica na konkretan videozapis na TikTok platformi.
- Statistički podaci: Aplikacija prikazuje ključne statističke podatke za svaki videozapis, uključujući broj pregleda, „lajkova“, komentara i dijeljenja. Ove informacije omogućuju uvid u popularnost i doseg videozapisa, što može pomoći u procjeni utjecaja sadržaja na širu publiku.
- Popis *hashtagova*: Aplikacija prikazuje sve *hashtagove* korištene u videozapisu. Ovi podaci omogućuju korisnicima da analiziraju povezane teme i trendove, te identificiraju druge relevantne *hashtagove* koji mogu biti povezani s terorističkim sadržajem.
- Opis videozapisa**:** Prikazuje se tekstualni opis koji je autor priložio uz video. Opis može pružiti dodatni uvid u namjeru ili kontekst iza videozapisa, što može biti ključno za identifikaciju terorističkog sadržaja.
- Lokacija: Aplikacija prikazuje državu iz koje je videozapis postavljen. Lokacijski podaci mogu biti ključni za razumijevanje geografskog širenja terorističkih poruka ili za identifikaciju specifičnih država/područja u kojima je teroristička propaganda najaktivnija.

3. Vizualizacija podataka

U aplikaciji za analizu TikTok videozapisa, prikazuju se grafovi koji pružaju detaljan uvid u sadržaj povezan s određenim *hashtagom* na TikToku. U nastavku je opis svakog grafa koji se prikazuje:

Angažman (engl. *Engagement*): Ovaj graf prikazuje odnos između broja dijeljenja videozapisa (x-os) i broja komentara (y-os) za različite TikTok videozapise. Veličina točaka na grafu prikazuje broj komentara, dok boja točaka predstavlja broj "lajkova". Vizualizacija omogućava korisniku brzo uočavanje videozapisa koji su izazvali najviše angažmana u smislu komentara, "lajkova" i dijeljenja. Na grafu su također dostupne dodatne informacije o korisničkom imenu i linku na videozapis prilikom prelaska mišem preko točke. Slika 3. prikazuje graf angažmana za pretragu po *hashtagu* "palestine".



Slika 3. Graf angažmana za pretragu po hashtagu "palestine"

