Sveučilište Jurja Dobrile u Puli

**„Utjecaj tehnologije na prevenciju terorističkih napada“**

Istraživačko izvješće

Pula, siječanj 2020.

Sveučilište Jurja Dobrile u Puli

**„Utjecaj tehnologije na prevenciju terorističkih napada“**

Istraživačko izvješće

Studenti:

Smjer:

Predmet:

Mentor:

Pula, siječanj 2020

Sadržaj

[1. Uvod 1](#_Toc30455040)

[2. Razrada 2](#_Toc30455041)

[3. Cilj i Hipoteza 4](#_Toc30455042)

[4. Simulacija istraživanja (odabir uzorka) 5](#_Toc30455043)

[5. Valjanost 5](#_Toc30455044)

[6. Zaključak 7](#_Toc30455045)

[7. Literatura 8](#_Toc30455046)

# Uvod

Terorizam je jedan od najgorih, ako ne i najgori oblik nasilja nad civilima. Definiran je kao bilo koji čin nasilja, najčešće oružanog protiv nedužnih osoba. Terorizam kao konstrukt rezultat je niza čimbenika – političkih, povijesnih, ideoloških, gospodarskih, socijalnih – a sa svojim učincima do danas ostaje neobjašnjiv fenomen i najveća prijetnja sigurnosti današnjeg društva. Primarni cilj terorizma je uglavnom društveno orijentiran, na primjer političke ili religiozne prirode te koristi izravni napad na žrtve ili razne oblike prijetnji kao metode širenja straha (od kud i vuče naziv teror - terorizam) među neizravnim žrtvama. Uglavnom se smatra oblikom političkog nasilja, iako je granica između vojnog i političkog nasilja često jako krhka u slučajevima terorizma na većoj razini. Iako često ispada tako u današnjem društvu i medijima, terorizam nije nešto novo ili strano, sama pojava kao takva je skoro pa sigurno postojala od kad su ljudi započeli prve oblike političkih uređenja odnosno sjedilačkih metoda života. Kao odgovor terorizmu stvorena je njegova protuteža odnosno protuterorizam koji se manifestira na razne načine poput specijalnih jedinica policije i vojske, državnih programa za promatranja potencijalno kritičnih skupina ili osoba i sličnoga. Najpoznatiji primjer državnog odgovora na terorizam je vjerojatno Američki „Patriot Act“, koji je proizašao iz jednog od najutjecajnijih terorističkog napada u svjetskoj povijesti odnosno napada 11. Rujna 2001. (9.11.). To je samo jedna od mnogih inicijativa korištenja tehnologije u svrhu borbe sa terorizmom. Iako je tehnologija definitivno pomogla u sprječavanju mnogih nesreća, također je pripomogla pojavi nove vrste terorizma, tako zvanog „cyber“ terorizma odnosno terorizma preko Interneta, korištenjem svakakvih ilegalnih metoda izrabljivanja ljudi i podataka. Razvoj tehnologije i masovnih medija uvelike je doprinijelo i razvijanju terorizma. Internet i Masovni mediji postali su ključno sredstvo komuniciranja i prenošenje ideala. Zbog toga možemo reći kako je informacija postala oružje novoga doba koje može stvoriti mnogo više negativnih posljedica od konvencionalnih vrsta naoružanja. Unatoč tome što tehnologija može biti opasna u krivim rukama, pokazuje se kao neprocjenjiv alat u borbi protiv terorizma, što je i tema ovog istraživanja.

