ISSN 2744-239X

ZAŠTITA I SIGURNOST

GODINA 5, BROJ 2., DECEMBAR 2025.

IZDAVAČ / PUBLISHER

Asocijacija za upravljanje rizicima AZUR

Association for Risk Management AZUR

ZA IZDAVAČA / FOR THE PUBLISHER:

Zlatko Moratić, predsjednik

ISSN: 2744-239X

Adresa uredništva / Adress: *Vitomira Lukića 12A, 71000 Sarajevo*

Časopis izlazi dva puta godišnje. Sadržaj i sažeci radova dostupni su na web stranici: www.zisjournal.com. Svi radovi podliježu anonimnim recenzijama. / The journal is published twice a year. The contents and abstracts of the papers are available on the website: www.zisjournal.com. All papers are subject to anonymous peer review.

Časopis „Zaštita i sigurnost“ je naučnoistraživački časopis u izdanju Asocijacije za upravljanje rizicima AZUR u Bosni i Hercegovini, koji je vođen idejom podsticanja i afirmacije naučnih istraživanja u tehničkim i društvenim naukama. Časopis pruža idealnu priliku autorima da artikuliraju i prezentiraju svoje naučne spoznaje s ciljem proširivanja postojećih znanja iz navedenih oblasti, te pruža priliku mladim autorima koji se nalaze na početku karijere i žele steći naučnu i istraživačku afirmaciju kako u okviru domaće, tako i u okviru međunarodne naučne javnosti. Kroz objavljivanje naučnih i stručnih radova u navedenom časopisu želimo da podstaknemo interdisiplinarno i multiperspektivno izučavanje kompleksnih tema, kao i savremeni metodološki i teorijski pristup.

Riječ glavnog urednika

Poštovane čitateljice i čitaoci,

Zadovoljstvo mi je predstaviti 10. elektronsko izdanje časopisa "Zaštita i sigurnost" sa 11 autorizovanih članaka iz oblasti sigurnosti i zaštite. Deseto izdanje časopisa obrađuje različite teme iz oblasti sigurnosnih rizika (saobraćajna infrastruktura, zračni i željeznički promet, zlostavljanje i seksualna eksploatacija djece, hibridni sukob, površinska miniranja, efikasnost krivičnih postupaka itd..). Ovog puta smo u prilici da predstavimo različite forme sigurnosnih rizika i koncept njihovog prepoznavanja, identifikovanja i eliminisanja, u aspektu preventivne i represivne aktivnosti prema subjektima prava, zbog nezakonitog činjenja ili propuštanja radnji propisanih određenim zakonskim rješenjima. Većina objavljenih članaka ima dimenziju humanističkog i društvenog, u fokusu zaštite života i integriteta ljudi, od najmlađih uzrasta, usljed problema s kojima se susreću društva u tranziciji, kakva je Bosna i Hercegovina, čije institucije još uvijek nisu dovoljno snažne da da mjerama prevencije i represije osujete svjesno ili nesvjesno ugrožavanje života ljudi i materijalnih dobara.

Glavni urednik

Prof. Dr. Danislav Drašković dipl.ing

SADRŽAJ / CONTENTS

IDENTIFIKACIJA I UPRAVLJANJE KRITIČNOM INFRASTRUKTUROM U ZONAMA PRUŽNIH PRELAZA - STUDIJA SLUČAJA GRAD PRIJEDOR -

DOI: *10.70329/2744-2403.2025.5.10.1*

Naučni rad

prof.dr.sc. Danislav Drašković,[1]

doc.dr. Edin Garaplija,[2]

doc.dr.sc. Zoran Injac,[3]

Sažetak:

U radu je izvršena analiza bezbjednosnih rizika na kritičnoj infrastrukturi u zonama pružnih prelaza, sinteza problema, prijedlozi mjera, sa posebnim osvrtom na vanredne događaje na putnim prelazima, na području Grada Prijedor. Akcenat je stavljen na identifikaciju generatora bezbjednosnih rizika za kritičnu infrastrukturu kroz nedorečenu zakonsku regulativu koju treba promijeniti. U dijelu upravljanja identifikovanim bezbjednosnim rizicima, posebno je apostrofirana potreba za opštom primjenom standarda i direktive EN 2557/2022, kao i prilagođavanje nacionalne zakonske regulative u pogledu geometrije ose puta u odnosu na kolosjek, međusobne udaljenosti putnih prelaza i nagibi pristupnih puteva u odnosu na kolosjek. Vizuelni ambijent sa aspekta primenjenih zakonskih kriterijuma koje treba da ispuni pružno-putni prelaz, takođe je tertian u ovom istarživačkom radu. Navedeni elementi su neophodni za obezbjeđenje putnih prelaza sa sistemskim pristupom rješavanju problema, a koji zahtjeva investicije u cilju omogućavanja bezbjednog saobraćaja u uslovima povećanja brzine kretanja vozova na teritoriji grada Prijedora.

Ključne riječi: *kritična infrastruktura**,** rizici, bezbjednost, vanredni događaj, pružno putni prelazi.*

[1] Panevropski univerzitet Apeiron, danislav.m.draskovic@apeiron-edu.eu

[2] INZA Group, info@azur.ba

[3] Panevropski univerzitet Apeiron, zoran.dj.injac@apeiron-edu.eu

1. Uvod

Prelaz puta preko željezničke pruge u nivou (putni prelaz ili putno-pružni prelaz) je četvorokraka raskrsnica preko kojeg se ukrštaju dva vida saobraćaja (drumski i željeznički). Tehničko-tehnološke i organizacione karakteristike željeznice odredile su joj prioritet kod ukrštanja u odnosu na drumski saobraćaj (od strane planera, organizatora i zakonodavaca), čime je i definisan način regulisanja saobraćaja preko prelaza.

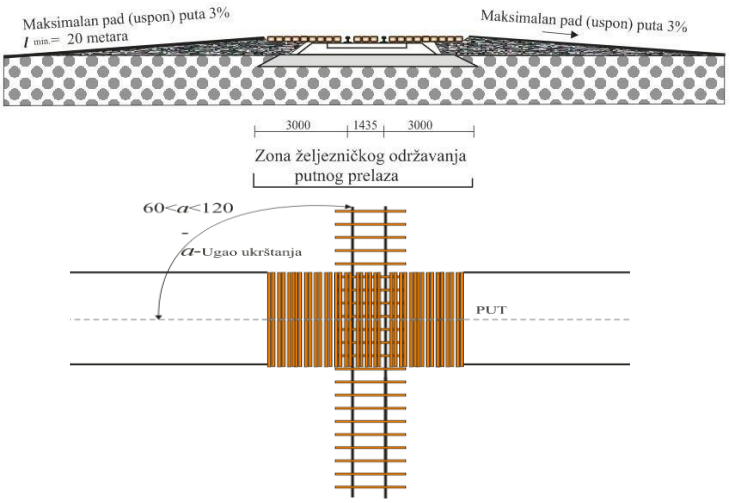
Željeznički saobraćaj (u kinematičkom smislu) s jedne strane je ograničen stepenom slobode kretanja, a sa druge strane (u dinamičkom smislu) generiše veliku kinetičku energiju prilikom kretanja što ima za posljedicu dugačak zaustavni put, a saobraćaj obavlja u kompozicijama voznih jedinica. Drumski saobraćaj se odlikuje većim stepenom slobode kretanja, pojedinačnim voznim jedinicama, manjom kinetičkom energijom, te kratkim zaustavnim putem.

Željeznički saobraćaj zahtjeva stroge režime tj. ispravnost i stabilnih i mobilnih kapaciteta u funkciji kompozicije, dok kod drumskog saobraćaja saobraćajnice po kojoj se kreću drumska vozila u kvalitetu variraju od običnog ruralnog puta do savremenog autoputa i vrlo su razgranate.

Kako bi se na sveobuhvatan način riješilo pitanje otpornosti subjekata koji su kritični za pravilno funkcionisanje unutrašnjeg transportnog sistema, EU Direktivom 2557/2022 uspostavlja se sveobuhvatan okvir koji se odnosi na otpornost kritičnih subjekata u pogledu svih opasnosti, bilo prirodnih ili uzrokovanih ljudskim djelovanjem, uzrokovanih slučajno ili namjerno [1], [10].

U skladu sa odredbama koje se odnose na kritičnu infrastrukturu kao i nacionalnih željezničkih propisa, ukrštanje željezničke pruge i puta mora se denivelisati u slučaju kada se na prelazu odvija intenzivan protok (preko 7000 vozila u danu) ili kada je preko pruge učestao saobraćaj (120 vozova na jednokolosiječnoj pruzi ili 240 vozova na dvokolosiječnoj pruzi). Učestalost vozova određuje željeznica, a protok drumskih vozila je direktno zavisan od pokretljivosti stanovništva, aktivnosti privrede i izbora puta od strane korisnika putne infrastructure [3].

Na Slici 1 šematski su prikazani osnovni elementi-propisani standardi kod projektovanja i izgradnje puta preko željezničke pruge u nivou.



Slika 1. *Prelaz puta preko željezničke pruge u primjeni propisanih standarda*

Na infrastrukturi željezničke korporacije u Republici Srpskoj postoji 278 prelaza puta preko željezničke pruge, od čega je u eksploataciji 259 prelaza.

U pogledu bezbjednosti, evidentan je sljedeći nivo osiguranja:

- Trougao preglednosti (259)
- Branici (18)
- Svjetlosno zvučna signalizacija (1)

Standard propisuje, da kod ukrštanja puta i pruge u nivou, drumska saobraćajnica bude u nivou sa GIŠ u dužini od 3 m od ose kolosjeka, poslije toga kolovoz puta ne smije imati veći nagib od 3 % na minimalnoj dužini od 20 metara i mora biti sa savremenim kolovozom. Takođe, ukrštanje mora biti pod uglom ne manjim od 60 stepeni i ne većim od 120 stepeni.

Postojeća regulative na željeznici, regulativa koja uređuje oblast javnih puteva, te propisi iz domena prostornog uređenja, definišu saobraćaj u zoni prelaska puta preko željezničke pruge, na sljedeći način [11], [12]:

- Ukrštanje željezničke pruge i puta, određivanje mjesta na kojima se može izvesti ukrštanje pruge i puta i utvrđivanje mjera koje se moraju preduzeti radi obezbjeđenja odvijanja saobraćaja na putnim prelazima propisuje se zavisno od protoka i gustine saobraćaja, preglednosti željezničke pruge, brzine vožnje na pruzi i putu, i od drugih mjesnih uslova koji su od značaja za bezbjednost saobraćaja.
- Ukrštanje željezničke pruge i autoputa i ukrštanje pruge i puta u

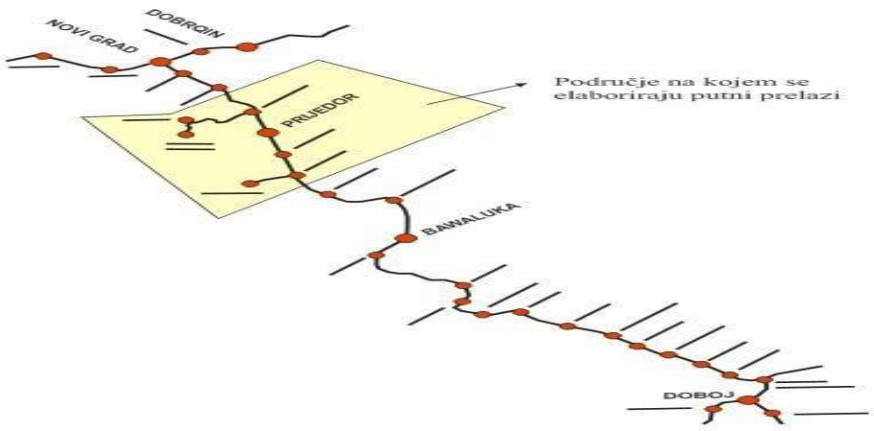
staničnom prostoru između ulaznih, odnosno izlaznih skretnica, od kojih počinju stanični kolosjeci, ne može biti u istom nivou.

- Ukrštanje željezničke pruge i puta koji nema svojstvo autoputa ne može biti u istom nivou ako je saobraćaj motornih vozila na putu vrlo gust ili ako je željeznički saobraćaj na pruzi učestao i ako to zahtjevaju posebni uslovi na mjestu ukrštanja pruge i puta, i drugi razlozi bezbjednosti željezničkog saobraćaja.
- Minimalno rastojanje između dva putna prelaza ne može biti manje od 1000 metara, odnosno izuzetno 700 metara.
- Nekategorisane puteve potrebno je preusmjeriti na najbliži javni put, a ako to nije moguće treba ih međusobno povezati i izvesti ukrštanje na jednom mjestu. Mjesto ukrštanja određuju u konkretnom slučaju željeznička korporacija i lokalna uprava.
- Putni prelaz je sastavni dio pruge sa obje strane kolosjeka u širini od 3 metra od ose kolosjeka sa produžetkom ukrštajućeg puta od 20 metara čiji nagib ne smije biti veći od 3%. Dio prelazne pruge i ukrštajući put u dužini od 3 metra od ose kolosjeka obavezni su održavati željeznička korporacija, a ostali dio upravljač puta, i lokalna uprava na čijoj se teritoriji nalazi putni prelaz.

2. Podaci o putnim prelazima

Upravljač željezničkog saobraćaja na prugama Republike Srpske, "ŽRS" AD Doboj, je sačinio Elaborat o evidenciji i stanju prelaza puta preko željezničke pruge. Na dionici pruge (Doboj)- Niševići-Svodna-(Novi Grad) počev od stacionaže pruge Doboj-Novi Grad km 128+714 do km 165+350, Omarska-Tomašica i Brezičani-Ljubija na teritoriji Grada Prijedor nalaze se 63 pružno-putna prelaza u nivou (željezničke pruge i drumskih saobraćajnica), i to 34 ukrštanja na pruzi (Doboj)-Niševići-Svodna-(Novi Grad), 10 ukrštanja na pruzi Omarska-Tomašica i 19 ukrštaja na pruzi Brezičani-Ljubija [2].

Na Slici 2 šematski je prikazana pruga Doboj-Novi Grad gdje se na osjenčenom dijelu analiziraju putni prelazi na teritoriji lokalne zajednice Grada Prijedora.



Slika 2: *Disperzija prelaza pute preko željezničke pruge, na relaciji Doboj-Novi Grad, sa apostrofiranjem na teritoriju Grada Prijedora*

Drumski saobraćaj na ovim putnim prelazima je u rasponu od slabog inteziteta do umjerenog i jakog inteziteta, prelaz na tzv. „trinaesta“. Iz navedenog, lako se zaključuje da postoji neopravdano veliki broj prelaza koji značajno umanjuju kvalitet pruge i njen rang upoređujući je sa ostalim savremenim prugama okruženja. Neophodno je preduzeti odgovarajuće mjere redukovanja i osiguranja putnih prelaza koje bi se sprovele u skladu sa zakonskim propisima, primjenjujući saobraćajne, građevinske, urbanističke i ekonomske kriterijume.

Postojeće stanje putnih prelaza posmatrano je kroz sledeće karakteristike:

A. Analitičko prezentovanje
B. Disperzija putnih prelaza
C. Bezbjednost saobraćaja na prelazu puta preko željezničke pruge
D. Vizuelno i šematsko prezentovanje (preko fotografija i šema)

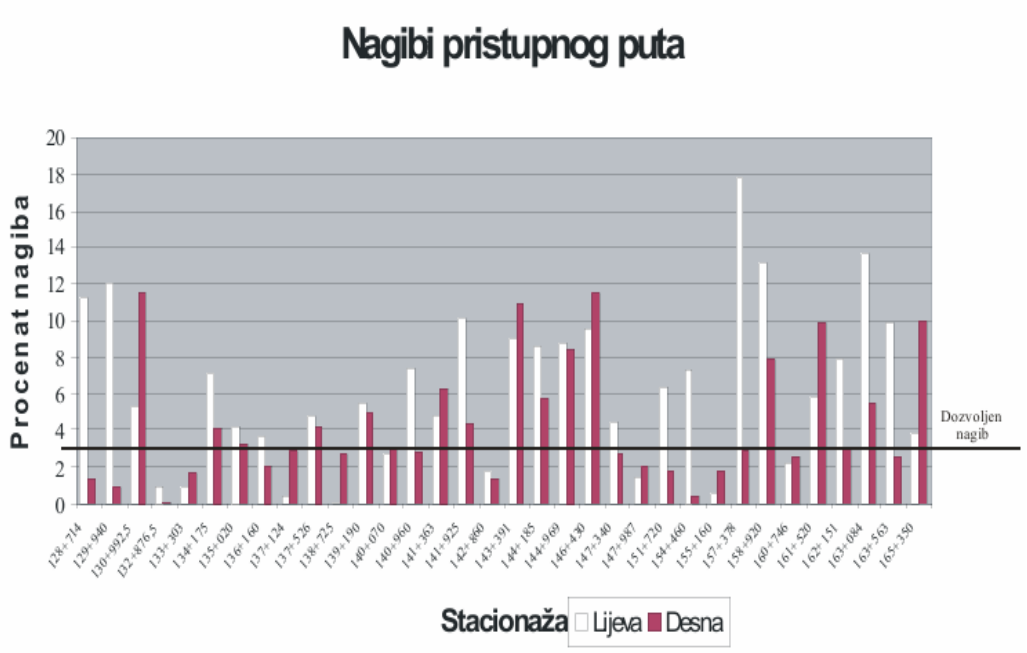
2.1 Analitička prezentacija

Na području Grada Prijedor postoje 54 putna prelaza, od čega su 33 putna prelaza zaštićena saobraćajnim znakovima na pristupnom putu („Andrejin krst“ i „znak zabrane“ STOP) i trouglom preglednosti, 2 putna prelaza, pored saobraćajnih znakova na putu, zaštićena su i branikom kojom se rukuje ručno i 19 neosiguranih putnih prelaza, na pruzi Brezičani – Ljubija, koja su van eksploatacije.

Posmatrajući i analizirajući pojedine karakteristika putnih prelaza uočava se da se radi o nižem nivou sigurnosti putnih prelaza, sa sljedećim karakteristikama:

- Trouglovi preglednosti na većini putnih prelaza nisu obezbjeđeni;
- Ukrštanje se obezbjeđuje preko drvenih pragova;
- Ugao ukrštanja puta i pruge preko 3 prelaza je veći od dozvoljenog;
- Nagibi puta su nestandardni, jer značajno premašuju 3% (Grafik 1).

Na Grafiku 1 prikazani su nagibi pristupnog puta u zonama prelaska puta preko željezničke pruge u nivou na teritoriji Grada Prijedora.



Grafik 1. *Grafički prikaz nagiba pristupnih puteva*

Na Grafiku 1 je očigledno je da su nagibi pristupnog puta na većem dijelu prelaza veći od dozvoljenih 3 % što značajno ugrožava bezbjednost saobraćaja na prelazima naročito u zimskom preiodu.

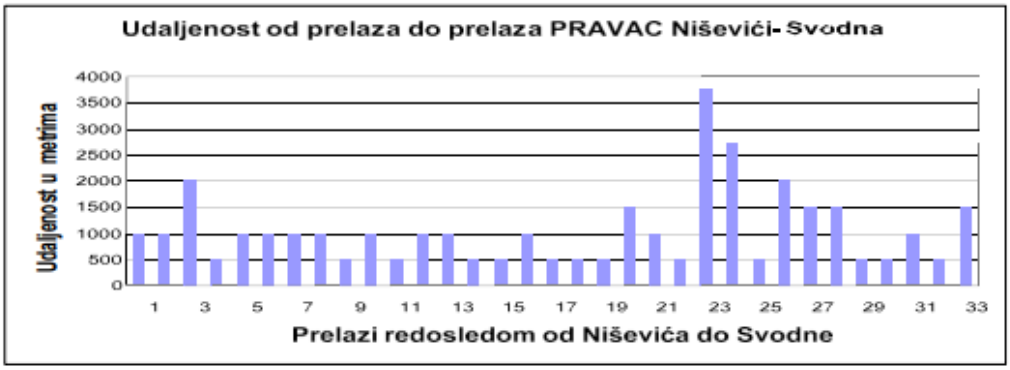
Takođe, evidentna su nepovoljna stanja, koja usložnjavaju situaciju u smislu bezbjednosti i kvaliteta saobraćaja, u formi:

- Kod velikog broja putnih prelaza, pri izgradnji, nisu poštovani Zakonom propisani uslovi (nedostaje tehnička dokumenatacija).
- Ne postoje ozvaničena podzakonska akta kojima se detaljnije definišu uslovi projektovanja, građenja i načina održavanja putnih prelaza.

- Postoji određeni broj prelaza na kojima je učestalost udesa značajno veće nego na ostalim prelazima, što ukazuje na potrebu za iznalaženjem boljih tehničkih rješenja i obezbjeđenje dodatnih materijalnih sredstava.
- U našoj zemlji nema dovoljno licenciranih preduzeća za opremanje prelaza niti je jasno definisan tehnički pregled i predaja u eksploataciju (saobraćaj) prelaza, u skladu sa Zakonom.
- Kod manjeg broja prelaza nisu ispunjeni jedan ili više Zakonom propisanih uslova (trougao preglednosti, ugao ukrštanja, nagib nivelete puta u dužini od 20 metara od ose kolosjeka, međusobna udaljenost mnogo manja od Zakonom propisane i dr.). Nameće se potreba za otklanjanjem značajnih nedostataka i usmjeravanje dva ili više javnih puteva na zajedničko mjesto ukrštanja, odnosno usmjeravanjem nekategorisanih puteva na javne puteve.
- Ako ne postoje uslovi da se ispoštuju zakonske norme, prelazi se moraju zatvoriti, nakon što se građanima omogući alternativni pristup objektima stanovanja.

2.2 Disperzija putnih prelaza

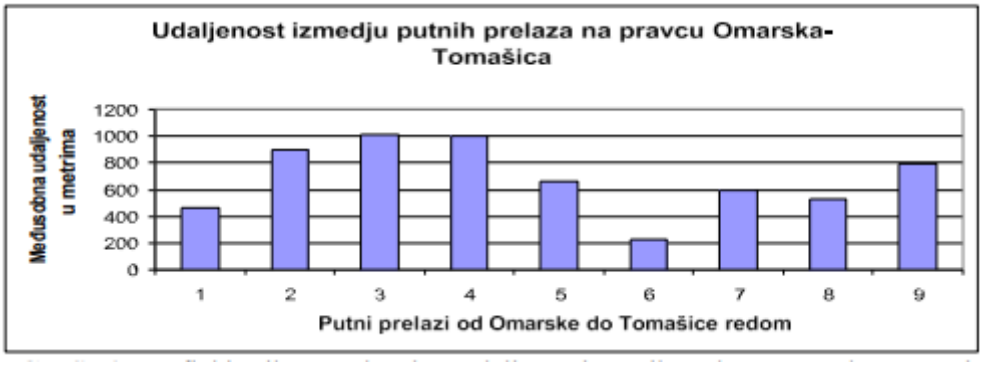
Na dionici Ništevići-Svodna, samo 12 prelaza ima međusobnu udaljenost veću od 1000 metara. Neki od prelaza (Grafik 2) su međusobno udaljeni manje od 500 metara, što je za konkretan nivo ranga pruge nedopustivo



Grafik 2. *Grafički prikaz međusobne udaljenosti putnih prelaza Ništevići-Svodna*

Evidentan je i mali broj putnih prelaza na međusobnoj udaljenosti većoj od 1000 metara. Zanemarljiv je broj prelaza na međusobnoj udaljenosti od 2000 metara (samo 3) što je veoma zabrinjavajuće.

Pruga Omarska-Tomašica (Grafik 3) je u još kompleksnijoj situaciji. Međusobne udaljenosti ne prelaze 1000 metara. Kao što se sa grafika može vidjeti postoje prelazi čija je međusobna udaljenost nešto više od 200 metara.



Grafik 3. *Grafički prikaz međusobne udaljenosti putnih prelaza Omarska-Tomašica*

Slična je situacija i na pruzi Brezičani-Ljubija, na kojoj su samo 4 prelaza na međusobnoj udaljenost većoj od 1000 metara

Grafik 4. *Grafički prikaz međusobne udaljenosti putnih prelaza Brezičani-Ljubija*

2.3 Bezbjednost saobraćaja na prelazu puta preko željezničke pruge

Pod pojmom vanrednog događaja, smatra se događaj zbog kojeg je nastala najmanje jedna od sljedećih posljedica: smrt, teža ozljeda, materijalna šteta, prekid saobraćaja, ugrožavanje ili otežavanje željezničkog saobraćaja.

Vanredni događaji na putnim prelazima na području koje pokriva željeznička korporacija u petogodišnjem vremenskom period [4], [9], predstaljeni su u Tabeli

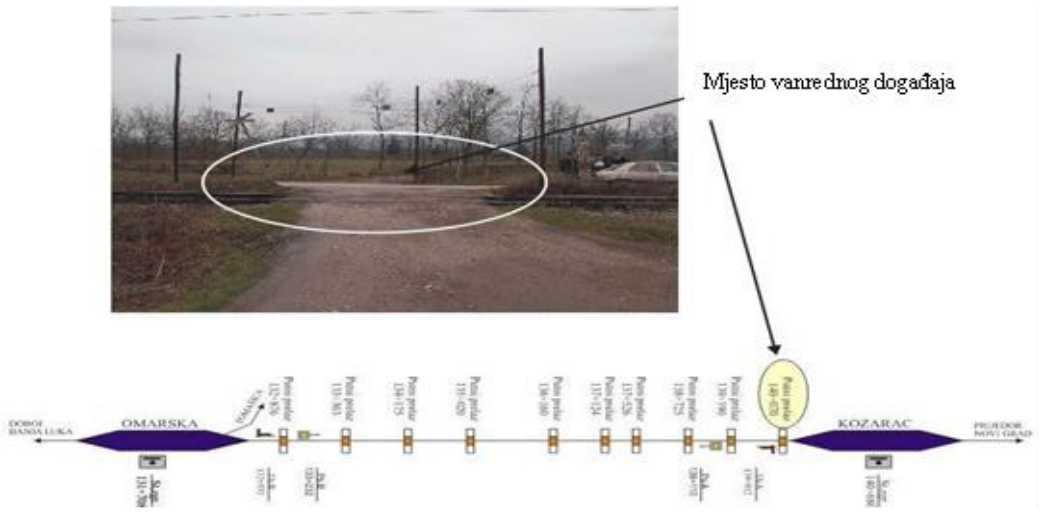
Tabela 1. *Pregled vanrednih događaja na PP u RS i na području Grada Prijedor u periodu 5 godina*

R.br.	VREMENSKI PERIOD	1.god		2.god		3.god		4.god		5.god		Ukupno	
		ŽRS	PD	ŽRS	PD	ŽRS	PD	ŽRS	PD	ŽRS	PD	ŽRS	PD
1	Vanredni događaj na PP	25	3	14	1	20	4	22	3	20	1	101	12
2	Smrtno stradalo lice		-		-	6	-	2	1	3	-	11	1
3	Teže ozlijeđeno lice	4	-	6	3	4	1	9	2	3	-	26	6
4	Prekid saobraćaja (h)	3	2	13	1	36	6	24	5	19	-	124	14
5	Materijalna šteta	24	-	14	1	20	4	20	3	20	-	100	8

Evidentno je da prelazi puta preko željezničke pruge na teritoriji lokalne zajednice Grada Prijedora, značajno učestvuju u dijelu ukupnog broja vanrednih događaja (12 %), teže ozlijeđenih je 6 od ukupno 26 koliko je u Republici Srpskoj evidentirano u posmatranom periodu. Evidentirano je i 14 prekida željezničkog saobraćaja, na teritoriji lokalne zajednice.

Ako se tome dodaju niske brzine saobraćanja vozova, tada se može zaključiti da je izuzetno nizak kvalitet prevoza, u direktnoj vezi sa bezbjednosnim ciljevima, koji se mogu postići samo niskim brzinama u eksploataciji željezničkog saobraćaja.

Na Slici 3 prikazan je jedan od fotografisanih prelaza puta preko željezničke pruge, koji može poslužiti kao reprezent stanja prelaza na teritoriji Grada Prijedora.



Slika 3. *Karakterističan prelaz puta preko željezničke pruge na teritoriji Grada Prijedor*

3. Metodologija rješavanja bezbjednosnog problema

U cilju podizanja nivoa bezbijednosti saobraćaja u zonama prelaza puta preko željezničke pruge u nivou, potrebno je utvrditi metodološki pristup rangiranja kriterija koji utiču na donošenje menadžerskih odluka, posebno kada je u pitanju podizanje nivoa maksimalnih brzina vozova [5], [6], [7].

S tim u vezi, obaveza upravljača puta i upravljača željezničkog saobraćaja, je da prije donošenja odluke (rekonstrukcija, modernizacija, investicije. itd.), utvrde sljedeća stanja:

1. Parametre toka drumskog saobraćaja preko preko željezničke pruge:
   - Protok vozila
   - Gustinu toka
   - Brzine
   - Vrijeme putovanja-prelaska vozila u toku
   - Jedinično vrijeme putovanja-prelaska vozila u toku
   - Vremenske intervale slijeđenja vozila u toku
   - Rastojanje sleđenja vozila u toku
2. Vidljivost na putnom prelazu:
   - Dobra
   - Djelomična i
   - Ograničena
3. Položaj putnog prelaza:
   - PP u stanici, i
   - PP na otvorenoj pruzi
4. Broj kolosjeka na putnom prelazu
5. Broj i karakter vanrednih događaja na konkretnom putnom prelazu
6. Geološki, građevinski, urbanistički i zakonski uslovi, i
7. Ekonomski pokazatelji.

Izabrani kriterijumi su fizički parametri koji imaju presudan uticaj na nivo osiguranja prelaza puta preko željezničke pruge, i poslužiće u svakom pojedinačnom slučaju kao osnov za određivanje vrste osiguranja putnih prelaza. Na osnovu navedenih kriterijuma vrši se rangiranje prelaza, u cilju utvrđivanja prioriteta u projektovanju i modernizaciji prelaza. U konkretnom

slučaju na bazi ustanovljenih kriterija, potrebno je utvrditi optimalan broj prelaza, iste projektovati u funkciji tehničko-trehnoloških i ekonomskih kriterija, te za svaki pojedinačni tvrditi nivo sigurnosti prelaza.

4. Zaključak

Veliki broj prelaza puta preko željezničke pruge na teritoriji Grada Prijedora, u najvećem broju slučajeva nisu urbanističko-građevinski legalizovani odnosno nisu projektovani i izvedeni u skladu sa propisima i standardima. Nastali su u vremenu nelegalne gradnje određenih gradskih naselja, koja nisu prethodno usklađena sa prostorno-planskim aktima lokalne zajednice.

U fazi legalizacije navedenih naselja, vršena je "sanacija" pojedinačnih objekata stanovanja, a da projekat saobraćajnog rješenja, posebno prelaska puta preko željezničke pruge nije rađen, čime se ostavila mogućnost građanima da pojedinačno ili grupno rješavaju problem, suprotno građevinskim ili saobraćajnim standardima, a pogotovo izostankom primjene directive EU 2557/2022 kojom se regulišu odnosi prema kritičnoj infrastrukturi.
Kako ne postoji mogućnost zatvaranja pojedinih prelaza, prije nego što se građanima ne omogući alternativni pristup objektima stanovanja, neophodno je ustanoviti sljedeće periode aktivnosti:

- Kratkoročni periodi, koje podrazumjevaju bolje obezbjeđenje postojećih prelaza, sa pozicije saobraćajne signalizacije (vertikalna, svjetlosna, zvučna), trougla preglednosti i stvaranja baze podataka za buduća planiranja redukovanja putnih prelaza, kako bi se došlo do zadovoljavajućih rješenja u budućnosti.

- Srednjoročni periodi, koje podrazumjevaju potrebu izrade prostorno-planske dokumentacije u cilju vršenja eksproprijacije zemljišta u zaštitnom pojasu pruge, kako bi se stvorili uslovi za gradnju "sabirne" saobraćajnice, koje bi prethodile aktivnostima smanjenja odnosno redukovanja broja prelaza puta preko željezničke pruge.

- Dugoročni periodi, koje podrazumjevaju utvrđivanje minimalno potrebnog broja prelaza i lociranje istih u prostoru, izrada tehničke dokumentacije, izgradnja i opremanje prelaza primjenom ITS – automatsko regulisanje saobraćaja na prelazu puta preko željezničke pruge, sa bezbjendosne distance kretanja šinskog vozila. Takođe, donošenje nacionalnog zakonskog okvira koji tertira kritičnu infrastrukturu i definiše subjekte odgovorne za upravljanje istom.

LITERATURA

[1] Brunner, E. M., Suter, M."International Critical Information Infrastructure Protection Handbook", Center for Security Studies, ETH Zurich, 2009

[2] Dakić, B." Elaborat o putnim prelazima na ŽRS", Republička uprava za inspekcije poslove Republike Srpske, Banja Luka. 2008

[3] Đuričić, R., Bošković, B., Rosić, S."European concept of railway safety", Faculty of Transportation, Doboj, 2017

[4] DG-ECHO,"European Emergency Response Capacity", Directorate-General for European Civil Protection and Humanitarian Aid Operations, 2015

[5] European Railway Agency (ERA), Railway Safety Management System, Version 1, 2010

[6] Kadić, A."MOGUĆNOST FORMIRANJA HRVATSKOG TIMA STRUKTURNIH INŽENJERA UNUTAR EUROPSKOG KAPACITETA ZA ODGOVOR NA HITNE SITUACIJE (EERC)", ZiS Journal 4(2), pp 94-108, 2024

[7] Kalač, S., Hodžić, J. and Lukač, D."Improvement of the Safety System in the Railway Infrastructure of Montenegro", TTTP 5(2), pp 57-63, 2020

[8] Railway Safety Directive 49/2004 / EC, European Commission, 2004

[9] Živojević, E. & Baručija, A."KORIŠTENJE GEO-BIM PLATFORME ZA UPRAVLJANJE U KRIZNIM SITUACIJAMA I NA KRITIČNOJ INFRASTRUKTURI", ZiS Journal 4(1), pp 94- 101, 2024

[10] https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[11] https://putevirs.com/korisnik/dokumenti/Zakon_o_javnim_putevima.pdf

[12] https://vladars.rs/sr-SP_Cyrl/Vlada/Ministarstva/msv/pravniiadministrativniokvir/PublishingImages/Pages/default/ЗаконожељезницамаРепубликеСрпскеСлужбенигласник РепубликеСрпске-број2019-17

IDENTIFICATION AND MANAGEMENT OF CRITICAL INFRASTRUCTURE IN RAILWAY CROSSING AREAS - CASE STUDY CITY OF PRIJEDOR -

DOI: *10.70329/2744-2403.2025.5.10.1*

Scientific article

prof.dr.sc. Danislav Drašković,[4]

doc.dr. Edin Garaplija,[5]

doc.dr.sc. Zoran Injac,[6]

ABSTRACT:

The paper analyzes safety risks in critical infrastructure in the areas of railway crossings, synthesizes problems, proposes measures, with special emphasis on emergency events at railway crossings in the area of the city of Prijedor. Emphasis is placed on identifying generators of safety risks for critical infrastructure through incomplete legal regulations that need to be changed. In the part of managing identified safety risks, the need for general application of standards and directives EN 2557/2022 is particularly emphasized, as well as the adjustment of national legal regulations regarding the geometry of the road axis in relation to the track, the mutual distance of railway-road crossings and the slopes of access roads in relation to the track, which is also emphasized in this paper. The visual environment from the aspect of the applied legal criteria that a railway-road crossing should meet is tertiary in this research manuscript. The above elements are necessary for securing railway-road crossings with a systematic approach to solving problems, which requires investments in order to enable safe traffic in conditions of increasing train speeds in the territory of the city of Prijedor.

Key words*: critical infrastructure, risks, safety, emergency, railway crossings.*

[4] Panevropski univerzitet Apeiron, danislav.m.draskovic@apeiron-edu.eu

[5] INZA Group, info@azur.ba

[6] Panevropski univerzitet Apeiron, zoran.dj.injac@apeiron-edu.eu

1. Introduction

A level crossing (road-rail crossing) represents a four-legged intersection where two types of traffic intersect: road and rail. The technical, technological, and organizational characteristics of the railway have determined its priority at intersections compared to road traffic (by planners, organizers, and legislators), thereby defining the method of regulating traffic at the crossing.

Railway traffic, in a kinematic sense, is on one hand limited by the degree of freedom of movement, while on the other hand, in a dynamic sense, it generates significant kinetic energy during motion, resulting in a long stopping distance, and traffic occurs in compositions of rolling stock units. Road traffic is characterized by a higher degree of freedom of movement, individual vehicles, lower kinetic energy, and a shorter stopping distance.

Railway traffic requires strict regimes, i.e., the reliability and stability of both mobile and fixed capacities according to the composition of rolling stock units, whereas in road traffic, the roads on which vehicles move vary in quality—from ordinary rural roads to modern highways—and are highly branched.

To comprehensively address the resilience of entities critical to the proper functioning of the internal transport system, EU Directive 2557/2022 establishes a comprehensive framework concerning the resilience of critical entities against all types of hazards, whether of natural origin or caused by human activity, accidentally or intentionally [1], [10].

In accordance with provisions relating to critical infrastructure as well as national railway regulations, the intersection of a railway line and a road must be grade-separated in cases where the crossing experiences intensive traffic flow (over 7,000 vehicles per day) or when rail traffic is frequent (120 trains on a single-track line or 240 trains on a double-track line). Train frequency is determined by the railway, while road traffic flow depends on population mobility, economic activity, and the route choice of road infrastructure users [3].

Figure 1 schematically presents the basic elements and prescribed standards for the design and construction of a road at a level railway crossing.

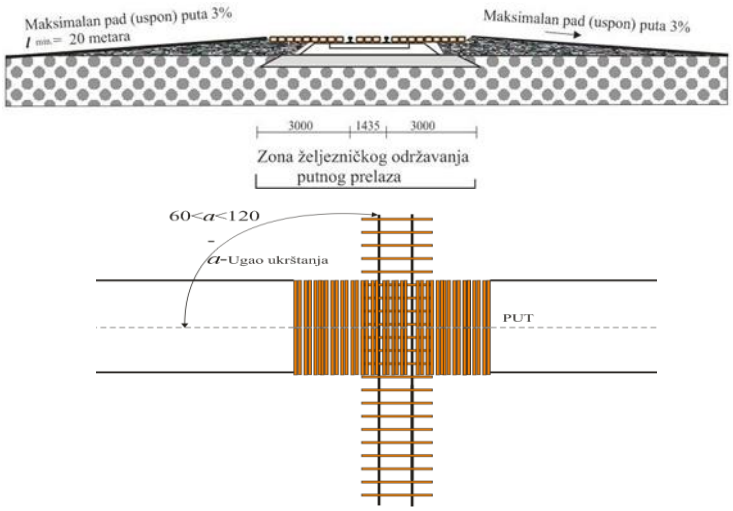


Figure 1. *Road crossing over a railway track in accordance with the prescribed standards*

On the railway infrastructure of the Railway Corporation in the Republic of Srpska, there are 278 level crossings, of which 259 are currently in operation.

Regarding safety, the following levels of protection are recorded:

- Sight triangle (259)
- Barriers (18)
- Light and sound signaling (1)

The standard prescribes that at a level crossing of a road and railway, the roadway must be level with the track gauge for a length of 3 m from the track centerline; beyond this, the road surface must not have a gradient greater than 3% over a minimum length of 20 meters and must be equipped with a modern pavement. Furthermore, the crossing must be at an angle of no less than 60 degrees and no more than 120 degrees.

Existing railway regulations, regulations governing public roads, and spatial planning regulations define traffic in the zone of a level railway crossing as follows [11], [12]:

- The intersection of a railway and a road, determination of locations where such crossings may be constructed, and the measures that must be taken to ensure safe traffic at level crossings are prescribed depending on

traffic flow and density, railway visibility, speed on the railway and the road, and other local conditions relevant to traffic safety.

- The intersection of a railway and a highway, as well as the intersection of a railway and a road within station areas between entry and exit switches, from which station tracks originate, must not be at the same level.
- The intersection of a railway and a road that is not classified as a highway must not be at the same level if motor vehicle traffic on the road is very heavy, if rail traffic is frequent, or if special conditions at the crossing site or other railway safety reasons require it.
- The minimum distance between two level crossings must not be less than 1,000 meters, or exceptionally 700 meters.
- Unclassified roads must be redirected to the nearest public road; if this is not possible, they should be connected to each other and the crossing constructed at a single location. The crossing location in each specific case is determined by the railway corporation and the local authority.
- The level crossing is considered an integral part of the railway on both sides of the track for a width of 3 meters from the track centerline, with an extension of the intersecting road for 20 meters, the gradient of which must not exceed 3%. The portion of the crossing within 3 meters from the track centerline is to be maintained by the railway corporation, while the remaining section is the responsibility of the road authority and the local administration in whose territory the crossing is located.

2. Data on Level Crossings

The railway traffic operator on the railways of the Republic of Srpska, "ŽRS" AD Doboj, prepared a Report on the Records and Condition of Road-Rail Crossings. On the railway section (Doboj)–Niševići–Svodna–(Novi Grad), from the Doboj–Novi Grad track kilometer 128+714 to km 165+350, as well as Omarska–Tomašica and Brezičani–Ljubija within the territory of the City of Prijedor, there are 63 level crossings (railway and road intersections), including 34 crossings on the (Doboj)–Niševići–Svodna–(Novi Grad) line, 10 crossings on the Omarska–Tomašica line, and 19 crossings on the Brezičani–Ljubija line [2].

Figure 2 schematically presents the Doboj–Novi Grad railway, where the shaded section highlights the level crossings analyzed within the territory of the local community of the City of Prijedor.

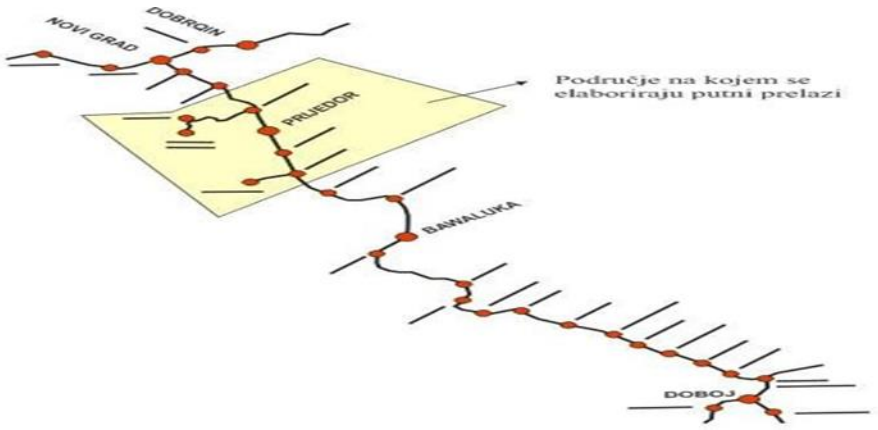


Figure 2: *Distribution of road-rail level crossings along the Doboj–Novi Grad route, highlighting the territory of the City of Prijedor*

Road traffic at these level crossings ranges from low to moderate and high intensity, with one crossing classified as "thirteenth." From this, it can be easily concluded that there is an unjustifiably large number of crossings, which significantly reduces the quality of the railway and its classification compared to other modern railways in the region. It is necessary to implement appropriate measures to reduce and secure level crossings in accordance with legal regulations, applying traffic, construction, urban planning, and economic criteria.

The current state of level crossings has been considered through the following characteristics:
A. Analytical presentation
B. Distribution of level crossings
C. Traffic safety at road-rail crossings
D. Visual and schematic presentation (through photographs and diagrams)

2.1 Analytical Presentation

In the territory of the City of Prijedor, there are 54 level crossings, of which 33 are protected by traffic signs on the access road ("Andrejin cross" and "STOP" sign) and a sight triangle, 2 crossings are additionally protected by a manually operated barrier, and 19 crossings on the Brezičani–Ljubija line are unsecured and out of operation.

Observing and analyzing the individual characteristics of the level crossings, it is evident that they represent a lower level of safety, with the following characteristics:

- Sight triangles are not provided at most level crossings;
- Intersections are secured with wooden sleepers;
- The crossing angle of the road and railway at 3 crossings exceeds the permitted limit;
- Road gradients are non-standard, significantly exceeding 3% (Figure 1).

Figure 1 shows the gradients of access roads in the zones of level railway crossings within the territory of the City of Prijedor.