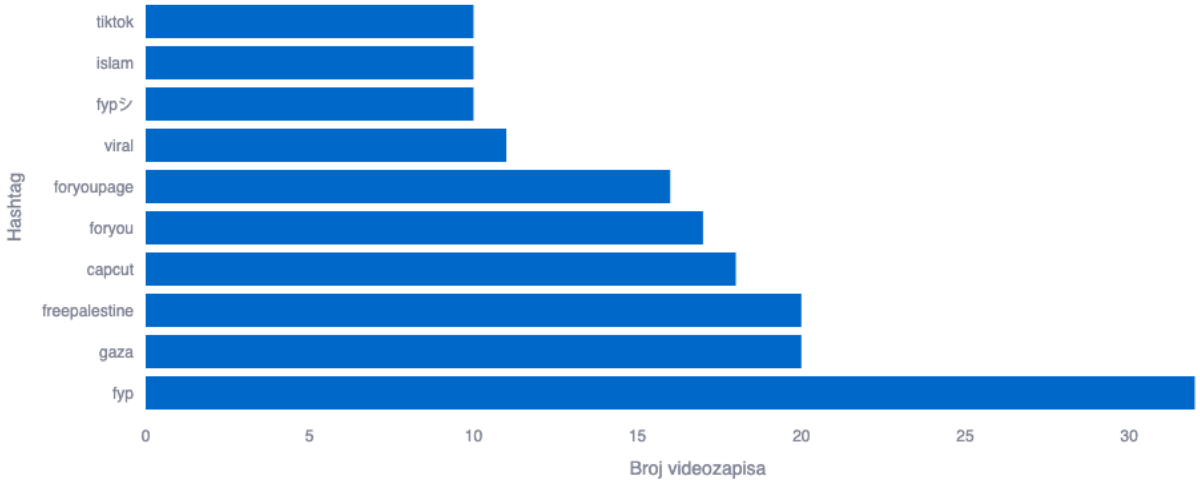
Izvor: Autor

Angažman prema državama (engl. *Engagement by Country*): Ovaj graf prikazuje angažman prema različitim državama (označene u obliku kodova). Prikazuju se tri ključna mjerila angažmana: broj "lajkova", broj pregleda i broj komentara. Svaka država je predstavljena grupom stupaca gdje svaki stupac predstavlja jednu od metrika. Graf omogućava korisnicima usporedbu angažmana između različitih država i identifikaciju koje države/područja generiraju najviše interesa za određeni *hashtag*. Graf angažmana prema državama koji aplikacija prikazuje za pretragu po *hashtagu* "palestine" može se vidjeti na slici 4.

Slika 4. Graf angažmana prema državama za pretragu po hashtagu "palestine"

Izvor: Autor

Top 10 *hashtagova* (engl. *Top 10 Hashtags*): Ovaj graf prikazuje top 10 *hashtagova* koji se najčešće pojavljuju uz traženi *hashtag*. Grafikon je horizontalni stupičasti, gdje y-os predstavlja *hashtagove*, a x-os prikazuje broj videozapisa koji koriste te *hashtagove*. Graf pomaže korisnicima shvatiti koji su popularni *hashtagovi* povezani uz onaj koji su tražili, što može biti korisno za optimizaciju sadržaja ili analizu trendova. Kako izgleda rezultat aplikacije za top 10 *hashtagova* uz *hashtag* "palestine", prikazuje slika 5.



Slika 5. Graf top 10 hashtagova za pretragu po hashtagu "palestine"

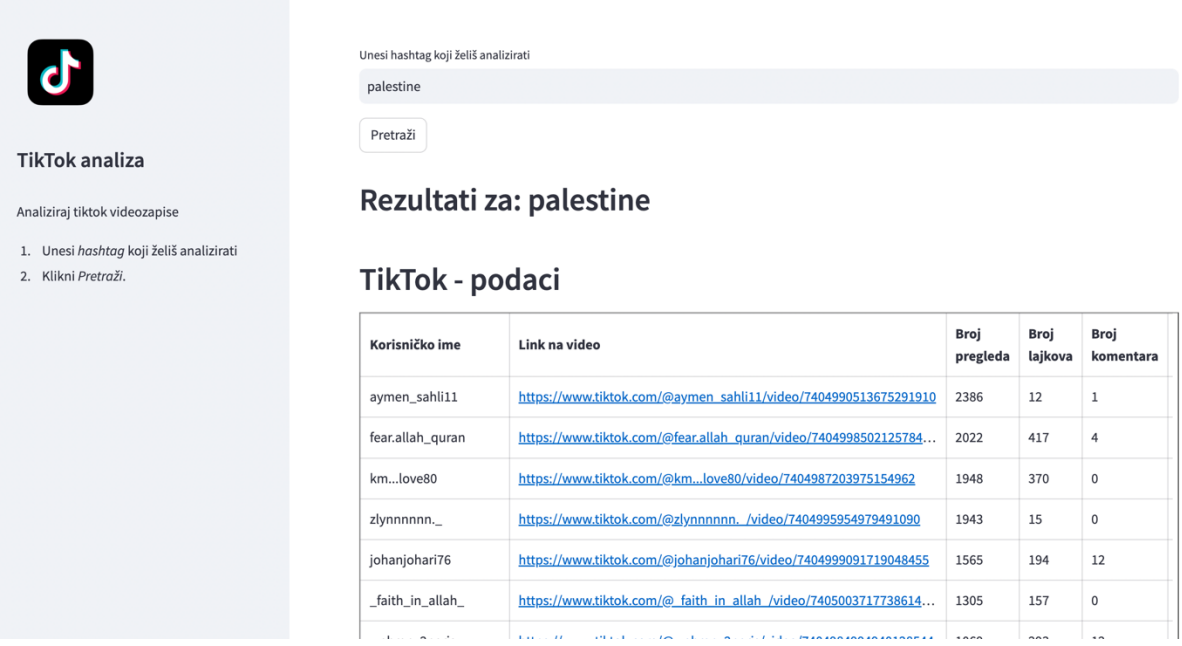
Izvor: Autor

Predstavljeni grafovi zajedno pružaju sveobuhvatan pregled angažmana i povezanih podataka na TikToku, omogućavajući korisnicima donošenje informirane odluke na osnovu vizualizacija i analize podataka.