# Razrada

Terorizam se radikalno promijenio u proteklim desetljećima, po istraživanjima iz SAD-a se vidi da se korištenjem preventivne tehnologije, kao i one za nagle sigurnosne reakcije zapravo relativno rečeno smanjio broj terorističkih napada. Unatoč tome treba se reći da iako se broj smanjio, sami napadi nerijetko su radikalniji i više ubojiti nego što su nekad bili. To u stvari iskazuje da iako je tehnologija veoma korisna u borbi sa terorizmom, još nije na definitivnoj razini odnosno onoj koja bi kompletno zaustavila terorističke napade prije nego sto se dogode. Američki Hoover institut nalaže kako postoji 5 glavnih točaka u sukobu sa terorizmom; senzori, tehnologije za identifikaciju, prikupljanje i analiza podataka, konstantno napredovanje tehnologije i najkritičniji tj. etičke i legalne zapreke. Upravo taj zadnji je problem koji izaziva najviše debata i sukoba sa svih strana političkog spektra, a radi se o sukobu probijanja privatnosti građana u ime borbe sa terorizmom. U ranije navedenom promatranju, objavljenom pod nazivom „Technology for preventing Terrorism“,[[1]](#footnote-1) Sofaer komentira kako uloga tehnologije neupitno treba porasti jer na skali današnjih uvoza i izvoza granična zaštita može posvetiti otprilike 2 minute vozilima koja prenose tko za što ili koga unutra. Nastavlja da investiranje u razne skenere i slične preventivne tehnologije je možda jedini pouzdan način sukoba sa tim problemom bez ekstremnih mjera poput zatvaranja granica ili drugih ekonomski destruktivnih metoda. Kao primjer se navodi vladina reakcija na trgovanje i zamrzavanje internacionalnih izmjena nakon napada 2001. što je pristup koji se dokazao minimalno uspješnim u odnosu na količine izgubljenih izmjena i trgovanja između legitimnih i korektnih tvrtki. Iz ovoga veoma realnog primjera možemo odmah vidjeti zašto je napredak tehnologije za predviđanje i zaustavljanje puno vrjedniji i iz perspektive zaštite žrtava kao i ekonomskih posljedica od „grubog“ pristupa. RAND je neprofitna organizacija koja se bavi analizom problema sa kojima se globalni privatni i javni sektor susreću, među njima je i terorizam odnosno borba sa njime. „Technology Acquisition by Terrorist Groups“ [[2]](#footnote-2) je članak objavljen od strane RAND korporacije i centra za internacionalnu znanost i tehnološku politiku George Washington sveučilišta u kojemu govore o razvoju tehnologije u sklopu protuterorizma odnosno kako tehnologija utječe na terorizam. Ističu kako je tehnologija za prevenciju terorizma odnosno skeneri, detektori za metal i slično jedni od definitivno neprocjenjivih alata u borbi sa terorizmom, tako je barem nekad bilo.

Današnji teroristi su upravo zbog tih preventivnih metoda prešli na razne oblike biokemijskog i čak primitivnog nuklearnog terorizma, koje je puno teže predvidjeti odnosno zaustaviti samim skenerima. Upravo zbog toga ističu da je potrebno razvijati tehnologiju koja direktno beneficira od današnjih računala i njihove moći obrađivanja. Nastavljaju kako se treba uzeti računalna sposobnost obrade masivnih količina podataka i kombinirati sa komunikacijom između raznih policijskih ili istraživačkih stanica da bi se ustvari mogla predvidjeti i shvatiti prijetnja putem raznih algoritama prepoznavanja nizova i povezivanja sličnih događaja koji su već evidentirani. Oni također objašnjavaju jedan od velikih problema protuterorizma današnjice, a to je utrka „naoružanja“ između vlada i terorista u smislu tehnologije. Razlog zašto je to komplicirano je upravo ono što čini tehnologiju onime što je – povezanost. Na primjer u terorističkom napadu sa bilo kojim standardnim oružjem često je potrebna samo jedna trenirana osoba dok računala i sva ostala „cyber“ oružja traže timove stručnjaka, stabilnu povezanost i druge elemente kako bi efektivno djelovali. Takve razine organiziranost su teške za postići i otežane time što su vođe i uprave terorističkih organizacija uglavnom organizirane ne po struci nego po ideologiji i uvjerenjima. Upravo je to jedna od slabosti koju moderna tehnologija može iskoristiti protiv ekstremističkih odnosno izoliranih skupina. Naime državna organizacija koja je povezana sa ostatkom svijeta te barata najmodernijom tehnologijom i stručnjacima može puno lakše probiti kodove i barijere terorističkih udruga, odnosno predvidjeti i zaustaviti potencijalne napade. Za kraj jedan primjer kako se države i pravne osobe u stvarnosti nose sa terorizmom iz jedne zakonodavne perspektivne, odnosno „Analiza pozitivnopravne Nacionalne strategije za prevenciju i suzbijanje terorizma“[[3]](#footnote-3) Đurđice Radaković. Iz ove perspektive trebamo na terorizam gledati kao jedan globalni fenomen, jedan koji ignorira državne granice i kao ranije navedeno zahtjeva koordinirano djelovanje raznih organizacija i državnih jedinica. Navodi kako strategije protiv terorizma uključuju sljedeće pojmove : onemogućavanje i sprječavanje širenja terorističkih ideala, prepoznavanje i zaustavljanje ekstremizma prije stadija terorizma, dobro proučavanje i među-državna suradnja u izmjeni podataka, iskustava i praksi te jačanje same tehnologije odnosno sektora za direktni sukob sa terorizmom.