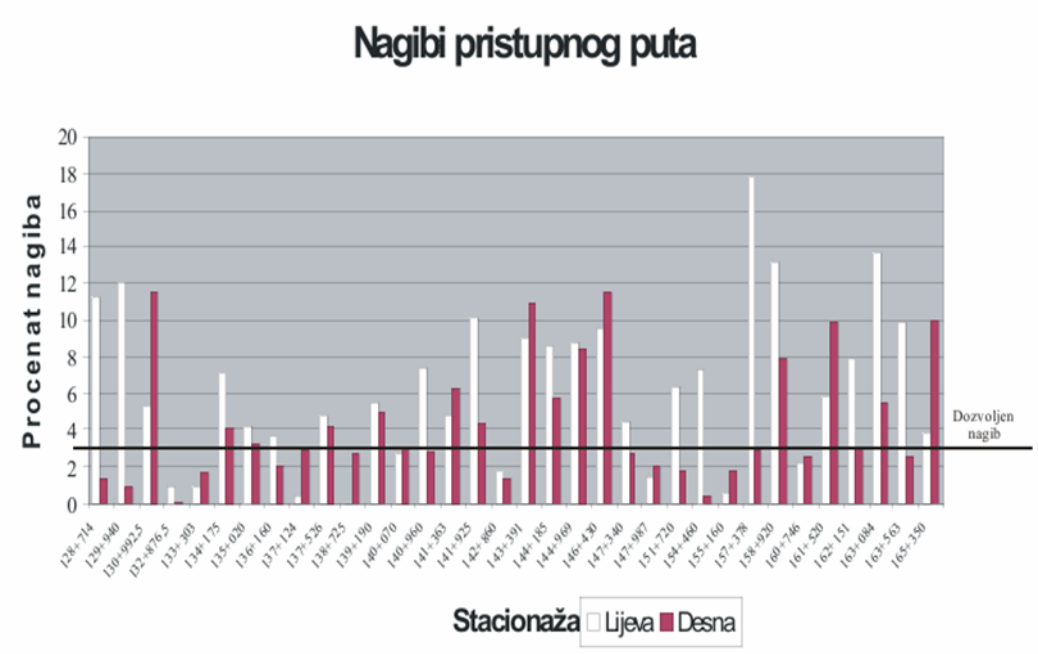


Figure 1. *Graphical representation of access road gradients*

In Figure 1, it is evident that the gradients of the access roads at most crossings exceed the permissible 3%, significantly compromising traffic safety at the crossings, especially during the winter period.

Furthermore, unfavorable conditions are apparent, complicating the situation in terms of traffic safety and quality, as follows:

- At a large number of level crossings, construction did not comply with legally prescribed conditions (technical documentation is missing).
- There are no officially enacted subordinate regulations that define in detail the conditions for designing, constructing, and maintaining level crossings.
- A certain number of crossings exhibit a significantly higher frequency of accidents compared to others, indicating the need for better technical solutions and the provision of additional material resources.
- In our country, there are insufficient licensed companies for equipping crossings, and the technical inspection and commissioning (traffic operation) of crossings in accordance with the Law are not clearly defined.
- At a smaller number of crossings, one or more legally prescribed conditions are not met (sight triangle, crossing angle, road gradient over 20 meters from the track centerline, minimum distance between crossings significantly shorter than legally required, etc.). This necessitates the elimination of major deficiencies and the direction of two or more public roads to a common crossing point, or the rerouting of unclassified roads to public roads.
- If it is not possible to comply with legal standards, crossings must be closed after providing residents with alternative access to their properties.

2.2 Distribution of Level Crossings

On the Ništevići–Svodna section, only 12 crossings are spaced more than 1,000 meters apart. Some crossings (Figure 2) are located less than 500 meters from each other, which is unacceptable for this specific railway classification.

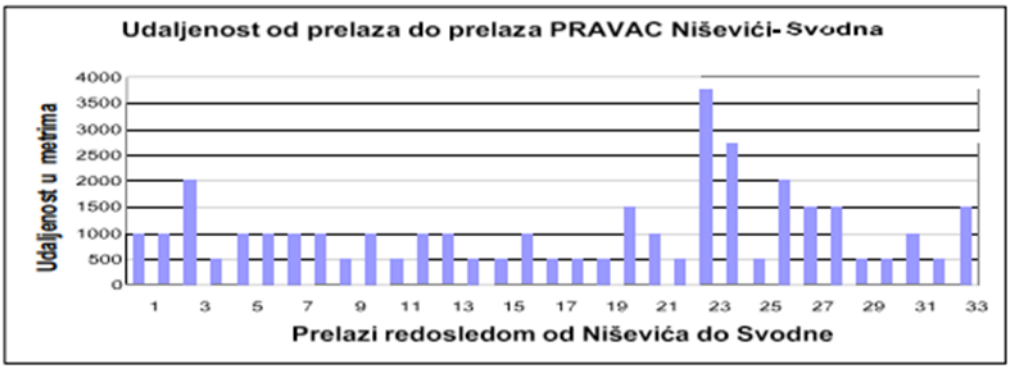


Figure 2. *Graphical representation of the spacing between level crossings on the Ništevići–Svodna section*

A small number of level crossings are spaced more than 1,000 meters apart, and the number of crossings with a spacing of 2,000 meters is negligible (only 3), which is highly concerning.

The Omarska–Tomašica railway (Figure 3) presents an even more complex situation. The distances between crossings do not exceed 1,000 meters. As shown in the figure, there are crossings with a spacing of just over 200 meters.

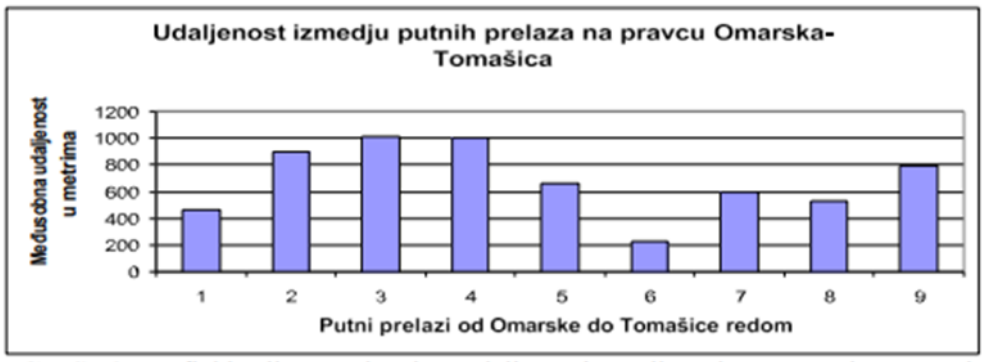


Figure 3. *Graphical representation of the spacing between level crossings on the Omarska–Tomašica section*

2.3 Traffic Safety at Road-Rail Level Crossings

An extraordinary event is defined as an incident that results in at least one of the following consequences: death, serious injury, material damage, traffic disruption, or endangerment or obstruction of railway operations. Extraordinary events at level crossings within the area covered by the railway corporation over a five-year period [4], [9] are presented in the Table.

Table 1*. Overview of extraordinary events at level crossings in the RS and in the territory of the City of Prijedor over a 5-year period*

S. num	TIME PERIOD	1. year		2. years		3. years		4. years		5. years		Total	
		ŽRS	PD	ŽRS	PD	ŽRS	PD	ŽRS	PD	ŽRS	PD	ŽRS	PD
1	Emergency event on PP	25	3	14	1	20	4	22	3	20	1	101	12
2	Fatality		-		-	6	-	2	1	3	-	11	1
3	Severely injured	4	-	6	3	4	1	9	2	3	-	26	6
4	Traffic interruption (h)	3	2	13	1	36	6	24	5	19	-	124	14
5	Material damage	24	-	14	1	20	4	20	3	20	-	100	8

It is evident that level crossings within the territory of the local community of the City of Prijedor account for a significant portion of the total number of extraordinary events (12%), with 6 of the 26 serious injuries recorded in the Republic of Srpska during the observed period occurring there. Additionally, 14 railway traffic disruptions were recorded within the local community.

Considering the low train operating speeds, it can be concluded that the quality of transport is extremely low, directly related to safety objectives, which can only be achieved through low speeds in railway operations.

Figure 3 shows one of the photographed level crossings, which can serve as a representative example of the condition of crossings within the territory of the City of Prijedor.

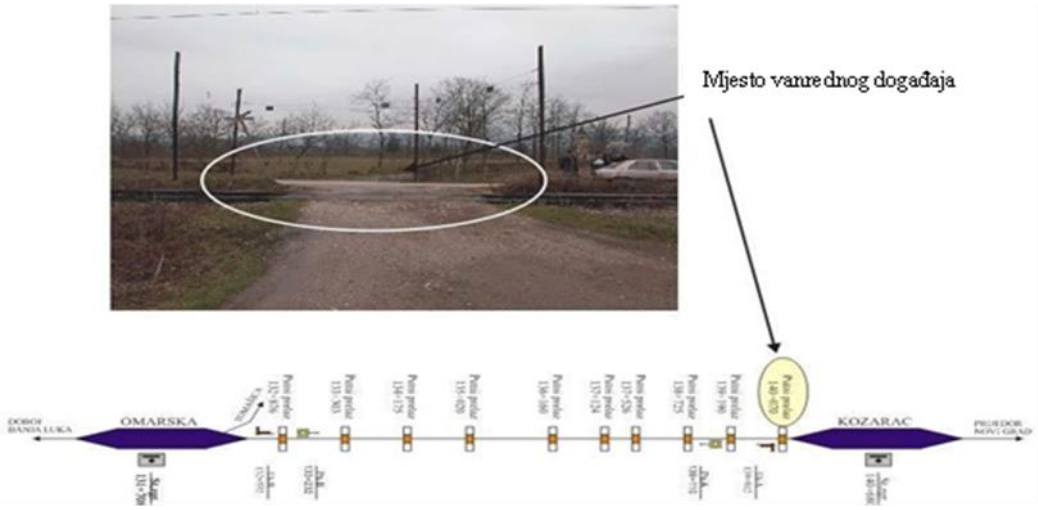


Figure 3. *Representative road-rail level crossing in the territory of the City of Prijedor*

3. Methodology for Addressing the Safety Issue

In order to increase traffic safety in the zones of level road-rail crossings, it is necessary to establish a methodological approach for ranking the criteria that influence managerial decision-making, particularly regarding the increase of maximum train speeds [5], [6], [7].

In this context, the responsibility of the road operator and the railway traffic operator is to determine the following conditions before making decisions (reconstruction, modernization, investments, etc.):

1. **Parameters of road traffic flow over the railway crossing:**

   - Vehicle flow
   - Traffic density
   - Speeds
   - Travel time of vehicles crossing
   - Unit travel time of vehicles crossing
   - Time intervals between successive vehicles
   - Vehicle spacing during crossing

2. **Visibility at the level crossing:**

- Good
- Partial
- Limited

3. **Position of the level crossing:**

- Crossing within a station
- Crossing on an open track

4. **Number of tracks at the level crossing**
5. **Number and nature of extraordinary events at the specific crossing**
6. **Geological, construction, urban planning, and legal conditions**
7. **Economic indicators**

The selected criteria are physical parameters that have a decisive impact on the safety level of a road-rail crossing and will serve in each individual case as the basis for determining the type of crossing protection. Based on these criteria, crossings are ranked to establish priorities in the design and modernization of crossings. In the specific case, it is necessary to determine the optimal number of crossings, design them according to technical, technological, and economic criteria, and assert the safety level for each individual crossing.

4. Conclusion

A large number of road-rail level crossings within the territory of the City of Prijedor, in most cases, are not urbanistically or constructionally legalized, meaning they were not designed and executed in accordance with regulations and standards. They emerged during a period of illegal construction of certain urban settlements, which were not previously aligned with the spatial planning acts of the local community.

During the legalization phase of these settlements, individual residential buildings were "remedied," but traffic planning, particularly the design of road-rail crossings, was not carried out. This allowed residents to address the issue individually or collectively, contrary to construction and traffic standards, and especially without the application of EU Directive 2557/2022, which regulates relations concerning critical infrastructure.

Since it is not possible to close individual crossings before providing residents with alternative access to their properties, the following activity periods need to be established:

- **Short-term periods**, involving better securing of existing crossings through traffic signage (vertical, light, and sound signals), sight triangles, and creating a database for future planning of level crossing reduction to achieve satisfactory solutions in the future.
- **Medium-term periods**, involving the preparation of spatial planning documentation for the expropriation of land within the railway protective zone, creating conditions for the construction of "collector" roads, which would precede activities aimed at reducing the number of road-rail level crossings.
- **Long-term periods**, involving the determination of the minimally required number of crossings and their spatial location, preparation of technical documentation, construction, and equipping of crossings using ITS – automatic traffic control at the road-rail crossing, ensuring safe train movement distances. Additionally, this includes the adoption of a national legal framework that regulates critical infrastructure and defines the entities responsible for its management.

LITERATURE

[1] Brunner, E. M., Suter, M."International Critical Information Infrastructure Protection Handbook", Center for Security Studies, ETH Zurich, 2009

[2] Dakić, B." Elaborat o putnim prelazima na ŽRS", Republička uprava za inspekcije poslove Republike Srpske, Banja Luka. 2008

[3] Đuričić, R., Bošković, B., Rosić, S."European concept of railway safety", Faculty of Transportation, Doboj, 2017

[4] DG-ECHO,"European Emergency Response Capacity", Directorate-General for European Civil Protection and Humanitarian Aid Operations, 2015

[5] European Railway Agency (ERA), Railway Safety Management System, Version 1, 2010

[6] Kadić, A."MOGUĆNOST FORMIRANJA HRVATSKOG TIMA STRUKTURNIH INŽENJERA UNUTAR EUROPSKOG KAPACITETA ZA ODGOVOR NA HITNE SITUACIJE (EERC)", ZiS Journal 4(2), pp 94-108, 2024

[7] Kalač, S., Hodžić, J. and Lukač, D."Improvement of the Safety System in the Railway Infrastructure of Montenegro", TTTP 5(2), pp 57-63, 2020

[8] Railway Safety Directive 49/2004 / EC, European Commission, 2004

[9] Živojević, E. & Baručija, A."KORIŠTENJE GEO-BIM PLATFORME ZA UPRAVLJANJE U KRIZNIM SITUACIJAMA I NA KRITIČNOJ INFRASTRUKTURI", ZiS Journal 4(1), pp 94- 101, 2024

[10] https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[11] https://putevirs.com/korisnik/dokumenti/Zakon_o_javnim_putevima.pdf

[12] https://vladars.rs/sr-SP_Cyrl/Vlada/Ministarstva/msv/pravniiadministrativniokvir/PublishingImages/Pages/default/ЗаконожељезницамаРепубликеСрпскеСлужбенигласник РепубликеСрпске-број2019-17

EFIKASNOST KRIVIČNIH POSTUPAKA

DOI: *10.70329/2744-2403.2025.5.10.2*

Naučni članak

Redžepović Adnan, MA iur.

Sažetak

Efikasnost krivičnih postupaka predstavlja jedan od temeljnih pokazatelja kvaliteta i funkcionalnosti pravosudnog sistema svake države. U radu se analizira pojam i značaj efikasnosti kroz normativne, institucionalne i praktične aspekte, s posebnim osvrtom na pravni okvir Bosne i Hercegovine i međunarodne standarde prava na suđenje u razumnom roku. Ukazuje se na uzroke neefikasnosti, uključujući preopterećenost sudova, nedostatak procesne discipline, kao i organizacione, kadrovske i normativne nedostatke koji utiču na dužinu trajanja krivičnih postupaka. Komparativnim pristupom prikazana su rješenja i dobre prakse pojedinih evropskih pravnih sistema koje su doprinijele ubrzanju i racionalizaciji procesnih faza, jačanju nadzora nad radom sudova i tužilaštava te unapređenju upravljanja predmetima. Posebna pažnja posvećena je ekonomskoj dimenziji efikasnosti i mogućnostima primjene alternativnih postupaka, kao što su oportunitet, sporazum o priznanju krivice i medijacija, kao mehanizama za rasterećenje sudova. Naglašava se potreba za jačanjem institucionalnih kapaciteta, digitalizacijom pravosuđa, uvođenjem naprednih informacionih sistema i dosljednom primjenom načela procesne ekonomičnosti. Zaključuje se da se efikasnost krivičnih postupaka mora graditi na uravnoteženom odnosu između brzine odlučivanja i poštivanja prava na pravično suđenje kao osnovnog elementa vladavine prava.

Ključne riječi: *efikasnost, krivični postupak, pravosuđe, razuman rok, procesna ekonomičnost, sudska praksa, reforme pravosuđa, komparativni pristup, ekonomska analiza, Bosna i Hercegovina*

1. Uvod

Efikasnost krivičnih postupaka predstavlja jedno od temeljnih pitanja savremenog pravosuđa, budući da direktno utiče na ostvarivanje prava na pravično suđenje, povjerenje građana u pravni sistem i vladavinu prava u cjelini. Ona nije samo tehničko pitanje brzine postupanja sudova, nego kompleksan pravni i institucionalni izazov koji obuhvata organizaciju pravosudnih organa, primjenu procesnih pravila, te sposobnost države da obezbijedi djelotvorno, pravedno i transparentno vođenje krivičnih postupaka. Efikasnost je stoga indikator ne samo funkcionalnosti sudskog sistema, nego i zrelosti demokratskog poretka i nivoa zaštite temeljnih ljudskih prava.

U savremenom pravu, posebno pod okriljem Evropske konvencije o ljudskim pravima, efikasnost je usko povezana s pravom na suđenje u razumnom roku iz člana 6. Konvencije. Evropski sud za ljudska prava u svojoj bogatoj praksi više puta je isticao da država ima pozitivnu obavezu da obezbijedi funkcionisanje sudova na način koji omogućava okončanje postupka u razumnom vremenu. Slično ističu i Kovačević i dr. (2025), naglašavajući da je „pravovremeno preduzimanje radnji u fazi kriminalističke obrade ključan korak“ u osiguravanju efikasnog krivičnog postupka. Kako navodi Petrović (2025), „iako su zakonske restrikcije neophodne, one moraju biti usklađene sa refleksijom ljudskih prava“. Time se efikasnost ne sagledava isključivo kao organizacioni standard, već kao ljudsko pravo čije se nepoštovanje može smatrati povredom osnovnih sloboda. Ovaj standard postaje još značajniji u tranzicijskim pravnim sistemima, među koje spada i Bosna i Hercegovina, gdje su institucionalni kapaciteti i normativni okviri često opterećeni naslijeđenim strukturnim problemima.

U pravosudnom sistemu Bosne i Hercegovine pitanje efikasnosti krivičnih postupaka dobija posebnu težinu usljed dugotrajnosti sudskih procesa, preopterećenosti sudova i neujednačene sudske prakse. Prema izvještajima Visokog sudskog i tužilačkog vijeća BiH i Evropske komisije, prosječno trajanje krivičnih predmeta u domaćim sudovima i dalje značajno premašuje standarde utvrđene u državama članicama Evropske unije. Takvo stanje utiče ne samo na ostvarivanje prava stranaka, već i na povjerenje građana u institucije, jer prolongirani postupci stvaraju percepciju nedjelotvornosti i nepravičnosti pravosudnog sistema. U takvom kontekstu, efikasnost postaje nužan preduslov legitimnosti pravosuđa i osnovni pokazatelj njegove sposobnosti da ispuni svoju društvenu funkciju.

Efikasni krivični postupci doprinose i ostvarivanju šireg društvenog interesa. Brzo i pravilno procesuiranje krivičnih djela ima preventivni karakter, jer šalje jasnu poruku o dosljednoj primjeni zakona i odgovornosti za protupravna ponašanja. Istovremeno, smanjuje rizik od sekundarne viktimizacije žrtava, jača osjećaj pravne sigurnosti i povjerenje javnosti u institucije. Neefikasnost, nasuprot tome, generira višestruke negativne posljedice: pravne, ekonomske i psihološke. Ona povećava troškove postupaka, opterećuje budžet pravosuđa, smanjuje produktivnost institucija i stvara osjećaj bespomoćnosti kod građana koji traže zaštitu svojih prava. S aspekta društvene stabilnosti i ekonomskog razvoja, neefikasno pravosuđe djeluje kao prepreka investicionom ambijentu i ukupnom razvoju društva, budući da neizvjesnost u pogledu sudske zaštite destimulira pravne subjekte da traže institucionalna rješenja sporova.

Pored pravnih i organizacionih, efikasnost ima i izraženu ekonomsku dimenziju. Troškovi koji nastaju zbog dugotrajnih postupaka ne odnose se samo na sudove i tužilaštva, već i na učesnike u postupku, advokate, svjedoke i društvo u cjelini. Neefikasni postupci generiraju dodatne budžetske izdatke, dok istovremeno smanjuju dostupnost pravde i produktivnost pravosudnih resursa. U tom smislu, unapređenje efikasnosti nije samo pitanje pravne reforme, nego i racionalnog upravljanja javnim resursima, što je naročito značajno u državama s ograničenim institucionalnim kapacitetima poput Bosne i Hercegovine. Stoga se pitanje efikasnosti krivičnih postupaka mora posmatrati i kroz prizmu ekonomske održivosti i dugoročne strategije razvoja pravosudnog sistema.

Analizom efikasnosti krivičnih postupaka potrebno je obuhvatiti tri osnovne dimenzije: normativnu, institucionalnu i praktičnu. Normativna dimenzija odnosi se na kvalitet procesnih propisa, njihovu usklađenost s međunarodnim standardima i dosljednost u primjeni. Institucionalna podrazumijeva organizaciju pravosudnog sistema, raspodjelu nadležnosti i resursa, te sistem nadzora nad radom sudova i tužilaštava. Praktična dimenzija obuhvata svakodnevno funkcionisanje pravosudnih organa, stepen profesionalnosti nosilaca pravosudnih funkcija, dostupnost tehnologije i razvijenost upravljačkih mehanizama u vođenju predmeta. Tek kombinovanom analizom ovih faktora moguće je razumjeti uzroke i posljedice neefikasnosti, te definisati realne mjere za njeno unapređenje.

Metodološki okvir rada zasniva se na kombinaciji doktrinarne, komparativne, deskriptivne i analitičke metode. Doktrinarna metoda korištena je za analizu zakonodavnog okvira i pravnih standarda koji regulišu krivične postupke u Bosni i Hercegovini, posebno Zakona o krivičnom postupku BiH, Zakona o sudovima i relevantnih međunarodnih instrumenata. Komparativna metoda omogućila je poređenje domaće prakse s praksama država koje su reformisale svoje krivične postupke u pravcu veće efikasnosti, poput Njemačke, Švedske i Hrvatske, sa posebnim naglaskom na iskustva u digitalizaciji pravosudnih procesa. Analitička metoda primijenjena je u obradi podataka i u identifikaciji uzroka prolongiranja

sudskih postupaka, dok je deskriptivna metoda omogućila pregled i interpretaciju izvještaja Visokog sudskog i tužilačkog vijeća BiH, Evropske komisije i Transparency Internationala o stanju efikasnosti pravosuđa. Ovakav interdisciplinarni pristup osigurava sveobuhvatan pogled na problem efikasnosti i pruža osnovu za izradu realnih i primjenjivih preporuka.

Cilj rada je da se, polazeći od analize važećih propisa, sudske prakse i komparativnih iskustava, identifikuju ključni uzroci neefikasnosti krivičnih postupaka u Bosni i Hercegovini, te da se predlože konkretne mjere za njihovo prevazilaženje. Istraživanje je usmjereno na analizu institucionalnih slabosti, procjenu stepena usklađenosti domaćeg sistema s evropskim standardima i identifikaciju rješenja koja mogu doprinijeti bržem, transparentnijem i racionalnijem vođenju postupaka. Očekuje se da rezultati analize doprinesu razumijevanju odnosa između efikasnosti i pravičnosti, te da posluže kao teorijska i praktična osnova za unapređenje pravosudnih politika, digitalizaciju procesa i jačanje profesionalne odgovornosti nosilaca pravosudnih funkcija. Efikasnost krivičnih postupaka, u tom kontekstu, ne predstavlja samo mjerilo tehničkog uspjeha pravosuđa, već i ključni indikator povjerenja građana u institucije i stabilnosti pravnog sistema koji čini temelj svakog demokratskog društva.

Dosadašnja istraživanja o efikasnosti krivičnih postupaka ukazuju na to da je riječ o višedimenzionalnom fenomenu koji obuhvata pravne, institucionalne i društvene aspekte. Bejatović (2015) u svom radu *Efikasnost krivičnog postupka kao međunarodni pravni standard i reforma krivičnog procesnog zakonodavstva Srbije* naglašava da je efikasnost od suštinskog značaja za ostvarivanje pravde te da zavisi ne samo od zakonskih normi, nego i od organizacije pravosuđa, stručnosti i motivisanosti procesnih subjekata. On ukazuje da kriminalno-politički razlozi i implementacija procesnih instrumenata efikasnosti u nacionalna zakonodavstva čine osnovu modernih reformi u ovoj oblasti.

Preporuka Komiteta ministara Vijeća Evrope (CM/Rec(2010)12) dodatno precizira da se efikasnost pravosuđa ne može mjeriti isključivo brzinom odlučivanja, već kvalitetom sudskih odluka donesenih u razumnom roku nakon nepristrasnog razmatranja svih relevantnih pitanja. Samo takve odluke, prema preporuci, ostvaruju svrhu krivičnog postupka – istovremenu zaštitu društva od kriminaliteta i očuvanje osnovnih ljudskih prava optuženih.

Međunarodna iskustva potvrđuju da su saradnja pravosudnih institucija i procesna disciplina ključni faktori efikasnosti. U okviru inicijativa Visokog sudskog i tužilačkog vijeća Bosne i Hercegovine i međunarodnih ekspertskih timova, analizirani su modeli međuinstitucionalne saradnje u Bijeljini, Zenici i Sarajevu. Zaključeno je da unapređenje komunikacije između sudova, tužilaštava i advokature doprinosi kraćem trajanju postupaka i većoj procesnoj disciplini stranaka.

Analiza zakonskog okvira pokazuje da je Zakon o krivičnom postupku Bosne i Hercegovine, kao temeljni procesni akt, usklađen s međunarodnim standardima, naročito s Evropskom konvencijom o ljudskim pravima. Međutim, u poređenju s evropskim praksama, domaći sistem se suočava s izazovima u dosljednoj primjeni procesnih pravila i ujednačavanju sudske prakse. U većini država članica EU prisutna je primjena inkvizitornog sistema, dok BiH koristi mješoviti model koji kombinuje elemente inkvizitornog i adversarnog postupka, što nerijetko dovodi do različitih interpretacija zakonskih normi.

Dalje, praksa država poput Njemačke i Švedske pokazuje da specijalizovani sudovi i digitalizacija procesnih tokova značajno doprinose ubrzanju postupaka i boljoj raspodjeli resursa. U Bosni i Hercegovini, iako postoje odjeljenja unutar sudova specijalizovana za određene vrste predmeta, nedostatak tehničkih resursa i kontinuirane obuke ograničava njihovu punu efikasnost.

Uspostavljanje efikasnog sistema međunarodne pravne pomoći, kao i jačanje saradnje s evropskim pravosudnim mrežama, ključni su preduslovi za borbu protiv transnacionalnog kriminala i osiguranje pravovremene razmjene informacija i dokaza. Iako BiH posjeduje solidan normativni okvir, implementacija međunarodnih standarda u praksi i dalje predstavlja izazov, što potvrđuju i izvještaji Evropske komisije i VSTV-a BiH (2022).

Zaključno, pregled literature i dosadašnjih istraživanja ukazuje da efikasnost krivičnih postupaka zavisi od kombinacije pravnih reformi, institucionalne koordinacije i primjene savremenih tehnologija. Komparativna iskustva evropskih država potvrđuju da digitalizacija, specijalizacija sudova i profesionalna obuka kadrova predstavljaju ključne faktore unapređenja efikasnosti pravosuđa u tranzicijskim sistemima poput Bosne i Hercegovine.

2. Analiza efikasnosti krivičnih postupaka: komparativni pristup i prijedlozi za unapređenje

Efikasnost krivičnih postupaka ključna je za osiguranje pravičnosti i povjerenja u pravosudni sistem. Analiza se fokusira na pojam efikasnosti u kontekstu krivičnih postupaka, usporedbu s praksama u drugim pravnim sistemima te identifikaciju problema i predlaganje konkretnih rješenja. Naglasak je na prepoznavanju faktora koji utiču na dugotrajnost postupaka i potencijalnim strategijama za njihovo unapređenje.

2.1. Analiza pojma efikasnosti u kontekstu krivičnih postupaka

Efikasnost u krivičnim postupcima podrazumijeva pravovremeno rješavanje predmeta uz istovremeno poštivanje principa pravičnosti. Prema pravnim standardima, efikasnost se ne odnosi samo na brzinu vođenja postupaka, već i na kvalitet donošenih odluka, koje moraju biti utemeljene na zakonima i dokazima. Neefikasni postupci rezultiraju ne samo produženjem suđenja, već i gubitkom povjerenja građana u pravni sistem.

U Bosni i Hercegovini analiza efikasnosti ukazuje na preopterećenost sudova, nedovoljnu obučenost osoblja i nedostatak resursa kao glavne prepreke. Prema Izvještaju Visokog sudskog i tužilačkog vijeća Bosne i Hercegovine (2022), prosječno trajanje krivičnih postupaka značajno premašuje preporučene rokove, što rezultira gomilanjem neriješenih predmeta. Transparency International (2023) navodi da ovakva situacija dodatno pogoršava percepciju javnosti o pravosudnim tijelima i smanjuje povjerenje građana u njihovu funkcionalnost.

Jedan od ključnih problema je nedostatak jasnih i dosljednih smjernica za primjenu zakonskih normi, što često dovodi do različitih interpretacija zakona među sudijama. Ovo ne samo da produžava trajanje procesa, već i otežava standardizaciju sudske prakse. Pored toga, sudovi se suočavaju sa izazovima kao što su zastarjela infrastruktura i neadekvatan sistem arhiviranja predmeta, što dodatno usporava administrativne procedure.

Modernizacija pravosudne infrastrukture mogla bi značajno unaprijediti efikasnost krivičnih postupaka. Ovo uključuje digitalizaciju sudskih procesa, što omogućava bržu razmjenu informacija između pravosudnih institucija i stranaka. Također, povećanje transparentnosti kroz javno dostupne baze podataka o sudskim predmetima može smanjiti broj grešaka i osigurati bolje praćenje toka postupaka. Obuka sudskog osoblja predstavlja još jedan ključni element za unapređenje efikasnosti. Ulaganje u kontinuiranu edukaciju sudija i tužilaca, posebno u oblastima kao što su primjena novih zakona i upotreba digitalnih tehnologija, može smanjiti broj proceduralnih grešaka i ubrzati donošenje odluka. Također, bolje upravljanje raspodjelom predmeta može pomoći u smanjenju preopterećenosti sudova, omogućavajući sudijama da se fokusiraju na složenije slučajeve.

Efikasnost krivičnih postupaka u konačnici zavisi od koordinisanog djelovanja svih pravosudnih institucija i političke volje za sprovođenje potrebnih reformi. Podrška međunarodnih organizacija, poput Evropske unije i Vijeća Evrope, može pružiti neophodne resurse i ekspertizu za implementaciju ovih promjena.

2.2. Poređenje sa praksama u drugim pravnim sistemima

Uporedna iskustva pokazuju da su sistemi poput onih u Njemačkoj i Švedskoj postigli visok nivo efikasnosti zahvaljujući automatizaciji pravosudnih procesa i primjeni specijalizovanih sudova za različite vrste predmeta. U Švedskoj je, primjerice, uvođenje digitalnih platformi smanjilo trajanje procesa za 30%, dok Njemačka koristi posebne komisije za rješavanje složenih predmeta, čime rasterećuje redovne sudove. Bosna i Hercegovina može koristiti iskustva ovih zemalja kao osnovu za reformu svog pravosudnog sistema, iako ključna razlika leži u pristupu resursima i stepenu investicija u pravosudnu infrastrukturu. Transparency International (2023) naglašava da je nedostatak političke volje za sprovođenje reformi često najveća prepreka implementaciji novih metoda.

U poređenju s Hrvatskom, koja je prošla slične reforme tokom procesa pristupanja Evropskoj uniji, Bosna i Hercegovina ima prednost u tome što može koristiti već razvijene modele. Hrvatska je, primjerice, smanjila broj zaostalih predmeta za 40% zahvaljujući boljoj koordinaciji između različitih pravosudnih tijela. Uvođenje mehanizama za ubrzanje procesa, poput obaveznih rokova za rješavanje predmeta, pokazalo se kao efektivna mjera u povećanju efikasnosti. Primjena automatizovanih sistema u Švedskoj primjer je dobrog upravljanja pravosudnim resursima. Integracija digitalnih alata omogućila je brzo evidentiranje i praćenje slučajeva, čime se smanjuje administrativno opterećenje sudova. Specijalizovani sudovi u Njemačkoj olakšavaju rješavanje složenih predmeta i istovremeno unapređuju kvalitet odluka kroz fokus na specifične oblasti prava.

Implementacija ovakvih praksi u Bosni i Hercegovini zahtijeva prilagođavanje domaćem kontekstu. Reforma pravosudne infrastrukture i ulaganje u edukaciju kadrova mogu omogućiti uspješnu primjenu najboljih međunarodnih praksi. Fokus na transparentnost i odgovornost pravosudnih institucija dodatno bi unaprijedio povjerenje javnosti u pravosudni sistem.

2.3. Identifikacija problema i prijedlozi za poboljšanje

Glavni problemi u krivičnim postupcima u Bosni i Hercegovini uključuju dugotrajnost procesa, nedostatak resursa i neravnomjernu raspodjelu predmeta. Analize ukazuju na manjak stručnog kadra i preopterećenost sudova kao ključne izazove, što uzrokuje kašnjenja u donošenju odluka. Dugotrajnost postupaka, posebno u predmetima korupcije, ističe se kao značajan problem. Prema izvještajima, disciplinski postupci protiv sudija i tužilaca u Bosni i Hercegovini često premašuju predviđene rokove, što dodatno otežava procesuiranje prioritetnih predmeta.

Nedostatak resursa, uključujući zastarjelu infrastrukturu i ograničene budžete, također negativno utiče na efikasnost pravosudnih postupaka. Analize pokazuju

da su sudovi u BiH preopterećeni predmetima, dok istovremeno nemaju adekvatne tehničke alate za upravljanje procesima. Transparency International (2023) i VSTV BiH (2022) potvrđuju da je jedan od uzroka niska stopa digitalizacije i nedostatak sistemskog pristupa optimizaciji sudskih procesa.

Prijedlozi za poboljšanje uključuju:

- Digitalizaciju procesa – uvođenje elektronskih sistema za praćenje predmeta i komunikaciju između sudova i stranaka, čime bi se smanjili administrativni troškovi i ubrzali postupci.
- Obuku sudskog osoblja – kontinuirana edukacija i specijalizacija sudija i tužilaca radi unaprjeđenja kvaliteta donošenja odluka. Njemačka iskustva pokazuju da ulaganje u ljudske resurse doprinosi standardizaciji sudske prakse (Hylton, 2017, str. 337).
- Bolju raspodjelu resursa – povećanje budžeta za pravosuđe i racionalizaciju raspodjele predmeta ključni su faktori za smanjenje opterećenosti sudova. Transparentno planiranje i pravedna alokacija sredstava omogućavaju bolji rad pravosudnih institucija.

Efikasnost krivičnih postupaka, dakle, zavisi od koordinisanog djelovanja svih pravosudnih tijela, političke volje za sprovođenje reformi i adekvatne međunarodne podrške. Implementacija ovih prijedloga zahtijeva posvećenost i integraciju najboljih međunarodnih praksi kako bi se osigurala pravičnost i djelotvornost pravosudnog sistema u Bosni i Hercegovini.

3. Ekonomska analiza efikasnosti krivičnih postupaka

Ekonomska analiza efikasnosti krivičnih postupaka predstavlja važan aspekt razumijevanja funkcionisanja pravosudnog sistema, jer omogućava procjenu ne samo pravnih, već i finansijskih posljedica svakog sudskog procesa. Kroz ovu analizu sagledavaju se ključni ekonomski parametri, uključujući troškove samog postupka, optimalnu raspodjelu resursa i dugoročne koristi efikasnog procesuiranja. Pored direktnih troškova suđenja, kao što su troškovi advokata, sudija i vještaka, posebna pažnja posvećuje se i ekonomskim posljedicama produženih sudskih postupaka, uključujući troškove pritvora, izgubljene radne sate i smanjenje povjerenja građana u pravosudni sistem. Također, analiziraju se prednosti alternativnih mjera poput sporazuma o priznanju krivice, medijacije i drugih metoda koje mogu smanjiti finansijski teret sudova uz očuvanje pravde i zakonitosti.

3.1. Troškovi krivičnih postupaka i analiza resursa

Ekonomsku efikasnost krivičnih postupaka određuju troškovi koji nastaju tokom njihovog trajanja, uključujući direktne i indirektne troškove. Direktni troškovi obuhvataju izdvajanja za plate sudija, advokata i vještaka, dok indirektni uključuju društvene troškove poput gubitka produktivnosti zbog dugotrajnih postupaka. Upravo su ovi faktori ključni za analizu kojom se nastoji postići optimalan balans između pravde i ekonomije u pravosudnim procesima.

3.2. Direktni troškovi krivičnih postupaka

Direktni troškovi uključuju finansijska sredstva potrebna za sprovođenje sudskih procesa. To podrazumijeva budžetska izdvajanja za rad sudova, tužilaštava i odbranu. U razvijenim pravosudnim sistemima postoji tendencija optimizacije ovih troškova kroz uvođenje tehnoloških rješenja i unapređenje procesnih normi. Hylton (2017, str. 329) ističe da povećanje efikasnosti u alokaciji sudskih resursa smanjuje ukupan finansijski teret pravosudnog sistema. Ova optimizacija zahtijeva koordinaciju između sudskih institucija i aktivnu ulogu države u obezbjeđivanju adekvatnih sredstava za pravosudne aktivnosti.

3.3. Indirektni troškovi i društveni uticaj

Indirektni troškovi krivičnih postupaka često su povezani s ekonomskim gubicima na nivou pojedinca i društva. Dugotrajni postupci mogu uzrokovati gubitak produktivnih radnih sati, smanjenje povjerenja u pravosudni sistem i povećanje rizika od recidivizma. Voigt (2006, str. 194) naglašava da su neracionalno dugi procesi često uzrokovani neefikasnim zakonskim okvirima i nedostatkom administrativne podrške. Ovi faktori ne samo da povećavaju troškove države, već i negativno utiču na ekonomski razvoj zbog smanjene pravne sigurnosti.

3.4. Komparativna analiza troškova suđenja i alternativnih mjera

Jedan od načina smanjenja troškova krivičnih postupaka je upotreba alternativnih mjera, poput sporazuma o priznanju krivice i medijacije. Posner (1973, str. 399–453) ističe da primjena alternativnih mjera može značajno smanjiti troškove suđenja i povećati efikasnost. On smatra da sudski sistem treba podsticati brzo rješavanje slučajeva kako bi se izbjeglo opterećenje sudova, što je posebno relevantno u predmetima manjeg značaja. U praksi, primjena ovih mjera zavisi od spremnosti pravosudnog sistema da usvoji inovativne pristupe i prilagodi zakonske okvire. Ekonomija krivičnih postupaka zahtijeva integrisan pristup koji uključuje analizu troškova, reformu zakonskih procedura i optimizaciju administrativnih resursa. Kombinovanjem direktnih i indirektnih mjera moguće

je unaprijediti efikasnost pravosudnog sistema uz očuvanje osnovnih principa pravde i zakonitosti.

3.5. Ekonomija suđenja i alternativne mjere

Troškovi krivičnih postupaka imaju značajan uticaj na efikasnost pravosudnih sistema, posebno u zemljama sa ograničenim budžetskim resursima. Efikasnost se ogleda u sposobnosti sistema da pravovremeno rješava slučajeve uz minimalne troškove, čime se postiže balans između ekonomičnosti i pravde. U savremenim pravosudnim sistemima ne analiziraju se samo finansijski troškovi, već i širi društveni uticaji, uključujući povjerenje građana u pravosudne institucije. Posner (1973, str. 403) ukazuje da troškovi povezani s dugotrajnim postupcima mogu značajno ugroziti percepciju pravosudne efikasnosti. Složenost proceduralnih normi dodatno povećava finansijsko opterećenje za sve učesnike u postupku – državu, optužene i oštećene.

Jedan od ključnih aspekata troškova krivičnih postupaka jeste njihova distribucija između strana u postupku. U slučajevima gdje država snosi većinu troškova, pravosudni sistem suočava se s izazovima racionalizacije resursa radi osiguranja optimalne efikasnosti. Ehrlich (2017, str. 246) ističe da neravnomjerna alokacija resursa može dovesti do preopterećenosti sudova i produženja rokova za donošenje presuda. Ovaj problem dodatno je izražen u pravosudnim sistemima koji se suočavaju s velikim brojem predmeta i ograničenim kapacitetima. Troškovi za optužene i oštećene uključuju ne samo finansijske izdatke, već i emocionalni i društveni stres, što negativno utiče na njihov odnos prema institucijama.

Troškovi postupka također utiču na kvalitet pravosudnih odluka. Kada sudovi rade pod finansijskim ograničenjima, postoji rizik da će se kompromitovati temeljitost istraga i kvalitet zastupanja. Adelstein i Miceli (2001, str. 47–67) upozoravaju da finansijska ograničenja mogu dovesti do nepravednih presuda, posebno u složenim predmetima koji zahtijevaju veće resurse. Ovo ukazuje na potrebu za strategijama koje omogućavaju efikasno upravljanje resursima i održavanje ravnoteže između ekonomičnosti i pravičnosti.

Tehnološka rješenja postaju ključni alat za smanjenje troškova i unapređenje efikasnosti. Digitalizacija pravosudnih procesa, uključujući online saslušanja i automatizaciju administrativnih procedura, može značajno smanjiti direktne troškove i ubrzati donošenje odluka. Primjena tehnologije posebno je korisna u složenim predmetima gdje tradicionalne metode zahtijevaju veća ulaganja u vrijeme i resurse. Osim smanjenja troškova, digitalizacija povećava transparentnost i povjerenje javnosti u pravosudni sistem. Međutim, implementacija ovih rješenja zahtijeva početne investicije, što može predstavljati izazov za sisteme s ograničenim budžetima.

Još jedan aspekt odnosi se na pristup pravdi. U sistemima s visokim troškovima postupka pojedinci iz socijalno ugroženih kategorija često nemaju jednak pristup pravdi. Posner (1973, str. 412) naglašava da pravosudni sistem mora obezbijediti mehanizme koji omogućavaju jednak pristup pravdi bez obzira na finansijske mogućnosti pojedinca. U suprotnom, sistem rizikuje da postane privilegija bogatih, čime se ugrožava osnovni princip jednakosti pred zakonom.

Smanjenje troškova moguće je postići optimizacijom procedura. Skraćivanje rokova za donošenje odluka, unapređenje upravljanja predmetima i promocija alternativnih oblika rješavanja sporova, poput arbitraže i medijacije, predstavljaju efikasne mjere za smanjenje troškova. Alternativni oblici rješavanja sporova često su manje skupi i vremenski zahtjevni u poređenju s tradicionalnim sudskim postupcima. Međutim, njihova primjena zavisi od pravne kulture i spremnosti stranaka da prihvate neformalnije mehanizme rješavanja sporova.

Dugotrajni postupci mogu stvoriti ekonomske gubitke na nivou društva, uključujući smanjenje produktivnosti i gubitak povjerenja investitora. Efikasan pravosudni sistem može, nasuprot tome, podstaći ekonomski razvoj pružanjem pravne sigurnosti i stabilnosti. Ovo je posebno važno za zemlje u tranziciji, gdje pravosudna reforma ima ključnu ulogu u privlačenju investicija i unapređenju poslovnog okruženja.

3.6. Dugoročni ekonomski efekti efikasnih postupaka

Ekonomske analize pravosudnih sistema igraju ključnu ulogu u oblikovanju reformi koje imaju za cilj povećanje efikasnosti i dostupnosti pravde. Uvođenje ekonomskih modela u pravosudne politike omogućava bolje razumijevanje odnosa između troškova i koristi različitih reformskih mjera. Voigt (2016, str. 198) navodi da analiza vremenskih troškova u vođenju predmeta može ukazati na proceduralne faze koje nepotrebno produžavaju procese i povećavaju troškove. Takve analize pomažu zakonodavcima da donesu informisane odluke o prioritetima reforme.

Uvođenje tehnologije, poput digitalizacije sudskih dokumenata i elektronskog upravljanja predmetima, često proizlazi upravo iz rezultata ekonomskih analiza. Pored tehničkih unapređenja, ekonomske analize doprinose razvoju alternativnih mehanizama rješavanja sporova, kao što su arbitraža i medijacija. Adelstein i Miceli (2001, str. 58) naglašavaju da ovakvi mehanizmi omogućavaju smanjenje opterećenja sudova i brže postizanje pravde uz manje troškove.

Primjena ekonomskih analiza ima i značajnu ulogu u borbi protiv korupcije. Analiza alokacije resursa i identifikacija ključnih tačaka slabosti omogućava izradu strategija za smanjenje korupcije i povećanje povjerenja javnosti u pravosudne institucije. Na primjer, adekvatna budžetska sredstva za obuku sudija

i tužilaca u specifičnim oblastima prava mogu povećati efikasnost i integritet sistema.