3. Intuitivno sučelje

Aplikacija je razvijena korištenjem Streamlit *frameworka*, koji omogućuje brzo i jednostavno stvaranje *web* aplikacija s intuitivnim korisničkim sučeljem. Streamlit je posebno prikladan za aplikacije koje zahtijevaju brzu analizu podataka i interaktivne vizualizacije, što je idealno za ovu vrstu alata.

Korisničko sučelje aplikacije dizajnirano je tako da bude jednostavno za korištenje, čak i za korisnike koji nemaju tehničko znanje. Sučelje omogućuje korisnicima da s lakoćom unesu željene *hashtagove*, pretražuju sadržaj, te pregledavaju i analiziraju podatke koji su im potrebni. Jednostavnost i preglednost sučelja omogućava stručnjacima usmjeravanje na analizu sadržaja, a ne na kompleksno ručno pretraživanje platforme, u svrhu što brže reakcije na potencijalne prijetnje. Izgled aplikacije prikazan je na slici 6.



Slika 6. Prikaz aplikacije za pretraživanje TikTok sadržaja po hashtagu

Izvor: Autor

4. Brza i učinkovita analiza

Jedna od glavnih prednosti aplikacije jest njena sposobnost da u stvarnom vremenu dohvaća i analizira podatke s TikToka. Korištenjem TikTok API-ja, aplikacija može brzo pretražiti veliku količinu sadržaja i pružiti korisnicima relevantne informacije u realnom vremenu. Brzina i učinkovitost ključni su u situacijama kada je potrebno brzo reagirati na širenje terorističkog sadržaja ili drugih sigurnosnih prijetnji.

Brza analiza sadržaja omogućuje korisnicima pravovremeno identificiranje potencijalne prijetnje i poduzimanje odgovarajućih mjera, bilo da se radi o prijavljivanju sadržaja TikToku za uklanjanje, praćenju širenja sadržaja, ili drugim sigurnosnim mjerama.

5.6.2.2. Tehnološka osnova

Aplikacija je razvijena koristeći nekoliko ključnih tehnologija:

- Python: Glavni programski jezik korišten za razvoj aplikacije. Python je odabran zbog svoje fleksibilnosti, široke primjene u analizi podataka, te bogate biblioteke alata koji olakšavaju rad s API-jima i obradom podataka.
- TikTok API: API omogućuje dohvaćanje podataka iz TikTokove baze u stvarnom vremenu. Integracija s TikTok API-jem omogućuje aplikaciji brzo i učinkovito pretraživanje i analiziranje sadržaja na platformi.
- Streamlit: Korišten je za izradu *web* sučelja aplikacije. Streamlit omogućuje jednostavno stvaranje interaktivnih aplikacija koje su intuitivne za korištenje, čak i za korisnike bez tehničkog znanja.

Programski kod aplikacije dostupan je na GitHub repozitoriju koji je naveden u privitku rada.

5.6.2.3. Namjena

Aplikacija je prvenstveno namijenjena stručnjacima u području sigurnosti, istraživačima i analitičarima koji se bave praćenjem i analizom sadržaja na društvenim mrežama. S obzirom na sve veći rizik od širenja terorističkog sadržaja na društvenim mrežama, ovakav alat može biti od velike koristi u borbi protiv digitalne propagande.

Stručnjaci mogu koristiti aplikaciju za brzo pretraživanje i analizu sadržaja, identificiranje trendova i tema povezanih s terorističkim sadržajem, te poduzimanje odgovarajućih mjera kako bi se spriječilo širenje opasnih poruka.