Pod metodama za direktan sukob sa terorizmom navode se razvoj i uspostava sustava za opću zaštitu i sigurnost infrastruktura te za ovu temu najviše bitan dio – stvaranja sigurnosne mreže zaštite civilnih zona te online zaštita od „cyber“ terorizma.

Cilj svega toga nije samo zaustaviti smrtne slučajeve i doslovne napade nego i zaustaviti materijalne i imovinske štete nad građanima, a i državnim institucijama.

Istaknut je i također jedan jako bitan element svakog oblika nadzora i skeniranja javnosti, a to je da unatoč prijetnji koju terorizam predstavlja država nikako ne smije prekoračiti osnovna ljudska prava slobode govora i djelovanja kao i na privatnost. To jest da iako države imaju sposobnost uzeti inicijativu i uspostaviti svakakve oblike nadzora i skenera, sve što rade mora biti u sklopu međunarodno dogovorenih ljudskih prava, odnosno da treba uspostaviti sistem koji balansira između privatnosti i slobodi građana kao i njihovoj općoj sigurnosti.

# Cilj i Hipoteza

Cilj našeg istraživanja jest analizirati utjecaj senzora za prepoznavanje lica i šarenice na prevenciju terorističkih napada na ulazu i unutar zračne luke u Amsterdamu za 2019. godinu.
Navedeni cilj se slaže sa SMART principima:

|  |  |  |
| --- | --- | --- |
| S | Specific | Specifično se fokusira na odnos Tehnologije i Terorizma |
| M | Measurable | Mjerljivo je budući da se može promotriti vrijeme proteklo od implementirane nove tehnologije i terorističkih napada ili vremenski razmak između počinjenih terorističkih činova od korištenja tehnologije |
| A | Achievable  | Preventivna tehnologija već danas može predvidjeti puno toga analizom podataka, u budućnosti će moći prolaziti kroz masovne baze podataka i algoritama u kratkom vremenu |
| R | Relevant | Implementacija tehnologije za promatranje i bilježenje je već u tijeku  |
| T | Trackable  | Cijela radnja je bazirana na prikupljanju i analizi podataka, tako da samo dodavanje nekakvih sredstva mjerenja ne bi trebalo biti komplicirano kao takvo.  |

Alternativna hipoteza (H1): Postoji statistički značajna veza između korištenja senzora za prepoznavanje lica i šarenice te prevencije terorističkih napada.

Nul hipoteza (H0): Ne postoji statistički značajna veza između korištenja senzora za prepoznavanje lica i šarenice te prevencije terorističkih napada

# Simulacija istraživanja (odabir uzorka)

Kao uzorak uzeti su svi ljudi koji su prošli kroz zračnu luku u Amsterdamu u 2019. godini. Istraživanje je veoma specifično, budući da se ne zna kada bi se neki teroristički napad mogao dogoditi, zbog toga testiramo tehnologiju senzora za prepoznavanje lica i šarenice kroz cijelu jednu godinu i na svim ljudima koji prođu kroz zračnu luku. To bi značilo da senzor snima svo osoblje i putnike zračne luke.