Još jedan važan aspekt primjene ekonomskih analiza jeste mogućnost poređenja pravosudnih sistema različitih zemalja. Upoređivanjem troškova i performansi moguće je identifikovati najbolje prakse koje se mogu prilagoditi i implementirati u domaći sistem. Skandinavske zemlje često se navode kao primjeri efikasnosti u pravosuđu, zbog čega njihove prakse postaju predmet ekonomskih analiza i preporuka za reforme u drugim državama.

Ekonomski pristupi pružaju osnovu za kvantitativno praćenje rezultata reformi. Mjerenjem napretka kroz indikatore, poput smanjenja trajanja postupaka ili povećanja broja riješenih predmeta, omogućava se procjena uspješnosti implementiranih promjena. Ova transparentnost povećava odgovornost pravosudnih institucija, što je ključno za održivost reformi. U zaključku, ekonomske analize pružaju vrijedne uvide u funkcionisanje pravosudnih sistema i ključne smjernice za njihovu reformu. Njihova efikasnost zavisi od sposobnosti donosilaca odluka da rezultate istraživanja pretoče u konkretne politike i mjere. Budućnost pravosudnih sistema u velikoj mjeri zavisi od njihove spremnosti da prihvate ekonomske pristupe kao osnovu za donošenje odluka, čime se osigurava održivost i efikasnost pravosudnih procesa.

4. Zaključak

Efikasnost krivičnih postupaka predstavlja ne samo pravni, već i društveni i ekonomski imperativ savremenih pravosudnih sistema. Kroz analizu normativnih, institucionalnih i praktičnih aspekata jasno se pokazuje da efikasnost nije puki tehnički pokazatelj brzine suđenja, već složen indikator funkcionalnosti države, vladavine prava i zaštite ljudskih prava. U pravnom smislu, ona je neraskidivo povezana s pravom na suđenje u razumnom roku, koje Evropska konvencija o ljudskim pravima definiše kao jedno od osnovnih jamstava pravičnog postupka. U tom kontekstu, efikasnost se posmatra kao materijalizacija tog prava u svakodnevnoj praksi, a ne samo kao ideal kojem se teži. Kada država ne uspije da obezbijedi razumno trajanje postupka, ne narušava se samo pravna sigurnost, već i povjerenje građana u institucije i legitimnost čitavog pravosudnog sistema.

Analiza je pokazala da u Bosni i Hercegovini problem neefikasnosti krivičnih postupaka ima višestruke uzroke: preopterećenost sudova, manjak kadrovskih i tehničkih resursa, normativne nejasnoće i nedostatak procesne discipline. Dugotrajni postupci često nisu rezultat samo složenosti predmeta, nego i nedostatka efikasnog upravljanja sudskim resursima i neujednačene primjene

zakonskih normi. Ovi problemi imaju domino-efekat — produženi postupci povećavaju troškove, smanjuju dostupnost pravde i utiču na percepciju javnosti o djelotvornosti pravosuđa. Uspostavljanje efikasnog pravosudnog sistema stoga mora počivati na sinergiji zakonodavnih, institucionalnih i tehničkih reformi koje zajedno omogućavaju brzo, pravedno i transparentno odlučivanje.

Komparativna iskustva iz zemalja Evropske unije, posebno Njemačke, Švedske i Hrvatske, pokazuju da su ključni elementi uspješnih reformi upravo specijalizacija sudova, digitalizacija pravosudnih procesa i kontinuirana edukacija pravosudnog osoblja. U Njemačkoj su, na primjer, posebne komisije za složene predmete doprinijele skraćenju trajanja postupaka bez narušavanja kvaliteta odluka. U Švedskoj je digitalizacija sudskih procesa rezultirala smanjenjem trajanja suđenja za trećinu, uz istovremeno povećanje transparentnosti i dostupnosti pravde. Hrvatska je reformama uvedenim tokom procesa pristupanja Evropskoj uniji uspjela značajno smanjiti broj zaostalih predmeta. Svi ovi primjeri ukazuju da efikasnost nije slučajan rezultat, već posljedica sistemskog pristupa koji uključuje i političku volju i odgovornost institucija.

U bosanskohercegovačkom kontekstu, neophodno je da se reforme pravosuđa ne posmatraju isključivo kroz formalne izmjene zakona, već i kroz razvoj institucionalne kulture odgovornosti. Efikasnost nije moguća bez transparentnog upravljanja predmetima, preciznog praćenja sudske statistike i razvijenih mehanizama unutrašnjeg nadzora. Digitalizacija pravosuđa treba biti strateški prioritet jer omogućava racionalizaciju resursa, automatsko praćenje rokova i veću dostupnost podataka javnosti. Pored toga, kontinuirana obuka sudija i tužilaca o novim procesnim instrumentima i primjeni međunarodnih standarda predstavlja ključnu komponentu jačanja profesionalnosti i integriteta pravosudnog sistema.

Ekonomskom analizom efikasnosti potvrđeno je da neefikasni postupci imaju direktne i indirektne troškove koji nadilaze okvire samog pravosuđa. Dugotrajni procesi generišu dodatne budžetske izdatke, gubitke produktivnosti i smanjenje povjerenja investitora, što utiče na cjelokupni ekonomski razvoj zemlje. S druge strane, racionalizacija postupaka, primjena alternativnih mjera kao što su sporazum o priznanju krivice i medijacija, te modernizacija infrastrukture mogu znatno smanjiti troškove i povećati dostupnost pravde. Time se efikasnost potvrđuje kao važan instrument ekonomske stabilnosti i društvenog prosperiteta. Posner (1973) i Voigt (2016) naglašavaju da je ekonomska dimenzija pravosuđa jednako važna kao i pravna, jer neefikasno pravosuđe generiše troškove koji se prenose na cijelo društvo.

Reforme pravosudnog sistema moraju biti dugoročne, planske i podržane adekvatnim finansijskim resursima. Potrebno je izgraditi funkcionalan sistem

praćenja performansi sudova i tužilaštava, koji bi omogućio objektivnu procjenu učinka i identifikaciju uskih grla u procesima. Transparentnost rada pravosudnih institucija i javno dostupne baze podataka o trajanju i ishodima predmeta doprinijele bi većem povjerenju građana i stvaranju kulture odgovornosti. Posebno je važno da efikasnost ne bude shvaćena kao cilj sama po sebi, već kao sredstvo za ostvarenje pravičnosti i zaštite ljudskih prava. Brzina postupanja mora biti uravnotežena s kvalitetom odlučivanja, jer svako ubrzanje koje ugrožava pravičnost suđenja narušava samu svrhu pravosuđa.

U konačnici, efikasnost krivičnih postupaka mora se posmatrati kao multidimenzionalni koncept koji povezuje pravne norme, institucionalne kapacitete i ekonomsku racionalnost. Njeno unapređenje zahtijeva integrisan pristup u kojem će svi akteri – zakonodavna i izvršna vlast, pravosudne institucije, akademska zajednica i međunarodni partneri – djelovati koordinirano. Samo na taj način moguće je ostvariti pravosudni sistem koji istovremeno osigurava brzinu, pravičnost i povjerenje građana. Efikasno pravosuđe ne znači samo kraće rokove, već stvaranje ambijenta u kojem građani vjeruju da će svaka presuda biti donijeta nepristrasno, stručno i u skladu sa zakonom. Time efikasnost postaje temeljni uslov za izgradnju vladavine prava i stabilnog demokratskog društva u Bosni i Hercegovini.

LITERATURA

Adelstein, R., & Miceli, T. J. (2001). *Toward a Comparative Economics of Plea Bargaining.* *European Journal of Law and Economics,* 11, 47–67.

Bejatović, S. (2015). Efikasnost krivičnog postupka kao međunarodni pravni standard i reforma krivičnog procesnog zakonodavstva Srbije: norma i praksa. *Zbornik radova Pravnog fakulteta u Novom Sadu*, 49(2), 27–53.

Council of Europe. (n.d.). *Strengthening the efficiency and quality of justice in Bosnia and Herzegovina (BHSEJ).* Dostupno na https://www.coe.int/en/web/sarajevo/bihsej

Durmišević, T. (2017). Pravda, efikasnost i pravo: Kritika ekonomske analize prava. *Pregled: časopis za društvena pitanja*, 2(2), 131–141.

Ehrlich, I. (2017). Economics of Criminal Law: Crime and Punishment. U F. Parisi (ur.), *The Oxford Handbook of Law and Economics: Volume 3 – Public Law and Legal Institutions* (str. 295–324). Oxford University Press.

Federalno ministarstvo pravde. (2023). *Povećavati efikasnost pravosudnog sistema – izvještaj za 2023.* Dostupno na https://fzzpr.gov.ba/bh/mjere/poveavati-efikasnost-pravosudnog-sistema/implementacija/monitoring-mjere/poveavati-efikasnost-pravosudnog-sistema---izvjetaj-za-2023

Filipović, Lj. (2017). *Kvalitet optužnica i presuda u Bosni i Hercegovini kao faktor efikasnog procesuiranja krivičnih djela korupcije.* Sarajevo: Analitika – Centar za društvena istraživanja. Dostupno na https://www.analitika.ba/sites/default/files/publikacije/Osvrt%20Kvalitet%20optuznica%20i%20presuda%20FINAL.pdf

Hylton, K. N. (2017). *Economics of Criminal Procedure. U F. Parisi (ur.), The Oxford Handbook of Law and Economics: Volume 3 – Public Law and Legal Institutions* (str. 325–343). Oxford University Press.

Imamović-Čizmić, K., & Nikolajev, A. (2018). Ključni aspekti ekonomskih

modela kriminala. *Pregled: časopis za društvena pitanja*, 2(2), 1–13.

Kolaković-Bojović, M. (2016). Efikasnost krivičnog pravosuđa kao sredstvo suzbijanja kriminaliteta. U L. Kron (ur.), *Kriminal, državna reakcija i harmonizacija sa evropskim standardima* (str. 237–254). Institut za kriminološka i sociološka istraživanja, Beograd.

Kovačević, A., Hadžić, M., & Petrović, D. (2025). Kriminalistička obrada u funkciji efikasnog krivičnog postupka. *Zaštita i sigurnost*, 4(2), 167–177. Dostupno na https://zisjournal-com-647393.hostingersite.com/wp-content/uploads/2025/01/ZIS_Godina4_Broj2_BHS-EN.pdf

Mlikotin Tomić, D., & Šega, A. (2006). Ekonomska analiza prava: Razvoj i aktualnost. *Zbornik Ekonomskog fakulteta u Zagrebu*, 4(1), 365–376.

Paragraf.ba. (n.d.). *Zakon o krivičnom postupku Bosne i Hercegovine.* Preuzeto 10. 12. 2024. Dostupno na https://www.paragraf.ba/propisi/bih/zakon-o-krivicnom-postupku-bosne-i-hercegovine.html

Petrović, Ž. (2025). *Pravni i evolutivni aspekti ograničenja i zabrana ratovanja*. *Zaštita i sigurnost*, 4(2), 62–63. Dostupno na https://www.azur.ba/wp-content/uploads/2021/12/5_Petrovic.pdf

Posner, R. A. (1973). *An Economic Approach to Legal Procedure and Judicial Administration. Journal of Legal Studies*, 2(2), 399–458.

Radio Sarajevo. (2023). *Pet stvari koje trebate znati: pravosuđe u BiH u izvještaju Evropske komisije.* Dostupno na https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/pet-stvari-koje-trebate-znati-pravosude-u-bih-u-izvjestaju-evropske-komisije/520430

Transparency International BiH. (2022). Efikasnost pravosuđa – Izvještaj 2022. Dostupno na https://ti-bih.org/wp-content/uploads/2022/11/EFIKASNOST-PRAVOSUDJA-UCESTALOST-ZAKAZIVANJA-I-ODRZAVANJA-SUDJENJA.pdf

Transparency International BiH. (2022). *Efikasnost pravosuđa: učestalost*

zakazivanja i održavanja suđenja. Dostupno na https://ti-bih.org/publikacije/efikasnost-pravosudja-ucestalost-zakazivanja-i-odrzavanja-sudjenja/

Visoko sudsko i tužilačko vijeće Bosne i Hercegovine. (2022). *Unapređenje efikasnosti i kvaliteta krivičnih postupaka kao produkt međuinstitucionalne saradnje.*

Visoko sudsko i tužilačko vijeće Bosne i Hercegovine. (2023). Unapređenje efikasnosti i kvaliteta krivičnih postupaka u fokusu saradnje VSTV-a BiH i međunarodnih partnera. Dostupno na https://vstv.pravosudje.ba/vstvfo/B/141/article/127121

EFFICIENCY OF CRIMINAL PROCEEDINGS

DOI: 10.70329/2744-2403.2025.5.10.2

Scientific article

Redžepović Adnan, MA iur

Abstract

The efficiency of criminal proceedings is one of the fundamental indicators of the quality and functionality of any state's judicial system. This paper analyzes the concept and significance of efficiency through normative, institutional, and practical aspects, with a special focus on the legal framework of Bosnia and Herzegovina and international standards for the right to a trial within a reasonable time. It points to the causes of inefficiency, including court overloads, a lack of procedural discipline, as well as organizational, personnel, and normative shortcomings that influence the length of criminal proceedings. Using a comparative approach, the paper presents solutions and good practices from specific European legal systems that have contributed to the acceleration and rationalization of procedural phases, strengthened oversight of the work of courts and prosecutor's offices, and improved case management. Special attention is paid to the economic dimension of efficiency and the possibilities of applying alternative procedures, such as the principle of opportunity, plea agreements, and mediation, as mechanisms to relieve the burden on the courts. The paper emphasizes the need to strengthen institutional capacities, digitize the judiciary, introduce advanced information systems, and consistently apply the principle of procedural economy. It concludes that the efficiency of criminal proceedings must be built on a balanced relationship between the speed of decision-making and respect for the right to a fair trial as a fundamental element of the rule of law.

Keywords: *efficiency, criminal procedure, judiciary, reasonable time, procedural economy, jurisprudence, judicial reforms, comparative approach, economic analysis, Bosnia and Herzegovina*

1. Introduction

The efficiency of criminal proceedings represents one of the fundamental issues of modern justice, as it directly affects the realization of the right to a fair trial, citizens' trust in the legal system, and the rule of law as a whole. It is not just a technical issue of the speed of court proceedings, but a complex legal and institutional challenge that encompasses the organization of judicial bodies, the application of procedural rules, and the state's ability to ensure effective, just, and transparent conduct of criminal proceedings. Efficiency is therefore an indicator not only of the functionality of the court system but also of the maturity of the democratic order and the level of protection of fundamental human rights.

In modern law, especially under the auspices of the European Convention on Human Rights, efficiency is closely linked to the right to a trial within a reasonable time, as stated in Article 6 of the Convention. The European Court of Human Rights, in its extensive jurisprudence, has repeatedly emphasized that the state has a positive obligation to ensure the functioning of the courts in a manner that allows for the conclusion of proceedings within a reasonable time. Kovačević et al. (2025) similarly stress that "the timely undertaking of actions in the phase of criminal investigation is a crucial step" in ensuring efficient criminal procedure. As Petrović (2025) states, "although legal restrictions are necessary, they must be harmonized with the reflection of human rights." Thus, efficiency is not viewed exclusively as an organizational standard, but as a human right whose disrespect can be considered a violation of fundamental freedoms. This standard becomes even more significant in transition legal systems, including Bosnia and Herzegovina, where institutional capacities and normative frameworks are often burdened by inherited structural problems.

In the judicial system of Bosnia and Herzegovina, the issue of the efficiency of criminal proceedings gains particular weight due to the long duration of court processes, the overload of courts, and inconsistent judicial practice. According to reports from the High Judicial and Prosecutorial Council of BiH and the European Commission, the average duration of criminal cases in domestic courts still significantly exceeds the standards established in European Union member states. Such a situation affects not only the realization of the parties' rights but also citizens' trust in institutions, as prolonged proceedings create a perception of ineffectiveness and unfairness in the judicial system. In this context, efficiency becomes a necessary prerequisite for the legitimacy of the judiciary and a basic indicator of its ability to fulfill its social function.

Efficient criminal proceedings also contribute to the realization of a broader social interest. The quick and proper prosecution of criminal offenses has a preventive

character, as it sends a clear message about the consistent application of the law and accountability for unlawful conduct. At the same time, it reduces the risk of secondary victimization of victims, strengthens the sense of legal security, and increases public trust in institutions. Inefficiency, conversely, generates multiple negative consequences: legal, economic, and psychological. It increases the costs of proceedings, burdens the judiciary's budget, reduces the productivity of institutions, and creates a feeling of helplessness among citizens seeking the protection of their rights. From the aspect of social stability and economic development, an inefficient judiciary acts as an obstacle to the investment environment and the overall development of society, as uncertainty regarding judicial protection discourages legal entities from seeking institutional dispute resolution.

In addition to legal and organizational aspects, efficiency also has a pronounced economic dimension. The costs arising from long-lasting proceedings pertain not only to courts and prosecutor's offices but also to the participants in the proceedings, lawyers, witnesses, and society as a whole. Inefficient proceedings generate additional budget expenditures while simultaneously reducing access to justice and the productivity of judicial resources. In this sense, improving efficiency is not just a matter of legal reform but also of rational management of public resources, which is particularly significant in states with limited institutional capacities like Bosnia and Herzegovina. Therefore, the issue of the efficiency of criminal proceedings must also be viewed through the prism of economic sustainability and a long-term strategy for the development of the judicial system.

The analysis of the efficiency of criminal proceedings needs to encompass three basic dimensions: normative, institutional, and practical. The normative dimension relates to the quality of procedural regulations, their harmonization with international standards, and consistency in application. The institutional dimension implies the organization of the judicial system, the distribution of competencies and resources, and the system of supervision over the work of courts and prosecutor's offices. The practical dimension covers the daily functioning of judicial bodies, the level of professionalism of judicial office holders, the availability of technology, and the development of case management mechanisms. Only by a combined analysis of these factors is it possible to understand the causes and consequences of inefficiency and to define realistic measures for its improvement.

The methodological framework of the paper is based on a combination of doctrinal, comparative, descriptive, and analytical methods. The doctrinal method was used for the analysis of the legislative framework and legal standards governing criminal proceedings in Bosnia and Herzegovina, especially the Law

on Criminal Procedure of BiH, the Law on Courts, and relevant international instruments. The comparative method enabled the comparison of domestic practice with the practices of states that have reformed their criminal proceedings towards greater efficiency, such as Germany, Sweden, and Croatia, with a special emphasis on experiences in the digitalization of judicial processes. The analytical method was applied in data processing and in identifying the causes of prolonged court proceedings, while the descriptive method allowed for the review and interpretation of reports from the High Judicial and Prosecutorial Council of BiH, the European Commission, and Transparency International on the state of judicial efficiency. Such an interdisciplinary approach ensures a comprehensive view of the problem of efficiency and provides a basis for the development of realistic and applicable recommendations.

The aim of the paper is, based on the analysis of valid regulations, judicial practice, and comparative experiences, to identify the key causes of inefficiency in criminal proceedings in Bosnia and Herzegovina, and to propose concrete measures for their overcoming. The research is focused on the analysis of institutional weaknesses, the assessment of the degree of harmonization of the domestic system with European standards, and the identification of solutions that can contribute to faster, more transparent, and more rational conduct of proceedings. It is expected that the results of the analysis will contribute to the understanding of the relationship between efficiency and fairness, and serve as a theoretical and practical basis for the improvement of judicial policies, the digitalization of processes, and the strengthening of the professional accountability of judicial office holders. The efficiency of criminal proceedings, in this context, is not just a measure of the technical success of the judiciary, but a key indicator of citizens' trust in institutions and the stability of the legal system that forms the foundation of every democratic society.

Previous research on the efficiency of criminal proceedings indicates that it is a multidimensional phenomenon encompassing legal, institutional, and social aspects. Bejatović (2015), in his paper Efficiency of criminal procedure as an international legal standard and the reform of criminal procedural legislation in Serbia: norm and practice, emphasizes that efficiency is essential for the realization of justice and that it depends not only on legal norms but also on the organization of the judiciary, the expertise, and the motivation of procedural subjects. He points out that criminological-political reasons and the implementation of procedural instruments of efficiency in national legislation form the basis of modern reforms in this area.

Recommendation of the Committee of Ministers of the Council of Europe (CM/Rec(2010)12) further specifies that the efficiency of the judiciary cannot be measured solely by the speed of decision-making, but by the quality of court

decisions rendered within a reasonable time after impartial consideration of all relevant issues. Only such decisions, according to the recommendation, achieve the purpose of criminal proceedings – the simultaneous protection of society from crime and the preservation of the fundamental human rights of the accused.

International experiences confirm that cooperation between judicial institutions and procedural discipline are key factors in efficiency. Within the initiatives of the High Judicial and Prosecutorial Council of Bosnia and Herzegovina and international expert teams, models of inter-institutional cooperation in Bijeljina, Zenica, and Sarajevo have been analyzed. It was concluded that improving communication between courts, prosecutor's offices, and the legal profession contributes to shorter proceedings and greater procedural discipline of the parties. The analysis of the legal framework shows that the Law on Criminal Procedure of Bosnia and Herzegovina, as the fundamental procedural act, is harmonized with international standards, especially the European Convention on Human Rights. However, in comparison with European practices, the domestic system faces challenges in the consistent application of procedural rules and the standardization of judicial practice. In most EU member states, an inquisitorial system is present, while BiH uses a mixed model that combines elements of inquisitorial and adversarial procedure, which often leads to different interpretations of legal norms.

Furthermore, the practice of states such as Germany and Sweden shows that specialized courts and the digitalization of procedural flows significantly contribute to the acceleration of proceedings and better resource allocation. In Bosnia and Herzegovina, although there are specialized departments within courts for certain types of cases, the lack of technical resources and continuous training limits their full efficiency.

Establishing an efficient system of international legal assistance, as well as strengthening cooperation with European judicial networks, are key prerequisites for the fight against transnational crime and ensuring the timely exchange of information and evidence. Although BiH possesses a solid normative framework, the implementation of international standards in practice remains a challenge, as confirmed by the reports of the European Commission and the HJPC BiH (2022). In conclusion, the review of literature and previous research indicates that the efficiency of criminal proceedings depends on a combination of legal reforms, institutional coordination, and the application of modern technologies. Comparative experiences of European countries confirm that digitalization, specialization of courts, and professional training of personnel are key factors in improving the efficiency of the judiciary in transition systems like Bosnia and Herzegovina.

2. Analysis of the Efficiency of Criminal Proceedings: Comparative Approach and Proposals for Improvement

The efficiency of criminal proceedings is crucial for ensuring fairness and trust in the judicial system. The analysis focuses on the concept of efficiency in the context of criminal proceedings, a comparison with practices in other legal systems, and the identification of problems and the proposal of concrete solutions. The emphasis is on recognizing the factors that influence the length of proceedings and potential strategies for their improvement.

2.1. Analysis of the Concept of Efficiency in the Context of Criminal Proceedings

Efficiency in criminal proceedings implies the timely resolution of cases while simultaneously respecting the principle of fairness. According to legal standards, efficiency refers not only to the speed of conducting proceedings but also to the quality of the decisions made, which must be based on laws and evidence. Inefficient proceedings result not only in the prolongation of trials but also in a loss of citizens' trust in the legal system.

In Bosnia and Herzegovina, the analysis of efficiency points to the overload of courts, insufficient staff training, and a lack of resources as the main obstacles. According to the Report of the High Judicial and Prosecutorial Council of Bosnia and Herzegovina (2022), the average duration of criminal proceedings significantly exceeds the recommended deadlines, resulting in a backlog of unresolved cases. Transparency International (2023) states that this situation further worsens the public perception of judicial bodies and reduces citizens' trust in their functionality.

One of the key problems is the lack of clear and consistent guidelines for the application of legal norms, which often leads to different interpretations of the law among judges. This not only prolongs the duration of the process but also hinders the standardization of judicial practice. In addition, courts face challenges such as outdated infrastructure and an inadequate system for archiving cases, which further slows down administrative procedures.

Modernization of the judicial infrastructure could significantly improve the efficiency of criminal proceedings. This includes the digitalization of court processes, which enables faster exchange of information between judicial institutions and parties. Also, increasing transparency through publicly available databases on court cases can reduce the number of errors and ensure better monitoring of the course of proceedings. Staff training is another key element for improving efficiency. Investing in continuous education for judges and prosecutors, especially in areas such as the application of new laws and the use of digital technologies, can reduce the number of procedural errors and accelerate

decision-making. Also, better management of case allocation can help reduce court overload, allowing judges to focus on more complex cases.
The efficiency of criminal proceedings ultimately depends on the coordinated action of all judicial institutions and the political will to implement the necessary reforms. Support from international organizations, such as the European Union and the Council of Europe, can provide the necessary resources and expertise for the implementation of these changes.

2.2. Comparison with Practices in Other Legal Systems

Comparative experiences show that systems such as those in Germany and Sweden have achieved a high level of efficiency thanks to the automation of judicial processes and the use of specialized courts for different types of cases. In Sweden, for example, the introduction of digital platforms has reduced the duration of processes by 30%, while Germany uses special commissions to resolve complex cases, thereby relieving the burden on ordinary courts. Bosnia and Herzegovina can use the experiences of these countries as a basis for reforming its judicial system, although the key difference lies in the approach to resources and the level of investment in judicial infrastructure. Transparency International (2023) emphasizes that the lack of political will to implement reforms is often the biggest obstacle to the implementation of new methods.

Compared to Croatia, which underwent similar reforms during the process of accession to the European Union, Bosnia and Herzegovina has the advantage of being able to use already developed models. Croatia, for example, reduced the number of pending cases by 40% thanks to better coordination between different judicial bodies. The introduction of mechanisms to accelerate processes, such as mandatory deadlines for resolving cases, has proven to be an effective measure in increasing efficiency. The application of automated systems in Sweden is an example of good management of judicial resources. The integration of digital tools has enabled quick recording and tracking of cases, thereby reducing the administrative burden on the courts. Specialized courts in Germany facilitate the resolution of complex cases and at the same time improve the quality of decisions through a focus on specific areas of law.

The implementation of such practices in Bosnia and Herzegovina requires adaptation to the domestic context. Reform of the judicial infrastructure and investment in staff education can enable the successful application of the best international practices. A focus on transparency and accountability of judicial institutions would further improve public trust in the judicial system.

2.3. Identification of Problems and Proposals for Improvement

The main problems in criminal proceedings in Bosnia and Herzegovina include the length of processes, a lack of resources, and an uneven distribution of cases. Analyses point to a lack of expert staff and the overload of courts as key challenges, which causes delays in decision-making. The length of proceedings, especially in corruption cases, stands out as a significant problem. According to reports, disciplinary proceedings against judges and prosecutors in Bosnia and Herzegovina often exceed the foreseen deadlines, which further complicates the processing of priority cases.

A lack of resources, including outdated infrastructure and limited budgets, also negatively affects the efficiency of judicial proceedings. Analyses show that courts in BiH are overloaded with cases, while at the same time lacking adequate technical tools for managing processes. Transparency International (2023) and the HJPC BiH (2022) confirm that one of the causes is the low rate of digitalization and the lack of a systemic approach to optimizing court processes.

Proposals for improvement include:

- **Digitalization of processes** – the introduction of electronic systems for tracking cases and communication between courts and parties, which would reduce administrative costs and speed up proceedings.
- **Training of judicial staff** – continuous education and specialization of judges and prosecutors to improve the quality of decision-making. German experiences show that investing in human resources contributes to the standardization of judicial practice (Hylton, 2017, p. 337).
- **Better resource allocation** – increasing the budget for the judiciary and rationalizing the distribution of cases are key factors for reducing the burden on the courts. Transparent planning and fair allocation of funds enable better work of judicial institutions.

The efficiency of criminal proceedings, therefore, depends on the coordinated action of all judicial bodies, the political will to implement reforms, and adequate international support. The implementation of these proposals requires dedication and the integration of the best international practices to ensure the fairness and effectiveness of the judicial system in Bosnia and Herzegovina.

3. Economic Analysis of the Efficiency of Criminal Proceedings

The economic analysis of the efficiency of criminal proceedings represents an important aspect of understanding the functioning of the judicial system, as it allows for the assessment of not only the legal but also the financial consequences of every court process. Through this analysis, key economic parameters are considered, including the costs of the proceedings themselves, the optimal allocation of resources, and the long-term benefits of efficient prosecution. In

addition to the direct costs of trials, such as the costs of lawyers, judges, and experts, special attention is also paid to the economic consequences of prolonged court proceedings, including the costs of detention, lost work hours, and the reduction of citizens' trust in the judicial system. Furthermore, the advantages of alternative measures such as plea agreements, mediation, and other methods that can reduce the financial burden on the courts while preserving justice and legality are analyzed.

3.1. Costs of Criminal Proceedings and Resource Analysis

The economic efficiency of criminal proceedings is determined by the costs incurred during their duration, including direct and indirect costs. Direct costs include allocations for the salaries of judges, lawyers, and experts, while indirect costs include social costs such as the loss of productivity due to long-lasting proceedings. These factors are precisely key to the analysis that seeks to achieve an optimal balance between justice and economics in judicial processes.

3.2. Direct Costs of Criminal Proceedings

Direct costs include the financial resources needed to conduct court processes. This implies budget allocations for the work of courts, prosecutor's offices, and defense. In developed judicial systems, there is a tendency to optimize these costs through the introduction of technological solutions and the improvement of procedural norms. Hylton (2017, p. 329) points out that increasing efficiency in the allocation of judicial resources reduces the overall financial burden of the judicial system. This optimization requires coordination between judicial institutions and an active role of the state in providing adequate funds for judicial activities.

3.3. Indirect Costs and Social Impact

Indirect costs of criminal proceedings are often associated with economic losses at the individual and societal level. Long-lasting proceedings can cause a loss of productive work hours, a reduction in trust in the judicial system, and an increased risk of recidivism. Voigt (2006, p. 194) emphasizes that irrationally long processes are often caused by inefficient legal frameworks and a lack of administrative support. These factors not only increase the state's costs but also negatively affect economic development due to reduced legal certainty.

3.4. Comparative Analysis of Trial Costs and Alternative Measures

One way to reduce the costs of criminal proceedings is the use of alternative measures, such as plea agreements and mediation. Posner (1973, pp. 399–453) points out that the application of alternative measures can significantly reduce trial costs and increase efficiency. He believes that the court system should encourage the rapid resolution of cases to avoid overloading the courts, which is especially relevant in minor cases. In practice, the application of these measures depends on the readiness of the judicial system to adopt innovative approaches and adapt legal frameworks. The economics of criminal proceedings requires an integrated approach that includes cost analysis, reform of legal procedures, and optimization of administrative resources. By combining direct and indirect measures, it is possible to improve the efficiency of the judicial system while preserving the basic principles of justice and legality.

3.5. The Economics of Trials and Alternative Measures

The costs of criminal proceedings have a significant impact on the efficiency of judicial systems, especially in countries with limited budgetary resources. Efficiency is reflected in the system's ability to resolve cases promptly with minimal costs, thereby achieving a balance between economy and justice. In modern judicial systems, not only financial costs are analyzed, but also broader social impacts, including citizens' trust in judicial institutions. Posner (1973, p. 403) points out that the costs associated with prolonged proceedings can significantly undermine the perception of judicial efficiency. The complexity of procedural norms further increases the financial burden for all participants in the proceedings – the state, the accused, and the injured parties.

One of the key aspects of the costs of criminal proceedings is their distribution among the parties to the proceedings. In cases where the state bears most of the costs, the judicial system faces challenges in rationalizing resources to ensure optimal efficiency. Ehrlich (2017, p. 246) points out that an uneven allocation of resources can lead to court overload and the prolongation of deadlines for rendering judgments. This problem is further exacerbated in judicial systems facing a large number of cases and limited capacities. Costs for the accused and the injured parties include not only financial expenses but also emotional and social stress, which negatively affects their relationship with the institutions.

The costs of the proceedings also affect the quality of judicial decisions. When courts operate under financial constraints, there is a risk that the thoroughness of investigations and the quality of representation will be compromised. Adelstein and Miceli (2001, pp. 47–67) warn that financial constraints can lead to unfair

judgments, especially in complex cases that require greater resources. This indicates the need for strategies that enable efficient resource management and maintain a balance between economy and fairness.

Technological solutions are becoming a key tool for reducing costs and improving efficiency. The digitalization of judicial processes, including online hearings and the automation of administrative procedures, can significantly reduce direct costs and speed up decision-making. The application of technology is especially useful in complex cases where traditional methods require greater investment in time and resources. In addition to reducing costs, digitalization increases transparency and public trust in the judicial system. However, the implementation of these solutions requires initial investments, which can be a challenge for systems with limited budgets.

Another aspect relates to access to justice. In systems with high procedural costs, individuals from socially vulnerable categories often do not have equal access to justice. Posner (1973, p. 412) emphasizes that the judicial system must provide mechanisms that enable equal access to justice regardless of the financial capacity of the individual. Otherwise, the system risks becoming a privilege of the rich, thereby jeopardizing the basic principle of equality before the law.

Cost reduction can be achieved by optimizing procedures. Shortening deadlines for decision-making, improving case management, and promoting alternative forms of dispute resolution, such as arbitration and mediation, are effective measures for reducing costs. Alternative forms of dispute resolution are often less expensive and time-consuming compared to traditional court proceedings. However, their application depends on the legal culture and the readiness of the parties to accept more informal dispute resolution mechanisms.

Long-lasting proceedings can create economic losses at the societal level, including reduced productivity and loss of investor confidence. An efficient judicial system can, conversely, encourage economic development by providing legal certainty and stability. This is especially important for countries in transition, where judicial reform plays a key role in attracting investments and improving the business environment.

3.6. Long-Term Economic Effects of Efficient Proceedings

Economic analyses of judicial systems play a crucial role in shaping reforms aimed at increasing the efficiency and accessibility of justice. The introduction of economic models into judicial policies allows for a better understanding of the relationship between the costs and benefits of various reform measures. Voigt (2016, p. 198) states that the analysis of time costs in case management can point

to procedural phases that unnecessarily prolong processes and increase costs. Such analyses help legislators make informed decisions about reform priorities. The introduction of technology, such as the digitalization of court documents and electronic case management, often results precisely from the results of economic analyses. In addition to technical improvements, economic analyses contribute to the development of alternative dispute resolution mechanisms, such as arbitration and mediation. Adelstein and Miceli (2001, p. 58) emphasize that such mechanisms allow for a reduction in court overload and faster achievement of justice at lower costs.

The application of economic analyses also has a significant role in the fight against corruption. The analysis of resource allocation and the identification of key points of weakness enables the development of strategies to reduce corruption and increase public trust in judicial institutions. For example, adequate budget funds for the training of judges and prosecutors in specific areas of law can increase the efficiency and integrity of the system.

Another important aspect of the application of economic analyses is the possibility of comparing the judicial systems of different countries. By comparing costs and performance, it is possible to identify the best practices that can be adapted and implemented in the domestic system. Scandinavian countries are often cited as examples of efficiency in the judiciary, which is why their practices become the subject of economic analyses and recommendations for reforms in other countries.

Economic approaches provide a basis for the quantitative monitoring of reform results. Measuring progress through indicators, such as the reduction of the duration of proceedings or the increase in the number of resolved cases, allows for the assessment of the success of implemented changes. This transparency increases the accountability of judicial institutions, which is crucial for the sustainability of reforms. In conclusion, economic analyses provide valuable insights into the functioning of judicial systems and key guidelines for their reform.

Their effectiveness depends on the ability of decision-makers to translate research results into concrete policies and measures. The future of judicial systems largely depends on their readiness to accept economic approaches as a basis for decision-making, thereby ensuring the sustainability and efficiency of judicial processes.

4. Conclusion

The efficiency of criminal proceedings represents not only a legal but also a social and economic imperative of modern judicial systems. Through the analysis of normative, institutional, and practical aspects, it is clearly shown that efficiency is not a mere technical indicator of the speed of trial, but a complex indicator of the functionality of the state, the rule of law, and the protection of human rights. In the legal sense, it is inextricably linked to the right to a trial within a reasonable time, which the European Convention on Human Rights defines as one of the basic guarantees of a fair trial. In this context, efficiency is viewed as the materialization of that right in daily practice, and not just as an ideal to strive for. When the state fails to ensure a reasonable duration of proceedings, it violates not only legal certainty but also citizens' trust in institutions and the legitimacy of the entire judicial system.

The analysis showed that in Bosnia and Herzegovina, the problem of inefficiency in criminal proceedings has multiple causes: court overload, a lack of personnel and technical resources, normative ambiguities, and a lack of procedural discipline. Long-lasting proceedings are often not the result of the complexity of the cases alone, but also of a lack of efficient management of judicial resources and inconsistent application of legal norms. These problems have a domino effect — prolonged proceedings increase costs, reduce access to justice, and affect the public perception of the effectiveness of the judiciary. Establishing an efficient judicial system must therefore be based on the synergy of legislative, institutional, and technical reforms that together enable quick, fair, and transparent decision-making.

Comparative experiences from European Union countries, especially Germany, Sweden, and Croatia, show that the key elements of successful reforms are precisely the specialization of courts, the digitalization of judicial processes, and the continuous education of judicial staff. In Germany, for example, special commissions for complex cases contributed to shortening the duration of proceedings without compromising the quality of decisions. In Sweden, the digitalization of court processes resulted in a one-third reduction in the duration of trials, while simultaneously increasing transparency and access to justice. Croatia, with the reforms introduced during the process of accession to the European Union, managed to significantly reduce the number of pending cases. All these examples indicate that efficiency is not a coincidence, but the consequence of a systemic approach that includes both political will and institutional responsibility.

In the Bosnian-Herzegovinian context, it is necessary for judicial reforms not to be viewed exclusively through formal changes to the law, but also through the development of an institutional culture of accountability. Efficiency is not possible without transparent case management, precise tracking of court statistics,

and developed mechanisms of internal oversight. The digitalization of the judiciary should be a strategic priority because it enables the rationalization of resources, automatic tracking of deadlines, and greater public availability of data. In addition, continuous training of judges and prosecutors on new procedural instruments and the application of international standards is a key component of strengthening the professionalism and integrity of the judicial system.

The economic analysis of efficiency confirmed that inefficient proceedings have direct and indirect costs that go beyond the framework of the judiciary itself. Long-lasting processes generate additional budget expenditures, productivity losses, and a reduction in investor confidence, which affects the country's overall economic development. On the other hand, the rationalization of proceedings, the application of alternative measures such as plea agreements and mediation, and the modernization of infrastructure can significantly reduce costs and increase access to justice. Thus, efficiency is confirmed as an important instrument of economic stability and social prosperity. Posner (1973) and Voigt (2016) emphasize that the economic dimension of the judiciary is just as important as the legal dimension, because an inefficient judiciary generates costs that are transferred to the entire society.

Reforms of the judicial system must be long-term, planned, and supported by adequate financial resources. It is necessary to build a functional system for monitoring the performance of courts and prosecutor's offices, which would allow for the objective assessment of performance and the identification of bottlenecks in the processes. The transparency of the work of judicial institutions and publicly available databases on the duration and outcomes of cases would contribute to greater citizen trust and the creation of a culture of accountability. It is especially important that efficiency is not understood as an end in itself, but as a means to achieve fairness and the protection of human rights. The speed of proceedings must be balanced with the quality of decision-making, because any acceleration that compromises the fairness of the trial violates the very purpose of the judiciary.

Ultimately, the efficiency of criminal proceedings must be viewed as a multidimensional concept that connects legal norms, institutional capacities, and economic rationality. Its improvement requires an integrated approach in which all actors – the legislative and executive authorities, judicial institutions, the academic community, and international partners – will act in a coordinated manner. Only in this way is it possible to achieve a judicial system that simultaneously ensures speed, fairness, and citizen trust. An efficient judiciary does not only mean shorter deadlines, but the creation of an environment in which citizens believe that every judgment will be rendered impartially, expertly, and in accordance with the law. Thus, efficiency becomes a fundamental condition for building the rule of law and a stable democratic society in Bosnia and Herzegovina.

LITERATURE

Adelstein, R., & Miceli, T. J. (2001). *Toward a Comparative Economics of Plea Bargaining.*
European Journal of Law and Economics, 11, 47–67.

Bejatović, S. (2015). Efikasnost krivičnog postupka kao međunarodni pravni standard i reforma krivičnog procesnog zakonodavstva Srbije: norma i praksa. *Zbornik radova Pravnog fakulteta u Novom Sadu*, 49(2), 27–53.

Council of Europe. (n.d.). *Strengthening the efficiency and quality of justice in Bosnia and Herzegovina (BHSEJ).* Dostupno na https://www.coe.int/en/web/sarajevo/bihsej

Durmišević, T. (2017). Pravda, efikasnost i pravo: Kritika ekonomske analize prava. *Pregled: časopis za društvena pitanja*, 2(2), 131–141.

Ehrlich, I. (2017). Economics of Criminal Law: Crime and Punishment. U F. Parisi (ur.), *The Oxford Handbook of Law and Economics: Volume 3 – Public Law and Legal Institutions* (str. 295–324). Oxford University Press.

Federalno ministarstvo pravde. (2023). *Povećavati efikasnost pravosudnog sistema – izvještaj za 2023.* Dostupno na https://fzzpr.gov.ba/bh/mjere/poveavati-efikasnost-pravosudnog-sistema/implementacija/monitoring-mjere/poveavati-efikasnost-pravosudnog-sistema---izvjetaj-za-2023

Filipović, Lj. (2017). *Kvalitet optužnica i presuda u Bosni i Hercegovini kao faktor efikasnog procesuiranja krivičnih djela korupcije.* Sarajevo: Analitika – Centar za društvena istraživanja. Dostupno na https://www.analitika.ba/sites/default/files/publikacije/Osvrt%20Kvalitet%20optuznica%20i%20presuda%20FINAL.pdf

Hylton, K. N. (2017). *Economics of Criminal Procedure. U F. Parisi (ur.), The Oxford Handbook of Law and Economics: Volume 3 – Public Law and Legal Institutions* (str. 325–343). Oxford University Press.

Imamović-Čizmić, K., & Nikolajev, A. (2018). Ključni aspekti ekonomskih modela kriminala. *Pregled: časopis za društvena pitanja*, 2(2), 1–13.

Kolaković-Bojović, M. (2016). Efikasnost krivičnog pravosuđa kao sredstvo suzbijanja kriminaliteta. U L. Kron (ur.), *Kriminal, državna reakcija i harmonizacija sa evropskim standardima* (str. 237–254). Institut za kriminološka i sociološka istraživanja, Beograd.

Kovačević, A., Hadžić, M., & Petrović, D. (2025). Kriminalistička obrada u funkciji efikasnog krivičnog postupka. *Zaštita i sigurnost*, 4(2), 167–177. Dostupno na https://zisjournal-com-647393.hostingersite.com/wp-content/uploads/2025/01/ZIS_Godina4_Broj2_BHS-EN.pdf

Mlikotin Tomić, D., & Šega, A. (2006). Ekonomska analiza prava: Razvoj i aktualnost. *Zbornik Ekonomskog fakulteta u Zagrebu*, 4(1), 365–376.

Paragraf.ba. (n.d.). *Zakon o krivičnom postupku Bosne i Hercegovine.* Preuzeto 10. 12. 2024. Dostupno na https://www.paragraf.ba/propisi/bih/zakon-o-krivicnom-postupku-bosne-i-hercegovine.html

Petrović, Ž. (2025). *Pravni i evolutivni aspekti ograničenja i zabrana ratovanja. Zaštita i sigurnost*, 4(2), 62–63. Dostupno na https://www.azur.ba/wp-content/uploads/2021/12/5_Petrovic.pdf

Posner, R. A. (1973). *An Economic Approach to Legal Procedure and Judicial Administration. Journal of Legal Studies*, 2(2), 399–458.