Aplikacija može biti korištena i u obrazovne svrhe, kako bi se istraživači i studenti bolje upoznali s načinima na koje se teroristički sadržaj širi na društvenim mrežama, te kako bi razvili alate i metode za borbu protiv ovakvih prijetnji u budućnosti.

Nastavak razvoja aplikacije uključivao bi integraciju UI tehnologije u obliku detekcije oružja, identifikacije osoba te analizu sentimenta za svaki videozapis koji je dobiven nakon filtriranja po *hashtagu*.

6. ZAKLJUČAK

Terorizam se tijekom posljednjih desetljeća razvio u jednu od najznačajnijih prijetnji globalnoj sigurnosti, prilagođavajući se tehnološkim promjenama i iskorištavajući moderne tehnologije. Terorističke organizacije koriste internet i društvene mreže za širenje svojih ideologija i organizaciju napada, zbog čega su nacionalne sigurnosne agencije prisiljene tražiti nove alate i strategije za učinkovitu prevenciju i suzbijanje terorističkih prijetnji.

Razvoj umjetne inteligencije (UI) značajno je unaprijedio sposobnosti sigurnosnih sustava, omogućujući im analizu velikih količina podataka, prepoznavanje obrazaca i predviđanje potencijalnih prijetnji s većom točnošću nego ikad prije. Na temelju istraživanja i analize dostupnih podataka, hipoteza da primjena umjetne inteligencije značajno poboljšava učinkovitost sustava nacionalne sigurnosti u prepoznavanju i sprječavanju terorističkih prijetnji smatra se dokazanom. Umjetna inteligencija se koristi u različitim aspektima sigurnosnih operacija, uključujući analizu podataka s društvenih mreža, prediktivnu analitiku, prepoznavanje lica i drugih biometrijskih podataka, kao i uklanjanje terorističkog sadržaja s interneta. Tehnologije poput strojnog učenja, dubokog učenja i obrade prirodnog jezika omogućuju sigurnosnim agencijama brzo identificiranje i reagiranje na prijetnje, često prije nego što dođe do stvarne opasnosti.

Unatoč brojnim prednostima, primjena umjetne inteligencije u borbi protiv terorizma nije bez izazova. Jedan od glavnih problema je pitanje privatnosti i etike. Korištenje UI za masovnu analizu podataka i praćenje komunikacija može narušiti privatnost građana i dovesti do zloupotrebe prikupljenih informacija. Hipoteza da integracija umjetne inteligencije u sigurnosne sustave predstavlja značajan rizik po privatnost i ljudska prava te zahtijeva razvoj strožih etičkih i pravnih okvira za njenu uporabu smatra se dokazanom. Također, na temelj istraživanja, utvrđeno je postojanje opasnosti od tehničkih pogrešaka i pristranosti u algoritmima, što može dovesti do netočnih rezultata i negativnih posljedica. Time se hipoteza da korištenje umjetne inteligencije u sigurnosnim sustavima može smanjiti potrebu za ljudskim nadzorom u određenim operacijama, ali istovremeno može povećati rizik od tehničkih pogrešaka s ozbiljnim posljedicama smatra potvrđenom. Osim toga, postavlja se pitanje globalne sigurnosti u širem smislu, jer sve veća ovisnost o tehnološkim rješenjima može potaknuti utrku u naoružanju među državama, što potvrđuje hipotezu da razvoj umjetne inteligencije specijalizirane za nacionalnu sigurnost može izazvati globalnu utrku u naoružanju UI tehnologijama te destabilizirati međunarodne odnose i

povećati rizik od sukoba. Kako bi se spriječila destabiliziracija međunarodnih odnosa, potrebno je osigurati međunarodnu suradnju i uspostaviti globalne standarde za upotrebu umjetne inteligencije u sigurnosnim sustavima.