Konstrukt 1 jest korištenje senzora za prepoznavanje lica i šarenice i nezavisna je varijabla broj senzora na ulazu i unutar zračne luke. Konstrukt 2 je prevencija terorističkih napada i zavisna varijabla će biti broj obranjenih terorističkih napada. Konstrukt 2 ovisi o implementaciji Konstrukta 1 budući da bi po hipotezi broj terorističkih napada trebao pasti korištenjem preventivne tehnologije

# Valjanost

Da bi sastavna valjanost bila ispunjena, odabrane varijable moraju precizno mjeriti pojmove u hipotezi. U ovom slučaju postoji veza između broja senzora za prepoznavanje lica i šarenice i broja preventiranih terorističkih napada u zračnoj luci u Amsterdamu za 2019. Kako bi se utvrdila interna valjanost, trebalo bi se izvesti istraživanje kako bi se vidjele posljedice. Bez provođenja istraživanja možemo pretpostavljati da korištenje senzora za prepoznavanje lica utječe na prevenciju terorističkih napada. Također, interna valjanost je potpuno ispunjena ako je prethodno ispunjena sastavna valjanost, koja je u ovom slučaju ispunjena. Eksterna valjanost je ispunjena, budući da su prethodno ispunjene sastavna i interna valjanost i naš se hipotetski odnos može dokazati i u ostalim situacijama, odnosno u našem slučaju moguće je generalizirati budući da sve novija preventivna tehnologija služi za obranu od terorističkih napada u svim poljima, a ne samo u zračnim lukama. Postoje 4 kriterija uzročnosti, odnosno uzrok i posljedica su povezani (korištenje senzora za prepoznavanje lica i šarenice povezano je sa prevencijom terorističkih napada). Uzrok prethodi posljedici, odnosno korištenje senzora za prepoznavanje lica i šarenice prethodi posljedici koja je u našem slučaju prevencija terorističkih napada.

Uzrok i posljedica se konzistentno zajedno događaju tj. kovariraju odnosno u slučaju postojanja uzroka (senzori za skeniranje lica i šarenice), uviđamo posljedicu (obrana od terorističkih napada). Alternativna objašnjenja, kao što su ta da se terorizam u zračnim lukama smanjio neovisno o implementaciji senzora za skeniranje iz razloga što bilo tko da je prošao kroz zračnu luku se snima i skenira prema tome ovo objašnjenje možemo odbaciti. Također postoje prijetnje internoj (uzročnoj) valjanosti. Prva prijetnja jest s obzirom na sudionike kod kojih se može dogoditi da u vrijeme provođenja eksperimenta sazriju odnosno da se dogodi prirodna promjena. To bi značilo da sudionici koji su kao mlađi radili teže prekršaje sada shvaćaju da je to loše za njihovu budućnost i promjene svoj način života na bolje. Takav razvoj situacije može dovesti do alternativnih objašnjenja, a da bismo to izbjegli, situaciju kontroliramo ostalim ljudima koji prođu kroz zračnu luku. To bi značilo da ako se prirodna promjena događa i kod ostalih ljudi koji prolaze, zanemarujemo u istraživanju mogućnost sazrijevanja kao moguće objašnjenje. Također, iduća prijetnja s obzirom na sudionike jest selekcija, odnosno to je razlika u karakteristikama odabranih subjekata. Takva prijetnja se može eliminirati budući da kroz zračnu luku prolaze ljudi koje mi, kao istraživači nismo namjerno izabrali.

Druga prijetnja jest s obzirom na instrumente koje koristimo prilikom mjerenja. Prilikom istraživanja može se dogoditi da imamo nisku valjanost konstrukata, odnosno kada instrumentom mjerimo neki drugi konstrukt ili svojstvo, a ne ono što promatramo. Slijedeća prijetnja jest ako se instrument promijeni tijekom istraživanja, tada se može dogoditi da pogrešno zaključimo jer smo promijenili metodu kojom mjerimo istraživanje. Iduća prijetnja jest testiranje (osjetljivost) koje utječe na sudionike. U ovoj prijetnji se može dogoditi da sudionik budući da zna da se objekt snima, može moderirati svoje ponašanje. S takvim ishodom situacije možemo izvesti potpuno krive zaključke. Treća prijetnja jest s obzirom na neprirodne/umjetne reakcije. Neprirodne reakcije ne mora imati samo sudionik već i sam istraživač – efekt očekivanja istraživača. Kod ove prijetnje se može dogoditi da mi kao istraživači inzistiramo naći korelaciju između naših konstrukata.Ovo je moguće riješiti kroz dizajn istraživanja koji je nepoznat za istraživača odnosno istraživač u tom slučaju ne zna što očekivati od sudionika istraživanja. Četvrta prijetnja jest s obzirom na dizajn/procedure. Prijetnja internoj valjanosti jest dvosmislena vremenska prednost koja označava situaciju kada nismo sigurni prethodi li naš hipotetski uzrok promatranoj posljedici. Slijedeća prijetnja jest povijest, odnosno ako se neki nepredviđeni događaj dogodi tijekom istraživanja, a nije dio istraživanja, može pružiti alternativno objašnjenje.