Radio Sarajevo. (2023). *Pet stvari koje trebate znati: pravosuđe u BiH u izvještaju Evropske komisije.* Dostupno na https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/pet-stvari-koje-trebate-znati-pravosude-u-bih-u-izvjestaju-evropske-komisije/520430

Transparency International BiH. (2022). Efikasnost pravosuđa – Izvještaj 2022. Dostupno na https://ti-bih.org/wp-content/uploads/2022/11/EFIKASNOST-PRAVOSUDJA-UCESTALOST-ZAKAZIVANJA-I-ODRZAVANJA-SUDJENJA.pdf

Transparency International BiH. (2022). *Efikasnost pravosuđa: učestalost zakazivanja i održavanja suđenja.* Dostupno na https://ti-bih.org/publikacije/efikasnost-pravosudja-ucestalost-zakazivanja-i-odrzavanja-sudjenja/

Visoko sudsko i tužilačko vijeće Bosne i Hercegovine. (2022). *Unapređenje efikasnosti i kvaliteta krivičnih postupaka kao produkt međuinstitucionalne saradnje.*

Visoko sudsko i tužilačko vijeće Bosne i Hercegovine. (2023). Unapređenje efikasnosti i kvaliteta krivičnih postupaka u fokusu saradnje VSTV-a BiH i međunarodnih partnera. Dostupno na https://vstv.pravosudje.ba/vstvfo/B/141/article/127121

SIGURNOSNI RIZICI I MJERE ZAŠTITE PRI POVRŠINSKOM MINIRANJU

DOI: *10.70329/2744-2403.2025.5.10.3*

Izvorni naučni rad

Ekrem Bektašević[7], *Satko Filipović*[8], *Kemal Gutić*[9]

Sažetak:
Miniranje na površinskim kopovima predstavlja jedan od najsloženijih i najrizičnijih procesa u rudarskoj praksi, gdje sigurnost ljudi i infrastrukture direktno zavisi od pravilnog planiranja, tehničke kontrole i poštivanja propisanih mjera zaštite. Ovaj rad daje sistematičan prikaz rizika koji prate sve faze površinskog miniranja, od bušenja i punjenja bušotina do detonacije i postdetonacione inspekcije, te definira ključne tehničke i organizacione mjere za njihovu prevenciju. Posebna pažnja posvećena je eksplozivnim, seizmičkim i akustičkim utjecajima, čija se kontrola vrši primjenom empirijskih modela, seizmičkog monitoringa i adekvatnog projektovanja minskih polja. U radu su analizirani relevantni zakonski propisi, međunarodni standardi i evropske direktive koji uređuju rukovanje eksplozivima, sigurnosne udaljenosti i obavezne postupke nadzora. Uloga geofizičkih metoda posebno je naglašena kao važan alat u planiranju sigurnih miniranja, jer iste omogućavaju identifikaciju nestabilnih zona i precizno određivanje geoloških parametara koji utiču na raspodjelu energije eksplozije. Dobijeni rezultati ukazuju na potrebu integrisanog pristupa koji povezuje tehničke, zakonske i organizacione mjere, čime se postiže viši nivo sigurnosti, efikasnosti i kontrole nad neželjenim efektima miniranja u površinskim eksploatacionim radovima.

Ključne riječi: *miniranje na površini, mjere zaštite, eksplozivni rizici, seizmički utjecaji, neeksplodirana sredstva, sigurnosne zone, geofizičke metode, zakonski propisi, organizacioni rizici*

[7] *Doc. dr. Faculty of Mining, Geology and Civil Engineering, University of Tuzla, Bosnia and Herzegovina, e-mail: ekrem.bektasevic@untz.ba, ORCID 0000-0001-6742-966X*
[8] *Ministry of Transport of Sarajevo Canton – The Road Directorate of Sarajevo Canton, e-mail: satko.filipovic.dpks@gmail.com, ORCID 0009-0003-7456-4773*
[9] *Redovni prof. dr. Faculty of Mining, Geology and Civil Engineering, University of Tuzla, Bosnia and Herzegovina, e-mail: kemal.gutic@untz.ba, ORCID 0009-0008-9107-4641*

1. Uvod

Miniranje na površini bilo da se izvodi na trasama, gradilištima, infrastrukturnim zonama ili eksploatacionim lokalitetima predstavlja jednu od najrizičnijih faza tehničkih operacija, s obzirom na prisustvo eksplozivnih materijala, dinamične sile, fragmentaciju stijenske mase i neposrednu izloženost radnika potencijalno štetnim utjecajima [1-3]. Zbog toga, mjere zaštite na radu u ovom segmentu zahtijevaju strogu tehničku, organizacionu i zakonsku kontrolu.

Prema podacima Administracije za sigurnost i zdravlje u rudnicima (Mine Safety and Health Administration-MSHA), svaka faza miniranja od skladištenja i transporta eksploziva do detonacije i pregled nakon provedenog miniranja mora biti regulisana preciznim protokolima kako bi se spriječile nesreće, povrede i štete na opremi [4]. Zaštita na radu ne podrazumijeva samo korištenje lične zaštitne opreme, već i sistemsku primjenu procedura koje obuhvataju planiranje, obuku, tehničku kontrolu i zakonsku usklađenost [5-8]. Poseban značaj imaju procedure za istraživanje incidenata, koje omogućavaju identifikaciju uzroka rizičnih događaja i definisanje korektivnih mjera, čime se direktno doprinosi sigurnijem radu na rizičnim radnim mjestima [9].

Kodeks dobre prakse za sigurnost miniranja (Blasting Safety Code of Practice) za površinske operacije naglašava da je procjena rizika temeljni korak u definisanju zona opasnosti, odabiru eksploziva, pripremi radne platforme i određivanju sigurnosnih udaljenosti [10]. U površinskom miniranju, svaka operacija mora biti prethodno analizirana kako bi se identificirali i procijenili svi potencijalni rizici povezani s geološkim uvjetima, prisustvom infrastrukture, meteorološkim faktorima i prethodnim incidentima fragmentacije stijenske mase. Ova sistemska analiza omogućava planiranje sigurnih procedura i minimiziranje opasnosti za radnike i okolinu [11].

Istraživanja su pokazala da zadržavanje radnika u zoni odbacivanja stijena tokom detonacije uzrokuje više od 40 % svih povreda u površinskom miniranju, što naglašava potrebu za strožijim procedurama i učinkovitijom kontrolom sigurnosti [12]. U modernim tehničkim sistemima miniranja, sigurnost radnika i kontrola detonacija sve više se oslanjaju na digitalne alate. Ovi sistemi omogućavaju praćenje zona miniranja u realnom vremenu, automatsko blokiranje pristupa opasnim područjima i senzorski nadzor nad detonacijom, čime se smanjuje rizik ljudske pogreške i povećava ukupna sigurnost operacija [13,14].

MSHA dodatno propisuje obaveznu inspekciju prostora na kojem je izvršeno miniranje nakon detonacije, zabranu ulaska u zonu miniranja prije signala „all clear“, te primjenu vizualnih i zvučnih upozorenja kao obaveznu proceduru [15].

Za provođenje sigurnog postupka bušenja i miniranja posebna pažnja mora se posvetiti označavanju zona miniranja, pravilnom transportu eksploziva, tretmanu neeksplodiranih sredstava i obaveznoj kontroli nakon detonacije. Ove mjere imaju za cilj smanjenje rizika od povreda uzrokovanih sekundarnim urušavanjem stijena, odbačenim stijenskim fragmentima i neeksplodiranim sredstvima te osiguranje zaštite radnika i sigurnog izvođenja miniranja [16].

U površinskim rudarskim i građevinskim radovima poseban izazov predstavlja postizanje precizne fragmentacije stijenske mase bez oštećenja korisnog materijala ili okolne infrastrukture. To zahtijeva pažljivo balansiranje između efikasnosti miniranja i sigurnosti radnika. Pravilna priprema bušotina, kontrola količine eksploziva i primjena odgovarajuće metode aktivacije minskog polja sa preciznom vremenskom sinhronizacijom ključni su faktori u smanjenju rizika od odbačenih stijenskih fragmenata i drugih nesreća, te istovremeno doprinose optimiziranju proces miniranja [17].

Zakonski okvir u Bosni i Hercegovini, kao i u zemljama EU, propisuje obaveznu izradu Elaborata o zaštiti na radu, koji mora sadržavati procjenu rizika, plan evakuacije, opis lične zaštitne opreme, te tehničke mjere za sprječavanje neželjenih efekata miniranja [18,19].

Uloga geofizičkih metoda u planiranju miniranja sve više dobiva na značaju. Seizmička karakterizacija podzemlja, georadarske prospekcije i elektromagnetna mjerenja omogućavaju detaljno mapiranje pukotinskih sistema, preciznu identifikaciju nestabilnih zona te i optimizaciju položaja bušotina. Time ne samo da se povećava efikasnost miniranja, već se značajno smanjuje rizik od neželjenih efekata, poput odbačenih stijenskih fragmenata, vibracija i sekundarnih urušavanja [20-24].

U konačnici, posebne mjere zaštite na radu pri miniranju na površini nisu samo tehnički izazov, već i etička obaveza izvođača, nadzora i projektanata. Svaka greška u planiranju, komunikaciji ili izvođenju može rezultirati ozbiljnim posljedicama po zdravlje radnika.

Ovaj rad ima za cilj da identifikuje i analizira ključne rizike pri miniranju na površinskim kopovima, te da predstavi tehničke i organizacione mjere zaštite u skladu sa važećim propisima i standardima. Fokus je na kontroli eksplozivnih i seizmičkih utjecaja, tretmanu neeksplodiranih sredstava i primjeni geofizičkih metoda radi unapređenja sigurnosti i efikasnosti miniranja.

2. Opis postupka miniranja

Miniranje na površinskom kopu tehničkog kamena obuhvata niz precizno definisanih operacija koje se moraju izvoditi u skladu s tehničkim normama, sigurnosnim protokolima i zakonskim propisima. Da bi se osigurala potpuna usklađenost sa važećim zakonodavstvom i tehničkim standardima, neophodno je prethodno razmotriti zakonski okvir koji definiše obaveznu dokumentaciju, mjere zaštite i tehničke zahtjeve za izvođenje miniranja.

2.1 Zakonski propisi i standardi za površinsko miniranje

Za svako miniranje na površinskom kopu tehničkog kamena obavezna je izrada Plana miniranja, koji mora sadržavati sve tehničke, sigurnosne i organizacione mjere u skladu sa važećim propisima. Prema Pravilniku o tehničkim normativima pri rukovanju eksplozivnim sredstvima i miniranju u rudarstvu [25], Plan mora uključivati tehničke parametre miniranja, vrstu i količinu eksploziva, način aktivacije, sigurnosne udaljenosti, mjere zaštite na radu, geološke i geofizičke podatke, opis radova, mjere zaštite od neželjenih efekata poput vibracija, urušavanja i rizika od neželjenog raspršivanja stijenskih komada, kao i obaveznu inspekciju zone miniranja nakon detonacije, pregled eventualnih neeksplodiranih sredstava i izdavanje signala za nastavak radova nakon potvrde da je zona sigurna. Usklađivanje domaćih propisa sa evropskim zakonodavstvom dodatno osigurava tehničku i pravnu validnost postupka miniranja. Direktiva 92/91/EEZ propisuje minimalne zahtjeve za sigurnost i zdravlje radnika u industriji ekstrakcije mineralnih sirovina, uključujući obaveznu procjenu rizika, tehničku kontrolu eksploziva i evakuacijske mjere [26]. Direktiva 2013/29/EU zahtijeva da eksplozivna sredstva budu tehnički dokumentovana, označena i praćena kroz sistem upravljanja sigurnošću [27], dok Direktiva 2014/28/EU definiše nadzor nad eksplozivima za civilnu upotrebu i njihovo stavljanje na tržište [28].

Primjena međunarodnog standarda EN ISO 45001:2018 omogućava sistematsko upravljanje zdravljem i sigurnošću na radu u svim fazama procesa miniranja, od planiranja do pregleda minskog polja nakon miniranja [29]. Tehnički standard EN 13631-10:2003 dodatno definiše metode ispitivanja eksploziva u vezi sa fragmentacijom, vibracijama i sigurnosnim udaljenostima [30].

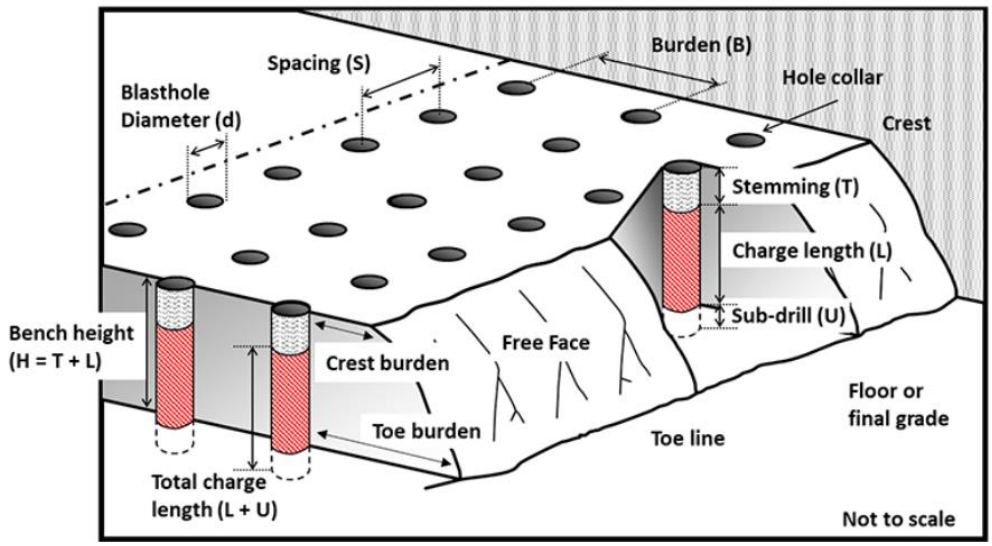
Plan miniranja mora biti izrađen i odobren prije početka operacija, a njegova primjena je obavezna u svim fazama miniranja. Usklađenost sa navedenim propisima predstavlja osnovu za tehnički ispravno, zakonski dozvoljeno i sigurnosno kontrolisano izvođenje miniranja.

Primjena zakonskih propisa, tehničkih normi i sigurnosnih procedura u oblasti miniranja potvrđena je kroz više stručnih radova koji dokumentuju primjenu kontrolisanog miniranja u složenim inženjerskim uslovima. Ovi primjeri iz prakse obuhvataju tehničku pripremu, izvođenje i postdetonacione mjere, uz dosljednu primjenu važećih propisa i standarda sigurnosti [31-33].

2.2 Priprema terena, bušenje punjenje eksplozivom i povezivanje

Prije početka miniranja, neophodno je izvršiti geološku i geofizičku karakterizaciju terena radi identifikacije pukotinskih sistema, nestabilnih zona i optimalnog rasporeda bušotina [34]. Seizmičke metode, georadar i elektromagnetna mjerenja omogućavaju precizno mapiranje strukture stijenske mase [35]. Raspored, međusobni razmak i dubina bušotina definišu se u skladu s lokalnim geofizičkim parametrima, strukturom stijenske mase i tehničkim ciljevima miniranja, uzimajući u obzir zahtjeve fragmentacije, stabilnosti i sigurnosne udaljenosti.

Bušenje se izvodi vertikalno ili pod blagim nagibom, uz kontrolu odstupanja od projektovane osi. Svaka bušotina mora biti označena, očišćena od ostataka, te provjerena na dubinu i eventualne blokade prije punjenja eksplozivom. Zabranjeno je bušenje u prethodno korištene bušotine ili u blizini neeksplodiranih sredstava [36]. Punjenje bušotina izvodi se patroniranim ili nepatroniranim eksplozivima, pri čemu se mora poštovati omjer mase eksploziva i zapremine izdvojenog stijenskog materijala kako bi se osigurala kontrolisana fragmentacija i ograničilo seizmičko djelovanje. Eksploziv se ne smije nasilno utiskivati, a alat koji se koristi prilikom punjenja minskih bušotina mora biti izrađen od drveta ili plastike i ne smije stvarati varnice. Inicijatori (detonatori) povezuju se serijski ili paralelno, a primjena sistema s vremenskom sinhronizacijom omogućava preciznu kontrolu redoslijeda paljenja radi smanjenja vibracija i optimizacije fragmentacije [37]. Na slici 1 prikazan je šematski raspored bušotina s označenim tehničkim parametrima miniranja.



Slika 1. Šematski prikaz rasporeda bušotina sa označenim parametrima: prečnik bušotine (d), rastojanje između bušotina (S), linija najmanjeg otpora (B), dužina punjenja (L), dužina čepa (T), probušenje/dodatna dubina bušotine (U) i visina etaže (H) [38].

2.3 Evakuacija i detonacija

Zona miniranja mora biti fizički ograđena, jasno označena tablama upozorenja i pod stalnim nadzorom ovlaštenih radnika koji učestvuju u procesu miniranja. Minimalna udaljenost evakuacije određuje se na osnovu prethodnih incidenata s izletnim kamenom, uz primjenu sigurnosnog faktora 1,5 puta najveće zabilježene udaljenosti odbačenog fragmenta. Ova udaljenost može se aproksimirati izrazom:

$$D = 1{,}5 \cdot R_{max}$$

gdje je R_{max} najveća zabilježena udaljenost odbacivanja fragmenta stijenske mase ustanovljena prilikom eksperimentalnog probnog miniranja. Navedeni izraz predstavlja empirijsku aproksimaciju koja se koristi u nedostatku preciznih mjerenja ili numeričkih modela, te služi kao praktičan kriterij za definisanje sigurnosne zone evakuacije.

Prije detonacije, obavezno je emitovanje zvučnog signala u tri faze: upozorenje, priprema i detonacija. Detonacija se smije izvršiti isključivo po nalogu odgovorne osobe, nakon potvrde da je zona u potpunosti evakuirana, da su svi električni i mehanički spojevi ispravni, te da meteorološki uvjeti omogućavaju sigurno izvođenje miniranja. U slučaju prisustva olujnih nepogoda, jakog vjetra ili smanjene vidljivosti, postupak miniranja mora se odgoditi do uspostavljanja povoljnih uslova [39].

2.4 Pregled zone miniranja nakon detonacije

Nakon izvođenja miniranja, radna zona se ne smije napuštati dok se ne emitira zvučni signal koji nedvosmisleno označava završetak operacije. Ova mjera ima za cilj sprečavanje prijevremenog ulaska osoblja u potencijalno opasno područje. Po završetku miniranja, obavezno je izvršiti detaljan vizuelni pregled kompletnog minskog polja, uključujući odminiranu masu, pristupačne dijelove radilišta i sve površine koje su bile izložene djelovanju eksploziva. Pregled se vrši radi provjere prisustva zaostalih eksplozivnih sredstava, procjene stabilnosti terena i identifikacije eventualnih deformacija ili pomjeranja stijenske mase [40].

U slučaju sumnje na prisustvo neeksplodiranog sredstva (NES), pristup zoni miniranja dozvoljen je isključivo stručno osposobljenom osoblju koje raspolaže odgovarajućom zaštitnom opremom i primjenjuje propisane sigurnosne postupke. Svaka intervencija mora biti dokumentovana, a daljnje aktivnosti se mogu nastaviti tek nakon što se potvrdi da je područje sigurno za rad [41].

3. Identifikacija rizika

Miniranje na površini uključuje niz složenih i potencijalno opasnih operacija koje generišu različite vrste rizika. Efikasna identifikacija i klasifikacija tih rizika predstavlja osnovu za primjenu odgovarajućih mjera zaštite na radu. Rizici se mogu sistematizirati u četiri glavne kategorije: mehanički, eksplozivni, seizmički/zvučni i organizacioni.

3.3 Mehanički rizici

Mehanički rizici u površinskom miniranju proizlaze iz interakcije radnika s tehničkim sistemima, dinamičnim radnim okruženjem i nestabilnim stijenskim materijalom. U kontekstu bušenja, punjenja i pripreme fronte, najčešće identificirane mehaničke prijetnje uključuju kontakt s rotirajućim dijelovima bušačke opreme, padove s visinskih etaža, te udare od odlomljenih blokova stijenske mase. Ovi rizici su inherentni procesu, ali se njihova učestalost i intenzitet značajno povećavaju u uslovima neadekvatne tehničke kontrole, nedostatka prostorne segregacije i odsustva sistemske zaštite.

Prema OSHA regulativi (29 CFR 1910.212), tehnički sistemi moraju biti projektovani i održavani na način koji onemogućava direktan kontakt s pokretnim dijelovima, dok se radna zona mora fizički i proceduralno izolovati tokom aktivnih operacija. Empirijska istraživanja ukazuju da je upravo nepostojanje barijera i neadekvatna signalizacija najčešći uzrok mehaničkih povreda u rudarstvu i građevinarstvu [12,42].

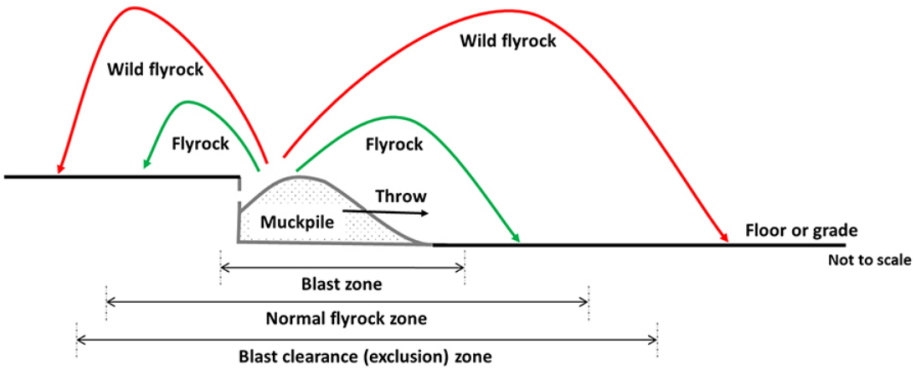
Lična zaštitna oprema, iako formalno obavezna, ne može kompenzirati sistemske propuste u organizaciji rada. Studije pokazuju da reflektirajuća odjeća, zaštitne kacige i obuća s čeličnim vrhom imaju preventivni učinak samo u kombinaciji s tehničkom kontrolom pristupa i obukom osoblja [43]. U tom smislu, mehanički rizici se ne mogu tretirati izolovano, već zahtijevaju integraciju tehničkih, organizacionih i edukativnih mjera u okviru sveobuhvatnog sistema upravljanja sigurnošću.

3.4 Eksplozivni rizici

Eksplozivni rizici predstavljaju najkritičniju kategoriju opasnosti u procesu površinskog miniranja, s obzirom na neposrednu energiju oslobađanja, nepredvidive efekte detonacije i mogućnost sekundarnih incidenata. U tehničkoj i sigurnosnoj literaturi, najčešće identificirani eksplozivni rizici uključuju: preranu detonaciju, prisustvo neeksplodiranih sredstava (tzv. misfire), nekontrolisano odbacivanje stijenskih fragmenata (flyrock), te prekomjernu količinu eksploziva u odnosu na projektovane parametre.

Nekontrolisano razbacivanje fragmenata stijenske mase izvan predviđene zone miniranja, posebno je opasno zbog svoje prostorne nepredvidivosti i kinetičke energije. Empirijski podaci ukazuju da fragmenti mogu dostići udaljenosti veće

od 300 metara od epicentra detonacije, pri čemu se bilježe slučajevi teških povreda i fatalnih ishoda [12,42]. U tom kontekstu, prostorna distribucija rizika mora biti precizno definisana, uz primjenu sigurnosnog faktora i prethodnih terenskih mjerenja. Prostorna raspodjela rizika usljed nekontrolisanog odbacivanja stijenskih fragmenata tokom miniranja prikazana je na slici 2, koja ilustrativno definiše zonu miniranja, sigurnosnu zonu evakuacije i moguće putanje odbačenih fragmenata stijenske mase.



Slika 2. Zona odbačenih stijenskih fragmenata pri miniranju – prostorna distribucija rizika i sigurnosnih granica [44]

Za procjenu incidentnog pritiska zračne eksplozije koristi se empirijski izraz poznat kao Kingery–Bulmash model [45]:

$$P = \frac{K \cdot Q^{1/3}}{R}$$

gdje je:

P - pritisak, izražen u bar.,
Q - količina eksploziva, u kg,
R - udaljenost od epicentra, u m' i
K - empirijski koeficijent, zavisan od vrste eksploziva i geometrije detonacije.

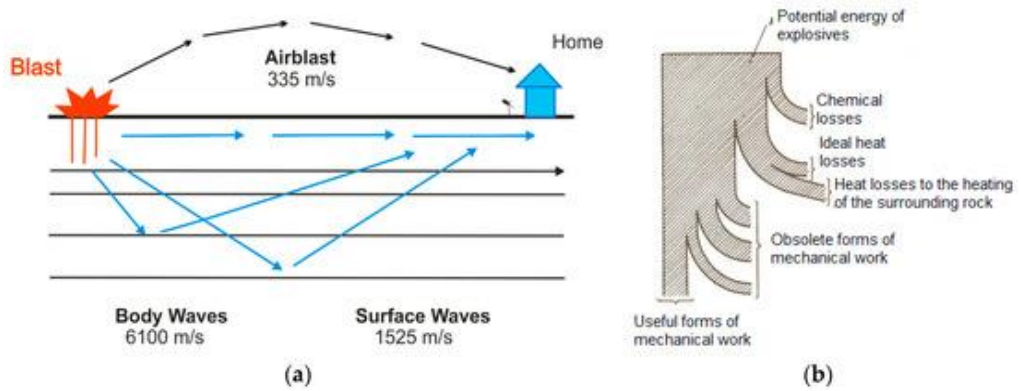
Ova formula se koristi u planiranju zone miniranja, posebno u blizini infrastrukture, naseljenih područja ili osjetljivih objekata. Neeksplodirana sredstva predstavljaju latentni rizik koji zahtijeva specijalizovanu intervenciju. Prema smjernicama MSHA, zona u kojoj se sumnja na prisustvo neeksplodiranih sredstava mora biti izolovana, a pristup dozvoljen isključivo stručno obučenom osoblju sa odgovarajućom zaštitnom opremom i tehničkom podrškom.

3.5 Seizmički, vibracioni i akustički rizici

Detonacija eksploziva u površinskom miniranju generiše seizmičke i zračne talase koji se šire kroz tlo i atmosferu, pri čemu dolazi do interakcije s okolnim objektima, infrastrukturom i ljudskim organizmima. Ovi talasi mogu uticati na stabilnost građevinskih struktura, integritet podzemnih instalacija, te izazvati fiziološke i psihološke reakcije kod radnika i stanovništva u blizini zone miniranja [46-49].

Vibracije tla prenose se u objekat putem temelja i podruma, dok zračni udar djeluje na zidne i krovne površine. Rezultantno podrhtavanje može izazvati zveckanje predmeta, pomjeranje opreme i osjećaj unutrašnje buke, koja kod ljudi izaziva alarmantne reakcije, iako sama buka ima zanemariv utjecaj na konstrukcijsku stabilnost [47-49].

U nastavku teksta, na slici 3a prikazan je mehanizam širenja seizmičkih i zračnih talasa generisanih detonacijom eksploziva. Talasi se prostiru radijalno od epicentra, pri čemu dolazi do diferencirane interakcije s tlom ili objektom. Slika 3b prikazuje energetsku bilancu eksplozije, gdje se jasno vidi da se samo manji dio oslobođene energije troši na drobljenje stijenske mase. Većina oslobođene energije prenosi se kroz neželjene efekte, kao što su širenje usitnjene mase te generisanje seizmičkih i zračnih talasa [50].



Slika 3. (a) Širenje seizmičkih i zračnih talasa tokom miniranja; (b) Šema energetske bilance tijekom miniranja [51]

Prema tehničkim smjernicama, dozvoljeni nivo vibracija na granici zone miniranja iznosi maksimalno 5 mm/s za stambene objekte, odnosno 10 mm/s za industrijske strukture [52]. Praćenje stvarnih vrijednosti vrši se seizmičkim monitoringom putem geofona, čime se omogućava prilagođavanje parametara miniranja u realnim uslovima [53]. Za tehničku procjenu seizmičkog utjecaja koristi se standardizovana empirijska formula [54]:

$$PPV = K \cdot \left(\frac{D}{Q^{1/2}}\right)^{-n}$$

gdje je:

PPV – maksimalna brzina vibracija, u mm/s,
D – udaljenost od epicentra eksplozije, u m',
Q – količina eksploziva po odgodi, u kg i
K,n – koeficijenti koji zavise od lokalnih geoloških uslova i vrste eksploziva.

Vrijednosti se određuju terenskim mjerenjem, najčešće metodom najmanjih kvadrata, čime se omogućava lokalna kalibracija modela i precizno planiranje miniranja u osjetljivim zonama [54].

Pored seizmičkih i vibracionih efekata, detonacija eksploziva generiše i zračni udar (airblast), koji nastaje usljed naglog širenja plinova iz eksplozije. Ovaj impulsni talas može izazvati oštećenje staklenih površina, poremećaj u radu elektronske opreme, te negativan utjecaj na sluh radnika. Preporučeni prag zračnog udara iznosi 120 dB za industrijske zone, dok se za naseljena područja preporučuje maksimalno 115 dB [55]. Akustički rizici se kontrolišu primjenom zvučnih barijera, pravilnim tempiranjem detonacije i obaveznim korištenjem zaštite za sluh.

3.6 Organizacioni rizici

Organizacioni rizici predstavljaju ključan faktor u sigurnosnoj analizi miniranja, jer se odnose na sistemske propuste u planiranju, komunikaciji i izvršenju operacija. Najčešći izvori ovih rizika uključuju nedostatak obuke, nejasnu raspodjelu odgovornosti, lošu komunikaciju među timovima, te neusklađenost sa važećim zakonskim propisima.

Prema Pravilniku o tehničkim normativima pri rukovanju eksplozivnim sredstvima i miniranju u rudarstvu [25], izvođač je dužan osigurati prisustvo ovlaštenog lica za rukovanje eksplozivima, evidentirati stručno osposobljavanje radnika, te obezbijediti fizičku zaštitu zone miniranja putem signalizacije i barijera. Iako evakuacione procedure nisu eksplicitno propisane, tehnički elaborat mora sadržavati mjere koje osiguravaju sigurnost radnika u zoni miniranja.

U domaćoj literaturi se ističe da su organizacioni propusti, posebno u fazi pripreme i koordinacije, čest uzrok odstupanja u sigurnosnim parametrima miniranja. Nedostatak formalizovanih procedura, neadekvatna komunikacija među timovima i nepostojanje jasnih operativnih uputa mogu dovesti do grešaka koje se u eksplozivnim operacijama manifestuju s ozbiljnim posljedicama [56].

4. Zaključak

Miniranje na površinskim kopovima predstavlja jednu od najzahtjevnijih i najrizičnijih faza tehničkih operacija u rudarskom i infrastrukturnom sektoru. Uspješno upravljanje rizicima koji proizlaze iz ovog procesa zahtijeva sistemsku integraciju zakonskih propisa, tehničkih normi, organizacionih mjera i geofizičkih metoda. Svaka faza, od planiranja i bušenja do detonacije i postdetonacione inspekcije, mora biti precizno definisana i kontrolisana kako bi se osigurala sigurnost radnika, stabilnost radne zone i zaštita okoline.

Analizom ključnih kategorija rizika utvrđeno je da eksplozivni, seizmički i organizacioni faktori imaju dominantan utjecaj na sigurnost operacija. Eksplozivni rizici, poput nekontrolisanog odbacivanja stijenskih fragmenata i prisustva neeksplodiranih sredstava, zahtijevaju primjenu empirijskih modela, tehničkih barijera i specijalizovanih procedura. Seizmički i akustički utjecaji moraju se kvantitativno pratiti i kontrolisati putem geofona i standardizovanih proračuna, dok organizacioni propusti, naročito u fazi pripreme i koordinacije, predstavljaju latentni izvor nesreća koji se može prevenirati uspostavljanjem jasnih procedura formalizacijom procedura i obukom osoblja.

Usklađenost sa Pravilnikom o tehničkim normativima pri rukovanju eksplozivnim sredstvima i miniranju u rudarstvu, kao i sa evropskim direktivama i međunarodnim standardima, predstavlja osnovu za zakonito i tehnički validno izvođenje miniranja. Primjena geofizičkih metoda, poput seizmičke tomografije i elektromagnetne prospekcije, omogućava preciznu karakterizaciju stijenske mase, identifikaciju nestabilnih zona i optimizaciju rasporeda bušotina, čime se direktno doprinosi smanjenju rizika i povećanju efikasnosti.

Zaključno, sigurnost pri miniranju nije samo tehnički izazov, već i profesionalna i etička obaveza svih učesnika u procesu. Samo dosljednom primjenom validiranih podataka, usklađenih procedura i multidisciplinarnog pristupa moguće je ostvariti kontrolisane, efikasne i sigurne minerske operacije u složenim inženjerskim uslovima.

1. Literatura

1. Bajpayee, T. S., Rehak, T. R., Mowrey, G. L., & Ingram, D. K. (2004). Blasting injuries in surface mining with emphasis on flyrock and blast area security. *Journal of Safety Research, 35*(1), 47–57. https://doi.org/10.1016/j.jsr.2003.07.003
2. Kecojevic, V., & Radomsky, M. (2005). Flyrock phenomena and area security in blasting-related accidents. *Safety Science*, 43(9), 739–750. https://doi.org/10.1016/j.ssci.2005.07.006
3. Valjevac, M., Bektašević, E., Gutić, K., Sakić, N., & Sikira, D. (2024). Exploitation and processing of technical stone from quarries Plješevac near Kiseljak. *Journal of Faculty of Mining, Geology and Civil Engineering, University of Tuzla*, 12, [Professional Paper]. https://doi.org/10.51558/2303-5161.2024.12.12.23
4. Mine Safety and Health Administration. (2002). *Module 11: Transportation, use, and storage of explosives*. U.S. Department of Labor. Retrieved from https://arlweb.msha.gov/safetypro_in_a_box/IG%2043%20OJT%20training%20modules%20surface%20MNM/Module%2011%20Transportation%20use%20and.%20storage%20of%20explosives.PDF
5. Festić, E., & Imamović, A. (2021). Značaj edukacije i opšti uslovi za bezbjedan transport opasnih materija prema ADR-u. *Zaštita i sigurnost*, 1(2), 95–106.
6. Bektašević, E., Gutić, K., Valjevac, M., & Sakić, N. (2025, April). The role and importance of preventive safety measures at work during the production and processing of technical stone at the quarry. In *15th Scientific/Research Symposium with International Participation „METALLIC AND NONMETALLIC MATERIALS“*, Bosnia and Herzegovina.
7. Bektašević, E., Gutić, K., Valjevac, M., & Konta, J. (2024, December). Unapređivanje mjera zaštite na radu u kamenolomima pri proizvodnji i preradi tehničkog kamena. *Rudarsko-geološki glasnik*, Hrvatsko rudarsko-geološko društvo Mostar, 49–61. ISSN 1840-0299.
8. Chen, X.-k., Zhu, H.-l., & Chen, J.-q. (2011). *Hazard identification and control in the pre-blasting process*. *Journal of Coal Science and Engineering (China), 17*(3), 331-335. https://doi.org/10.1007/s12404-011-0320-0
9. Imamović, A., Softić, S., Kablar, O., & Oruč, M. (2022). Značaj procedure istraživanja incidenta za sigurniji rad na rizičnim radnim mjestima. *Zaštita i sigurnost*, 2(1), 22–31.
10. Manitoba Labour and Immigration. (2006). *Code of practice for the use of explosives*. Workplace Safety and Health Division. Retrieved from https://www.gov.mb.ca/labour/safety/pdf/cop_useof_explosives.pdf
11. Strzałkowski, P., Woźniak, J., Górniak-Zimroz, J., & et al. (2025). Identification and systematics of safety hazards in surface rock mining. *Scientific Reports, 15*, 30492. https://doi.org/10.1038/s41598-025-16437-z

12. Bajpayee, T. S., Rehak, T. R., Mowrey, G. L., & Ingram, D. K. (2004). Blasting injuries in surface mining with emphasis on flyrock and blast area security. *Journal of Safety Research, 35*(1), 47–57. https://doi.org/10.1016/j.jsr.2003.07.003
13. Engineer Live. (2023). *Better blasting: Improving safety in mining operations*. Retrieved October 1, 2025, from https://www.engineerlive.com/content/better-blasting
14. Identec Solutions. (2023). *Blasting safety in daily mining operations*. Retrieved October 1, 2025, from https://www.identecsolutions.com/news/blasting-safety-in-daily-mining-operations
15. Mine Safety and Health Administration. (n.d.). *Blasting safety*. U.S. Department of Labor. Retrieved October 1, 2025, from https://www.msha.gov/safety-health/safety-health/safety-health-materials/safety-topics/blasting-safety
16. National Institute for Occupational Safety and Health. (2006). *Blast area security: Flyrock safety* (NIOSH Report No. 2007-112). U.S. Department of Health and Human Services. https://www.cdc.gov/niosh/docs/mining/UserFiles/works/pdfs/2007-112.pdf
17. Orica. (2010). *Safety of blasting with electronic detonators*. Orica Technical Bulletin. https://www.orica.com/ArticleDocuments/2606/200415_Safety%20of%20Electronic%20Detonators%20for%202010%20ISEE%20Lownds%2C%20Steiner.pdf.aspx
18. Vlada Federacije Bosne i Hercegovine. (2020). *Zakon o zaštiti na radu*. Službene novine Federacije BiH, broj 17/20. https://fbihvlada.gov.ba/bosanski/zakoni/2020/Zakoni/17.htm
19. Vijeće Europske unije. (1989). *Direktiva 89/391/EEZ o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja radnika na radu*. Službeni list Europske unije, L 183, 1–8. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A31989L0391
20. Reynolds, J. M. (2011). *An introduction to applied and environmental geophysics* (2nd ed.). Wiley-Blackwell.
21. Bektašević, E., Antičević, H., Gutić, K., & Sikira, D. (2024). Determination of the depth of the rock mass damage zone around the excavation profile by blasting with seismic cross-hole tomography in the „Šubir“ tunnel on the Zagreb-Split motorway. *Nauka+Praksa*, (27), 13–19. https://doi.org/10.62683/NiP27.13-19
22. Bektašević, E., & Gutić, K. (2025). Seismic impact assessment of blasting on surrounding population using geophysical methods. *Engineering and Technology Journal*, 10(4), 4468–4475. https://doi.org/10.47191/etj/v10i04.12

23. Bektašević, E., Antičević, H., Gutić, K., & Sikira, D. (2024). Application of seismic methods for determining the depth of the rock mass damage zone around the excavation profile by blasting. *Global Journal of Engineering and Technology Advances*, 18(3), 139–151. https://doi.org/10.30574/gjeta.2024.18.3.0051
24. Husejnagić, E., Bektašević, E., Osmanović, F., Žutić, Đ., Konta, J., & Hasić, E. (2016). Geofizičko-seizmička ispitivanja vještački izazvanih potresa i njihov uticaj na sigurnost i stabilnost objekata na PK Koritnik-Breza. In *Zbornik radova petog međunarodnog naučno-stručnog savetovanja*, Savez građevinskih inženjera Srbije, Sremski Karlovci (pp. 205–222).
25. Službeni list SFRJ. (1988). Pravilnik o tehničkim normativima pri rukovanju eksplozivnim sredstvima i miniranju u rudarstvu.
26. European Commission. (1992). *Council Directive 92/91/EEC on the minimum requirements for improving the safety and health protection of workers in the mineral-extracting industries through drilling*. https://eur-lex.europa.eu/eli/dir/1992/91/oj/eng
27. European Parliament and Council. (2013). *Directive 2013/29/EU on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles*. https://eur-lex.europa.eu/eli/dir/2013/29/oj/eng
28. European Parliament and Council. (2014). *Directive 2014/28/EU on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses*. https://eur-lex.europa.eu/eli/dir/2014/28/oj/eng
29. International Organization for Standardization. (2018). *ISO 45001:2018 – Occupational health and safety management systems – Requirements with guidance for use*. https://www.iso.org/standard/63787.html
30. European Committee for Standardization. (2003). *EN 13631-10:2003 – Explosives for civil uses – High explosives – Part 10: Verification of initiation methods*. https://standards.iteh.ai/catalog/standards/cen/9b294e02-391f-47cd-85fe-60101faf6341/en-13631-10-2003
31. Bektašević, E., Kadrić, R., Nikolić, M., Gutić, K., & Kadrić, S. (2023). Excavation of the foundation of piers S1L and S1R of the Vranduk I bridge by controlled blasting on the motorway route: Zenica Municipality Northern Administrative Boundary – Zenica North. *Electronic Collection of Papers, Faculty of Civil Engineering, University of Mostar*, 26, 9–26. https://doi.org/10.47960/2232-9080.2023.26.13.9
32. Bektaševič, E., Kadrić, R., Gutić, K., & Kadrić, S. (2023). Primjena kontrolisanog miniranja pri iskopu ulaznog portala desne tunelske cijevi tunela „Vranduk“ na koridoru Vc. *Zbornik radova GEO-EXPO 2023*, Društvo za geotehniku u Bosni i Hercegovini, 163–172. https://doi.org/10.35123/GEO-EXPO_2023_17

33. Bektaševič, E., Antičević, H., Osmanović, F., Kadrić, S., Žutić, Đ., & Konta, J. (2023). Tehnologija miniranja pri iskopu evakuacionog tunela „Vranduk II“ na magistralnoj cesti M-17. *Elektronički zbornik radova Građevinskog fakulteta Sveučilišta u Mostaru*, 49–60. https://doi.org/10.47960/2232-9080
34. Ilić, M. (2017). Application of results of geological exploration of deposits of solid mineral raw materials in mining. *Tehnika – Mining, Geological and Metallurgical Engineering*, *72*(2), 204–211. https://doi.org/10.5937/tehnika1702204I
35. Bektašević, E., Strelec, S., Sakić, N., & Gutić, K. (2025). Multichannel surface wave analysis in the context of shallow geophysical investigations. Academia Engineering, 2(3). https://doi.org/10.20935/AcadEng7876
36. Occupational Safety and Health Administration (OSHA). (2024). *1926.905 - Loading of explosives or blasting agents*. U.S. Department of Labor. Retrieved from https://www.osha.gov/laws-regs/regulations/standardnumber/1926/1926.905
37. Tang, H.-L., Liu, X., Yang, J., & Yu, Q. (2023). Experimental Study on the Influence of Delay Time on Rock Fragmentation in Bench Blasting. *Applied Sciences*, *13*(1), 85. https://doi.org/10.3390/app13010085
38. Szendrei, T. & Tose, S.. (2024). Flyrock in surface mining Part II - Causes, sources, and mechanisms of rock projection. Journal of the Southern African Institute of Mining and Metallurgy. 123. 557-564. 10.17159/2411-9717/2583/2023.
39. Božić, B. (1998). *Miniranje u rudarstvu, graditeljstvu i geotehnici*. Varaždin: Geotehnički fakultet Sveučilišta u Zagrebu.
40. Bektašević, E. (2022). *Blasting: Examples of surface blasting and tunnel construction with occupational safety measures*. LAP LAMBERT Academic Publishing.
41. QNJAC. (2020). *Post-blast inspection guidance for quarries*. Quarries National Joint Advisory Committee. https://minex.org.nz/training/toolbox/the-post-blast-inspection.pdf
42. Kecojevic, V., & Radomsky, M. (2005). *Flyrock phenomena and area security in blasting-related accidents*. Safety Science, 43(9), 739–750. https://doi.org/10.1016/j.ssci.2005.07.006
43. ISEE. (2022). *Personal Protective Equipment in Blasting Operations*. International Society of Explosives Engineers.
44. Little, T. N. (2007). *Flyrock risk*. In *Proceedings of EXPLO2007: Blasting—Techniques and Technology* (pp. 35–43). Australasian Institute of Mining and Metallurgy.
45. Kingery, C. N., & Bulmash, G. (1984). *Airblast parameters from TNT spherical air burst and hemispherical surface burst* (ARBRL-TR-02555). U.S. Army Ballistic Research Laboratory. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA955203.pdf

46. Bektašević, E., & Gutić, K. (2025). *Seismic impact assessment of blasting on surrounding population using geophysical methods*. *Engineering and Technology Journal*, *10*(4), 4468–4475. https://doi.org/10.47191/etj/v10i04.12
47. tagg, M. S., & Siskind, D. E. (1987). *Effects of blast vibration on construction material cracking in residential structures* (p. 43). Bureau of Mines Technology Transfer Seminar, Chicago, MI, USA.
48. Siskind, D. E., & Stagg, M. S. (1987). *Blast vibration measurements near structures* (pp. 46–50). Bureau of Mines Technology Transfer Seminar, Chicago, MI, USA.
49. Hustrulid, W. A. (1999). *Blasting principles for open pit mining* (Vol. 2). CRC Press.
50. Malbašić, V., & Stojanović, L. (2017). *Determination of seismic safety zones during the surface mining operation development in the case of open pit „Buvač“*. In *Proceedings of the 6th International Symposium MEP 17* (pp. 138–144), Vrdnik, Serbia, June 21–24.
51. Malbasic, V., & Stojanovic, L. (2018). Determination of Seismic Safety Zones during the Surface Mining Operation Development in the Case of the „Buvač“ Open Pit. *Minerals*, *8*(2), 71. https://doi.org/10.3390/min8020071
52. Husejnagić, E., Bektašević, E., Osmanović, F., Žutić, Đ., Konta, J., & Hasić, E. (2015). *Geofizičko-seizmička ispitivanja vještački izazvanih potresa i njihov uticaj na sigurnost i stabilnost objekata na PK Koritnik–Breza. Rudarsko-geološki glasnik*, Hrvatsko rudarsko geološko društvo, Mostar, 67–82. (ISSN 1840-0299).
53. Bektašević, E., Frljak, N., Sarajlić, M., Konta, J., & Lapandić, E. (2013). *Komparativni pregled uticaja prirodnih i vještački izazvanih potresa na primjeru „Rudnika krečnjaka Breza“–Breza*. *Rudarsko-geološki glasnik*, Hrvatsko rudarsko geološko društvo, Mostar, 70–77. (ISSN 1840-0299).
54. Boon, C. W., & Ooi, L. H. (2015). *Rock blasting — peak particle velocity against distance*. In Proceedings of the 11th International Symposium on Rock Fragmentation by Blasting (FRAGBLAST 11), Sydney, Australia. Australian Centre for Geomechanics. Dostupno na: https://papers.acg.uwa.edu.au/d/1508_23_Boon/23_Boon.pdf
55. Gregurović, N. (2013). *Kontrola seizmičkih efekata pri opreznim miniranjima u urbanim sredinama* [Diplomski rad, Geotehnički fakultet Sveučilišta u Zagrebu]. Repozitorij GFV. https://repozitorij.gfv.unizg.hr/islandora/object/gfv%3A75/datastream/PDF/view
56. Katalinić, M. (2021). *Netipične vrijednosti kod mjerenja seizmičkih utjecaja miniranja* [Diplomski rad, Rudarsko-geološko-naftni fakultet, Sveučilište u Zagrebu]. Repozitorij RGNF. https://zir.nsk.hr/islandora/object/rgn%3A1783/datastream/PDF/download

Popis slika

SAFETY RISKS AND PROTECTIVE MEASURES IN SURFACE BLASTING

DOI: 1*0.70329/2744-2403.2025.5.10.3*

Original scientific paper

Ekrem Bektašević[10], Satko Filipović[11], Kemal Gutić[12]

Abstract:
Surface blasting represents one of the most complex and high-risk processes in mining practice, where the safety of people and infrastructure directly depends on proper planning, technical control, and compliance with prescribed safety measures. This paper provides a systematic overview of the risks accompanying all phases of surface blasting from drilling and borehole charging to detonation and post-detonation inspection and defines key technical and organizational measures for their prevention. Special attention is devoted to explosive, seismic, and acoustic impacts, which are controlled through the application of empirical models, seismic monitoring, and appropriate blast-field design. The paper analyzes relevant legal regulations, international standards, and European directives governing the handling of explosives, safety distances, and mandatory supervision procedures. The role of geophysical methods is particularly emphasized as an important tool in the planning of safe blasting operations, as they enable the identification of unstable zones and precise determination of geological parameters influencing the distribution of explosion energy. The obtained results indicate the need for an integrated approach that connects technical, legal, and organizational measures, thereby achieving a higher level of safety, efficiency, and control over undesirable effects of blasting in surface exploitation operations.