Primjer korištenja umjetne inteligencije u terorističke svrhe, može se vidjeti na platformi TikTok, koja je privukla stotine milijuna korisnika širom svijeta zbog svoje jednostavnosti korištenja i mogućnosti stvaranja i dijeljenja kratkih videozapisa. Izvještaj „*Hatescape*“ otkrio je da od 1.030 analiziranih videozapisa na TikToku, 246 (24%) veliča ili promovira pojedince i organizacije povezane s ekstremizmom i terorizmom, uključujući Adolf Hitlera i Brenton Tarranta. Također, čak 30% analiziranih videozapisa promiče nadmoć bijelaca koristeći teorije zavjere poput „velike zamjene“ i „bijelog genocida“. Dodatno, 81,5% problematičnih videozapisa i dalje je bilo dostupno na platformi unatoč pravilima TikToka protiv promicanja nasilnog ekstremizma. Ovi podaci jasno pokazuju kako društvene mreže, unatoč svojim naporima, često nisu u stanju u potpunosti kontrolirati širenje ekstremističkog sadržaja, što zahtijeva hitne akcije i primjenu naprednih UI alata za poboljšanje nadzora i moderiranja sadržaja.

Kako bi se odgovorilo na navedene izazove, razvijena je aplikacija za detekciju terorističkog sadržaja na TikToku. Aplikacija omogućuje brzo pretraživanje i analizu videozapisa prema *hashtagovima*, koristeći TikTok API i razvijena je u Pythonu s intuitivnim sučeljem u Streamlit *frameworku*. Njene funkcionalnosti, poput analize videozapisa i vizualizacije podataka, omogućuju pravovremeno prepoznavanje i uklanjanje štetnog sadržaja. Ovaj alat pokazuje kako umjetna inteligencija može biti učinkovito korištena za borbu protiv terorizma i ekstremizma na društvenim mrežama.

Umjetna inteligencija predstavlja moćan alat u borbi protiv terorizma, ali njena primjena mora biti pažljivo regulirana kako bi se osigurala pravednost, učinkovitost i zaštita osnovnih ljudskih prava. Budući razvoj UI u sigurnosnim sustavima zahtijeva uravnotežen pristup koji uključuje tehnološke inovacije, etičke standarde i međunarodnu suradnju. Samo na navedeni način, moguće je iskoristiti puni potencijal umjetne inteligencije u zaštiti nacionalne sigurnosti i održavanju globalnog mira.

7. LITERATURA

- Akilli, E. (2024). *Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics, and Privacy*. SETA, str. 2,3,4.
- Alom, M. Z. et al. (2018). *The history began from AlexNet: A comprehensive survey on deep learning approaches.*
- Andrić, J., Terzić, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. *International Journal of Information and Operations Management Education*, 17(1), str. 6-9.
- Antiterorističke mjere. Struna. Dostupno na: http://struna.ihjj.hr/naziv/antiteroristicke-mjere/49619/#naziv (21.7.2024.).
- *Artificial Intelligence Index Report 2024*. Institute for Human-Centered AI, Stanford University. Dostupno na: https://aiindex.stanford.edu/report/ (15.8.2024.).
- *Big data analytics: What it is and why it matters*. SAS. Dostupno na: https://www.sas.com/en_us/insights/analytics/big-data-analytics.html (15.8.2024.).
- Bilandžić, M. (2010). *Sjeme zla – elementi sociologije terorizma*, Plejada, Zagreb, str. 14.
- Cataleta, M. S. (2020). *Humane Artificial Intelligence: The Fragility of Human Rights Facing AI*. East-West Center.
- Cena, J. (2024). *Exploring the Evolution of Artificial Intelligence: From Early Concepts to Modern Applications*. Artificial Life.
- Countering Terrorism. NATO. Dostupno na: https://www.nato.int/cps/en/natohq/topics_77646.htm (5.8.2024.)
- Europol. (2023). *European Union Terrorism Situation and Trend Report 2023*. Publications Office of the European Union. Dostupno na: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat (2.8.2024.)
- Foster, D. (2023). *Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play* (2nd ed.). O'Reilly Media.
- Gandomi, A., Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), str. 138-139.