# Zaključak

Ovim smo radom potvrdili alternativnu hipotezu, odnosno dokazali smo da postoji veza između korištenja senzora za prepoznavanje lica i šarenice te prevencije terorističkih napada. U zračnoj luci, uporabom napredne tehnologije poput senzora za prepoznavanje lica i šarenice smanjena je mogućnost terorističkih napada budući da senzor služi kao prevencija i odmah se u startu može reagirati i prije nego što terorist pokuša nešto učiniti.

Terorizam može zahvatiti bilo koje mjesto na kugli zemaljskoj, ali njegove posljedice postaju globalne. Ne smijemo zaboraviti kako je terorizam uvijek bio i ostat će nasilje s transparentnim ciljem sijanja straha, razlika se javlja jedino u načinu na koji to postiže. Nikada to nije riječ o nepromišljenim akcijama pojedinaca, iza svakog čina stoji dobro razrađena taktika organizacije.

Masovni mediji daju terorizmu globalni doseg, utječu na način na koji javnost percipira terorizam i opasnost od njega, utječu na političke odluke kojima se odgovara na terorizam, ali i na odnose koji su oblikovani nacionalnim i međunarodnim politikama. No, unatoč tome današnja tehnologija se razvila do te mjere da se pravilnim baratanjem mogu učiniti mjere opreza svjetskih razmjera.

# Literatura

Fahmy, S. S., 2017.. Media, Terrorism, and Society: Perspectives and Trends in the Digital Age. *Mass Communication and Society*, 24. Listopad, Issue 6, pp. 735-739.

Jackson, B. A., 2001.. Technology Acquisition by Terrorist Groups. *Studies in Conflict and Terrorism*, p. 49.

Jackson, R., n.d. *ENCYCLOPÆDIA BRITANNICA.* [Mrežno]
Available at: https://www.britannica.com/topic/war-on-terrorism

Jenkins, J. P., n.d. *ENCYCLOPÆDIA BRITANNICA.* [Mrežno]
Available at: https://www.britannica.com/topic/terrorism

Plungis, J., n.d. *ENCYCLOPÆDIA BRITANNICA.* [Mrežno]
Available at: https://www.britannica.com/topic/Reassessing-Airport-and-Airline-Security-1947186

Radaković, Đ., 2016. Analiza pozitivnopravne Nacionalne strategije za prevenciju i suzbijanje terorizma. *Policija i sigurnost*, 25(3/2016), pp. 244-258.

Ricijaš, N., Kovčo-Vukadin, I. & Hundrić, D. D., 2017.. *Strengthening Juvenile Justice Systems in the counter-terrorism context: capacity-building and peer-learning among stakeholders.* [Mrežno]
Available at: https://www.bib.irb.hr/971726?&rad=971726

Sofaer, A. D., n.d. *TECHNOLOGY FOR PREVENTING TERRORISM,* Stanford: Hoover Institution, Stanford University.

1. Technology for preventing Terrorism - Abraham D. Sofaer, Hoover Institution, Stanford University [↑](#footnote-ref-1)
2. Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption - Brian A. Jackson, Center for International science and Technology Policy, Elliott School of International Affairs George Washington University [↑](#footnote-ref-2)
3. Analiza pozitivnopravne Nacionalne strategije za prevenciju i suzbijanje terorizma – Đurđica Radaković [↑](#footnote-ref-3)