Keywords: *surface blasting, protective measures, explosive risks, seismic impacts, unexploded ordnance, safety zones, geophysical methods, legal regulations, organizational risks*

[10] *Doc. dr. Faculty of Mining, Geology and Civil Engineering, University of Tuzla, Bosnia and Herzegovina, e-mail: ekrem.bektasevic@untz.ba, ORCID 0000-0001-6742-966X*
[11] *Ministry of Transport of Sarajevo Canton – The Road Directorate of Sarajevo Canton, e-mail: satko.filipovic.dpks@gmail.com, ORCID 0009-0003-7456-4773*
[12] *Redovni prof. dr. Faculty of Mining, Geology and Civil Engineering, University of Tuzla, Bosnia and Herzegovina, e-mail: kemal.gutic@untz.ba, ORCID 0009-0008-9107-4641*

1. Introduction

Surface blasting, whether carried out along road alignments, construction sites, infrastructure zones, or exploitation areas, represents one of the most hazardous phases of technical operations due to the presence of explosive materials, dynamic forces, rock mass fragmentation, and the direct exposure of workers to potentially harmful effects [1–3].

Therefore, occupational safety measures in this segment require strict technical, organizational, and legal control. According to data from the Mine Safety and Health Administration (MSHA), every stage of the blasting process from the storage and transport of explosives to detonation and post-blast inspection must be regulated by precise protocols to prevent accidents, injuries, and equipment damage [4]. Occupational safety does not only imply the use of personal protective equipment but also the systematic implementation of procedures that include planning, training, technical supervision, and legal compliance [5–8]. Special importance is given to incident investigation procedures, which enable the identification of the causes of hazardous events and the definition of corrective measures, thereby directly contributing to safer working conditions in high-risk environments [9].

The Blasting Safety Code of Practice for surface operations emphasizes that risk assessment is the fundamental step in defining danger zones, selecting explosives, preparing the working platform, and determining safety distances [10]. In surface blasting, each operation must be analyzed in advance to identify and assess all potential risks associated with geological conditions, nearby infrastructure, meteorological factors, and previous incidents of rock mass fragmentation. This systematic analysis enables the planning of safe procedures and the minimization of hazards to workers and the environment [11].

Research has shown that retaining workers within the rock-throw zone during detonation accounts for more than 40% of all surface blasting injuries, highlighting the need for stricter procedures and more effective safety control [12]. In modern blasting systems, worker safety and detonation control increasingly rely on digital tools. These systems enable real-time monitoring of blasting zones, automatic restriction of access to hazardous areas, and sensor-based detonation supervision, thereby reducing the risk of human error and increasing overall operational safety [13,14].

MSHA further prescribes mandatory post-blast site inspection, prohibition of entry into the blasting area before the “all clear” signal, and the use of visual and audible warnings as standard procedures [15].

To ensure safe drilling and blasting operations, particular attention must be given to marking blasting zones, proper transport of explosives, handling unexploded ordnance, and mandatory post-detonation inspections. These measures aim to reduce the risk of injuries caused by secondary rock collapses, flying rock fragments, and unexploded materials, ensuring worker safety and controlled execution of blasting [16].

In surface mining and construction works, achieving precise rock fragmentation without damaging valuable material or nearby infrastructure presents a particular challenge. This requires a careful balance between blasting efficiency and worker safety. Proper borehole preparation, control of explosive quantities, and the application of suitable blast-field initiation methods with precise timing synchronization are key factors in minimizing the risk of flyrock and other accidents, while simultaneously optimizing the blasting process [17].

The legal framework in Bosnia and Herzegovina, as well as in EU countries, prescribes the mandatory preparation of a Safety Protection Study, which must include a risk assessment, evacuation plan, description of personal protective equipment, and technical measures for preventing adverse blasting effects [18,19].

The role of geophysical methods in blasting design is gaining increasing importance. Seismic subsurface characterization, ground-penetrating radar (GPR) surveys, and electromagnetic measurements enable detailed mapping of fracture systems, precise identification of unstable zones, and optimization of borehole placement. This not only enhances blasting efficiency but also significantly reduces the risk of adverse effects such as flyrock, vibrations, and secondary collapses [20–24].

Ultimately, specific occupational safety measures in surface blasting are not only a technical requirement but also an ethical obligation for contractors, supervisors, and designers. Every error in planning, communication, or execution can result in serious consequences for worker safety.

The aim of this paper is to identify and analyze key risks associated with surface blasting operations and to present the corresponding technical and organizational protection measures in accordance with current regulations and standards. The focus is on the control of explosive and seismic impacts, treatment of unexploded ordnance, and the application of geophysical methods to improve the safety and efficiency of blasting operations.

2. Description of the Blasting Procedure

Blasting at a surface quarry for technical stone involves a series of precisely defined operations that must be carried out in accordance with technical standards, safety protocols, and legal regulations. To ensure full compliance with applicable legislation and technical standards, it is essential first to consider the legal framework that defines mandatory documentation, safety measures, and technical requirements for performing blasting operations.

2.1 Legal Regulations and Standards for Surface Blasting

For every blasting operation at a surface quarry for technical stone, it is mandatory to prepare a Blasting Plan that must include all technical, safety, and organizational measures in accordance with applicable regulations. According to the Rulebook on Technical Standards for the Handling of Explosives and Blasting in Mining [25], the Plan must include technical blasting parameters, the type and quantity of explosives, the initiation method, safety distances, occupational safety measures, geological and geophysical data, a description of the works, measures for protection against undesirable effects such as vibrations, collapses, and the risk of rock scattering, as well as a mandatory post-detonation inspection of the blasting zone, examination of potential unexploded charges, and issuance of clearance signals for resuming work once the area is confirmed to be safe. The harmonization of domestic regulations with European legislation further ensures the technical and legal validity of the blasting process.

Directive 92/91/EEC prescribes minimum requirements for the safety and health of workers in the extractive industries, including mandatory risk assessment, technical control of explosives, and evacuation measures [26].

Directive 2013/29/EU requires that explosive materials be technically documented, labeled, and traceable through a safety management system [27], while Directive 2014/28/EU defines the supervision of explosives for civil use and their placement on the market [28].

The application of the international standard EN ISO 45001:2018 enables systematic management of occupational health and safety in all stages of the blasting process, from planning to post-blast inspection of the blast site [29].

The technical standard EN 13631-10:2003 further defines methods for testing explosives concerning fragmentation, vibrations, and safety distances [30]. The Blasting Plan must be developed and approved before the commencement of operations, and its implementation is mandatory throughout all stages of blasting. Compliance with these regulations forms the basis for technically sound, legally permitted, and safely controlled blasting operations.

The implementation of legal regulations, technical standards, and safety procedures in the field of blasting has been confirmed through numerous professional studies documenting the application of controlled blasting in

complex engineering conditions. These case studies encompass technical preparation, execution, and post-detonation measures, with consistent adherence to current regulations and safety standards [31–33].

2.2 Site preparation, drilling, charging and connection

Prior to blasting, it is necessary to perform geological and geophysical characterization of the site to identify fracture systems, unstable zones, and the optimal layout of boreholes [34]. Seismic methods, ground-penetrating radar, and electromagnetic measurements enable precise mapping of the rock-mass structure [35]. The arrangement, spacing, and depth of boreholes are defined in accordance with local geophysical parameters, rock-mass structure, and the technical objectives of blasting, taking into account fragmentation requirements, stability, and safety distances. Drilling is performed vertically or with a slight inclination, with control of deviation from the designed axis. Each borehole must be marked, cleared of debris, and checked for depth and possible obstructions before charging with explosives. Drilling into previously used boreholes or near unexploded ordnance is prohibited [36]. Borehole charging is carried out with cartridge or non-cartridge explosives, respecting the ratio of explosive mass to the volume of the separated rock mass in order to ensure controlled fragmentation and limit seismic effects. Explosives must not be forcibly rammed, and tools used when charging blast holes must be made of wood or plastic and must not produce sparks. Initiators (detonators) are connected in series or parallel, and the use of timing-synchronized systems enables precise control of firing sequences to reduce vibrations and optimize fragmentation [37]. Figure 1 shows a schematic layout of boreholes with indicated technical blasting parameters.

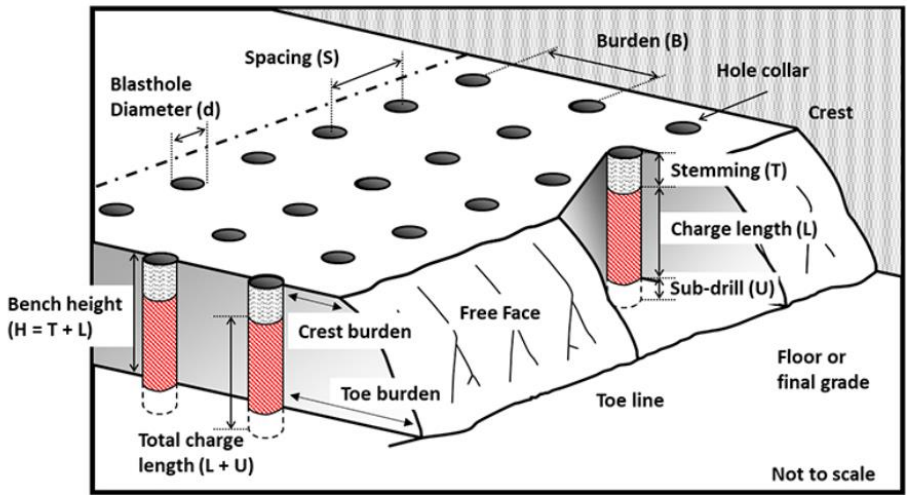


Figure 1. Schematic diagram of the borehole layout with indicated parameters: borehole diameter (d), spacing between boreholes (S), line of least resistance (B), charge length (L), stemming length (T), pre-drill/additional borehole depth (U), and bench height (H) [38].

2.3 Evacuation and detonation

The blasting zone must be physically fenced, clearly marked with warning signs, and kept under constant supervision by authorized personnel involved in the blasting process. The minimum evacuation distance is determined based on previous incidents of flyrock, applying a safety factor of 1.5 times the greatest recorded distance of a thrown fragment. This distance can be approximated by the expression:

$$D = 1{,}5 \cdot R_{max}$$

where R_{max} is the greatest recorded distance of rock-fragment ejection determined during experimental trial blasting. The given expression represents an empirical approximation used in the absence of precise measurements or numerical models, and serves as a practical criterion for defining the evacuation safety zone.

Prior to detonation, an audible signal must be emitted in three stages: warning, preparation, and detonation. Detonation may be carried out only on the order of the responsible person, after confirmation that the area has been completely evacuated, that all electrical and mechanical connections are functional, and that meteorological conditions allow safe execution of the blast. In the event of severe weather, high winds, or reduced visibility, the blasting procedure must be postponed until favorable conditions are reestablished [39].

2.4 Post-Blast Inspection of the Blasting Zone

After blasting operations, the work area must not be vacated until an audible signal clearly indicates the completion of the operation. This measure aims to prevent premature entry of personnel into a potentially hazardous area. Upon completion of blasting, a detailed visual inspection of the entire blast site must be carried out, including the blasted rock mass, accessible parts of the work area, and all surfaces exposed to explosive effects. The inspection is conducted to check for the presence of residual explosive materials, assess ground stability, and identify any potential deformations or displacements of the rock mass [40].

In case of suspected unexploded ordnance (UXO), access to the blasting zone is permitted only to professionally trained personnel equipped with appropriate protective gear and following prescribed safety procedures. Every intervention must be documented, and further activities may continue only after confirmation that the area is safe for work [41].

3. Risk Identification

Surface blasting involves a series of complex and potentially hazardous operations that generate various types of risks. Effective identification and classification of these risks form the basis for implementing appropriate occupational safety measures. Risks can be categorized into four main groups: mechanical, explosive, seismic/acoustic, and organizational.

3.1 Mechanical Risks

Mechanical risks in surface blasting arise from the interaction of workers with technical systems, dynamic work environments, and unstable rock material. In the context of drilling, charging, and face preparation, the most frequently identified mechanical hazards include contact with rotating parts of drilling equipment, falls from elevated benches, and impacts from dislodged rock blocks. These risks are inherent to the process, but their frequency and severity significantly increase under conditions of inadequate technical control, lack of spatial segregation, and absence of systematic protection.

According to OSHA regulations (29 CFR 1910.212), technical systems must be designed and maintained to prevent direct contact with moving parts, while the work area must be physically and procedurally isolated during active operations. Empirical studies indicate that the absence of barriers and inadequate signaling is the most common cause of mechanical injuries in mining and construction [12,42].

Personal protective equipment, although formally mandatory, cannot compensate for systemic shortcomings in work organization. Studies show that reflective clothing, protective helmets, and steel-toe footwear provide preventive benefits only when combined with technical access control and personnel training [43].

In this sense, mechanical risks cannot be addressed in isolation but require the integration of technical, organizational, and educational measures within a comprehensive safety management system.

3.2 Explosive Risks

Explosive risks represent the most critical category of hazards in surface blasting due to the immediate energy release, unpredictable effects of detonation, and potential for secondary incidents. In technical and safety literature, the most frequently identified explosive risks include premature detonation, the presence of unexploded ordnance (misfire), uncontrolled ejection of rock fragments (flyrock), and excessive explosive quantity relative to the designed parameters.

Uncontrolled scattering of rock fragments beyond the intended blasting zone is particularly dangerous due to its spatial unpredictability and kinetic energy. Empirical data indicate that fragments can reach distances exceeding 300 meters from the detonation epicenter, with recorded cases of severe injuries and fatalities [12,42].

In this context, the spatial distribution of risks must be precisely defined, applying safety factors and previous field measurements. The spatial distribution of risks due to uncontrolled flyrock during blasting is shown in Figure 2, which illustratively defines the blasting zone, the evacuation safety zone, and potential trajectories of ejected rock fragments.

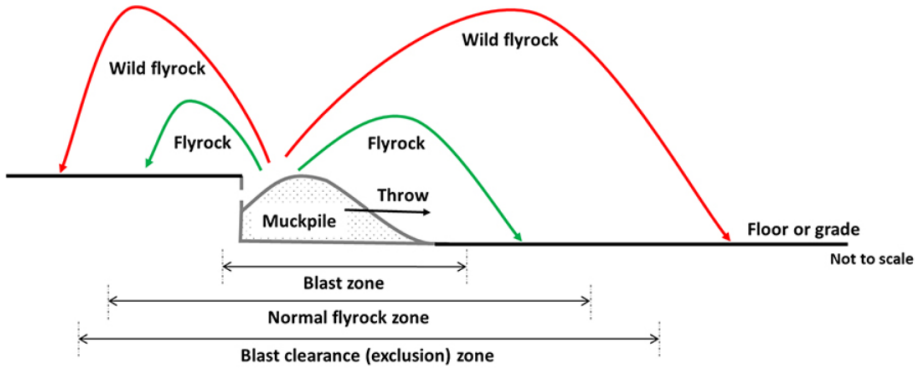


Figure 2. Zone of ejected rock fragments during blasting – spatial distribution of risk and safety boundaries [44].

To estimate the incident overpressure from an air blast, an empirical expression known as the Kingery–Bulmash model is used [45]:

$$P = \frac{K \cdot Q^{1/3}}{R}$$

where:

P – pressure, expressed in bar,
Q – amount of explosive, in kg,
R – distance from the epicenter, in m, and
K – empirical coefficient, dependent on the type of explosive and detonation geometry.

This formula is used in planning the blasting zone, especially near infrastructure, populated areas, or sensitive facilities. Unexploded ordnance (UXO) represents a latent risk requiring specialized intervention. According to MSHA guidelines, areas suspected of containing unexploded ordnance must be isolated, and access is permitted only to professionally trained personnel equipped with appropriate protective gear and technical support.

3.3 Seismic, Vibrational, and Acoustic Risks

Detonation of explosives in surface blasting generates seismic and air waves that propagate through the ground and atmosphere, interacting with surrounding structures, infrastructure, and human organisms. These waves can affect the

stability of buildings, the integrity of underground installations, and induce physiological and psychological reactions in workers and nearby populations [46–49]. Ground vibrations are transmitted to structures via foundations and basements, while the air blast impacts walls and roof surfaces. The resulting shaking can cause rattling of objects, displacement of equipment, and an internal noise sensation, which may trigger alarmed reactions in people, even though the noise itself has negligible impact on structural stability [47–49].

In the following text, Figure 3a illustrates the propagation mechanism of seismic and air waves generated by explosive detonation. The waves radiate outward from the epicenter, interacting differently with the ground or structures.

Figure 3b shows the energy balance of the explosion, highlighting that only a small portion of the released energy is used for rock fragmentation. The majority of the energy is transmitted through undesired effects, such as the dispersion of fragmented material and the generation of seismic and air waves [50].

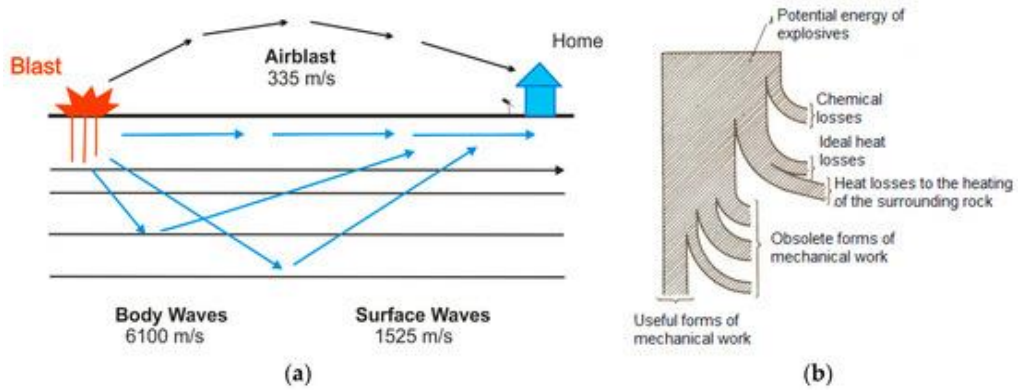


Figure 3. (a) Propagation of seismic and air waves during blasting; (b) Schematic representation of the energy balance during blasting [51].

According to technical guidelines, the permissible vibration level at the boundary of the blasting zone is a maximum of 5 mm/s for residential buildings and 10 mm/s for industrial structures [52]. Monitoring of actual values is performed through seismic monitoring using geophones, which enables the adjustment of blasting parameters under real conditions [53]. For the technical assessment of the seismic impact, a standardized empirical formula is used [54]:

$$PPV = K \cdot \left(\frac{D}{Q^{1/2}}\right)^{-n}$$

where:

PPV – peak particle velocity, in mm/s,

D – distance from the explosion epicenter, in m,

Q – amount of explosive per delay, in kg, and
K, n – coefficients dependent on local geological conditions and the type of explosive.

The values are determined through field measurements, most commonly using the least squares method, enabling local calibration of the model and precise blasting planning in sensitive zones [54].

In addition to seismic and vibrational effects, explosive detonation generates an airblast, which occurs due to the rapid expansion of gases from the explosion. This impulsive wave can cause damage to glass surfaces, disrupt electronic equipment, and negatively affect workers' hearing. The recommended airblast threshold is 120 dB for industrial zones, while a maximum of 115 dB is advised for residential areas [55]. Acoustic risks are mitigated through the use of sound barriers, proper timing of detonations, and mandatory hearing protection.

3.4 Organizational Risks

Organizational risks represent a key factor in the safety analysis of blasting, as they relate to systemic failures in planning, communication, and execution of operations. The most common sources of these risks include lack of training, unclear allocation of responsibilities, poor inter-team communication, and non-compliance with applicable legal regulations.

According to the Rulebook on Technical Standards for the Handling of Explosives and Blasting in Mining [25], the contractor is obliged to ensure the presence of an authorized person for handling explosives, to record the professional training of workers, and to provide physical protection of the blasting zone by means of signage and barriers. Although evacuation procedures are not explicitly prescribed, the technical documentation must include measures that ensure worker safety within the blasting area.

Domestic literature emphasizes that organizational shortcomings, especially in the preparation and coordination phase, are a frequent cause of deviations from the safety parameters of blasting. Lack of formalized procedures, inadequate communication among teams, and absence of clear operational instructions can lead to errors that, in explosive operations, manifest with serious consequences [56].

4. Conclusion

Blasting at surface quarries represents one of the most demanding and high-risk phases of technical operations in the mining and infrastructure sectors. Effective management of the risks arising from this process requires a systematic integration of legal regulations, technical standards, organizational measures, and geophysical methods. Each phase, from planning and drilling to detonation and post-blast inspection, must be precisely defined and controlled to ensure worker safety, stability of the work area, and environmental protection.

Analysis of the key risk categories indicates that explosive, seismic, and organizational factors have a dominant impact on operational safety. Explosive risks, such as uncontrolled flyrock and the presence of unexploded ordnance, require the application of empirical models, technical barriers, and specialized procedures. Seismic and acoustic impacts must be quantitatively monitored and controlled using geophones and standardized calculations, while organizational shortcomings, particularly in the preparation and coordination phases, represent latent sources of accidents that can be prevented through the establishment of clear procedures, formalization of protocols, and personnel training.

Compliance with the Rulebook on Technical Standards for the Handling of Explosives and Blasting in Mining, as well as with European directives and international standards, provides the foundation for legally and technically valid execution of blasting operations. The application of geophysical methods, such as seismic tomography and electromagnetic surveys, enables precise characterization of the rock mass, identification of unstable zones, and optimization of drill hole layouts, thereby directly contributing to risk reduction and operational efficiency.

In conclusion, safety in blasting is not only a technical challenge but also a professional and ethical obligation for all participants in the process. Only through consistent application of validated data, harmonized procedures, and a multidisciplinary approach is it possible to achieve controlled, efficient, and safe mining operations under complex engineering conditions.

1. Literatura

57. Bajpayee, T. S., Rehak, T. R., Mowrey, G. L., & Ingram, D. K. (2004). Blasting injuries in surface mining with emphasis on flyrock and blast area security. *Journal of Safety Research, 35*(1), 47–57. https://doi.org/10.1016/j.jsr.2003.07.003
58. Kecojevic, V., & Radomsky, M. (2005). Flyrock phenomena and area security in blasting-related accidents. *Safety Science*, 43(9), 739–750. https://doi.org/10.1016/j.ssci.2005.07.006
59. Valjevac, M., Bektašević, E., Gutić, K., Sakić, N., & Sikira, D. (2024). Exploitation and processing of technical stone from quarries Plješevac near Kiseljak. *Journal of Faculty of Mining, Geology and Civil Engineering, University of Tuzla*, 12, [Professional Paper]. https://doi.org/10.51558/2303-5161.2024.12.12.23
60. Mine Safety and Health Administration. (2002). *Module 11: Transportation, use, and storage of explosives*. U.S. Department of Labor. Retrieved from https://arlweb.msha.gov/safetypro_in_a_box/IG%2043%20OJT%20training%20modules%20surface%20MNM/Module%2011%20Transportation%20use%20and.%20storage%20of%20explosives.PDF
61. Festić, E., & Imamović, A. (2021). Značaj edukacije i opšti uslovi za bezbjedan transport opasnih materija prema ADR-u. *Zaštita i sigurnost*, 1(2), 95–106.
62. Bektašević, E., Gutić, K., Valjevac, M., & Sakić, N. (2025, April). The role and importance of preventive safety measures at work during the production and processing of technical stone at the quarry. In *15th Scientific/Research Symposium with International Participation „METALLIC AND NONMETALLIC MATERIALS“*, Bosnia and Herzegovina.
63. Bektašević, E., Gutić, K., Valjevac, M., & Konta, J. (2024, December). Unapređivanje mjera zaštite na radu u kamenolomima pri proizvodnji i preradi tehničkog kamena. *Rudarsko-geološki glasnik*, Hrvatsko rudarsko-geološko društvo Mostar, 49–61. ISSN 1840-0299.
64. Chen, X.-k., Zhu, H.-l., & Chen, J.-q. (2011). *Hazard identification and control in the pre-blasting process*. *Journal of Coal Science and Engineering (China), 17*(3), 331-335. https://doi.org/10.1007/s12404-011-0320-0
65. Imamović, A., Softić, S., Kablar, O., & Oruč, M. (2022). Značaj procedure istraživanja incidenta za sigurniji rad na rizičnim radnim mjestima. *Zaštita i sigurnost*, 2(1), 22–31.
66. Manitoba Labour and Immigration. (2006). *Code of practice for the use of explosives*. Workplace Safety and Health Division. Retrieved from https://www.gov.mb.ca/labour/safety/pdf/cop_useof_explosives.pdf
67. Strzałkowski, P., Woźniak, J., Górniak-Zimroz, J., & et al. (2025). Identification and systematics of safety hazards in surface rock mining. *Scientific Reports, 15*, 30492. https://doi.org/10.1038/s41598-025-16437-z

68. Bajpayee, T. S., Rehak, T. R., Mowrey, G. L., & Ingram, D. K. (2004). Blasting injuries in surface mining with emphasis on flyrock and blast area security. *Journal of Safety Research, 35*(1), 47–57. https://doi.org/10.1016/j.jsr.2003.07.003
69. Engineer Live. (2023). *Better blasting: Improving safety in mining operations*. Retrieved October 1, 2025, from https://www.engineerlive.com/content/better-blasting
70. Identec Solutions. (2023). *Blasting safety in daily mining operations*. Retrieved October 1, 2025, from https://www.identecsolutions.com/news/blasting-safety-in-daily-mining-operations
71. Mine Safety and Health Administration. (n.d.). *Blasting safety*. U.S. Department of Labor. Retrieved October 1, 2025, from https://www.msha.gov/safety-health/safety-health/safety-health-materials/safety-topics/blasting-safety
72. National Institute for Occupational Safety and Health. (2006). *Blast area security: Flyrock safety* (NIOSH Report No. 2007-112). U.S. Department of Health and Human Services. https://www.cdc.gov/niosh/docs/mining/UserFiles/works/pdfs/2007-112.pdf
73. Orica. (2010). *Safety of blasting with electronic detonators*. Orica Technical Bulletin. https://www.orica.com/ArticleDocuments/2606/200415_Safety%20of%20Electronic%20Detonators%20for%202010%20ISEE%20Lownds%2C%20Steiner.pdf.aspx
74. Vlada Federacije Bosne i Hercegovine. (2020). *Zakon o zaštiti na radu*. Službene novine Federacije BiH, broj 17/20. https://fbihvlada.gov.ba/bosanski/zakoni/2020/Zakoni/17.htm
75. Vijeće Europske unije. (1989). *Direktiva 89/391/EEZ o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja radnika na radu*. Službeni list Europske unije, L 183, 1–8. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A31989L0391
76. Reynolds, J. M. (2011). *An introduction to applied and environmental geophysics* (2nd ed.). Wiley-Blackwell.
77. Bektašević, E., Antičević, H., Gutić, K., & Sikira, D. (2024). Determination of the depth of the rock mass damage zone around the excavation profile by blasting with seismic cross-hole tomography in the „Šubir“ tunnel on the Zagreb-Split motorway. *Nauka+Praksa*, (27), 13–19. https://doi.org/10.62683/NiP27.13-19
78. Bektašević, E., & Gutić, K. (2025). Seismic impact assessment of blasting on surrounding population using geophysical methods. *Engineering and Technology Journal*, 10(4), 4468–4475. https://doi.org/10.47191/etj/v10i04.12

79. Bektašević, E., Antičević, H., Gutić, K., & Sikira, D. (2024). Application of seismic methods for determining the depth of the rock mass damage zone around the excavation profile by blasting. *Global Journal of Engineering and Technology Advances*, 18(3), 139–151. https://doi.org/10.30574/gjeta.2024.18.3.0051
80. Husejnagić, E., Bektašević, E., Osmanović, F., Žutić, Đ., Konta, J., & Hasić, E. (2016). Geofizičko-seizmička ispitivanja vještački izazvanih potresa i njihov uticaj na sigurnost i stabilnost objekata na PK Koritnik-Breza. In *Zbornik radova petog međunarodnog naučno-stručnog savetovanja*, Savez građevinskih inženjera Srbije, Sremski Karlovci (pp. 205–222).
81. Službeni list SFRJ. (1988). Pravilnik o tehničkim normativima pri rukovanju eksplozivnim sredstvima i miniranju u rudarstvu.
82. European Commission. (1992). *Council Directive 92/91/EEC on the minimum requirements for improving the safety and health protection of workers in the mineral-extracting industries through drilling*. https://eur-lex.europa.eu/eli/dir/1992/91/oj/eng
83. European Parliament and Council. (2013). *Directive 2013/29/EU on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles*. https://eur-lex.europa.eu/eli/dir/2013/29/oj/eng
84. European Parliament and Council. (2014). *Directive 2014/28/EU on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses*. https://eur-lex.europa.eu/eli/dir/2014/28/oj/eng
85. International Organization for Standardization. (2018). *ISO 45001:2018 – Occupational health and safety management systems – Requirements with guidance for use*. https://www.iso.org/standard/63787.html
86. European Committee for Standardization. (2003). *EN 13631-10:2003 – Explosives for civil uses – High explosives – Part 10: Verification of initiation methods*. https://standards.iteh.ai/catalog/standards/cen/9b294e02-391f-47cd-85fe-60101faf6341/en-13631-10-2003
87. Bektašević, E., Kadrić, R., Nikolić, M., Gutić, K., & Kadrić, S. (2023). Excavation of the foundation of piers S1L and S1R of the Vranduk I bridge by controlled blasting on the motorway route: Zenica Municipality Northern Administrative Boundary – Zenica North. *Electronic Collection of Papers, Faculty of Civil Engineering, University of Mostar*, 26, 9–26. https://doi.org/10.47960/2232-9080.2023.26.13.9
88. Bektaševič, E., Kadrić, R., Gutić, K., & Kadrić, S. (2023). Primjena kontrolisanog miniranja pri iskopu ulaznog portala desne tunelske cijevi tunela „Vranduk“ na koridoru Vc. *Zbornik radova GEO-EXPO 2023*, Društvo za geotehniku u Bosni i Hercegovini, 163–172. https://doi.org/10.35123/GEO-EXPO_2023_17

89. Bektaševič, E., Antičević, H., Osmanović, F., Kadrić, S., Žutić, Đ., & Konta, J. (2023). Tehnologija miniranja pri iskopu evakuacionog tunela „Vranduk II“ na magistralnoj cesti M-17. *Elektronički zbornik radova Građevinskog fakulteta Sveučilišta u Mostaru*, 49–60. https://doi.org/10.47960/2232-9080
90. Ilić, M. (2017). Application of results of geological exploration of deposits of solid mineral raw materials in mining. *Tehnika – Mining, Geological and Metallurgical Engineering*, *72*(2), 204–211. https://doi.org/10.5937/tehnika1702204I
91. Bektašević, E., Strelec, S., Sakić, N., & Gutić, K. (2025). Multichannel surface wave analysis in the context of shallow geophysical investigations. Academia Engineering, 2(3). https://doi.org/10.20935/AcadEng7876
92. Occupational Safety and Health Administration (OSHA). (2024). *1926.905 - Loading of explosives or blasting agents*. U.S. Department of Labor. Retrieved from https://www.osha.gov/laws-regs/regulations/standardnumber/1926/1926.905
93. Tang, H.-L., Liu, X., Yang, J., & Yu, Q. (2023). Experimental Study on the Influence of Delay Time on Rock Fragmentation in Bench Blasting. *Applied Sciences*, *13*(1), 85. https://doi.org/10.3390/app13010085
94. Szendrei, T. & Tose, S.. (2024). Flyrock in surface mining Part II - Causes, sources, and mechanisms of rock projection. Journal of the Southern African Institute of Mining and Metallurgy. 123. 557-564. 10.17159/2411-9717/2583/2023.
95. Božić, B. (1998). *Miniranje u rudarstvu, graditeljstvu i geotehnici*. Varaždin: Geotehnički fakultet Sveučilišta u Zagrebu.
96. Bektašević, E. (2022). *Blasting: Examples of surface blasting and tunnel construction with occupational safety measures*. LAP LAMBERT Academic Publishing.
97. QNJAC. (2020). *Post-blast inspection guidance for quarries*. Quarries National Joint Advisory Committee. https://minex.org.nz/training/toolbox/the-post-blast-inspection.pdf
98. Kecojevic, V., & Radomsky, M. (2005). *Flyrock phenomena and area security in blasting-related accidents*. Safety Science, 43(9), 739–750. https://doi.org/10.1016/j.ssci.2005.07.006
99. ISEE. (2022). *Personal Protective Equipment in Blasting Operations*. International Society of Explosives Engineers.
100. Little, T. N. (2007). *Flyrock risk*. In *Proceedings of EXPLO2007: Blasting—Techniques and Technology* (pp. 35–43). Australasian Institute of Mining and Metallurgy.
101. Kingery, C. N., & Bulmash, G. (1984). *Airblast parameters from TNT spherical air burst and hemispherical surface burst* (ARBRL-TR-02555). U.S. Army Ballistic Research Laboratory. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA955203.pdf

102. Bektašević, E., & Gutić, K. (2025). *Seismic impact assessment of blasting on surrounding population using geophysical methods*. *Engineering and Technology Journal*, *10*(4), 4468–4475. https://doi.org/10.47191/etj/v10i04.12
103. tagg, M. S., & Siskind, D. E. (1987). *Effects of blast vibration on construction material cracking in residential structures* (p. 43). Bureau of Mines Technology Transfer Seminar, Chicago, MI, USA.
104. Siskind, D. E., & Stagg, M. S. (1987). *Blast vibration measurements near structures* (pp. 46–50). Bureau of Mines Technology Transfer Seminar, Chicago, MI, USA.
105. Hustrulid, W. A. (1999). *Blasting principles for open pit mining* (Vol. 2). CRC Press.
106. Malbašić, V., & Stojanović, L. (2017). *Determination of seismic safety zones during the surface mining operation development in the case of open pit „Buvač“*. In *Proceedings of the 6th International Symposium MEP 17* (pp. 138–144), Vrdnik, Serbia, June 21–24.
107. Malbasic, V., & Stojanovic, L. (2018). Determination of Seismic Safety Zones during the Surface Mining Operation Development in the Case of the „Buvač“ Open Pit. *Minerals*, *8*(2), 71. https://doi.org/10.3390/min8020071
108. Husejnagić, E., Bektašević, E., Osmanović, F., Žutić, Đ., Konta, J., & Hasić, E. (2015). *Geofizičko-seizmička ispitivanja vještački izazvanih potresa i njihov uticaj na sigurnost i stabilnost objekata na PK Koritnik–Breza. Rudarsko-geološki glasnik*, Hrvatsko rudarsko geološko društvo, Mostar, 67–82. (ISSN 1840-0299).
109. Bektašević, E., Frljak, N., Sarajlić, M., Konta, J., & Lapandić, E. (2013). *Komparativni pregled uticaja prirodnih i vještački izazvanih potresa na primjeru „Rudnika krečnjaka Breza“–Breza*. *Rudarsko-geološki glasnik*, Hrvatsko rudarsko geološko društvo, Mostar, 70–77. (ISSN 1840-0299).
110. Boon, C. W., & Ooi, L. H. (2015). *Rock blasting — peak particle velocity against distance*. In Proceedings of the 11th International Symposium on Rock Fragmentation by Blasting (FRAGBLAST 11), Sydney, Australia. Australian Centre for Geomechanics. Dostupno na: https://papers.acg.uwa.edu.au/d/1508_23_Boon/23_Boon.pdf
111. Gregurović, N. (2013). *Kontrola seizmičkih efekata pri opreznim miniranjima u urbanim sredinama* [Diplomski rad, Geotehnički fakultet Sveučilišta u Zagrebu]. Repozitorij GFV. https://repozitorij.gfv.unizg.hr/islandora/object/gfv%3A75/datastream/PDF/view
112. Katalinić, M. (2021). *Netipične vrijednosti kod mjerenja seizmičkih utjecaja miniranja* [Diplomski rad, Rudarsko-geološko-naftni fakultet, Sveučilište u Zagrebu]. Repozitorij RGNF. https://zir.nsk.hr/islandora/object/rgn%3A1783/datastream/PDF/download

List of Figures

PROPAGANDA, MEDIJI I SPECIJALNI RAT: OD ISTORIJSKIH KORIJENA DO DIGITALNOG DOBA

DOI: *10.70329/2744-2403.2025.5.10.4*

Izvorni naučni članak

mr Nemanja Doder[13]

Sažetak:

Propaganda je dugo predstavljala moćno sredstvo u okviru specijalnog rata, koristeći se za uticanje, manipulaciju i kontrolu javnog mnjenja i ponašanja. Kao nekonvencionalni oblik sukoba, propaganda đeluje putem informacija, emocija i percepcije, a ne fizičke sile. Ovaj rad istražuje ulogu propagande unutar savremenih koncepata specijalnog rata, analizirajući njen istorijski razvoj, načine širenja i strateške ciljeve. Poseban akcenat stavlja se na način na koji se propaganda koristi za destabilizaciju društava, slabljenje protivnika i ostvarivanje političkih ili vojnih ciljeva bez otvorenog sukoba. Rad takođe razmatra njenu povezanost sa psihološkim operacijama i informacionim ratovanjem, naročito u eri digitalnih medija i hibridnih konflikata.

Ključne riječi: *propaganda, specijalni rat, psihološke operacije, dezinformacije, informacioni rat*

[13] diplomirani kriminalista i magistar sigurnosti. Ministarstvo unutrašnjih poslova Republike Srpske, Bosna i Hercegovina. E-mail: dodernemanja@gmail.com. Rođen 1994. godine.

1. Uvod

U ovom radu se tvrdi da je propaganda u funkciji psihološke destabilizacije društava, pri čemu objedinjuje tehnike političkog marketinga, obavještajnog rada i digitalne komunikacije kako bi se oblikovale percepcije, manipulisale emocije i podrivala javna svijest o institucijama i stvarnosti. Ovaj rad se tematski nadovezuje na istraživanje Alispahića (2020), ali umjesto deskriptivnog prikaza fenomena propagande, fokusira se na njene psihološke mehanizme i ulogu u destabilizaciji društva. Cilj je izgraditi originalan analitički pristup koji razmatra kako propaganda u savremenim uslovima postaje sredstvo kognitivne i emocionalne manipulacije.

Novi vijek je sa sobom donio niz novih pitanja, pokrenutih zapanjujućim tehnološkim razvojem koji je uticao na preoblikovanje odnosa između politike, propagande i javnog mnjenja. Velike društvene i tehnološke promjene duboko su transformisale način života, komunikacije i percepcije u posljednjih 150 godina. Rat, kao stalni pratilac razvoja ljudske civilizacije, imao je svoju evoluciju. Od najranijih vremena do danas, fizičko nasilje bilo je praćeno nastojanjem da se utiče na umove neprijatelja, čime propaganda dobija sve značajniju ulogu. Savremeni oblici ratovanja napuštaju klasične vojne metode i usmjeravaju se na informacione i psihološke operacije u kojima mediji i digitalne platforme igraju ključnu ulogu. Često se ističe da u modernim sukobima pobjeđuje onaj ko kontroliše medijski prostor. Specijalni rat predstavlja nekonvencionalni vid sukoba u kojem se koriste informacije kao oružje. Propaganda je u tom kontekstu jedno od osnovnih sredstava za oblikovanje javnog mnjenja, destabilizaciju društava i demoralizaciju protivnika. Prema tumačenju Alispahića (2020) verbalno djelovanje i komunikacija mogu imati dublji i dugotrajniji uticaj od fizičke sile, posebno u kontekstu kontrole svijesti i ponašanja.

Predmet ovog rada je analiza istorijskog razvoja i savremene uloge propagande u okviru specijalnog rata. Istraživački problem ogleda se u potrebi dubljeg razumijevanja mehanizama propagande u digitalnom dobu, kao i uloge obavještajnih službi u oblikovanju medijskog prostora. Cilj istraživanja je naučno sagledavanje uloge propagande kao sredstva savremenog ratovanja, sa posebnim osvrtom na informacione tehnologije i medije.

Društveni cilj je upoznavanje stručne i šire javnosti sa prijetnjama koje nose savremeni oblici manipulacije informacijama. Polazeći od hipoteze da je propaganda jedno od najefikasnijih sredstava specijalnog rata, u radu se ispituju pretpostavke o njenoj sposobnosti da mijenja javno mnjenje, slabosti njene etike i uloge u manipulaciji masama. Metode istraživanja obuhvataju komparativnu metodu, metodu definicije, istorijsku metodu i analizu sadržaja relevantne literature.

2. Terminološko određivanje propaganda

2.1 Definicija i karakteristike propagande

Propaganda se u savremenoj nauci sve češće posmatra kao kompleksna komunikacijska praksa čiji cilj nije samo informisanje, već prije svega oblikovanje percepcije i usmjeravanje ponašanja. Dok klasični komunikacijski modeli naglašavaju elemente kao što su pošiljalac, poruka, kanal i publika u slučaju propagande u prvi plan dolazi namjera — plansko i sistematsko djelovanje u svrhu proizvodnje određenog društvenog efekta.

Šiber (1998, str. 293) u svojoj knjizi Osnove političke psihologije ističe da se propaganda prvi put pojavila izvan crkvenih krugova u 20. vijeku, naglašavajući da ova pojava ima dugu istoriju različitih percepcija i funkcija. On definiše propagandu kao „plansko i namjerno djelovanje na promjenu i kontrolisanje stavova radi stvaranja predispozicija za određeno ponašanje“.

U leksičkom značenju, propaganda (lat. propaganda — širenje uticaja) podrazumijeva organizovanu i smišljenu djelatnost usmjerenu na uticanje na javno mnjenje, grupe i pojedince radi pridobijanja za određene ideje, shvatanja i ciljeve političkih ili društvenih organizacija. Cilj propagande je prije svega uticati na mišljenje i ponašanje ciljne publike. Mediji predstavljaju snažan instrument za širenje propagandnih sadržaja među šire mase.

Dewey, koga citira Skoko (2006, str. 98), definiše javno mnjenje kao sud koji formiraju oni koji sačinjavaju javnost, a koji se odnosi na javne poslove. On razlikuje četiri vrste javnosti: svestrane, apatične, jednoteme i javnosti „vrućih tema“. Metode propagande uključuju: širenje glasina, manipulisanje efektom većine, izazivanje sukoba, falsifikovanje dokumenata, ucjenjivanje, prijetnje i otvorene pozive na predaju.