- Ganor, B. (2021). Artificial or Human: A New Era of Counterterrorism Intelligence? *Studies in Conflict and Terrorism,* str. 605–624.
- Hartland-Thunberg P. (1982). *National economic security: interdependence and vulnerability*. John F. Kennedy Institute, str. 50.
- inteligencija. Školski rječnik hrvatskog jezika. Dostupno na: https://rjecnik.hr/search.php?q=inteligencija (21.7.2024.).
- Esmailzadeh, Y., & Motaghi, E. (2024). International terrorism and social threats of artificial intelligence. *Journal of Globalization Studies*, 15(1), str. 172-174.
- Latif, E., et al. (2023). *Artificial General Intelligence (AGI) for Education*. AI4STEM Education Center, University of Georgia, str. 2-4.
- LeCun, Y., Bengio, Y., Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), str. 440.
- Lewulis, Piotr. (2024). Social Media Intelligence as a Tool for Immigration and National Security Purposes. *Internal Security Review*. ResearchGate, str. 407-408.
- Lutz, B., Lutz, J. (2008). *Global Terrorism*. Routledge, str. 9.
- McCarthy, J. (2007). *What is Artificial Intelligence?*. Dostupno na: http://www-formal.stanford.edu/jmc/whatisai.pdf (27.7.2024.).
- McKendrick, K. (2019). *Artificial Intelligence Prediction and Counterterrorism*. International Security Department, Chatham House, str. 12.
- Montasari, R. (2022). The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights. *Artificial Intelligence and National Security*. Springer, str. 33-34, 72-73, 76, 180.
- National Cyber Crime Research & Innovation Centre. (2021). *Manual on Social Media Intelligence (SOCMINT) for Law Enforcement Agencies*. Bureau of Police Research & Development, Ministry of Home Affairs, Government of India.
- O'Connor, C. (2021). *Hatescape: An in-depth analysis of extremism and hate speech on TikTok*. Institute for Strategic Dialogue. Dostupno na: https://www.isdglobal.org/isd-publications/hatescape-an-in-depth-analysis-of-extremism-and-hate-speech-on-tiktok/ (3.8.2024.).
- protuterorističke mjere. Struna. Dostupno na: http://struna.ihjj.hr/naziv/protuteroristicke-mjere/49620/#naziv (21.7.2024.).

- Russell, S. (2019). *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking, str. 112-115.
- Schwarz, B. (2019). *Welcome BERT: Google's latest search algorithm to better understand natural language*. Search Engine Land. Dostupno na: https://searchengineland.com/welcome-bert-google-artificial-intelligence-for-understanding-search-queries-323976 (15.8.2024.).
- sigurnost. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2024. Dostupno na: https://www.enciklopedija.hr/clanak/sigurnost (1.8.2024.).
- Šegvić, S. (2009). Antiterorizam u kontekstu borbe protiv organiziranog kriminala. *Zbornik radova Pravnog fakulteta u Splitu*, 46(4), str. 667.
- Tatalović, S.,Bilandžić, M. (2005). *Osnove nacionalne sigurnosti*. Zagreb, str. 23.
- terorizam. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2024. Dostupno na: https://www.enciklopedija.hr/clanak/terorizam (21.7.2024.).
- The Institute for Economics & Peace. (2014). *Global Terrorism Index 2014: Measuring and Understanding the Impact of Terrorism*. Dostupno na: https://www.economicsandpeace.org/wp-content/uploads/2023/12/GTI-2014-web.pdf (27.7.2024.).
- The Institute for Economics & Peace. (2024). *Global Terrorism Index 2024*. Dostupno na: https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf (27.7.2024.).
- Ujedinjeni narodi. (1994). Rezolucija 49/60, *Measures to eliminate international terrorism*. Generalna skupština. Dostupno na https://digitallibrary.un.org/record/172281?ln=en&v=pdf (21.7.2024.).
- umjetna inteligencija. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2024. Dostupno na: https://enciklopedija.hr/clanak/umjetna-inteligencija (24.7.2024.).
- Vijeće Europske unije. (2002). *Okvirna odluka Vijeća 2002/475/PUP o borbi protiv terorizma*. Dostupno na: https://eur-lex.europa.eu/eli/dec_framw/2002/475/oj (21.7.2024.).
- Wechsler, D. (1939). *The Measurement of Adult Intelligence*. Williams & Wilkins, str. 3.
- Whitlock, C., Strickland, F. (2023). *Winning the National Security AI Competition: A Practical Guide for Government and Industry Leaders*. Apress, str. 85, 209.