U savremenim sukobima, propaganda predstavlja moćno sredstvo psihološkog uticaja usmjerenog na izazivanje podjela, demoralizaciju i smanjenje otpornosti zajednice. U dugoročnoj perspektivi, takvo djelovanje može imati snažniji efekat od fizičke sile. Tehnike propagande često se oslanjaju na emocije i vrijednosne asocijacije. Politički akteri povezuju se sa dominantnim normama društva, dok se suparnici demonizuju kroz etiketiranje i stereotipizaciju (Alispahić, 2020, str. 75).

3. Istorijski razvoj propagande

3.1 Antičko doba

Iako se institucionalizovana propaganda najčešće vezuje za period Novog doba, njene preteče prisutne su već u antičkom svijetu. U Rimskom carstvu i staroj Grčkoj, državna simbolika, kao što su novčići, statue i javni govori, služila je za oblikovanje percepcije o vladaru i državi. Kovani novac, na kojem su se nalazili likovi imperatora i poruke o snazi i vrlinama Rima, nije imao isključivo ekonomsku funkciju – bio je i sredstvo političkog uticaja. Širenje glasina i selektivna interpretacija događaja bili su ključni mehanizmi u konstruisanju stvarnosti, što se može smatrati ranim oblicima psihološkog ratovanja . Jedan od ilustrativnih primjera je okrivljavanje hrišćana za požar u Rimu tokom vladavine cara Nerona. Ovdje je riječ o svjesnoj manipulaciji informacijom sa ciljem skretanja javnog nezadovoljstva i kanalisanja straha prema manjinskoj zajednici – tehnika koja je i danas prisutna u političko-propagandnoj praksi.

3.2 Srednji vijek

U srednjem vijeku propaganda poprima oblik religijskog poziva na mobilizaciju. Krstaški ratovi, podsticani papskim bulama i besjedama, predstavljaju klasičan primjer gdje je komunikacija sa masama u službi ideološke i vojne mobilizacije. Sa izumom Gutenbergove štamparske mašine (1450), dolazi do prekretnice – kontrola nad informacijama više nije monopol elita, već se ubrzano širi mogućnost masovnog uticaja. Ova tehnološka inovacija stvara preduslove za modernu propagandu, jer omogućava umnožavanje poruka, njihovu brzu cirkulaciju i veći domet. Katolička crkva, reagujući na protestantsku reformu, 1622. godine osniva Congregatio de Propaganda Fide – što predstavlja prvo institucionalno priznanje i formalizovanje propagande kao sistematske aktivnosti u funkciji ideološke kontrole . U pitanju nije samo borba za teološku nadmoć, već za kontrolu nad tumačenjem stvarnosti – upravo ona dimenzija koja će biti centralna u kasnijim formama psihološke destabilizacije.

3.3 Propaganda novog doba

Ulaskom u novo doba, glavni fokus evropskih kraljevstva je bio sukob sa Osmanlijama u kojima su Osmanlije prikazivali kao okrutne barbare. Putem rapoloživih sredstava širila se propaganda. Prema Cullu i saradnicima, prva organizovana služba u savremenom obliku je nastala za vrijeme Napoleonovih ratova. Napoleon je istu nazvao služba za javno mnjenje, a glavna funkcija te službe je bila informisanje javnosti, objašenjenje politike i ratnih operacija. Same vijesti su bile prilagođene različitim skupinama te su prema tome posebne novine izlazile za osvojene zemlje, posebno za Francusku te posebno za vojsku. Tim činom, Napoleonova Francuska je vrlo lukavo slala iste informacije na različite

načine različitim publikama, prilagođene svakoj grupi. Francuska je za vrijeme Napoleonovih ratova koristila propagandu aktivno.

3.4 Politički marketing-put prema propagandi

Da bi se razumjela veza između političkog marketinga i propagande, neophodno je najprije razlikovati političku komunikaciju od političkog marketinga. Politička komunikacija tradicionalno je postojala kao osnovno sredstvo ostvarivanja i održavanja političke vlasti, obuhvatajući sve vidove prenošenja poruka biračkom tijelu putem političkih programa, platformi i zvaničnih dokumenata.

S druge strane, politički marketing predstavlja savremeni oblik političke prakse, koji koristi metode i principe poslovnog marketinga u cilju ostvarivanja političkih ciljeva. Političke stranke, interesne grupe i lokalne zajednice primjenjuju marketinška istraživanja kako bi bolje razumjele potrebe građana, oblikovale političke poruke i povećale podršku među biračima.

Politički marketing obuhvata niz analitičkih, kreativnih i planskih aktivnosti kojima politički subjekti nastoje da obezbijede što širu podršku javnosti za realizaciju svojih ciljeva i programa. U suštini, riječ je o primjeni savremenih marketinških metoda i menadžmenta u političkom kontekstu, uključujući upotrebu propagande, socijalizacije, političkog obrazovanja i javnih odnosa. Primjena političkog marketinga preko masovnih medija dodatno je unaprijedila političku komunikaciju, sa posebnim akcentom na izgradnju ličnog imidža kandidata, razvoj odnosa sa javnošću i fokusiranje na potrebe i interese građana.

4. Informacioni rat i propaganda

Informacije u savremenom dobu postaju ključno sredstvo političke i bezbjednosne borbe. Njihova vrijednost nije isključivo u sadržaju, već u načinu na koji oblikuju percepciju i utiču na proces donošenja odluka. Kada se selektivno obrađuju, kontekstualno mijenjaju ili namjerno iskrivljuju, one prestaju biti neutralno sredstvo komunikacije i postaju instrument psihološkog uticaja. Upravo taj prelazak iz informisanja u manipulaciju predstavlja osnovni mehanizam i propagande i informacionog rata.

Vinston Čerčil je ovu dinamiku sažeto opisao izjavom: „U ratnom vremenu, istina je toliko dragocjena da je treba čuvati prateći je tjelohraniteljem laži“ (Churchill, prema Knežević, 2023, str. 50). Ova metafora naglašava stratešku upotrebu dezinformacije kao zaštitnog sloja oko ključnih činjenica. U digitalnom okruženju, gdje se vrijeme reakcije mjeri sekundama, ovaj pristup postaje posebno efikasan — brzina širenja poruke često nadjača potrebu publike da provjeri njenu istinitost.

Pojam „propaganda“ označava kontinuirano širenje ideja i narativa — često selektivno oblikovanih ili namjerno iskrivljenih — sa ciljem da se stvori željena slika stvarnosti (Luchinskaya et al., 2018). „Informacioni rat“, prema Todoroviću (2022), predstavlja intenzivnu i vremenski ograničenu kampanju u kojoj se informacije koriste kao oružje tokom specifičnih političkih, vojno-političkih ili hibridnih konflikata. Razlika je, dakle, u ritmu i fokusu: propaganda je stalan proces oblikovanja percepcije, dok je informacioni rat koncentrisan i usmjeren na konkretan cilj u ograničenom vremenskom okviru. Mehanizmi informacionog rata obuhvataju manipulaciju istinitim podacima, njihovo selektivno predstavljanje i stvaranje lažnih konteksta (Barabash & Kotelenets, 2019). Cilj nije isključivo da se protivnik dezinformiše, već i da se demoriše njegovo stanovništvo, oslabi institucionalna kohezija i izazove unutrašnja nestabilnost. Ovo se postiže kroz istovremenu ofanzivu — oštećenjem protivnikovih informacionih sistema — i defanzivu — zaštitom sopstvenih komunikacionih kanala.

Savremene evropske bezbjednosne službe sve češće upozoravaju na činjenicu da informacioni rat više ne podrazumijeva samo državne aktere, već i ekstremističke grupe koje putem interneta i društvenih mreža šire radikalne narative i propagandne sadržaje. Polarizacija svijeta, porast antisemitizma i govor mržnje na internetu stvaraju plodno tlo za radikalizaciju i destabilizaciju društava, pri čemu propaganda postaje jedno od ključnih oružja psihološkog pritiska i regrutacije (Lakić, Kovačević & Kovačević, 2024). Istorijska praksa pokazuje da se psihološki uticaj na stanovništvo druge države često intenzivira u miru, kada pažnja javnosti nije usmjerena na klasične bezbjednosne prijetnje. U takvom okruženju, primarno oružje postaje narativ koji ponavlja princip: „naša strana je uvijek u pravu, neprijatelj uvijek griješi“. Ova pojednostavljena logika služi kao efikasan okidač za polarizaciju javnosti i smanjenje kapaciteta društva da kritički analizira primljene informacije.

5. Mediji i medijska propaganda

Razvoj medija predstavljao je ključni faktor u evoluciji propagande. Njena uloga postala je presudna u trenutku kada se većina stanovništva u evropskim društvima opismenila, čime su nastali uslovi za masovnu distribuciju informacija. Pojavom novina i časopisa krajem 19. vijeka, informacije su postale dostupne široj javnosti, dok su plakati, brošure, razglednice i filmske projekcije dodatno doprinijele formiranju ranih oblika masovne komunikacije. Štampana izdanja knjiga u početku su bila namijenjena užem, obrazovanom sloju društva, ali se poslije Prvog svjetskog rata njihova uloga proširila zahvaljujući povećanoj produkciji i dostupnosti (Šiber, 1998).

Pojavom radija dvadesetih godina 20. vijeka započinje novo doba propagande. Radio postaje moćno oruđe političke i ideološke mobilizacije, naročito u državama sa visokim stepenom nepismenosti. Istovremeno, kinematografija poprima sve značajniju propagandnu funkciju kroz filmove i dokumentarne zapise. Od sredine 20. vijeka, televizija preuzima dominantnu ulogu u oblikovanju javnog mnjenja i do danas ostaje jedno od najuticajnijih sredstava masovne komunikacije (Vertovšek & Adrić, 2015).

Krajem 20. i početkom 21. vijeka dolazi do digitalne revolucije — internet i društvene mreže (Facebook, Twitter, YouTube, Instagram) postaju centralna polja savremenog propagandnog djelovanja. Online platforme omogućavaju neposredan kontakt između pojedinaca, organizacija i državnih struktura, što daje novu dimenziju širenju propagandnih sadržaja. Za razliku od tradicionalnih medija, digitalni prostori nude decentralizovan i interaktivan model komunikacije, u kojem svako može postati izvor informacija, ali i manipulacije (Karabulatova et al., 2015).

Propaganda i informacioni rat najefikasniji su u autoritarnim društvima, gdje vlast kontroliše medije i oblikuje javni diskurs putem cenzure i centralizovanih narativa. U takvim režimima prelazak sa propagandnog na informacijski ratni režim odvija se brzo i bez većeg otpora javnosti. Nasuprot tome, u demokratskim državama, propaganda je suptilnija i često se sprovodi pod maskom informisanja, javne diplomatije ili nacionalne sigurnosti. Vlade nastoje da utiču na medije kroz zakonske regulative, ekonomske podsticaje i diskretne pritiske, čime se kreiraju narativi koji podržavaju državne interese (Todorović, 2022).

Savremeni medijski pejzaž karakteriše hiperprodukcija informacija, koja rezultira

smanjenjem njihove tačnosti i pouzdanosti. U takvom okruženju dolazi do zamora publike, gubitka povjerenja u izvore i smanjenja sposobnosti kritičkog prosuđivanja. Obrazovani korisnici nisu imuni na ove procese — privid noviteta i senzacionalizam često nadvladavaju racionalno promišljanje. Arhivi, muzeji, pa čak i naučne institucije, postaju dio šireg informacionog sistema u kojem se istina zamjenjuje emocijom, a činjenice narativom (Barabash & Kotelenets, 2019).

Rast lažnih vijesti, manipulisanih sadržaja i vizuelnih efekata stvorio je okruženje u kojem propagandni proizvodi funkcionišu kao komercijalna roba. Oni su obogaćeni vizuelnim i emocionalnim stimulansima koji prikrivaju odsustvo stvarnih činjenica, čime se oblikuje površna percepcija stvarnosti. U tom smislu, medijska propaganda u 21. vijeku ne teži samo informisanju ili ubjeđivanju, već i kontroli pažnje, emocija i identiteta savremenog čovjeka.

6. Društvene mreže i propaganda

Razvoj digitalnih tehnologija doveo je do stvaranja virtuelnog prostora koji obuhvata sve sfere ljudskog života. Ni država, ni politika, niti sukobi nisu ostali izvan tog procesa. Pojava lažnih vijesti, žute štampe, stotina hiljada portala i društvenih mreža doprinijela je nastanku specifičnog oblika ratovanja – propagande u okviru informacionog i specijalnog rata.

Društveni mediji kao što su Facebook, Twitter, Instagram i YouTube omogućili su direktnu komunikaciju između pojedinaca, grupa i šire publike, bez posredovanja tradicionalnih medija. Platforme poput Reddit-a dodatno su proširile mogućnosti informacione manipulacije, jer omogućavaju dijeljenje sadržaja kroz moderirane kanale, često podložne ideološkoj kontroli. Neki autori ističu da takve mreže, posebno kada su pod kontrolom interesnih grupa ili država, mogu funkcionisati kao propagandne mašine (Karabulatova et al., 2015).
Primjer sukoba u Gazi 2012. godine, u kojem su Izraelske odbrambene snage i Hamas koristili društvene mreže za mobilizaciju podrške i oblikovanje međunarodne percepcije, pokazuje kako je informacioni rat evoluirao. Umreženo društvo omogućava disintermedijaciju i decentralizaciju – propagandisti mogu direktno doprijeti do ciljne publike, bez kontrole tradicionalnih medija .

Pored direktnog dopiranja do publike, propagandni akteri danas koriste i saradnju sa takozvanim „influenserima“ – pojedincima sa velikim brojem pratilaca – kako bi njihove poruke dobile veći domet i kredibilitet u digitalnom prostoru.

U kontekstu savremenog specijalnog rata, Rusija je tokom vojne operacije na Ukrajinu primjenila višeslojni propagandni pristup, koji uključuje državne medije, društvene mreže i obavještajne operacije. Centralni narativi kao što su 'denacifikacija', 'zaštita ruskog naroda' i 'borba protiv NATO hegemonije' sinhronizovano su plasirani preko brojnih kanala. Uloga botova i trolova, kao i manipulacija snimcima, fotografijama i lažnim izjavama, doprinijela je konfuziji i dezinformaciji na globalnom nivou. Ovaj slučaj ilustruje kako propaganda funkcioniše ne samo kao sredstvo uticaja, već i kao alat destabilizacije i fragmentacije javnog diskursa.

7. Obavještajne službe i propaganda

Formiranje obavještajnih službi kao posebnih državnih organa predstavlja jedan od ključnih koraka u institucionalizaciji bezbjednosnih funkcija moderne države. Već u XV vijeku, francuski kralj Luj XI prepoznao je značaj organizovanog prikupljanja informacija u funkciji očuvanja državnog interesa i sopstvene političke moći. Korišćenjem mreže špijuna, ne samo da je prikupljao obavještenja od značaja, već je i razvijao strategije za zaštitu od stranih agenata, što se smatra začetkom savremene obavještajne prakse. Prikupljanje podataka je tradicionalno bila najosnovnija funkcija obavještajne službe, te je predstavljalo njenu osnovnu djelatnost (Abazović, 2012, prema Kovačević i Šeta Čavčić, 2024).

Savremena teorijska razmatranja pozicioniraju obavještajnu službu kao institucionalizovani, stalni, specijalizovani organ države sa obavještajnom funkcijom . Razvojem tehnologije, globalizacijom i intenziviranjem političkih i ekonomskih odnosa između država, obavještajna đelatnost postaje sve kompleksnija, integrisana u gotovo sve aspekte savremenog društva — od bezbjednosti i diplomatije, do ekonomije i informisanja. Značajan pomak u razvoju obavještajnih službi ogleda se u činjenici da se one danas, osim prikupljanja informacija, bave i tzv. neobavještajnim djelatnostima — propagandom, dezinformacijama, psihološkim operacijama, diverzijama, sabotažama i kreiranjem raznih organizacija koje služe prikrivenim ciljevima službe

.

Propaganda, kao jedno od sredstava obavještajnog djelovanja, ima dugu istorijsku genezu. Još od svojih početaka korišćena je kao sredstvo za ostvarenje političkih, ideoloških i vojnih ciljeva pojedinaca i elita. Kroz istoriju, posebno u vremenima kriza i ratova, propaganda je korišćena za manipulaciju masama, prikrivanje istine i kreiranje lažne slike o unutrašnjim i spoljnim neprijateljima.

U praksi su dominirale tehnike širenja dezinformacija, iskorišćavanje slabosti javnog mnjenja i manipulacija emocijama stanovništva.

U totalitarnim sistemima, kao što je bio fašizam, propaganda je bila podignuta na sistemski nivo. Ona nije samo plasirala iskrivljene informacije, već je služila kao instrument za mobilizaciju masa, izazivanje nasilja i legitimizaciju rata. Alispahić navodi da je tokom Drugog svjetskog rata britanska obavještajna služba MI6 koristila propagandu kako bi destabilizovala nacističko rukovodstvo, šireći informacije o Hitlerovim navodnim fizičkim i mentalnim slabostima.

U savremenom dobu, posebno u 21. vijeku, obavještajne službe svjetskih sila (poput SAD, Rusije i Kine) u značajnoj mjeri koriste propagandu kao instrument meke moći. One ne samo da plasiraju pozitivne informacije o sopstvenoj politici, već aktivno šire negativne narative o konkurentima na globalnoj sceni. Glavni cilj takve propagande jeste formiranje tzv. kritične akcione mase koja može izazvati željene promjene, kao i oblikovanje stavova javnosti tako da bude naklonjena tim promjenama ili, u najmanju ruku, ostane pasivna i neutralna .

U današnje doba interneta i društvenih mreža, propaganda više ne dolazi isključivo iz centralizovanih državnih izvora. Obavještajne službe koriste brojne posredne kanale: lažne naloge na mrežama, prikrivene nevladine organizacije, „nezavisne“ medije i influensere koji plasiraju poruke ciljanim grupama. Ovakva difuzna, sofisticirana propaganda ne mora biti agresivna ili eksplicitna — njena snaga leži u prilagođavanju jeziku i interesovanjima publike, prikrivanju porijekla i stvaranju iluzije autentičnosti.

Kao rezultat, sve je teže razlikovati istinu od manipulacije. Stanovništvo se suočava sa hiperprodukcijom informacija, što dovodi do zamora i gubitka sposobnosti za kritičko rasuđivanje. Propaganda danas ne mora nužno ubijediti — dovoljno je da zbuni, demoriše i relativizuje istinu. Krajnji efekat je formiranje pasivnih i konfuznih građana koji nemaju jasan stav, ne znaju kome da vjeruju i postaju podložni političkim manipulacijama.

8. Zaključak

U eri digitalne komunikacije i hibridnih prijetnji, propaganda sve češće preuzima ulogu primarnog sredstva destabilizacije društava, ne kroz otvoreno ubjeđivanje, već kroz suptilnu eroziju percepcije, povjerenja i racionalnog promišljanja. Njena snaga ne leži u neposrednoj agresiji, već u stvaranju ambivalencije, zbunjenosti i pasivnosti.

U ovom radu pokazano je da se savremena propaganda sve više oslanja na psihološke mehanizme — naročito strah, identifikaciju i kognitivne predrasude — kako bi ciljano uticala na kolektivnu svijest. Umjesto da bude jednosmjeran proces prenošenja ideja, ona postaje dvosmjerni oblik manipulativne komunikacije, gdje se poruke oblikuju u skladu sa profilima ciljne publike i kulturološkim kontekstom.

Ključnu ulogu u tom procesu imaju digitalni mediji i društvene mreže, koji su omogućili dezintermedijaciju — odnosno ukidanje posrednika u komunikaciji — što je dalo prostor i državnim i nedržavnim akterima da izgrade sopstvene narative. Istovremeno, obavještajne službe koriste propagandu kao instrument meke moći i kao sredstvo za vođenje psiholoških operacija, što dodatno povećava rizike po društvenu koheziju i bezbjednost.

Da bi se razumjele duboke posljedice savremene propagande, potrebno je više od deskripcije tehnika i istorijskih primjera — potrebna je detaljna analiza njenih psiholoških i kulturoloških efekata. U tom smislu, ovaj rad predstavlja pokušaj da se rasvijetli ne samo „šta“ je propaganda, već i „kako“ i „zašto“ ona funkcioniše unutar specijalnog rata u 21. vijeku.

Buduća istraživanja bi trebalo usmjeriti ka empirijskoj analizi konkretnih studija slučaja, kao i razvoju odbrambenih strategija koje će omogućiti društvima da očuvaju kapacitet za kritičko rasuđivanje, povjerenje u institucije i otpornost na psihološke I informacione manipulacije.

LITERATURA

Abazović, M. (2021). Državna bezbjednost. Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.

Alispahić, V. (2020). Propaganda kao oblik specijalnog rata. Društvena i tehnička istraživanja, 2. Kiseljak: Visoka škola za „CEPS-Centar za poslovne studije.“ str. 71-90.

Baterl, M. (2017). Propaganda kao manipulativni oblik informisanja. Zadar: Odjel za turizam i komunikacijske znanosti.

Bernays, E. (1928). Propaganda. Horace Liveright.

Culliy, M. (2012). History of Propaganda. London: Routledge.

Jowett, G.S., O'Donnell, V. (2015). Propaganda and Persuasion. Thousand Oaks, CA: Sage.

Karabulatova, I., Polivara, Z., & Vasylieva, N. (2015). "Network Wars" as a New Type of Devitiaon Processes in the Modern Electronic and Information Society in the Context of Social and Economic Security. Information space and propaganda. Journal of Social Sciences, 10(3), 150–159.

Knežević, S. (2023). Informacioni ratovi i bezbjednosna kultura. Beograd: Institut za bezbednost.

Kotelenets, E., Barabash, V. (2019). Propaganda and Information Warfare in Contemporary World: Definition Problems, Instruments and Historical Context. Advances in Social Science, Education and Humanities Research, volume 374. pp. 368-371.

Lakić, Z., Kovačević, Z. & Kovačević, I. (2024). *Terorizam – bezbjednosna prijetnja Zapadnom Balkanu.* Zaštita i sigurnost, 4(2), www.zisjournal.com

Kovačević, Z. & Šeta Čavčić, A. (2024). *Savremeni izazovi obavještajnih službi i bezbjednosne prijetnje u globalnom kontekstu.* Zaštita i sigurnost, 4(1), www.zisjournal.com.

Luchinskaya, T., Deyneka, O., & Rudenko, I. (2018). Propaganda techniques in modern information warfare. Journal of Political Psychology, 6(2), 789–800.

Seo, H., & Ebrahim, H. (2016). Visual Propaganda on Facebook: A Comparative Analysis. Journal of Communication Inquiry, 40(1), 1–25.

Todorović, N. (2022). Informacioni rat kao instrument specijalnog rata. Bezbednost, Beograd, 64(2), 22–34.

Vertovšek, N., Adrić, M. (2015). Masmedijski trenuci istine-od političke komunikacije i političkog marketinga do ratne prpagande. Časopis filozofije medija „In medias res“,4(6), 970–993.

Vorontsova, L., Frolov, D. (2006). The history and present day of information confrontation. Moscow: Moscow State University, 73-82

Šiber, I. (1998). Osnove političke psihologije. Zagreb: Alinea.

PROPAGANDA, MEDIA AND SPECIAL WARFARE: FROM HISTORICAL ROOTS TO THE DIGITAL AGE

DOI: *10.70329/2744-2403.2025.5.10.4*

Original Scientific Article

mr Nemanja Doder

Abstract:
Propaganda has long represented a powerful tool within the framework of special warfare, being used to influence, manipulate, and control public opinion and behavior. As a non-conventional form of conflict, propaganda operates through information, emotions, and perception rather than physical force. This paper explores the role of propaganda within contemporary concepts of special warfare, analyzing its historical development, methods of dissemination, and strategic objectives. Special emphasis is placed on how propaganda is used to destabilize societies, weaken opponents, and achieve political or military goals without open conflict. The paper also examines its connection to psychological operations and information warfare, particularly in the era of digital media and hybrid conflicts.

Keywords: *propaganda, special warfare, psychological operations, disinformation, information warfare.*

1. Introduction

This paper argues that propaganda represents one of the key instruments of psychological destabilization in contemporary societies. It combines techniques of political marketing, intelligence operations, and digital communication with the aim of shaping perceptions, manipulating emotions, and undermining public trust in institutions and reality itself. The study builds upon the research of Alispahić (2020), yet, instead of a descriptive approach, it focuses on analyzing the psychological mechanisms of propaganda and its function in the destabilization of social structures. The objective is to construct an original analytical framework that explains how propaganda in the digital era becomes a tool of cognitive and emotional manipulation.

The modern era has brought profound social and technological changes that have reshaped the relationship between politics, information, and public opinion. War, as a constant element of human civilization, has evolved from physical confrontation to psychological and informational conflict. Contemporary warfare increasingly abandons traditional military methods and relies on informational and psychological operations in which media and digital platforms play a decisive role. As Alispahić (2020) points out, verbal action and communication can have a more profound and lasting impact than physical force, as they influence collective consciousness and behavior.

The subject of this research is the analysis of the historical development and contemporary role of propaganda within the framework of special warfare. The research problem lies in the need for a deeper understanding of propaganda mechanisms in the digital age and the role of intelligence agencies in shaping the media space. The aim of the study is to provide a scientific perspective on propaganda as an instrument of modern warfare, with particular emphasis on information and communication technologies and the media.

The social objective of this paper is to enhance the understanding of contemporary forms of information manipulation among both the expert and the general public. Based on the hypothesis that propaganda represents one of the most effective instruments of special warfare, this paper examines its ability to shape public opinion, influence social attitudes, and undermine social cohesion. The methodological framework includes the comparative method, the method of definition, the historical method, and the content analysis of relevant literature.

2. Terminological definition of propaganda

2.1 Definition and Characteristics of Propaganda

In contemporary scholarship, propaganda is increasingly viewed as a complex communicative practice whose purpose is not merely to inform, but primarily to shape perception and direct behavior. While classical communication models emphasize elements such as the sender, message, channel, and audience, in the case of propaganda the key element becomes *intent* — a deliberate and systematic effort aimed at producing a specific social effect. Šiber (1998, p. 293), in his book *Osnove političke psihologije* (*Fundamentals of Political Psychology*), notes that propaganda first appeared outside religious contexts in the 20th century, emphasizing that this phenomenon has a long history of diverse perceptions and functions. He defines propaganda as "a planned and intentional activity aimed at changing and controlling attitudes in order to create predispositions for a particular behavior."

In its lexical meaning, the term *propaganda* (from Latin *propaganda* — "to be propagated") denotes an organized and deliberate activity directed at influencing public opinion, groups, and individuals in order to gain support for certain ideas, beliefs, and objectives of political or social organizations. The main goal of propaganda is to shape the attitudes and behavior of its target audience. The media serve as a powerful tool for disseminating propaganda content to the wider public.

Dewey, as cited in Skoko (2006, p. 98), defines public opinion as a judgment formed by those who constitute the public and which refers to matters of public concern. He distinguishes four types of publics: comprehensive, apathetic, single-issue, and "hot-topic" publics. Methods of propaganda include spreading rumors, manipulating majority effects, inciting conflict, falsifying documents, blackmail, threats, and open calls for surrender.

In modern conflicts, propaganda represents a powerful tool of psychological influence, aimed at provoking divisions, demoralizing the opponent, and reducing social resilience. In the long term, such activity can have a stronger impact than physical force. Propaganda techniques often rely on emotions and value associations. Political actors align themselves with dominant social norms, while opponents are demonized through labeling and stereotyping (Alispahić, 2020, p. 75).

3. Historical development of propaganda

3.1 Ancient Period

Although institutionalized propaganda is most often associated with the Modern Era, its precursors can be traced back to the ancient world. In the Roman Empire and ancient Greece, state symbols such as coins, statues, and public speeches served to shape public perception of rulers and the state. Minted coins bearing the image of the emperor and inscriptions highlighting the power and virtues of Rome did not serve merely an economic purpose — they were also a tool of political influence. The spread of rumors and selective interpretation of events were key mechanisms in constructing reality, which can be regarded as early forms of psychological warfare. One illustrative example is the blaming of Christians for the Great Fire of Rome during Emperor Nero's reign. This represents a deliberate manipulation of information aimed at diverting public discontent and channeling fear toward a minority community — a technique still present in contemporary political and propaganda practices.

3.2 Middle Ages

In the Middle Ages, propaganda took the form of religious mobilization. The Crusades, fueled by papal bulls and sermons, represent a classic example of communication with the masses in the service of ideological and military mobilization. The invention of Gutenberg's printing press (1450) marked a turning point — control over information was no longer the monopoly of elites, and the potential for mass influence expanded rapidly. This technological innovation laid the foundation for modern propaganda, enabling the multiplication of messages, their swift circulation, and broader reach. In response to the Protestant Reformation, the Catholic Church founded the *Congregatio de Propaganda Fide* in 1622, representing the first institutional recognition and formalization of propaganda as a systematic activity for ideological control. This was not merely a struggle for theological supremacy, but also for control over the interpretation of reality — a dimension that would become central in later forms of psychological destabilization.

3.3 Propaganda in the Modern Era

With the advent of the Modern Era, European kingdoms increasingly focused their propaganda on conflicts with the Ottoman Empire, portraying the Ottomans as cruel barbarians. Propaganda was spread through all available means. According to Cull and colleagues, the first organized propaganda service in the modern sense emerged during the Napoleonic Wars. Napoleon called it

the *Public Opinion Service*, and its main function was to inform the public, explain policies, and report on military operations. News was tailored for different audiences — separate newspapers were published for occupied territories, for France, and for the army. In this way, Napoleonic France skillfully disseminated the same information in different ways, adapting it to each group. Thus, during the Napoleonic Wars, France actively and strategically employed propaganda.

3.4 Political Marketing — The Path Toward Propaganda

To understand the connection between political marketing and propaganda, it is first necessary to distinguish political communication from political marketing. Political communication has traditionally existed as a fundamental means of exercising and maintaining political power, encompassing all forms of message transmission to the electorate through political programs, platforms, and official documents.

In contrast, political marketing represents a modern form of political practice that applies the methods and principles of commercial marketing to achieve political goals. Political parties, interest groups, and local communities use marketing research to better understand citizens' needs, shape political messages, and increase electoral support.

Political marketing encompasses a range of analytical, creative, and strategic activities through which political actors seek to secure broad public support for the realization of their objectives and programs. Essentially, it involves applying modern marketing methods and management techniques in a political context — including the use of propaganda, socialization, political education, and public relations. The application of political marketing through mass media has further advanced political communication, with particular emphasis on building the personal image of candidates, developing public relations, and focusing on the needs and interests of citizens.

4. Media and media propaganda

The development of media has represented a key factor in the evolution of propaganda. Its role became crucial at the moment when the majority of the population in European societies became literate, creating the conditions for mass information distribution. With the emergence of newspapers and magazines at the end of the 19th century, information became accessible to the wider public, while posters, brochures, postcards, and early film projections further contributed to the formation of the first forms of mass communication. Printed books were initially intended for the educated elite, but after the First World War, their role expanded due to increased production and accessibility (Šiber, 1998).

The advent of radio in the 1920s marked a new era of propaganda. Radio became

a powerful tool for political and ideological mobilization, especially in countries with high levels of illiteracy. Simultaneously, cinematography assumed an increasingly important propagandistic function through films and documentary recordings. From the mid-20th century onward, television took on a dominant role in shaping public opinion and remains one of the most influential means of mass communication to this day (Vertovšek & Adrić, 2015). At the end of the 20th and the beginning of the 21st century, a digital revolution occurred — the internet and social networks (Facebook, Twitter, YouTube, Instagram) became the central arenas of contemporary propaganda activities. Online platforms enable direct contact between individuals, organizations, and state structures, providing a new dimension to the dissemination of propaganda content. Unlike traditional media, digital spaces offer a decentralized and interactive model of communication in which anyone can become both a source of information and a potential agent of manipulation (Karabulatova et al., 2015).

Propaganda and information warfare are most effective in authoritarian societies where governments control the media and shape public discourse through censorship and centralized narratives. In such regimes, the transition from a propaganda system to an information warfare regime occurs rapidly and with little public resistance. Conversely, in democratic societies, propaganda tends to be more subtle, often disguised under the pretext of information dissemination, public diplomacy, or national security. Governments seek to influence the media through legislative regulation, economic incentives, and discreet pressure, thereby creating narratives that support state interests (Todorović, 2022).

The contemporary media landscape is characterized by the hyperproduction of information, resulting in a decline in accuracy and reliability. In such an environment, audiences experience fatigue, loss of trust in sources, and a reduced capacity for critical judgment. Even educated users are not immune to these processes — the illusion of novelty and sensationalism often prevail over rational reflection. Archives, museums, and even scientific institutions have become part of a broader information system in which truth is frequently replaced by emotion, and facts by narrative (Barabash & Kotelenets, 2019). The rise of fake news, manipulated content, and visual effects has created an environment in which propaganda products function as commercial commodities. Enriched with visual and emotional stimuli that conceal the absence of factual substance, they shape a superficial perception of reality. In this sense, media propaganda in the 21st century no longer seeks merely to inform or persuade but to control attention, emotion, and identity in the digital age.

5. Information war and propaganda

Information in the contemporary era has become a key instrument of political and security struggle. Its value lies not only in its content but also in the way it shapes perception and influences decision-making processes. When information is selectively processed, contextually altered, or deliberately distorted, it ceases to be a neutral means of communication and becomes a tool of psychological influence. This transition—from informing to manipulating—constitutes the fundamental mechanism of both propaganda and information warfare.

Winston Churchill succinctly captured this dynamic in his statement: "In wartime, truth is so precious that she should always be attended by a bodyguard of lies" (Churchill, as cited in Knežević, 2023, p. 50). This metaphor highlights the strategic use of disinformation as a protective layer around key facts. In the digital environment, where reaction time is measured in seconds, such an approach becomes particularly effective— the speed at which a message spreads often outweighs the audience's need to verify its accuracy.

The term *propaganda* refers to the continuous dissemination of ideas and narratives—often selectively shaped or intentionally distorted—with the aim of creating a desired image of reality (Luchinskaya et al., 2018). *Information warfare*, according to Todorović (2022), represents an intensive and time-limited campaign in which information is used as a weapon during specific political, politico-military, or hybrid conflicts. The difference lies in rhythm and focus: propaganda is a constant process of shaping perception, while information warfare is concentrated and directed toward a specific objective within a limited time frame. The mechanisms of information warfare include manipulating truthful data, presenting it selectively, and creating false contexts (Barabash & Kotelenets, 2019). The goal is not merely to misinform the opponent, but also to demoralize its population, weaken institutional cohesion, and provoke internal instability. This is achieved through a simultaneous offensive— by damaging the opponent's information systems— and defensive— by protecting one's own communication channels.

Modern European security services increasingly warn that information warfare no longer involves only state actors but also extremist groups that disseminate radical narratives and propaganda through the internet and social media. Global polarization, the rise of antisemitism, and online hate speech create fertile ground for radicalization and societal destabilization, with propaganda becoming one of the key instruments of psychological pressure and recruitment (Lakić, Kovačević & Kovačević, 2024). Historical experience shows that psychological influence on the population of another state often intensifies during peacetime, when public attention is not focused on traditional security threats. In such an environment, the primary weapon becomes a narrative that reinforces the principle: "our side is always right, the enemy is always wrong." This simplified logic serves as an

effective trigger for public polarization and reduces a society's capacity for critical analysis of the information it receives.

6. Social networks and propaganda

The development of digital technologies has led to the creation of a virtual space encompassing all spheres of human life. Neither the state, nor politics, nor conflicts have remained outside this process. The emergence of fake news, yellow journalism, hundreds of thousands of online portals, and social networks has contributed to the rise of a specific form of warfare — propaganda within the framework of information and special warfare.

Social media platforms such as Facebook, Twitter, Instagram, and YouTube have enabled direct communication between individuals, groups, and the broader public without the mediation of traditional media. Platforms like Reddit have further expanded the potential for informational manipulation, as they allow content sharing through moderated channels that are often subject to ideological control. Some authors point out that such networks, especially when controlled by interest groups or states, can operate as propaganda machines (Karabulatova et al., 2015).

An example of this evolution can be seen in the 2012 Gaza conflict, during which both the Israeli Defense Forces and Hamas used social media to mobilize support and shape international perception. The networked society enables disintermediation and decentralization — propagandists can reach target audiences directly, without the oversight of traditional media.

In addition to direct outreach to audiences, propaganda actors today also collaborate with so-called "influencers" — individuals with large followings — to amplify their messages and enhance their credibility in the digital environment.

In the context of modern special warfare, Russia, during its military operation in Ukraine, employed a multilayered propaganda strategy that included state-controlled media, social networks, and intelligence operations. Central narratives such as "denazification," "protection of the Russian people," and "the struggle against NATO hegemony" were synchronously disseminated through numerous channels. The role of bots and trolls, along with the manipulation of videos,

photographs, and fabricated statements, contributed to widespread confusion and disinformation on a global scale. This case illustrates how propaganda functions not only as a tool of influence but also as an instrument of destabilization and fragmentation of public discourse.

7. Intelligence services and propaganda

The formation of intelligence services as distinct state institutions represents one of the key steps in the institutionalization of the security functions of the modern state. As early as the 15th century, French King Louis XI recognized the importance of organized information gathering for preserving state interests and maintaining political power. By employing a network of spies, he not only collected intelligence of strategic importance but also developed measures for protection against foreign agents — a practice considered the origin of modern intelligence activity. The collection of information has traditionally been the most fundamental function of an intelligence service and represented its primary field of activity (Abazović, 2012, as cited in Kovačević & Šeta Čavčić, 2024).

Modern theoretical perspectives define the intelligence service as an institutionalized, permanent, and specialized organ of the state tasked with intelligence functions. With the development of technology, globalization, and the intensification of political and economic relations among states, intelligence activity has become increasingly complex, integrated into almost all aspects of modern society — from security and diplomacy to economics and information management. A significant development in the evolution of intelligence services lies in the fact that today, in addition to collecting information, they engage in so-called non-intelligence activities — propaganda, disinformation, psychological operations, sabotage, diversion, and the creation of various organizations serving covert state objectives. Propaganda, as one of the instruments of intelligence operations, has a long historical genesis.

From its earliest use, it served as a tool for achieving political, ideological, and military objectives of individuals and elites. Throughout history — particularly in times of crisis and war — propaganda was used to manipulate the masses, conceal the truth, and construct a false image of internal and external enemies. In practice, it relied on techniques such as spreading disinformation, exploiting weaknesses in public opinion, and manipulating citizens' emotions.

In totalitarian systems, such as fascism, propaganda was elevated to a systematic and institutionalized level. It did not merely disseminate distorted information but also served as a mechanism for mass mobilization, incitement to violence, and the legitimization of war. Alispahić (2020) notes that during World War II, the British intelligence agency MI6 used propaganda to destabilize the Nazi leadership by spreading information about Hitler's alleged physical and mental weaknes

In contemporary times, particularly in the 21st century, the intelligence services of global powers such as the United States, Russia, and China have increasingly utilized propaganda as an instrument of soft power. These services not only promote positive narratives about their own policies but also actively spread negative narratives about competitors on the global stage. The main objective of such propaganda is to shape what is known as a "critical mass for action," capable of inducing desired political or social changes, or at least fostering public attitudes that are either supportive or passive and neutral.

In the modern era of the internet and social media, propaganda no longer originates exclusively from centralized state sources. Intelligence services employ numerous indirect channels — fake online accounts, covert non-governmental organizations, "independent" media outlets, and influencers who deliver targeted messages to specific audiences. This diffuse and sophisticated form of propaganda need not be overtly aggressive or explicit — its strength lies in adapting to the language and interests of the audience, concealing its origin, and creating an illusion of authenticity.

Consequently, it has become increasingly difficult to distinguish truth from manipulation. Societies face an overproduction of information, leading to cognitive fatigue and a decline in critical reasoning capacity. Propaganda today does not necessarily need to persuade — it is often sufficient for it to confuse, demoralize, and relativize truth. The ultimate effect is the formation of passive and disoriented citizens who lack clear convictions, distrust institutions, and become increasingly susceptible to political manipulation.

8. Conclusion

In the era of digital communication and hybrid threats, propaganda increasingly assumes the role of a primary instrument for the destabilization of societies — not through overt persuasion, but through the subtle erosion of perception, trust, and rational reflection. Its power does not lie in direct aggression but in creating ambivalence, confusion, and passivity. This paper has shown that modern propaganda relies heavily on psychological mechanisms — particularly fear, identification, and cognitive biases — to influence collective consciousness. Rather than a one-way process of transmitting ideas, propaganda today functions as a two-way form of manipulative communication, in which messages are shaped according to the profiles of target audiences and their cultural contexts.

Digital media and social networks play a crucial role in this process, enabling disintermediation — the removal of traditional intermediaries in communication — thus providing both state and non-state actors the ability to construct their own narratives. At the same time, intelligence services employ propaganda as an instrument of soft power and as a means of conducting psychological operations, which further increases risks to social cohesion and security.

Understanding the profound consequences of modern propaganda requires more than a description of its techniques and historical examples — it demands an in-depth analysis of its psychological and cultural effects. In this sense, this paper represents an attempt to explore not only *what* propaganda is, but also *how* and *why* it operates within the framework of special warfare in the 21st century.

Future research should focus on empirical analyses of specific case studies, as well as on the development of defensive strategies that will enable societies to preserve their capacity for critical thinking, trust in institutions, and resilience against psychological and informational manipulation.

REFERENCES

Abazović, M. (2021). *Državna bezbjednost.* Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.

Alispahić, V. (2020). *Propaganda kao oblik specijalnog rata.* Društvena i tehnička istraživanja, 2, 71–90. Kiseljak: Visoka škola „CEPS – Centar za poslovne studije.“ Baterl, M. (2017). *Propaganda kao manipulativni oblik informisanja.* Zadar: Odjel za turizam i komunikacijske znanosti.

Bernays, E. (1928). *Propaganda.* New York: Horace Liveright.

Culliy, M. (2012). *History of Propaganda.* London: Routledge.

Jowett, G. S., & O'Donnell, V. (2015). *Propaganda and Persuasion.* Thousand Oaks, CA: Sage.

Karabulatova, I., Polivara, Z., & Vasylieva, N. (2015). "Network Wars" as a New Type of Deviation Processes in the Modern Electronic and Information Society in the Context of Social and Economic Security. *Journal of Social Sciences,* 10(3), 150–159.

Knežević, S. (2023). *Informacioni ratovi i bezbjednosna kultura.* Beograd: Institut za bezbednost.

Kotelenets, E., & Barabash, V. (2019). Propaganda and Information Warfare in the Contemporary World: Definition Problems, Instruments, and Historical Context. *Advances in Social Science, Education and Humanities Research,* 374, 368–371.

Lakić, Z., Kovačević, Z., & Kovačević, I. (2024). *Terrorism – A Security Threat to the Western Balkans. Zaštita i sigurnost,* 4(2). Retrieved from www.zisjournal.com

Kovačević, Z., & Šeta Čavčić, A. (2024). *Contemporary Challenges of Intelligence Services and Security Threats in the Global Context. Zaštita i sigurnost,* 4(1). Retrieved from www.zisjournal.com

Luchinskaya, T., Deyneka, O., & Rudenko, I. (2018). Propaganda Techniques in Modern Information Warfare. *Journal of Political Psychology,* 6(2), 789–800.

Seo, H., & Ebrahim, H. (2016). Visual Propaganda on Facebook: A Comparative Analysis. *Journal of Communication Inquiry,* 40(1), 1–25.

Todorović, N. (2022). *Informacioni rat kao instrument specijalnog rata. Bezbednost,* 64(2), 22–34.

Vertovšek, N., & Adrić, M. (2015). Mass-Media Moments of Truth – From Political Communication and Marketing to War Propaganda. *In Medias Res,* 4(6), 970–993.

Vorontsova, L., & Frolov, D. (2006). *The History and Present Day of Information Confrontation.* Moscow: Moscow State University, 73–82.

Šiber, I. (1998). *Osnove političke psihologije.* Zagreb: Alinea.

POJAM HIBRIDNOG RATA

DOI: *10.70329/2744-2403.2025.5.10.5*

Pregledni naučni članak

Dragutin Šimić

Sažetak

U članku je izvršeno kritičko promišljanje definiranja hibridnog rata. Analiza sadržaja postojeće literature upućuje da se ova problematika razmatra na tri načina. Prvom, da je to evoluirani pojam specijalnog rata, drugom, da je ova sintagma podudarna, slična sa konceptima sukoba niskog intenziteta, rata četvrte generacije, složenog rata, asimetričnog rata, uključujući i specijalnog rata i trećem, da je to novi koncept rata. U članku se pokušava dokazati da je najprihvatliviji prvi pristup. Pored toga, ukazano je i na značaj konceptualno-doktrinarnog određenja hibridnog rata. Između ostalog, razmatra se i praksa na primjeru primjene metoda hibridnog rata Rusije u pripremi i izvođenju agresije na Ukrajinu.

Ključne riječi*: hibridni rat, hibridne prijetnje*

1. Uvod

Za razumijevanje pojma *hibridnog rata* polazište predstavlja etimološko[14] određenje riječi hibridno. „Izraz hibrid potječe iz grčkog i znači otprilike 'djeca oholosti, bahatosti'. .. U svim modernim jezicima naziv je izgubio negativan prizvuk i danas označava samo mješavinu ili kombinaciju. Korištenjem izraza **hibrid** uz oznaku vrste ili procesa samo se naglašava da je tako dobivena cjelina rezultat spajanja dvije različite vrste ili procesa.[15] Pored toga, prihvaćen je i stav da da „Riječ, kao takva, dolazi od latinskog *hybrĭda*.“[16] „Od latinskog *ibrida* pod utjecajem starogrčkog ὕβρις (*húbris*, 'bijes').[17] Ta latinska riječ je imala značenje – „mješanca, osobe rođene od oca Rimljana i strane majke ili od slobodnjaka i roba.“[18]

Etimološko određenje riječi hibrid upućuje na višeznačnost te riječi. Ona se koristi u znanosti, tehnici, sportu, politici … Kolokvijalno rečeno označava proizvod, proces koji je sastavljen od elemenata različitog podrijetla, u figurativnom smislu „ono što je sastavljeno od elemenata različitog porekla.“[19] Primjerice, „u botanici i zoologiji *hibridom* se označava sjeme ili živo biće nastalo križanjem roditelja različitih uzgojnih linija, pasmina ili vrsta. U molekularnoj biologiji za spajanje jedne uzdužne polovine vrpce DNK ili RNK s drugom komplementarnom polovinom vrpce.“[20] „ U tehnici se općenito pod *hibridom* podrazumijeva sistem kod kojeg se kombiniraju dvije tehnologije.“[21] U najopćijem, kolokvijalnom smislu, pod hibridom se podrazumijeva sve ono što je sastavljeno od elemenata različitog podrijetla.

U teoriji rata pod pojmom hibridni rat smatra se kombinirana uporaba konvencionalnih metoda rata i tzv. nevojnih sredstava. „Hibridni rat vojna je strategija koja sadrži elemente konvencionalnog ratovanja, nekonvencionalnog

[14] „Etimologija je grana lingvistike koja proučava podrijetlo riječi.“- https://hr.wikipedia.org/wiki/Hibrid ;
„Lingvistička znanost koja proučava postanje, razvoj oblika i značenja riječi prema korijenu riječi“ - https://hjp.znanje.hr/

[15] https://hr.wiktionary.org/wiki/hibrid
[16] https://hr.encyclopedia-titanica.com/significado-de-h-brido

[17] https://en.wiktionary.org/wiki/hybrida#Latin

[18] Isti izvor
[19] https://www.opsteobrazovanje.in.rs/sta-znaci/hibrid/
[20] https://hr.wiktionary.org/wiki/hibrid
[21] Isti izvor

ratovanja i kibernetskog ratovanja.“[22] To je relativno novi pojam koji u vojnoj teoriji i praksi egzistira tek od početka XXI stoljeća. U svezi njegovog definiranja stavovi vojnih stručnjaka su podijeljena na tri pristupa. Prema prvom, da je to samo evoluirani pojam specijalnog rata i prema drugom, da je blizak, sličan sa određenjema rata kao sukoba niskog intenziteta, rata četvrte generacije, složenog rata, asimetričnog rata, uključujući i specijalnog rata i trećem da je to novi koncept rata. Problemsko područje članka je ovo pitanje. Stajalište autora je ispravnost prvog spomenutog pristupa. Sukladno tome teorijsko-hipotetski okvir članka predstavljaju postulati koji dokazuju da je hibridni rat evaluirani koncept specijalnog rata. Zasniva se na analizi sadržaja relevantnih stavova vodećih svjetskih autora, kao i u zemljama regije.

Obzirom da je u regiji najdominantniji teorijski opus o ovoj tematici znanstvenika iz Srbije, kao i da se također, i u Hrvatskoj temeljito proučava. Zbog toga je najviše razmatran opus srpskih i hrvatskih autora. Pored njih, spominju se i autori iz BiH. Predmetni okvir članka su elementi koji potvrđuju spomenutu hipotezu da je hibridni rat usavršeni, modernizirani koncept specijalnog rata. Pored toga, obuhvaća i konceptualno-doktrinarno određenje hibridnog rata, kao i primjer prakse provedbe hibridnog rata. Zbog toga je članak podijeljen na tri poglavlja: 1. Pojmovno određenje hibridnog rata, 2. Konceptualno-doktrinarno određenje hibridnog rata i 3. Hibridno rusko djelovanje u pripremi i izvođenju nastavka agresije na Ukrajinu.

Teorijski cilj rada je davanje elemenata za studioznije sagledavanje fenomena hibridnog rata. Kao što je poznato, ne postoji još konsenzus o definiciji hibridnog ratovanja. Sistematizacija dosadašnjih definiranja fenomena hibridnog rata na spomenuta tri pristupa, kao i ukazivanje na njegovo konceptualno-doktrinarno određenje, može doprinijeti, stvoriti pretpostavke za preciznije definiranje ovog fenomena. Praktični cilj je također davanje elemenata za što adekvatnije donošenje konceptualno-doktrinarnih i normativnih akata u kojima se razmatra ova tematika. Isto tako, i da potakne praktičare – stručnjake da što potpunije sagledaju ovu iznimno kompleksnu problematiku.

2. Pojmovi određenja hibridnog rata

Termin rat je vremenom, od poimanja sa većim oružanim sukobom između država, počeo da se koristi i u izražavanju sukoba u drugim oblastima društvenog delovanja, uz korišćenje prideva za formiranje sintagmi – hladni rat, specijalni rat, totalni rat, višedimenzionalni, neograničeni, hibridni rat. Hibridni rat je termin čija uporaba je doživjela poseban intenzitet posljednjih nekoliko godina, a sam

[22] https://hr.unionpedia.org/i/Konvencionalni_rat

termin se pojavio početkom 21. stoljeća. Iako je zaključak većine autora da on ne označava ništa novo u odnosu na neke druge slične pojmove, do jedinstvene ili opće prihvaćene definicije, se nije došlo. U stručnoj javnosti postoje različita mišljenja o sadržaju hibridnog rata, koriste se različiti pojmovi i termini, no ipak, može se primjetiti suglasnost oko toga da je hibridni rat kombinacija neoružanih i oružanih oblika ugrožavanja. (Cvetković, Kovač i Joksimović, 2019: 323)

Hibridni rat je možda i najširi pojam do sada, jer se sa globalizacijom i evolucija rata proširila sa bojnog polja, na kojem je taktika i asimetrija ratnih lukavstava mijenjala tokove i ishode bitaka i ratova, rastući do međunarodnih granica zatim regionalnih i na kraju globalnih, šireći se od sukoba u koje su bili uključeni samo vojnici, do granica cijelog, čak i globalnog, međunarodnog društva, i svih njegovih institucija, potencijala i resursa. (Ahić i Alishapić, 2019:163)

Kao što je već naglašeno, u svezi odnosa ovog pojma sa ranijim sličnim postoje dva stajališta. Prvo, da je to samo suvremeni naziv za stare oblike ratovanja koji su odavno poznati pod pojmom *specijalnog rata*, a koji je podrazumijevao skup organiziranih i koordiniranih političkih, diplomatskih, ekonomskih, psihološko-propagandnih, obavještajnih, podrivačkih, terorističkih, a ponekad i prikrivenih vojnih akcija i postupaka." (Cvrtila, 2017:1,2) I drugo, da su se kao posebno slični termini i pojmovi današnjem hibridnom ratu, do 1990. godine su se spominjali *totalni, hladni, specijalni rat, sukob niskog intenziteta*, a od 1990. i *rat 4. generacije, neograničeno ratovanje, složeni, asimetrični, neregularni rat*. (Cvetković, Kovač i Joksimović, 2019: 331)

Valjano pojmovno određenje ove sintagme trebalo bi da izražava njene suštinske i konstantne odredbe, uz navođenje i specifičnih svojstava, čije markiranje omogućava da se pojam *hibridni rat* razlikuje od drugih, sličnih koncepata. U stvari, zbog postojanja nekoliko pojmova koji su po svom sadržaju bliski sintagmi *hibridni rat,* poput *sukoba niskog intentiteta, rata četvrte generacije, složenog rata, asimetričnog rata* i *specijalnog rata*, detektiranje i označavanje tih specifičnih svojstava predstavlja glavni izazov prilikom definiranja *hibridnog rata*. (Vuković, 2018:12)

Više autora je analiziralo sličnosti i razlike pojma hibridnog rata i navedenih drugih sličnih. Primjerice, Ahić i Alishapić razmatraju razlike pojma hibridnog rata u odnosu na specijalni rat, sukob niskog intenziteta, rat IV generacije. (Ahić i Alishapić, 2019:165, 167)

Od svih spomenutih sintagmi po podudarnosti sa *hibridnim ratom* najviše se izdvaja *specijalni rat*. Kad se usporedi sa definicijom hibridnog ratovanja, uočavaju, vide se mnoge podudarnosti. U vrijeme hladnog rata, tzv. s*pecijalni rat* povezivan je primarno sa SAD, zbog toga što su one imale razvijene snage koje

su mogle da preduzimaju široke aktivnosti u društvu države koja je bila izloženu pritisku ili agresiji. Sada, Rusija koristi potpuno identične postupke definirane prije više desetljeća u SAD kombinacijom, kako se to sada kaže, *meke* moći – propagande, podržane političkim potezima svih subverzivnih aktivnosti. (Milošević,2018:72)

Pojedini autori osporavaju navedenu podudarnost s obrazloženjem da su cyber operacije differentia specifica za pojam *hibridnog rata* to jest ono po čemu se ovi ratovi razlikuju od sličnih pojmova poput *specijalnog rata* koji je sadržajno vrlo blizak pojmu *hibridnog rata.* (Vuković, 2018:25) Ovakvo stajalište je s pravom osporavano. Teorija da hibridni rat predstavlja nešto novo je više nego nepovijesna. Da se u određenjima hibridnog rata ne spominju cyber napadi, ovaj narativ bi se mogao primijeniti na praktično svaki rat ikad vođen. (Subotić:2018:31)

U dosadašnjoj terminologiji hibridne prijetnje[23] (ili hibridni rat) su nazivani kao *specijalni rat.* Ova dva termina imaju isto značenje. U suštini su potpuno iste metode, postupci koji su provođeni u *specijalnom ratu* koji su provodile kako države NATO i VU za vrijeme tzv. hladnog rata. Jedina razlika je što je tehničko-tehnološki napredak doveo do aktualnog sveprisutnog interneta i njegove zlouporabe *cyber* djelovanjem (ratovanjem[24]) koji se medijski naziva i ratom i kao što je već spomenuto, najprepoznatljivijim elementom hibridnih sukoba.

Visokosofisticirane informacijske tehnologije se koriste u brojnim djelatnostima, pa tako, primjerice, i u zračnom prometu kako bi osiguralo siguran, učinkovit i pouzdan zračni promet. On igra ključnu ulogu u globalnoj povezanosti i prijevozu putnika i tereta. Međutim, tehnološki napredak doprinosi povećanoj složenosti sustava, otvarajući vrata raznim izazovima i potencijalnim opasnostima. U kontekstu rastuće međusobne povezanosti i digitalizacije zrakoplovnog sektora, naglašava se rizik od kibernetičkih prijetnji u sustavima upravljanja zračnim prometom. (Prskalo, 2023: 123)

Pored navedenog, izdvajaju se psihološke operacije, provođene u *specijalnom ratu* za vrijeme hladnog rata. Razvoj interneta je doveo do stvaranja duštvenih mreža koje su, između ostalog, otvorile mogućnost da se u njima provode i

[23] Prema mišljenju autora pravilnija je uporaba termina *hibridne prijetnje* u odnosu na *hibridni rat.* Osnovni razlog je što se time pravi distinkcija u odnosu na pojam rata koji podrazumijeva dominantnu ulogu oružane borbe, a u hibridnim prijetnjama kojima se izazivaju hibridni sukobi (rat) ne dominira.

[24] „**Cyber-ratovanje** (ratovanje u kibernetskom prostoru) je pojam koji označava upotrebu računala, interneta i drugih sredstava za pohranu ili širenje informacija za provođenje napada na neprijateljske informacijske sustave pomoću sredstava informatičke tehnologije.“ (https://hr.wikipedia.org/wiki/Kiberneti%C4%8Dki_rat)

psihološke operacije, znatno naprednije u odnosu na prijašnje. Emir Muhić je u članku Psihološke operacije na društvenim mrežama – primjeri, tehnike, taktike i procedure (Muhić, 2025) istražio transformaciju ratovanja i sigurnosnih sukoba pod utjecajem suvremenih tehnoloških dostignuća, s posebnim naglaskom na ulogu društvenih mreža u provođenju psiholoških operacija. U članku se analiziraju tehnike, taktike i procedure koje se koriste za oblikovanje javnog mnijenja, manipulaciju percepcijama i širenje dezinformacija putem digitalnih komunikacijskih kanala. Kroz detaljnu analizu specifičnih strategija primijenjenih na društvenim mrežama, raspravlja se i o sigurnosnim implikacijama za nacionalne institucije i demokratski poredak.

Na temelju navedenog može se zaključiti da je pojam *hibridni rat* podudaran sa *specijalnim*. Isto tako, i da ima sličnosti i sa drugim spomenutim određenjima rata ali da je najveći stupanj poduranosti sa *specijalnim ratom* te ima isto značenje. Zbog kojih je onda razloga došlo do afirmacije i neprikosnovenog primata termina *hibridni rat*? Polazni razlog treba tražiti u domeni ideologije i politike.

Termin ima svoju političku dimenziju, posebno od zaoštravanja odnosa SAD, nekih europskih zemalja i Rusije, te služi da alarmira, pre svega zapadnu javnost, kroz semantički novi izraz. Teško se može preći preko činjenice da je hibridni rat doživeo svoje redizajniranje značenja a zatim i masovnu upotrebu i diskusiju upravo tada kada su se odnosi velikih sila zaoštrili i došli skoro na nivo na kojem su bili u vreme hladnog rata. Ovoga puta su se SAD i europske zemlje u NATO-u opredjelile za korišćenje drugačijeg termina.“ (Cvetković, Kovač i Joksimović, 2019: 328)

Često se naglašava da je hibridno ratovanje samo jedan novi termin koji ublažava zvučnost staroga termina *specijalni rat* koji su u vojni vokabular i praksu uveli Amerikanci u vrijeme hladnog rata. Prema jugoslavenskom Vojnom leksikonu „specijalni rat predstavlja skup organizovanih i koordiniranih političkih, diplomatskih, ekonomskih, psihološko-propagandnih, obaveštajno-subverzivnih, terorističkih, a često i vojnih akcija i postupaka.“ (Subotić:2018:29,30)

Afirmacija hibridnog rata je dovela i do preispitivanja, kritičkog promišljanja o tome da li on utječe na redefiniranje pojma rata. Od samih početaka uvođenja ovog pojma u teoriju i praksu traje rasprava o tome da li se radi o novom konceptualnom određenju rata ili je to samo evoluirani, usavršeni model rata u savremenim uvjetima koji ne dovodi u pitanje postojeće definiranje rata. U akademskoj javnosti prisutna su sporenja da li je riječ o novom pojavnom obliku rata koji je u nekim aspektima transformiran ili je riječ o staroj pojavi obogaćenoj novim terminom. (Ćurčić:2018:47)

Uvjetno rečeno, možemo da razlikujemo dvije faze razvoja koncepta hibridni rat. Prva fazu rata koja je trajala od uspostavljanja koncepta hibridni rat krajem XX. stoljeća pa sve do Ukrajinske krize (ruske agresije na Ukrajinu). Druga faza razvoja koncepta hibridni rat započinje nastankom Ukrajinske krize (ruske agresije na Ukrajinu) i aneksijom Krima od strane Rusije 2014. godine i traje sve do danas. Neki autori ove dve faze razvoja nazivaju nedržavnocetrični i državnocetrični pristup izučavanju pojma hibridni rat, prema određenju aktera koji primjenjuju ovaj tip rata. (Ćurčić:2018:48)

Hibridno ratovanje nije revolucionaran pristup jer izučavanjem povijesti možemo identificirati veliki broj ratova koji sadržavaju elemente hibridnog rata. Međutim, iako sami čimbenici koji definiraju hibridni rat nisu novi, već su uglavnom svi već prije korišteni u nekim od povijesnih ratova, ruski hibridni model sadržava neke dosad neizučavane aspekte – velika nepredvidivost i dinamičnost i fleksibilnost u primjeni različitih čimbenika, rastuća uloga informacijskog, ekonomskog, energetskog i drugih aspekata koji u suvremenom hibridnom modelu postaju gotovo jednako (ako ne i više) važni u odnosu na klasični vojni aspekt. (Brzica, 2018:42)

Izučavanjem dostupne literature jasno je da već postoji značajan broj stranih teoretičara i vojnih analitičara koji su u svojim međunarodno priznatim knjigama i člancima obradili pojam hibridnog rata, kao što su Frank Hoffman, Karber, McCulloh, Martin van Creveld, David Kilcullen, Janis Berzins i Robert Gates. Oni su u svojim radovima koristeći različite pristupe definirali ključne čimbenike, preduvjete, faze razvoja i čimbenike hibridnog rata kao operativnog pristupa za ostvarivanje nekih ciljeva o kojima teorija hibridnog rata ne govori ništa. (Brzica, 2018:43)

Postoji niz pojmova koji se upotrebljavaju za hibridni ratni koncept: hibridni rat, hibridne prijetnje, hibridni utjecaj ili hibridni protivnik (kao i nelinearni rat, netradicionalni rat ili specijalni rat). Vojna strategija često govori o hibridnoj prijetnji, dok akademska literatura govori o hibridnom ratovanju.“ (Ahmić, Dautbegović i Korajlić, 2018:83)

Ako se u utvrđivanju njegove definicije poslužimo najvećom (i često nepravedno omalovažavanom) internet-enciklopedijom, Wikipedijom, vidjet ćemo da je hibridno ratovanje (koje se još opisuje i kao nelinearno ili specijalno ratovanje) vojna strategija koja kombinira konvencionalno, iregularno i cyber ratovanje. (Ahmić, Dautbegović i Korajlić, 2018:84)
Hibridno ratovanje (engl. Hybrid Warfare, skraćeno HW), ili kako ga Rusi nazivaju „ratovanje nove generacije“ (engl. New Generation Warfare, skraćeno NGW) , temelji se na ideji Sun Tzua da se vrhunska vještina sastoji od slamanja

protivnikovog otpora bez borbe. Upravo na tim temeljima započeli su Rusi rat u Ukrajini. (Brzica, 2018:44)

S obzirom na složenost pojave teže je dati sažetu definiciju a istovremeno obuhvatiti sve aspekte hibridnog rata. U tom smislu bi kao riješenje moglo da posluži definiranje pojma užom[25] i širom[26] definicijom. (Cvetković, Kovač i Joksimović, 2019: 339)

3. Konceptualno-doktrinirano određenje hibridnog rata

Za razumijevanje pojma hibridnog rata od iznimne je važnosti sagledavanje njegovog određenja u konceptualno-doktrinarnim dokumentima NATO i EU. Kao što je poznato u njima je sadržana operacionalizacija postulata najviše razine odlučivanja NATO i EU u području obrane i sigurnosti kojima se određuje način uporabe sustava obrane i sigurnosti. Ovim dokumentima se definiraju temeljna načela koncepcije, doktrine i strategije obrane i sigurnosti NATO i EU. Oni su i polazišta za donošenje konceptualno-doktrinarnih dokumenata, koji se često nazivaju strateški, zemalja članica ovih organizacija. Pored toga, oni utječu i na propitivanje postavki ovih dokumenata najvažnih rivala NATO i EU – Rusije i Kine.

Strateški koncept koji su usvojili šefovi država i vlada na NATO summitu u Madridu 29.06. 2022. predstavlja polazni konceptualno-doktrinarni dokument NATO pakta. On je zamijenio prethodni Strateški koncept iz 2010. Novi koncept predstavlja temeljne postulate djelovanja da NATO „Savez ostane spreman i opremljen resursima za budućnost.“ (Uvodni dio Strateškog koncepta) Nastale vojno-političke promjene u međunarodnim odnosima su uvjetovale, između ostalog, potrebu donošenja novog Strateškog koncepta. Novi koncept sadrži

[25] „Uža definicija pojma bi mogla da bude sledeća: Hibridni rat predstavlja sukob dve ili više država i/ili organizacija u kome one koriste političke, ekonomske, informativne i bezbednosne elemente svoje moći, da vrše neoružanu a po potrebi i oružanu agresiju, na stanovništvo i materijalne resurse protivnika, kako bi ga potčinili svojim interesima i volji.“ (Cvetković, Kovač i Joksimović, 2019: 339)

[26] „Šira definicija hibridnog rata bi mogla da bude sledeća: Hibridni rat predstavlja višedimenzionalni sukob u kome učestvuju jedna ili više država, i/ili organizacija formiranih na političkim, ideološkim, nacionalnim ili verskim osnovama, u okviru koga najmanje jedna strana, sa strateški centralizovanog nivoa, sinhronizovano, adaptivno, prikriveno ili javno, u okviru neoružane i oružane agresije, sprovodi informaciono-psihološko-ideološke, političke, ekonomske, obaveštajno-subverzivne, informatičke, kriminalne, terorističke i vojne aktivnosti, utičući na fizičke i mentalne resurse, društvene odnose, vrednosti i interese protivnika, a radi prisiljavanja na postupanje u skladu sa svojim političkim, ekonomskim i vojnim ciljevima i interesima.“(Cvetković, Kovač i Joksimović, 2019: 340)

stajališta o odgovoru NATO saveza na brojne ugroze među kojima su potencirane i hibridne prijetnje.

„Strateški koncept je ključni dokument za Savez. Ponovno potvrđuje vrijednosti i svrhu NATO-a i daje zajedničku procjenu sigurnosnog okruženja. Također pokreće stratešku prilagodbu NATO-a i usmjerava njegov budući politički i vojni razvoj.Strateški koncept se redovito revidira i ažurira. Od kraja Hladnog rata ažuriran je otprilike svakih 10 godina kako bi se uzele u obzir promjene u globalnom sigurnosnom okruženju i kako bi se osiguralo da je Savez spreman za budućnost. Prethodni Strateški koncept usvojen je na NATO summitu u Lisabonu 2010. Novi Strateški koncept opisuje novu sigurnosnu stvarnost s kojom se suočava Savez, ponovno potvrđuje vrijednosti NATO-a i navodi ključnu svrhu NATO-a da osigura kolektivnu obranu saveznika.“[27]

Novi Strateški koncept razmatra problematiku hibridnog rata prilično sveobuhvatno. Analiza sadržaja novog koncepta upućuje da se ova problematika razmatra u više točaka ovog dokumenta. Dio poglavlja Strateško okruženje u točkama 7., 8. i 13. odnosi se na hibridna sredstva i metode koje provode strateški konkurenti NATO-a. U točki 7. se ne određuje na koji se to strateške konkurenti, oni se preciziraju u točkama 8 i 13. U točki 27 potpogljavlja Odvraćanje i obrana poglavlja Temeljne zadaće NATO-a se najviše potencira značaj hibridnog rata. Točka 43 potpoglavlja Kooperativna sigurnost poglavlja Temeljne zadaće NATO-a razmatra partnerstvo NATO i EU na suprotstavljanju kibernetičkim i hibridnim prijetnjama i rješavanje sustavnih izazova koje NRK postavlja euroatlantskoj sigurnosti.

U točki 7 se naglašava da strateški konkurenti „Miješaju se u naše demokratske procese i institucije i ciljaju na sigurnost naših građana putem hibridnih taktika, izravno i putem posrednika.“ U točki 8 se precizira strateški konkurent. „Ruska Federacija je najznačajnija i izravna prijetnja sigurnosti saveznika te miru i stabilnosti u euroatlantskom području.“
Jasno se ukazuje da ona (Ruska Federacija) „Protiv nas i naših partnera koristi konvencionalna, cyber i hibridna sredstva.“ Uočava se da se cyber sredstva izdvajaju da nisu u okviru hibridnih, da su istog ranga. Postavlja se pitanje da li je takav pristup u suprotnosti sa prihvaćenim teorijskim odredbama – definicijama prema kojima je cyber djelovanje sastavnica hibridnog rata?
U točki 13 se jasno izražava zabrinutost i od djelovanja i od strane drugog strateški konkurenta - NRK (Narodne Republike Kina). „Zlonamjerne hibridne i cyber operacije NRK-a i njezina konfrontirajuća retorika i dezinformacije ciljaju na Saveznike i štete sigurnosti Saveza.“ I u ovoj točki se uočava da su hibridne i

[27] https://www.nato.int/strategic-concept/

cyber operacije istog ranga značaja. U točki 15 se naglašava da „Cyberspace je osporavan u svakom trenutku. Zlonamjerni akteri nastoje degradirati našu kritičnu infrastrukturu, ometati naše vladine službe, izvlačiti obavještajne podatke, ukrasti intelektualno vlasništvo i ometati naše vojne aktivnosti." U kojoj mjeri se pridaje značaj cyberspacu najviše se može uočiti u točki 25. U njoj se navodi da „Jedan ili kumulativni skup zlonamjernih cyber aktivnosti; ili neprijateljske operacije prema, iz ili unutar svemira; moglo bi doći do razine oružanog napada i može navesti Sjevernoatlantsko vijeće da se pozove na članak 5. Sjevernoatlantskog ugovora."

Kao što je već spomenuto u točki 27 najviše se potencira značaj hibridnog rata. U njoj se naglašava da će NATO ulagati u vlastite sposobnosti pripreme, odvraćanja i obrane od hibridnih taktika od strane država i nedržavnih aktera. Pored toga, posebno je važna odredba da: „Hibridne operacije protiv saveznika mogu doseći razinu oružanog napada i dovesti Sjevernoatlantsko vijeće u situaciju da se pozove na članak 5. Sjevernoatlantskog ugovora." Njome se nedvosmisleno jasno određuje da hibridne operacije mogu dovesti do aktivacije članka Sjevernoatlantskog ugovora kojim je određeno da se oružani napad na jednu ili više članica smatra napadom na sve, cjelokupni Savez. Ova odredba, kao i spomenuti napadi iz točke 25, između ostalog, implicira potrebu redefiniranja dosadašnjeg određenja *oružanog napada.* Isto tako, i potrebu šireg, kompleksnijeg razumijavanja članka 5. Sjevernoatlantskog ugovora.

U točki 43 se ukazuju na značaj partnerstva NATO i EU i unaprjeđenje njegove strategije. Naglašava se da NATO-EU strateško partnerstvo stvara pretpostavke za učinkovitije „suprotstavljanje kibernetičkim i hibridnim prijetnjama."

Značaj NATO-EU strateškog partnerstva se naglašava i Strateškim kompasom za sigurnost i obranu - za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru i sigurnosti (u daljem tekstu Strateški kompas EU), polaznim konceptualno-doktrinarnim dokumentom EU u oblasti obrane i sigurnosti. U uvodu se naglašava da se Strateškim kompasom utvrđuje nova djelovanja i sredstva koja omogućuju, između ostalog, „produbljivanje suradnje s partnerima, posebno s UN-om i NATO-om, kako bi se postigli zajednički ciljevi." Ovaj dokument ima za EU isto značenje kao što Strateški koncept ima za NATO. Njime se utvrđuje plan za jačanje sigurnosne i obrambene politike EU do 2030. „Ovim Strateškim kompasom utvrđujemo zajedničku stratešku viziju sigurnosne i obrambene politike EU-a za razdoblje od sljedećih pet do deset godina te ćemo odmah započeti s njezinom provedbom." (uvod) To je prvi cjeloviti konceptualno-doktrinarni dokument EU. „Ovim Strateškim kompasom utvrđujemo zajedničku stratešku viziju sigurnosne i obrambene politike EU-a za razdoblje od sljedećih pet do deset godina te ćemo odmah započeti s njezinom provedbom." (Uvod Strateškog kompasa)

„Prvu verziju Strateškog kompasa visoki predstavnik podnio je u studenome 2021. na temelju prve analize prijetnji kojoj su doprinijele obavještajne službe 27 država članica EU-a i faze strukturiranog dijaloga između država članica EU-a, institucija EU-a i stručnjaka. O naknadnim verzijama raspravljalo se u veljači i ožujku 2022. kako bi se uzela u obzir rasprava država članica i Komisijin paket o obrani i svemiru od 15. veljače te najnovija međunarodna zbivanja, posebno vojna agresija Rusije na Ukrajinu. Izravno doprinosi provedbi programa iz Versaillesa.“[28]

U uvodnom dijelu Sažetka Europskog kompasa se naglašava – „Hibridne prijetnje sve su češće, sa sve većim učinkom.“ U točki 5 Sažetka se navodi da će se „stvoriti instrumentarij EU-a za obranu od hibridnih prijetnji koji objedinjuje različite instrumente za otkrivanje širokog raspona hibridnih prijetnji i odgovor na njih.“

U svezi cyber prijetnji one se kao i u Strateškom konceptu NATO izdvajaju iz hibridnih. U točki 6 Sažetka se navodi da će EU „dodatno razviti okvir za politiku cyber obrane EU-a kako bismo bili bolje pripremljeni i odgovorili na cyber napade.“

U potpoglavlju Povratak politike moći u multipolarnom svijetu u sukobu prvog poglavlja Svijet s kojim se suočavamo Europskog kompasa se naglašava „Oružana agresija na Ukrajinu pokazuje spremnost na upotrebu najviše razine vojne sile, neovisno o pravnim ili humanitarnim razlozima, u kombinaciji s hibridnim taktikama, cyber napadima i manipuliranjem informacijama i uplitanjem u inozemstvu, ekonomskom i energetskom prisilom i agresivnom nuklearnom retorikom.“ Opasnost od hibridnog djelovanja Rusije se prepoznaje i u potpoglavlju istog poglavlja - Naše strateško okruženje „Utjecaj snažno pogoršanog odnosa s ruskom vladom posebno je ozbiljan u mnogima od tih područja.
Ona se aktivno upliće s pomoću hibridnih taktika, čime se ugrožavaju stabilnost zemalja i njihovi demokratski procesi.“

U već spomentom potpoglavlju prvog poglavlja Strateškog kompasa spominje se i suparništvo sa Kinom. „Kina je partner za suradnju, gospodarski konkurent i sistemski suparnik.“ „Radi na ostvarenju svojih politika, među ostalim sve većom prisutnošću na moru i u svemiru te upotrebom cyber alata i primjenom hibridnih taktika“

[28] https://www.consilium.europa.eu/hr/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

U potpoglavlju Nove i transnacionalne prijetnje i izazovi prvog poglavlja jasno se ukazuje da „Državni i nedržavni akteri upotrebljavaju hibridne strategije, cyber napade, kampanje dezinformiranja, izravno uplitanje u naše izbore i političke procese, ekonomsku prisilu i instrumentalizaciju tokova nezakonitih migracija.“ Ova odredba je posebno značajna zbog što se njome ističe da hibridne strategije pored državnih aktera mogu provoditi i nedržavni.

Dio potpoglavlja Zajedničko djelovanje drugog poglavlja Djelovanje odnosi se na ulogu i značaj civilnih misija ZSOP, na rješavanju više sigurnosnih izaziva, uključujući i hibridne prijetnje. „Našim civilnim misijama ZSOP-a pružamo važan doprinos vladavini prava, civilnoj upravi, policiji i reformi sigurnosnog sektora u kriznim područjima. One su ključne i kao dio šireg odgovora EU-a na sigurnosne izazove potaknute nevojnim sredstvima, uključujući one povezane s nezakonitim migracijama, hibridnim prijetnjama, terorizmom, organiziranim kriminalom, radikalizacijom i nasilnim ekstremizmom.“

Citirani dio ukazuje da se hibridne prijetnje tretiraju kao dio sigurnosnih izazova potaknutih nevojnim sredstvima. Diskutabilno je izjednačavanje hibridnih prijetnji sa nezakonitim migracijama, terorizmom, organiziranim kriminalom, radikalnim i nasilnim ekstremizmom. U teoriji i praksi je poznato da spektar hibridnog djelovanja može uključivati i te navedene prijetnje. Isto tako, i da se mogu zasebno provoditi. Zbog toga, bi bilo primjerenije da su u tom kontekstu i navedene, kao samostalne i kao dio hibridnih prijetnji. Pored toga, ovaj citirani dio problematizira i pitanje da li su doista dominantne hibridne prijetnje iz „arsenala“ nevojnih sredstvava. Što je s hibridnim prijetnjaama iz spektra vojnog djelovanja? Da li su one manjeg značaja? Potenciranje ove dileme može isključiti jedino preciznije određenje, u citiranom dijelu, hibridnih prijetnji kao sastavnice nevojnih sredstava.

U uvodnom dijeli trećeg poglavlja Sigurnost naglašava se „Sve se više suočavamo s hibridnim prijetnjama.“ U potpoglavlju trećeg poglavlja - Hibridne prijetnje, kiberdiplomacija te inozemna manipulacija informacijama i uplitanje je najvažnije. Ono najizravnije tretira problematika hibridnih prijetnji. U njemu se precizira da će EU razviti instrumentarij EU-a za obranu od hibridnih prijetnji i timove za brzi hibridni odgovor, te time objediniti različite instrumente za otkrivanje širokog raspona hibridnih prijetnji i davanja adekvatnog odgovora na njih.
U završnom dijelu trećeg poglavlja Ciljevi potencira se integriranje alata za suzbijanje hinbridnih prijetnji „Okupit ćemo svoje alate za bolje suzbijanje hibridnih prijetnji razvojem instrumentarija za obranu od hibridnih prijetnji.“ Pored toga, precizira se i vremenski period razvijanja instrumentarija za obranu od hibridnih prijetnji. „U 2022. razvit ćemo instrumentarij EU-a za obranu od

hibridnih prijetnji koji bi trebao pružiti okvir za koordinirani odgovor na hibridne kampanje koje utječu na EU i njegove države članice i koji, na primjer, obuhvaća preventivne mjere i mjere suradnje, stabilnosti, ograničavanja i oporavka te kojim bi se podupirala solidarnost i uzajamna pomoć." Između ostalog, navodi se i i da: „Preispitat će se i Priručnik EU-a za suzbijanje hibridnih prijetnji."

Peto poglavlje Partneri - Multilateralni i regionalni partneri posvećeno je EU-NATO partnerstvu. „Strateško partnerstvo EU-a i NATO-a ključno je za našu euroatlantsku sigurnost, što se iznova pokazalo u kontekstu vojne agresije Rusije na Ukrajinu 2022. EU je i dalje u potpunosti predan daljnjem jačanju tog ključnog partnerstva i radi poticanja transatlantske veze." Na kraju poglavlju u dijelu Ciljevi navodi se: „Surađivat ćemo s partnerima na suzbijanju hibridnih prijetnji, dezinformacija i kibernapada. Naš pristup bit će usmjeren i na potrebu partnera za izgradnjom kapaciteta i potporom."

Kratka analiza sadržaja odredbi o hibridnom ratu u polaznim konceptualno-doktrinarnim dokumentima NATO i EU, Strateškog koncepta NATO i Strateškog kompasa ukazuje na njihovu usaglašenost. Ova dva dokumenta su podudarna u svezi pogleda na hibridni rat. U odnosu na definiranje sadržaja hibridnog rata, kao što je u analizi ukazano, u oba dokumenta se cyber djelovanje ne tretira kao dio hibridnog djelovanja. To je u suprotnosti sa teorijskim određenjima hibridnog rata u kome je djelovanje u cyber domeni bitna sastavnica njegovog određenja. Zbog toga se postavlja pitanje: da li će ova dva dokumenta dovesti do teorijskog redefiniranja pojma hibridnog rata ili će doći do revidiranja njihovog sadržaja?

4. Hibridno Rusko djelovanje u pripremi i izvođenju nastavka agresije na Ukrajinu

Ruska agresija na Ukrajinu pokrenula je brojna vojno-politička pitanja koja uključuju sagledavanje i njihove ekonomske dimenzije. Isto tako, ova agresija (koja se u medijima često naziva i invazija) koju je izvršila Rusija 24. veljače 2022. aktualizira i brojna druga pitanja među kojima poseban značaj ima sagledavanje pitanje sagledavanje polazišta odluke za njeno pokretanje. Ova agesija je, kao što je poznato, samo nastavak rata koji je započet 2014. i koji je rezultirao ruskom aneksijom Krima i okupacijom istočnog dijela Ukrajine i stvaranjem dvije samoproglašenih tzv. narodnih republika Donjeck i Lugansk.
Postavlja se pitanje na temelju kojih procjena je Rusija donijela odluku o nastavku agresije na Ukrajinu krajem veljače 2022. koja je otvorena, neskrivena za razliku od one izvršene 2014. koju je pokušavala prikriti.

Bliske povijesne činjenice upućuju na nerazumnost aktualne ruske politike da pokreće rat koji može eskalirati u svjetski. Odnosi ekonomskih, vojnih i

demografskih potencijala Rusije i EU i NATO više nego jasno ukazuju na premoć Zapada. Taj paritet je jedino relativno uravnotežen u odnosu potencijala oružja za masovno uništavanje (nuklearnog, kemijskog i biološkog). Međutim, on ne može biti ishodište razumijevanja ruske politike za nastavak agresije na Ukrajinu i riskiranje eskalacije rata. Bilo bi potpuno banaliziranje i trivijaliziranje ove kompleksne problematike na svođenje razumijevanje ruske agresivne politike na oslanjanje na moć svog oružja za masovno uništavanje, prije svega nuklearnog koje se najviše naglašava. Davanje odgovora na to polazno pitanje: Koja su polazišta ruske odluke da se usudi na nastavak agresije 2022. godine na Ukrajinu koji uključuje realni rizik eskalacije rata i političko-ekonomsku konfrontaciju sa Zapadom? Kako je moguće da se Rusija odvažila na vođenje takve politike konfrontacije sa Zapadom koja ju vodi porazu? Da li je u pitanju pogreška ruskog strateškog promišljanja?

Odgovor na ovo pitanje je iznimno kompleksan, uključuje sagledavanje vojne,političke i ekonomske komponente. Sa vojnog aspekta je poznato da svaka zemlja, pa tako i Rusija u ovom slučaju, nastoji da prije početka rata sagleda svoje prednosti u odnosu na protivničke.

Mogući razlozi za donošenje ove odluke najvjerojatnije ishodište imaju u kontinuirano stvaranoj euforiji zbog dosadašnjih uspješnih rezultata provođenja imperijalne politike i stvorenoj projekciji vojno-političke moći.[29] Ova problematika nije predmet ovog članka. Pored toga, prevazilazi opseg članka.
Pored spomenutog kontinuiteta uspjeha vojnog angažmana koji je nesumnjivo imao polazni značaj za donošenje ruske odluke o nastavku agresije na Ukrajinu, isto tako su najvjerojatnije utjecali i postignuti rezultati tzv. *hibridnog djelovanja*. Od 1991. Rusija provodi relativno samostalne aktivnosti iz spektra *hibridnih prijetnji*. Ove aktivnosti predstavljaju kontinuitet djelovanja, provođenja

[29] Rusija je već u prvim godinama svog postojanja kao neovisne države poslije raspada SSSR uspjela ostvariti svoj prve uspjehe. 1992.[29] – de facto okupacijom dijela Moldavije (oko 17% njenog teritorija) stvaranjem tzv. Pridnjestrovlja (Pridnjestrovska Moldavska Republika). Po osamostaljenju, poslije raspada SSSR Gruzija je također ostala bez svoje dvije regije Južne Osetije i Abhazije. Ruska pomoć je kao i slučaju Moldavije bila presudna za stvaranje tzv Republike Južne Osetije i Republike Abhazije na teritoriju Gruzije. Poslije toga je slijedilo zatišje do otvorenog ruskog vojnog djelovanja 2008. u Gruziji koje je rezultiralo ruskim priznavanjem tzv Republike Južne Osetije i Republike Abhazije. Nakon toga je slijedio najambiciozniji poduhvat – razmatrana agresija 2014. na Ukrajinu i njen nastavak krajem veljače 2022. Pored ove tri spomenute agresije, Rusija je više puta demonstrirala svoju vojnu moć. Po značaju i pokazanoj brutalnosti i razornosti izdvaja se vojna intervencija u Siriji. Razoreni Alep i tisuće pobijenih civila u Siriji su do nastavka agresije na Ukrajini 2022. su bili najvjerodostojniji dokazi demonstracije brutalnosti ruske vojne moći. Rusija je prezentirala svoju vojnu moć i na druge načine. Među njima, se može izdvojiti nekoliko primjera: Armenija, teritorij bivše SFRJ, Kazahstan.

aktivnosti bivšeg SSSR protiv Zapada. U tom vremenu te aktivnosti su nazivane kao specijalni rat.

Poznati su primjeri intenzivnog djelovanja sovjetske obavještajne službe KGB u provođenju specijalnog rata za vrijeme tzv. hladnog rata. Sljednik te službe, ruska FSB je na temelju tih iskustava korištenja metoda KGB uspjela ih modernizirati i usavršiti ih i, mora se priznati, ostvariti zavidne rezultate. Nastavak ruske agresije na Ukrajinu je razotkrio samo neke najznačajnije. Među njima, po značaju se izdvajaju razmjere političke korupcije, utjecaja na izborne procese u više značajnih europskih zemalja kao rezultata ruskog subverzivnog djelovanja koji su utjecali na određivanje smjera politika tih zemalja. Ona je potpuno očita u pogledu stvaranja energetske ovisnosti od uvoza ruskog plina, nafte i ugljena. Primjerice, njemačka ovisnost od uvoza ruskog plina u iznosu od 40%, austrijska čak od 80% itd. Više je nego jasno da je Njemačka kao ekonomski vodeća zemlja Europe mogla da svoje energetske potrebe podmiri na druge načine. Nije uvažavala američka upozorenja na opasnosti vođenja te politike te je suprotno njima sa Rusijom izgradila Sjeverni tok 2 koji je trebao još više da poveća postotak njemačke ovisnosti od ruskog plina. Poznato je da nastavak ruske agresije na Ukrajinu onemogućio ostvarenje tog plana. Isto tako, je poznato i da je ovaj nastavak ruske agresije doveo i zaokreta njemačke politike prema Rusiji.

Spomenuti primjeri ruskog uspješnog vojnog angažmana u fusnoti br.16 , kao i postignuti rezultati hibridnog djelovanja su bili temelji stvaranja uvjerenja i da će nastavak agresije na Ukrajinu biti još jedan uspješni vojni angažman koji će „zasjeniti“ sve ranije. Isto tako, polazište je bilo da neće biti značajnije reakcije NATO i EU, da će ona biti na sličnoj razini kao i prije. Pri tome, ruski planeri su također, računali na dosadašnje nesuglasje stajališta u okviru samog NATO i EU, kao i između EU i SAD i na relaciji EU – NATO prema provedbi politike prema Rusiji. Razmjere globalne krize koje je izazvao nastavak ruske agresije su potaknule potpuno suprotne – integracione procese. Došlo je do jačanja kohezije NATO i afirmacije njegove uloge kao najvećeg jamstva sigurnosti, aktualno najviše europskih članica Istočne Europe od ruskih prijetnji. Najveći dokaz te afirmacije je prijam Finske i Švedske u NATO koji, kao što je poznato, još nije formalno-pravno završen.

Značajno je naglasiti da je rusko hibridno djelovanje utemljeno i na postulatima teorije. Ona je u Rusiji razvijena, ni malo ne zaostaje u odnosu na zapadnu. Razvoj ruske teorijske misli o fenomenu fibridnog rata je uočljiv. On je je evoluirao od početnog otpora ruskog vojnog establišmenta prema uporabi novog termina. U ruskoj vojnoj treminologiji je prihvaćena sintagma nelinearna vojna strategija. Ratovi u Iraku i Libiji kao i tzv. arapske revolucije utjecali su na ruske vojne krugove da usvoje koncept nelinearnog ratovanja.

Načelnik Generalštaba Oružanih snaga Rusije general Valerij Gerasimov se smatra autorom koncepta *totalnog rata*, ruske nove generacije rata koja je po njemu nazvana Gerasimljova doktrina. Ovaj koncept je po brojnim elementima podudaran sa pojmom hibridnog rata te se, u uvjetnom smislu, može smatrati njegovom ruskom inačicom. Razradio ga je 2013. godine general Gerasimov, nakon čega je objavio dokument od 2 000 stranica pod nazivom Važnost znanosti je u predviđanju, a dio je objavio ruski tjednik "Vojno-industrijski kurir" (Gerasimov, 2013). U radu su postavljena nova pravila ruskog vojnog djelovanja. Opravdano se smatra da objavljivanjem ovog djela – tzv. Gerasimovljeve doktrine ruska vojna strategija evaulira u nov pristup u kojem se potencira uporabu nevojnih metoda kako bi se postigli strateški i politički ciljevi.