8. SAŽETAK

Integracija umjetne inteligencije u sustave nacionalne sigurnosti: perspektive, izazovi i primjene u prevenciji terorizma

Ovaj diplomski rad istražuje ulogu umjetne inteligencije (UI) u jačanju nacionalne sigurnosti, s posebnim fokusom na prevenciju terorističkih prijetnji. Kroz analizu različitih tehnologija UI, kao što su strojno učenje, analiza velikih podataka, obrada prirodnog jezika i računalni vid, rad prikazuje kako su navedene tehnologije postale ključne za sigurnosne agencije u prepoznavanju i suzbijanju terorističkih aktivnosti.

Rad započinje pregledom suvremenih izazova u globalnoj sigurnosti, ističući kako su se terorističke organizacije prilagodile korištenju interneta i društvenih mreža za širenje svojih ideologija i organizaciju napada. Kao odgovor, nacionalne sigurnosne agencije su se okrenule umjetnoj inteligenciji kako bi poboljšale svoje kapacitete za analizu velikih količina podataka i prepoznavanje obrazaca koji ukazuju na potencijalne prijetnje.

Središnji dio rada fokusira se na praktične aplikacije UI u sigurnosnim sustavima, uključujući analizu podataka s društvenih mreža, prediktivnu analitiku, prepoznavanje lica te filtriranje terorističkog sadržaja s interneta. Prediktivni modeli posebno su korisni za analizu povijesnih podataka o terorističkim aktivnostima i predviđanje budućih prijetnji.

Uz prednosti, naglašavaju se i izazovi korištenja UI, poput pitanja privatnosti i etike. Korištenje UI za masovnu analizu podataka može narušiti privatnost građana i otvoriti mogućnosti zloupotrebe prikupljenih informacija, što potvrđuje potrebu za strožim etičkim i pravnim okvirima.

Kao praktični primjer, rad analizira TikTok, platformu koja je, unatoč svojoj popularnosti, postala prostor za širenje ekstremizma. Izvještaj „Hatescape“ pokazuje da je značajan postotak sadržaja na TikToku povezan s ekstremizmom, uključujući 24% videozapisa koji veličaju teroriste. Kao odgovor, razvijena je aplikacija koja koristi UI za prepoznavanje i uklanjanje terorističkog sadržaja na TikToku, pokazujući kako UI može biti alat za suzbijanje terorizma na društvenim mrežama, ali i ističući potrebu za regulacijom njezine uporabe.

Zaključno, rad ističe da, iako je umjetna inteligencija moćan alat u borbi protiv terorizma, njena primjena mora biti regulirana kako bi se osigurala zaštita ljudskih prava i etičkih standarda. Potrebna je međunarodna suradnja i uravnotežen pristup za učinkovito korištenje UI u sigurnosnim sustavima.

Ključne riječi: *terorizam, umjetna inteligencija, UI, nacionalna sigurnost, sigurnosni sustavi, sigurnost*

9. SUMMARY

Integration of Artificial Intelligence into National Security Systems: Perspectives, Challenges, and Applications in the Prevention of Terrorism

This thesis explores the role of artificial intelligence (AI) in strengthening national security, with a particular focus on the prevention of terrorist threats. Through the analysis of various AI technologies, such as machine learning, big data analysis, natural language processing and computer vision, the paper shows how these technologies have become crucial for security agencies in identifying and suppressing terrorist activities.

The paper begins with an overview of contemporary challenges in global security, highlighting how terrorist organizations have adapted to the use of the Internet and social networks to spread their ideologies and organize attacks. In response, national security agencies have turned to artificial intelligence to improve their capacity to analyze large amounts of data and identify patterns that indicate potential threats.

The central part of the work focuses on practical applications of UI in security systems, including analysis of data from social networks, predictive analytics, facial recognition and filtering terrorist content from the Internet. Predictive models are particularly useful for analyzing historical data on terrorist activity and predicting future threats.

Along with the benefits, the challenges of using UI, such as privacy and ethical issues, are also highlighted. The use of AI for mass data analysis can violate the privacy of citizens and open the possibility of misuse of collected information, which confirms the need for stricter ethical and legal frameworks.

As a practical example, the paper analyzes TikTok, a platform that, despite its popularity, has become a space for the spread of extremism. The Hatescape report shows that a significant percentage of content on TikTok is related to extremism, including 24% of videos glorifying terrorists. In response, an application that uses UI to identify and remove terrorist content on TikTok was developed, showing how UI can be a tool to counter terrorism on social networks, but also highlighting the need to regulate its use.

In conclusion, the paper points out that, although artificial intelligence is a powerful tool in the fight against terrorism, its application must be regulated to ensure the protection of human rights and ethical standards. International cooperation and a balanced approach are needed for the effective use of AI in security systems.

Keywords: *terrorism, artificial intelligence, AI, national security, security systems, security*

10. ŽIVOTOPIS

Osobni podaci:

Ime i prezime: Matea Bešlić

Datum i mjesto rođenja: 6.5.1994, Posušje, Bosna i Hercegovina

e-mail: mateabeslic1@gmail.com

Obrazovanje:

2009. – 2013. III. Gimnazija, Split

2013. – 2018. Fakultet elektrotehnike, strojarstva i brodogradnje u Splitu, preddiplomski studij računarstva

2019. – 2021. Visoka škola ASPIRA, Split, preddiplomski stručni studij računarstva, prvostupnik računarstva (bacc.ing.comp.)

2022. – 2024. Sveučilišni odjel za forenzične znanosti, Sveučilište u Splitu, diplomski studij forenzike, modul Forenzika i nacionalna sigurnost

---

Iskustva:

Tijekom studiranja, aktivno sam volontirala u Klubu mladih Split, gdje sam vodila besplatne pripreme za državnu maturu iz matematike, organizirala brojna predavanja, volonterske i humanitarne aktivnosti te provodila projekte. Zahvaljujući iskustvu na upravljačkim pozicijama Kluba mladih i velikom broju uspješno provedenih projekata, zaposlila sam se u ŽNK Hajduk Split, gdje sam predsjednica udruge od 2018. godine. Također, za vrijeme studiranja na FESB-u, sudjelovala sam u organizaciji i provođenju znanstvenih konferencija SpliTech, SoftCOM, IEEES i ICH2P. Na FESB-u sam, osim navedenoga, pokrenula i prvo regionalno eSport natjecanje Battle4Split. U sklopu studija na Sveučilišnom odjelu za forenzične znanosti, sudjelovala sam na dva događaja u organizaciji RACVIAC-a, *„Course of Non-proliferation and Disarmament law“* i *„Weapons of Mass Destruction Cyber Crimes Investigation“*.

Publikacije:

M. Bešlić, T. Perković, I. Stančić, G. Pavlov i M. Čagalj, „eMoorings: Distributed low power wide area system to control moorings“, *2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, Split, Croatia, 2017.

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, **Matea Bešlić**, izjavljujem da je moj diplomski rad pod naslovom **Integracija umjetne inteligencije u sustave nacionalne sigurnosti: perspektive, izazovi i primjene u prevenciji terorizma** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ničija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u nijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, 23. rujna 2024. godine

Potpis studenta/studentice: _____

POPIS SLIKA

POPIS TABLICA

PRILOZI

1. Programski kod aplikacije za analizu TikTok sadržaja: https://github.com/MB-matea/TikTok-analysis