"Važnost nevojnih sredstava u postizanju političkih i strateških ciljeva je povećana i često u učinkovitosti nadmašuje snagu oružja", 2013. u svom djelu naglašava general Gerasimov. Prevladavanjem ograničenja zbog ograničenih financijskih sredstava, Rusija je uspjela stvoriti strategiju jačanja nevojnih metoda koje su se pokazale učinak gotovo kao i vojne. Postoje i mišljenja koja relativiziraju ovu novu doktrinu. Ona se zasnivaju na stajalištu da je ona zbroj pojmova koji proizlaze iz sovjetske strategije obogaćenih elementima totalnog rata i novom teorijom o specifičnim uvjetima ratovanja. U suštini, ovakva stajališta proizilaze iz definiranja hibridnog rata, uključujući i ovu doktrinu, kao evauliranog, medernizranog koncepta specijalnog rata i sovjetske strategije. Time se dovodi u pitanje da li je tzv. Gerasimljova doktrina inovativni teorijski koncept. No, i pored toga, ona je afirmirana u praksi, kao najvažnijem kriteriju valorizacije teorije. Uspješnost ruskih aktivnosti, između ostalog, i na temelju ove doktrine, ukazuje da ova relativizacija nije objektivna.

Afirmaciji sintagme hibridnog rata je značajno doprinio Andrej Koribko, ruski novinar i publicista. On je *obojene revolucije* u zemljama kao što su Ukrajina, Libija, Egipat, Sirija, od kojih su neke prerasle i u oružane sukobe nedržavnih oružanih formacija protiv zvaničnih oružanih snaga tih država, nazvao kao hibridni rat koji sprovode SAD i pojedine zemlje Europe. U svojoj knjizi „Hibridni ratovi: Indirektni adaptivni pristup promeni režima" (Korybko,2015) je kao elemente ovakvog hibridnog rata naveo: diplomaciju, informatičke napade, ekonomski rat, informativni rat i propagandu, podrška lokalnim grupama, neregularne oružane snage (terorizam), regularne oružane snage i specijalne jedinice.

Najveći doprinos ruskom teorijskom utemeljenju hibridnog rata je dao akademik Igor Panarain. Njegovo kapitalno djelo je knjiga Hibridni rat: teorija i praksa.[30] U ovoj knjizi su definirani, sistematizirani i razmatrani ciljevi ,referentna područja,

[30] Knjiga je prevedena na srpski jezik i objavljena 2019. u izdanju Vojne knjižare u Begradu.

satavnice i vrste hibridnog rata. Pored toga, u njoj se inicira i stvaranje institicije za provedbu metoda hibridnog rata. Ova zamisao je prepoznatljiva u zadnjem, 23 poglavlju knjige – Tehnologija pobjede Rusije, potpoglavlju Hibridna ratna matrica, ili Zašto nam je potreban informativni Glavni stožer? Ne iznenađuje operacionalizacija teorijskih promišljanja akademika Panarina iznesenih u ovom poglavlju, obzirom da je on i koordinacijski stručnjak Analitičkog vijeća, važnog savjetodavnog tijela Predsjednika Ruske Federacije.

Ova knjiga predstavlja, uvjetno rečenu, nadogradnju autorovih ideja objavljenih u prethodnom djelu Hibridni rat protiv Rusije (1816-2016). Akademik Panarin je autor i knjige Hibridni rat i geopolitika, isto tako, značajnog djela koje razmatra geopolitički aspekt hibridnog rata. Opseg članka ne dopušta prikaz opusa i drugih ruskih autora. Među njima, se izdvaja knjiga A.A.Bartoša – Siva zona: kazalište hibridnog ratovanja.[31]

5. Zaključak

Sagledavanje dosadašnjih pristupa definiranja hibridnog rata je iznimno značajano. U dosadašnjem definiranju uočavaju se tri pristupa: prvi, da je to evoluirani pojam specijalnog rata, drugi, da je ova sintagma podudarna, slična sa konceptima sukoba niskog intenziteta, rata četvrte generacije, složenog rata, asimetričnog rata, uključujući i specijalnog rata i treći, da je to novi koncept rata. U članku se afirmira prvi pristup. Obrazloženo je da je pojam *hibridni rat* podudaran sa *specijalnim*. Isto tako, i da ima sličnosti i sa drugim spomenutim određenjima rata ali da je najveći stupanj poduranosti sa *specijalnim ratom* te ima isto značenje. Otvoreno je i pitanje - zbog kojih je onda razloga došlo do afirmacije i neprikosnovenog primata termina *hibridni rat*? Ukazano je da polazni razlog treba tražiti u domeni ideologije i politike.

Ovaj rad nema pretenzija da afirmira odabrani pristup kao rješenje definiranja hibridnog rata. Obzirom na kompleksnost i značaj razmatrane tematike članak ima za cilj da inicira raspravu o tri navedena pristupa i da usmjeri dalja potpunija istraživanja koja bi rezultirala prihvatanjem ili odbacivanjem predloženog pristupa definiranju hibridnog rata.

Pored toga, u članku je ukazano i na značaj razmatranja odnosa teorijskog i konceptualno-doktrinarnog određenja hibridnog rata. Sukladno tome, analiziran je sadržaj odredbi o hibridnom ratu u polaznim konceptualno-doktrinarnim dokumentima NATO i EU, Strateškog koncepta NATO i Strateškog kompasa.

[31] Aleksandar Aleksandrovič Bartoš je autor i značajnih monografija "Sukobi 21. stoljeća. Hibridni rat i obojena revolucija" i "Magla hibridnog rata. Neizvjesnosti i rizici 21. stoljeća".

Obrazloženo je da su ova dva dokumenta podudarna u svezi pogleda na hibridni rat. U odnosu na definiranje sadržaja hibridnog rata, kao što je u analizi ukazano, u oba dokumenta se cyber djelovanje ne tretira kao dio hibridnog djelovanja. Ukazano je da je ovo izostavljanje u suprotnosti sa teorijskim određenjima hibridnog rata u kome je djelovanje u cyber domeni bitna sastavnica njegovog određenja.

Između ostalog, aktualizirano je i pitanje da li afirmacija teorije i prakse hibridnog rata implicira na potrebu redefiniranja dosadašnjeg teorijskog koncepta rata. Isto tako, je razmatrana praksa primjene ruskog hibridnog djelovanja u pripremi i izvršenju agresije na Ukrajinu. Na ovom primjeru koji se može uvjetno nazvati mini studija slučaja mogu se prepoznati značajna iskustva i pouke. Kritičko propitivanje ruskog hibridnog djelovanja na ovom primjeru upućuje na zaključak da doseg učinka hibridnog djelovanja ne treba precjenjivati.

Neupitan je značaj pokrenutih pitanja za dogradnju i profilaciju teorije i prakse hibridnog rata. Može se zaključiti da je ostvaren teorijski i praktični cilj članka. S teorijskog aspekta dati su elementi koji mogu doprinijeti definiranju pojma hibridnog rata. Praktični aspekt je značajan, ukazuje, kao što je već spomenuto, da ne treba precjenjivati doseg metoda hibridnog rata u praksi. On ima za cilj i da potakne stručnjake, praktičare u području obrane i sigurnosti na proučavanje temeljnih postulata hibridnog rata kako bi sa više razumijevanja mogli pratiti razvoj teorije i prakse njegove primjene.

LITERATURA:

Autorska djela

1. Akrap, G. (2012). Specijalni rat 3. Večernji list, Zagreb.
2. Ahić,J., Alishapić, B. (2019): Horizontalno i vertikalno hibridno djelovanje i/ili rat/ studija slučaja Bosne i Hercegovine, Kriminalističke teme, br. 5/2019, https://krimteme.fkn.unsa.ba/index.php/kt/article/view/221/218
3. Ahmić, E., Dautbegović, A. i Korajlić, N. (2018): Pojam i determinante hibridnog ratovanja, Zbornik radova 11. Međunarodna znanstveno-stručna konferencija „Dani kriznog upravljanja 2018“, Veleučilište Velika Gorica, 2018., str. 83-88, file:///C:/Users/Admin/Downloads/967749.DKU-Radovi-2018%20(1).pdf
4. Arnel P., D., Lt Col Dave, A., Dr Nesic, A. and Krohley, N. (2020): Why We Need A Modern Theory of Special Warfare to Thrive in the Human Domain, https://wavellroom.com/2020/05/14/why-we-need-a-modern-theory-of-special-warfare-to-thrive-in-the-human-domain/
5. Brzica, N. (2018): Hibridno ratovanje i suvremeni sukobi - doktorski rad, Fakultet političkih znanosti, Zagreb, 2018, https://www.fpzg.unizg.hr/_download/repository/hibridno_ratovanje_i_suvremeni_sukobi_brzica.pdf
6. Cvrtila, Ž. (2017): HIbridni rat suvremeni naziv za već poznate oblike ratovanja, Zaštita, br. 12/2017, https://www.bib.irb.hr/1086183
7. Cvetković, N., Kovač, M. i Joksimović, B. (2019): Pojam hibridnog rata, Vojno delo, br. 7/2019, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo411/vd-411-2019-71-7-24-Cvetkovic.pdf
8. Gerasimov, V. (2013): Vrijednost znanosti je u predviđanju: Novi izazovi zahtijevaju ponovno promišljanje oblika i metoda provedbe borbenih operacija. VoyennoPromyshlennyy Kurier (VPK) (Military-Industrial Courier). http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf
9. Hibridno ratovanje – dilema koncepta savremenih sukoba, Tematski zbornik radova, Institut za strategijska istraživanja, Beograd, 2018., http://www.isi.mod.gov.rs/multimedia/dodaci/hr_tematski_zbornik_2_1555574872.pdf
10. Korybko, A., Hybrid Wars (2015): The Indirect Adaptive Approach to Regime Change, People's Friendship University of Russia, Moscow, http://resistir.info/livros/hybrid_wars_updated.pdf
11. Kolobara,R (2019): Hibridne prijetnje u 21. stoljeću – teorija i istraživanje nazivlja u Bosni i Hercegovini, National security and the future, br. 1-2/2019, https://hrcak.srce.hr/file/337151
12. Maher, A. (2016): An Australian doctrinal concept for Special Warfare: Lessons and ConsiderationsThe Australian Army Research Centre (AARC) ,

https://researchcentre.army.gov.au/library/occasional-papers/australian-doctrinal-concept-special-warfare-lessons-and-considerations
13. Muhić, E. (2025): Psihološke operacije na društvenim mrežama – primjeri, tehnike, taktike i procedure, Zaštita i sigurnost, godina 5., broj 1/2025, 129-164 https://zisjournal.com/psiholoske-operacije-na-drustvenim-mrezama-primjeri-tehnike-taktike-i-procedure/
14. Mandić,I. (2016):Definiranje rata za 21. stoljeće, Polemos, br. 37/2016, https://hrcak.srce.hr/file/250352
15. Milošević, M., D. (2018): Pojmovno određenje fenomena hibridnog ratovanja, Vojno delo, br. 3/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo399/vd-399-2018-70-3-20-Milosevic.pdf
16. Milošević, M., D. (2018): Percepcija savremenih oružanih sukoba kao indikatora hibridnog koncepta rata, modeli prevencije i suprotstavljanja hibridnim pretnjama, Vojno delo, br. 5/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo401/vd-401-2018-70-5-19-Milosevic.pdf
17. Milenković, R., M. i Mitrović, M. (2019): Obojene revolucije u paradigmi hibridnog rata, Vojno delo, br. 6/2019, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo410/vd-410-2019-71-6-17-Milenkovic.pdf
18. Madden,D.,Hoffmann,D., Johnson, Krawchuk, T.,F., Nardulli,R.,B., Peters,E.,J., Robinson, L., Doll, A.: Toward Operational Art in Special Warfare - file:///C:/Users/Admin/Downloads/RAND_RR779%20(1).pdf
19. Pejić, I. (2019): Ruske vojne hibridne operacije u Ukrajini: prilagođavanje strategije i taktike savremenoj strukturi rata, Međunarodni problemi, br. 4/2019 (str. 423-446), http://www.doiserbia.nb.rs/img/doi/0025-8555/2019/0025-85551904423P.pdf
20. Prskalo, M. (2023.): *Suvremeni kibernetički rizici u upravljanju zračnim prometom*, Zaštita i sigurnost, godina 3., broj 2/2023, 132-143 https://zisjournal-com-647393.hostingersite.com/wp-content/uploads/2024/06/Godina_3.Broj_2.pdf
21. Petrović, R., J. (2021): Psihološki rat i vojne nauke, Baština, Priština-leposavić, sv. 55, 2021., https://scindeks-clanci.ceon.rs/data/pdf/0353-9008/2021/0353-90082155267P.pdf
22. Rančić, I. i Beriša, H. (2018): Hibridni rat – mit ili stvarnost (Rekonceptualizacija hibridnog rata), Vojno delo, br. 5/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo401/vd-401-2018-70-5-18-Rancic.pdf
23. Saković, R. i Terzić, R., M. (2018): Upotreba društvenih mreža u hibridnom ratovanju, Vojno delo, br. 7/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo403/vd-403-2018-70-7-21-Sakovic.pdf

24. Vračar, S., M. (2017): Razmatranje adekvatnog teorijsko- -epistemološkog pristupa u istraživanju fenomena hibridnog ratovanja, Vojno delo, br. 7/2017, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo395/vd-395-2017-69-7-20-Vracar.pdf
23. Vuković,N. (2021): Konceptualizacija fenomena rata u savremenoj ruskoj vojnoj misli – doprinos generala Gerasimova, Međunarodni problemi, br. 2/2021 (str. 259-283), http://www.doiserbia.nb.rs/img/doi/0025-8555/2021/0025-85552102259V.pdf
25. Vračar, S.,M. i Tikhova, V.,V.(2018): Diskurzivni pristup fenomenu „hibridnog ratovanja“, Vojno delo, br. 3/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo399/vd-399-2018-70-3-21-Vracar.pdf

Dokumenti

1. Military Doctrine of the Russian Federation”, 2014, https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf
2. Rezolucija Europskog parlamenta od 17. veljače 2022. o provedbi zajedničke sigurnosne i obrambene politike – godišnje izvješće za 2021. (2021/2183(INI)), 17. veljače 2022. – Strasbourg, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0040_HR.pdf
3. Strateški koncept, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
4. Strateški kompas za sigurnost i obranu - za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru i sigurnosti, Vijeće Europske unije, Bruxelles, 21. ožujka 2022., https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/hr/pdf
5. Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije, Visoki predstavnik unije za vanjske poslove i sigurnosnu politiku, Bruxelles, 06.04.2016., https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX:52016JC0018

Intrnetski izvori:

1. Hibrid - https://hr.wikipedia.org/wiki/Hibrid
2. Hibrid https://hr.wiktionary.org/wiki/hibrid
3. Hibridi https://www.enciklopedija.hr/natuknica.aspx?ID=25351
4. Hibridni rat https://hr.wikipedia.org/wiki/Hibridni_rat
5. Hibridni rat - https://ru.wikipedia.org/wiki/Гибридная_война
6. Prijevod 'hibridni rat' https://hr.glosbe.com/hr/en/Hibridni%20rat
7. Specijanje operacije - https://ru.wikipedia.org/wiki/Специальные_операции
8. Specijalni rat - https://sh.wikipedia.org/wiki/Specijalni_rat

9. Specijalni rat - https://www.enciklopedija.hr/natuknica.aspx?ID=57361
10. Special operations warfare - https://www.britannica.com/topic/special-operations-warfare
11. Special Warfare, https://www.dvidshub.net/publication/372/special-warfare
12. Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center and School, Department of Defense (DOD),Department of the Army, Army Training and Doctrine Command (TRADOC), https://bookstore.gpo.gov/products/special-warfare-professional-bulletin-john-f-kennedy-special-warfare-center-and-school

THE CONCEPT OF HYBRID WAR

DOI: *10.70329/2744-2403.2025.5.10.5*

Review scientific article

Dragutin Šimić

Anstract:

In the article, a critical consideration of the definition of hybrid war was carried out. Analysis of the content of the existing literature indicates that this issue is considered in three ways. Firstly, that it is an evolved concept of special war, secondly, that this syntagm is consistent, similar to the concepts of low-intensity conflict, fourth-generation war, complex war, asymmetric war, including special war, and thirdly, that it is a new concept of war. The article tries to prove that the first approach is the most acceptable. In addition, the significance of the conceptual-doctrinal definition of hybrid war was also pointed out. Among other things, the practice on the example of the application of Russia's hybrid war methods in the preparation and execution of aggression against Ukraine is considered.

Keywords*: hybrid war, hybrid threats*

1. Introduction

To understand the concept of hybrid war, the starting point is the etymological[32] definition of the word hybrid. "The term hybrid comes from Greek and means approximately 'children of arrogance, haughtiness'. .. In all modern languages, the term has lost its negative connotation and today it only denotes a mixture or combination. Using the term hybrid with the designation of a species or process only emphasizes that the resulting whole is the result of the merging of two different species or processes.[33] In addition, the position is also accepted that "The word, as such, comes from the Latin hybrĭda.[34] "From the Latin ibrid under the influence of the ancient Greek ὕβρις (húbris, 'rage')[35]. This Latin word had the meaning – "a mixed breed, a person born of a Roman father and a foreign mother or of a freeman and a slave.[36]

The etymological definition of the word hybrid indicates the ambiguity of this word. It is used in science, technology, sports, politics … Colloquially speaking, it denotes a product, a process that is composed of elements of different origin, in the figurative sense "that which is composed of elements of different origin."[37] For example, "in botany and zoology, a hybrid is a seed or living being created by crossing parents of different breeding lines, breeds or species. In molecular biology, for joining one longitudinal half of a DNA or RNA strand with the other complementary half of the strand."[38] "In technology, a hybrid generally means a system in which two technologies are combined."[39] In the most general, colloquial sense, a hybrid means anything that is composed of elements of different origin.

In the theory of war, the term hybrid war is considered to be the combined use of conventional methods of war and so-called non-military means. "Hybrid war is a military strategy that contains elements of conventional warfare, unconventional

---

[32] Etymology is a branch of linguistics that studies the origin of words. "- https://hr.wikipedia.org/wiki/Hibrid ;"Linguistic science that studies the origin, development of the form and meaning of words according to the root of the word" - https://hjp.znanje.hr/

[33] https://hr.wiktionary.org/wiki/hibrid

[34] https://hr.encyclopedia-titanica.com/significado-de-h-brido

[35] https://en.wiktionary.org/wiki/hybrida#Latin

[36] Same source

[37] https://www.opsteobrazovanje.in.rs/sta-znaci/hibrid/

[38] https://hr.wiktionary.org/wiki/hibrid

[39] Same source

warfare and cyber warfare."[40] This is a relatively new term that has existed in military theory and practice only since the beginning of the 21st century. Regarding its definition, the positions of military experts are divided into three approaches. According to the first, that it is only an evolved concept of special war and according to the second, that it is close, similar to the definitions of war as a low-intensity conflict, fourth-generation war, complex war, asymmetric war, including special war and the third that it is a new concept of war. The problem area of the article is this issue. The author's point of view is the correctness of the first mentioned approach. Accordingly, the theoretical and hypothetical framework of the article is represented by postulates that prove that hybrid war is an evaluated concept of special war. It is based on an analysis of the content of relevant positions of leading world authors, as well as in the countries of the region.

Considering that in the region the most dominant theoretical opus on this topic is by scientists from Serbia, and that it is also thoroughly studied in Croatia. For this reason, the work of Serbian and Croatian authors is considered the most. In addition to them, authors from BiH are also mentioned. The subject frame of the article is the elements that confirm the aforementioned hypothesis that hybrid war is a perfected, modernized concept of special war. In addition, it also includes a conceptual-doctrinal definition of hybrid war, as well as an example of the practice of implementing hybrid war. For this reason, the article is divided into three chapters: 1. Conceptual definition of hybrid war, 2. Conceptual-doctrinal definition of hybrid war, and 3. Hybrid Russian action in the preparation and execution of the continuation of aggression against Ukraine.

The theoretical goal of the paper is to provide elements for a more studious observation of the hybrid war phenomenon. As is known, there is still no consensus on the definition of hybrid warfare. The systematization of the previous definitions of the phenomenon of hybrid war into the three approaches mentioned, as well as indicating its conceptual and doctrinal determination, can contribute, create assumptions for a more precise definition of this phenomenon. The practical goal is also to provide the elements for the most adequate adoption of conceptual-doctrinal and normative acts in which this topic is considered. Also, to encourage practitioners - experts to look at this extremely complex issue as fully as possible.

[40] https://hr.unionpedia.org/i/Konvencionalni_rat

2. Definition of hybrid war

Over time, the term war, from the notion of a larger armed conflict between states, began to be used to express conflicts in other areas of social activity, with the use of adjectives to form syntagms - cold war, special war, total war, multidimensional, unlimited, hybrid war. Hybrid war is a term whose use has experienced a special intensity in the last few years, and the term itself appeared at the beginning of the 21st century. Although the conclusion of most authors is that it does not mean anything new in relation to some other similar terms, a unique or generally accepted definition has not been reached. In the professional public, there are different opinions about the content of hybrid war, different concepts and terms are used, but nevertheless, one can notice the agreement that hybrid war is a combination of unarmed and armed forms of threat. (Cvetković, Kovač and Joksimović, 2019: 323)

Hybrid war is perhaps the broadest term so far, because with globalization and the evolution of war, it has expanded from the battlefield, where the tactics and asymmetry of war tricks changed the course and outcome of battles and wars, growing to international borders, then regional and finally global, spreading from conflicts in which only soldiers were involved, to the borders of the entire, even global, international society, and all its institutions, potential and resources. (Ahić and Alishapić, 2019:163)

As already emphasized, there are two points of view regarding the relationship of this term with earlier similar ones. First, that it is just a modern name for old forms of warfare that have long been known under the term special war, and which meant a set of organized and coordinated political, diplomatic, economic, psychological-propaganda, intelligence, subversive, terrorist, and sometimes covert military actions and procedures." (Cvrtila, 2017:1,2) And secondly, that until 1990, total, cold, special war, low-intensity conflict, and 4th generation war, unlimited warfare, complex, asymmetric, irregular war were mentioned as terms and concepts that are particularly similar to today's hybrid war. (Cvetković, Kovač and Joksimović, 2019: 331)

A valid conceptual definition of this phrase should express its essential and constant provisions, along with specifying specific properties, the marking of which enables the term hybrid war to be distinguished from other, similar concepts. In fact, due to the existence of several terms that are close to the phrase hybrid war, such as low intensity conflict, fourth generation war, complex war, asymmetric war and special war, detecting and labeling these specific characteristics is the main challenge when defining hybrid war. (Vuković, 2018:12)

Several authors have analyzed the similarities and differences between the concept of hybrid war and the aforementioned others. For example, Ahić and Alishapić consider the differences between the concept of hybrid war in relation to special war, low-intensity conflict, and IV generation war. (Ahić and Alishapić, 2019:165, 167)

Of all the mentioned syntagms, special war stands out the most in terms of compatibility with hybrid war. When compared with the definition of hybrid warfare, they observe, many similarities are visible. During the Cold War, the so-called the special war was associated primarily with the USA, because they had developed forces that could undertake wide-ranging activities in the society of a state that was exposed to pressure or aggression. Now, Russia uses exactly the same procedures defined decades ago in the USA by combining, as it is now called, soft power - propaganda, supported by political moves of all subversive activities. (Milošević, 2018:72)

Some authors dispute the above coincidence with the explanation that cyber operations are differentia specifica for the concept of hybrid war, that is, what distinguishes these wars from similar concepts such as special war, which is very close in content to the concept of hybrid war. (Vuković, 2018:25) This point of view is rightly contested. The theory that hybrid warfare represents something new is more than ahistorical. If the definitions of hybrid warfare did not mention cyber attacks, this narrative could be applied to virtually every war ever fought. (Subotić:2018:31)

In the previous terminology, hybrid threats[41] (or hybrid war) were referred to as special war. These two terms have the same meaning. In essence, they are exactly the same methods, procedures that were carried out in special war, which was carried out by both NATO and VU countries during the so-called Cold War. The only difference is that technical and technological progress has led to the current ubiquitous Internet and its misuse by cyber operations (warfare[42]), which is also called war in the media and, as already mentioned, the most recognizable element of hybrid conflicts.

Highly sophisticated information technologies are used in numerous industries, including, for example, in air transport to ensure safe, efficient and reliable air

[41] In the author's opinion, the term hybrid threat is more appropriate to use in relation to hybrid war. The main reason is that it distinguishes the concept of war, which implies a dominant role for armed struggle, while hybrid threats that provoke hybrid conflicts (war) do not dominate.

[42] "Cyber-warfare (warfare in cyberspace) is a term that denotes the use of computers, the Internet, and other means of storing or disseminating information to carry out attacks on enemy information systems using information technology."
(https://hr.wikipedia.org/wiki/Kiberneti%C4%8Dki_rat)

traffic. It plays a key role in global connectivity and the transport of passengers and cargo. However, technological advances contribute to increased system complexity, opening the door to various challenges and potential dangers. In the context of increasing interconnectedness and digitalization of the aviation sector, the risk of cyber threats in air traffic management systems is highlighted. (Prskalo, 2023: 123)

In addition to the above, there are psychological operations carried out in the special war during the cold war. The development of the Internet led to the creation of spiritual networks, which, among other things, opened up the possibility of conducting psychological operations in them, significantly more advanced compared to the previous ones. In the article Psychological operations on social networks – examples, techniques, tactics and procedures (Muhić, 2025), Emir Muhić investigated the transformation of warfare and security conflicts under the influence of modern technological achievements, with special emphasis on the role of social networks in conducting psychological operations. The article analyzes the techniques, tactics and procedures used to shape public opinion, manipulate perceptions and spread misinformation through digital communication channels. Through a detailed analysis of specific strategies applied on social networks, the security implications for national institutions and the democratic order are also discussed.

Based on the above, it can be concluded that the term hybrid war coincides with special war. Likewise, and that it has similarities with the other mentioned definitions of war, but that the greatest degree of agreement is with special war and has the same meaning. What are the reasons for the affirmation and indisputable primacy of the term hybrid war? The initial reason should be sought in the domain of ideology and politics.

The term has its own political dimension, especially since the tightening of relations between the USA, some European countries and Russia, and serves to alarm, primarily the Western public, through a semantically new term. It is difficult to get over the fact that the hybrid war experienced its redesigning of meaning and then its mass use and discussion exactly when the relations of the great powers intensified and reached almost the level they were at during the Cold War. This time, the USA and the European countries in NATO decided to use a different term." (Cvetković, Kovač and Joksimović, 2019: 328)

It is often emphasized that hybrid warfare is just a new term that softens the sonority of the old term special war, which was introduced into the military vocabulary and practice by the Americans during the Cold War. According to the Yugoslav Military Lexicon, "special war is a set of organized and coordinated political, diplomatic, economic, psychological-propaganda, intelligence-

subversive, terrorist, and often military actions and procedures." (Subotić:2018:29,30)

The affirmation of the hybrid war also led to a reconsideration, a critical reflection on whether it affects the redefinition of the concept of war. From the very beginning of the introduction of this term into theory and practice, there has been a debate about whether it is a new conceptual definition of war or whether it is just an evolved, perfected model of war in contemporary conditions that does not call into question the existing definition of war. There are debates in the academic public as to whether it is a new form of war that has been transformed in some aspects, or whether it is an old phenomenon enriched with a new term. (Ćurčić:2018:47)

Conditionally speaking, we can distinguish two phases of the development of the hybrid war concept. The first phase of the war, which lasted from the establishment of the hybrid war concept at the end of the 20th century until the Ukrainian crisis (Russian aggression against Ukraine). The second phase of the development of the hybrid war concept begins with the emergence of the Ukrainian crisis (Russian aggression against Ukraine) and the annexation of Crimea by Russia in 2014 and continues until today. Some authors call these two phases of development non-state-centered and state-centered approaches to the study of the concept of hybrid war, according to the determination of the actors who apply this type of war. (Ćurčić:2018:48)

Hybrid warfare is not a revolutionary approach because by studying history we can identify a large number of wars that contain elements of hybrid war. However, although the factors that define hybrid war are not new, but have mostly all been used before in some of the historical wars, the Russian hybrid model contains some previously unstudied aspects – great unpredictability and dynamism and flexibility in the application of various factors, the growing role of information, economic, energy and other aspects that in the modern hybrid model become almost equally (if not more) important compared to the classic military aspect. (Brzica, 2018:42)

By studying the available literature, it is clear that there is already a significant number of foreign theoreticians and military analysts who have discussed the concept of hybrid war in their internationally recognized books and articles, such as Frank Hoffman, Karber, McCulloh, Martin van Creveld, David Kilcullen, Janis Berzins and Robert Gates. In their works, using different approaches, they defined the key factors, prerequisites, stages of development and factors of hybrid war as an operational approach to achieve some goals that the theory of hybrid war does not say anything about. (Brzica, 2018:43)

There are a number of terms used for the hybrid warfare concept: hybrid warfare, hybrid threats, hybrid influence or hybrid adversary (as well as non-linear warfare, non-traditional warfare or special warfare). Military strategy often talks about the hybrid threat, while the academic literature talks about hybrid warfare." (Ahmić, Dautbegović and Korajlić, 2018:83)

If we use the largest (and often unfairly maligned) internet encyclopedia, Wikipedia, to determine its definition, we will see that hybrid warfare (which is also described as non-linear or special warfare) is a military strategy that combines conventional, irregular and cyber warfare. (Ahmić, Dautbegović and Korajlić, 2018:84)

Hybrid warfare (eng. Hybrid Warfare, abbreviated HW), or as the Russians call it "new generation warfare" (eng. New Generation Warfare, abbreviated NGW), is based on Sun Tzu's idea that the ultimate skill consists in crushing the opponent's resistance without fighting. It was on these foundations that the Russians started the war in Ukraine. (Brzica, 2018:44)

Given the complexity of the phenomenon, it is more difficult to give a concise definition and at the same time cover all aspects of hybrid war. In this sense, a narrower[43] and broader[44] definition of the term could serve as a solution. (Cvetković, Kovač and Joksimović, 2019: 339)

[43] "A narrower definition of the term could be the following: A hybrid war is a conflict between two or more states and/or organizations in which they use the political, economic, information and security elements of their power, to carry out unarmed and, if necessary, armed aggression, on the population and material resources of the opponent, in order to subjugate it to their interests and will." (Cvetković, Kovač and Joksimović, 2019: 339)

[44] "A broader definition of a hybrid war could be the following: A hybrid war represents a multidimensional conflict involving one or more states and/or organizations formed on political, ideological, national or religious grounds, in which at least one side, from a strategically centralized level, synchronized, adaptive, covert or public, within the framework of unarmed and armed aggression, conducts informational-psychological-ideological, political, economic, intelligence-subversive, IT, criminal, terrorist and military activities, affecting the physical and mental resources, social relations, values and interests of the adversary, and in order to force them to act in accordance with their political, economic and military goals and interests." (Cvetković, Kovač and Joksimović, 2019: 340)

3. Conceptual-doctrinal determination od hybrid war

To understand the concept of hybrid war, it is of utmost importance to consider its definition in the conceptual and doctrinal documents of NATO and the EU. As is known, they contain the operationalization of the postulates of the highest level of decision-making of NATO and the EU in the field of defense and security, which determine the manner of using the defense and security system. These documents define the fundamental principles of the concept, doctrine and strategy of defense and security of NATO and the EU. They are also the starting points for the adoption of conceptual and doctrinal documents, which are often called strategic, by the member states of these organizations. In addition, they also influence the questioning of the positions of these documents by the most important rivals of NATO and the EU – Russia and China.

The Strategic Concept adopted by the heads of state and government at the NATO summit in Madrid on June 29, 2022, represents the initial conceptual and doctrinal document of the NATO pact. It replaced the previous Strategic Concept from 2010. The new concept represents the fundamental postulates of action so that NATO "remains ready and equipped with resources for the future." (Introductory part of the Strategic Concept) The military-political changes that have occurred in international relations have necessitated, among other things, the need to adopt a new Strategic Concept. The new concept contains positions on the NATO alliance's response to numerous threats, including hybrid threats.

"The Strategic Concept is a key document for the Alliance. It reaffirms NATO's values and purpose and provides a common assessment of the security environment. It also drives NATO's strategic adaptation and guides its future political and military development. The Strategic Concept is regularly reviewed and updated. Since the end of the Cold War, it has been updated approximately every 10 years to take account of changes in the global security environment and to ensure that the Alliance is future-proof. The previous Strategic Concept was adopted at the NATO Summit in Lisbon in 2010. The new Strategic Concept describes the new security reality facing the Alliance, reaffirms NATO's values and states NATO's core purpose of ensuring the collective defence of its Allies."[45]

The new Strategic Concept considers the issue of hybrid war quite comprehensively. Analysis of the content of the new concept indicates that this

[45] https://www.nato.int/strategic-concept/

issue is considered in several points of this document. Part of the Strategic Environment chapter in points 7, 8 and 13 refers to hybrid means and methods implemented by NATO's strategic competitors. Point 7 does not specify which strategic competitors they are, they are specified in points 8 and 13. In point 27 of the Deterrence and Defense subchapter of the Basic Tasks of NATO, the importance of hybrid war is emphasized the most. Item 43 of the Cooperative Security subchapter of the NATO Core Tasks chapter considers the NATO-EU partnership in countering cyber and hybrid threats and addressing the systemic challenges posed by the PRC to Euro-Atlantic security.

Point 7 emphasizes that strategic competitors "Interfere with our democratic processes and institutions and target the security of our citizens through hybrid tactics, directly and through intermediaries."

Point 8 specifies the strategic competitor. "The Russian Federation is the most significant and direct threat to the security of allies and peace and stability in the Euro-Atlantic area."It is clearly indicated that she (the Russian Federation) "uses conventional, cyber and hybrid means against us and our partners." It can be seen that cyber assets are not classified as hybrid assets, that they are of the same rank. The question arises whether such an approach contradicts the accepted theoretical provisions - definitions according to which cyber action is a component of hybrid war?

Point 13 clearly expresses concern from the actions of another strategic competitor - the PRC (People's Republic of China). "The PRC's malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target Allies and harm the security of the Alliance." And at this point, it is observed that hybrid and cyber operations are of the same level of importance. Point 15 emphasizes that "Cyberspace is contested at all times. Malicious actors seek to degrade our critical infrastructure, disrupt our government services, extract intelligence, steal intellectual property, and disrupt our military activities." The extent to which the importance of cyberspace is given is best seen in point 25. It states that "A single or cumulative set of malicious cyber activities; or hostile operations towards, from or within outer space; may rise to the level of an armed attack and may lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty."

As already mentioned in point 27, the importance of hybrid war is emphasized the most. It emphasizes that NATO will invest in its own capabilities to prepare, deter and defend against hybrid tactics by states and non-state actors. In addition, the provision that: "Hybrid operations against allies may reach the level of an armed attack and put the North Atlantic Council in a situation to invoke Article 5 of the North Atlantic Treaty" is particularly important. It unequivocally clearly

determines that hybrid operations can lead to the activation of the article of the North Atlantic Treaty, which stipulates that an armed attack on one or more members is considered an attack on all, the entire Alliance. This provision, as well as the aforementioned attacks from point 25, among other things, implies the need to redefine the previous definition of an armed attack. Likewise, the need for a broader, more complex understanding of Article 5 of the North Atlantic Treaty.

Point 43 highlights the importance of the NATO-EU partnership and the improvement of its strategy. It is emphasized that the NATO-EU strategic partnership creates the conditions for more effective "countering cyber and hybrid threats."

The importance of the NATO-EU strategic partnership is also highlighted by the Strategic Compass for Security and Defence - for a European Union that protects its citizens, values and interests and contributes to international peace and security (hereinafter referred to as the EU Strategic Compass), the EU's initial conceptual and doctrinal document in the field of defence and security. The introduction emphasises that the Strategic Compass sets out new actions and means that enable, among other things, "deepening cooperation with partners, in particular with the UN and NATO, in order to achieve common goals." This document has the same meaning for the EU as the Strategic Concept has for NATO. It sets out a plan for strengthening the EU's security and defence policy until 2030. "With this Strategic Compass, we set out a common strategic vision for the EU's security and defence policy for the next five to ten years and will begin its implementation immediately." (introduction) It is the EU's first comprehensive conceptual and doctrinal document. "With this Strategic Compass, we set out a common strategic vision for the EU's security and defence policy for the next five to ten years and will begin its implementation immediately." (Introduction to the Strategic Compass)

"The first version of the Strategic Compass was presented by the High Representative in November 2021, based on a first threat analysis contributed by the intelligence services of the 27 EU Member States and a phase of structured dialogue between EU Member States, EU institutions and experts. Subsequent versions were discussed in February and March 2022 to take into account the discussion of Member States and the Commission's defence and space package of 15 February, as well as the latest international developments, in particular

Russia's military aggression against Ukraine. It directly contributes to the implementation of the Versailles agenda."[46]

[46]https://www.consilium.europa.eu/hr/press/press-releases/2022/03/21/a-strategic-compass-for-

The introductory part of the European Compass Executive Summary emphasizes – "Hybrid threats are becoming more frequent, with increasing impact." Point 5 of the Executive Summary states that "an EU toolbox for defence against hybrid threats will be created that brings together different instruments to detect and respond to a wide range of hybrid threats."

In connection with cyber threats, they are distinguished from hybrid ones, as in the Strategic Concept of NATO. Point 6 of the Summary states that the EU will "further develop the EU cyber defense policy framework so that we are better prepared and respond to cyber attacks."

In the sub-chapter The Return of Power Politics in a Multipolar World in Conflict of the first chapter The World We Face in the European Compass it is emphasized that "The armed aggression against Ukraine demonstrates a willingness to use the highest level of military force, regardless of legal or humanitarian reasons, in combination with hybrid tactics, cyber attacks and information manipulation and interference abroad, economic and energy coercion and aggressive nuclear rhetoric." The danger of Russia's hybrid actions is also recognized in the sub-chapter of the same chapter - Our Strategic Environment "The impact of the sharply deteriorating relationship with the Russian government is particularly serious in many of these areas. It is actively interfering using hybrid tactics, thereby jeopardizing the stability of countries and their democratic processes."

The aforementioned sub-chapter of the first chapter of the Strategic Compass also mentions the rivalry with China. "China is a partner for cooperation, an economic competitor, and a systemic rival." "It works to achieve its policies, including through an increasing presence at sea and in space, and through the use of cyber tools and the application of hybrid tactics."

In the subsection New and transnational threats and challenges of the first chapter, it is clearly indicated that "State and non-state actors use hybrid strategies, cyber attacks, disinformation campaigns, direct interference in our elections and political processes, economic coercion and instrumentalization of illegal migration flows." This provision is particularly significant because it emphasizes that hybrid strategies can be implemented by non-state actors in addition to state actors.

Part of the sub-chapter Joint action of the second chapter Action refers to the role and significance of civil missions of the CSDP, to solve multiple security challenges, including hybrid threats. "With our civilian CSDP missions, we make

a-stronger-eu-security-and-defence-in-the-next-decade/

an important contribution to the rule of law, civil administration, policing and security sector reform in crisis areas. They are also crucial as part of the EU's broader response to security challenges driven by non-military means, including those related to illegal migration, hybrid threats, terrorism, organized crime, radicalization and violent extremism."

The quoted section indicates that hybrid threats are treated as part of security challenges driven by non-military means. Equating hybrid threats with illegal migration, terrorism, organized crime, radical and violent extremism is debatable. It is known in theory and practice that the spectrum of hybrid action can also include these mentioned threats. Also, that they can be carried out separately. For this reason, it would be more appropriate if they were listed in this context, both as independent and as part of hybrid threats. In addition, this quoted part also problematizes the question of whether hybrid threats from the "arsenal" of non-military means are really dominant. What about hybrid threats from the spectrum of military action? Are they of lesser importance? Potentiation of this dilemma can only exclude a more precise determination, in the quoted part, of hybrid threats as a component of non-military means.

In the introductory part of the third chapter, Security, it is emphasized that "We are increasingly facing hybrid threats." In the subchapter of the third chapter - Hybrid threats, cyber diplomacy and foreign manipulation of information and interference is the most important. It deals most directly with the issue of hybrid threats. It specifies that the EU will develop an EU toolkit for defense against hybrid threats and teams for a rapid hybrid response, thus unifying various instruments for detecting a wide range of hybrid threats and providing an adequate response to them.

The final part of the third chapter, Objectives, emphasizes the integration of tools for countering hybrid threats: “We will bring together our tools to better counter hybrid threats by developing a toolbox for defending against hybrid threats.” In addition, the timeframe for developing the toolbox for defending against hybrid threats is specified. “In 2022, we will develop an EU toolbox for defending against hybrid threats, which should provide a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States, covering, for example, preventive and cooperative measures, stability, containment and recovery, and supporting solidarity and mutual assistance.” Among other things, it states that: “The EU Handbook for Countering Hybrid Threats will also be reviewed.”

Chapter 5 Partners - Multilateral and regional partners is dedicated to the EU-NATO partnership. “The EU-NATO strategic partnership is essential for our Euro-Atlantic security, as demonstrated once again in the context of Russia’s

military aggression against Ukraine in 2022. The EU remains fully committed to further strengthening this crucial partnership and to fostering the transatlantic bond." At the end of the chapter, in the Objectives section, it states: "We will work with partners to counter hybrid threats, disinformation and cyberattacks. Our approach will also be focused on partners' needs for capacity building and support."

A brief analysis of the content of the provisions on hybrid warfare in the initial conceptual and doctrinal documents of NATO and the EU, the Strategic Concept of NATO and the Strategic Compass indicates their compatibility. These two documents are congruent in their view of hybrid warfare. In relation to the definition of the content of hybrid war, as indicated in the analysis, in both documents cyber action is not treated as part of hybrid action. This is in contrast to the theoretical definitions of hybrid war, in which action in the cyber domain is an essential component of its definition. Because of this, the question arises: will these two documents lead to a theoretical redefinition of the concept of hybrid war or will there be a revision of their content?

4. RUSSIAN HYBRID ACTION IN PREPARING AND CARRYING OUT CONTINUED AGGRESSION AGAINST UKRAINE

Russia's aggression against Ukraine has raised a number of military-political issues that include the consideration of their economic dimensions. In the same way, this aggression (which is often called an invasion in the media) carried out by Russia on February 24, 2022, also actualizes numerous other issues, among which the consideration of the starting point of the decision for its initiation is of particular importance. This aggression, as is known, is only a continuation of the war that started in 2014 and which resulted in the Russian annexation of Crimea and the occupation of the eastern part of Ukraine and the creation of two self-proclaimed so-called of the people's republics of Donetsk and Luhansk.

The question arises as to what assessments Russia based its decision to continue its aggression against Ukraine at the end of February 2022, which is open, undisguised, unlike the one carried out in 2014, which it tried to cover up.

Close historical facts point to the unreasonableness of the current Russian policy to start a war that can escalate into a world war. The relations between the economic, military and demographic potential of Russia and the EU and NATO more than clearly indicate the supremacy of the West. This parity is only relatively balanced in relation to the potential of weapons of mass destruction (nuclear, chemical and biological). However, it cannot be the starting point for understanding Russian policy for continuing aggression against Ukraine and risking the escalation of the war. It would be a complete banalization and

trivialization of this complex issue to reduce the understanding of Russia's aggressive policy to reliance on the power of its weapons of mass destruction, above all nuclear, which is emphasized the most. Answering that initial question: What are the starting points for Russia's decision to dare to continue aggression in 2022 against Ukraine, which includes the real risk of war escalation and political-economic confrontation with the West? How is it possible that Russia dared to pursue such a policy of confrontation with the West that leads it to defeat? Is this a mistake in Russian strategic thinking?

The answer to this question is extremely complex, involving consideration of military, political and economic components. From a military perspective, it is known that every country, including Russia in this case, tries to assess its advantages over its opponent before starting a war.

The possible reasons for making this decision most likely originate in the continuously created euphoria due to the successful results of implementing imperial policy and the created projection of military-political power.[47] This issue is not the subject of this article. Besides, it goes beyond the scope of the article.

In addition to the mentioned continuity of success of the military engagement, which undoubtedly had a starting point for the adoption of the Russian decision to continue the aggression against Ukraine, the results achieved in the so-called hybrid action. Since 1991, Russia has been conducting relatively independent activities in the spectrum of hybrid threats. These activities represent the continuity of activities, the implementation of activities of the former USSR against the West. At that time, these activities were called special war.

[47] Already in the first years of its existence as an independent state after the collapse of the USSR, Russia managed to achieve its first successes. 1992 - de facto occupation of part of Moldova (about 17% of its territory) by creating the so-called Transnistria (Transnistrian Moldavian Republic). Upon independence, after the collapse of the USSR, Georgia was also left without its two regions of South Ossetia and Abkhazia. As in the case of Moldova, Russian aid was crucial for the creation of the so-called Republic of South Ossetia and the Republic of Abkhazia on the territory of Georgia. After that, there was a lull until the open Russian military action in 2008 in Georgia, which resulted in Russian recognition of the so-called Republic of South Ossetia and the Republic of Abkhazia. This was followed by the most ambitious undertaking – the contemplated aggression against Ukraine in 2014 and its continuation at the end of February 2022. In addition to these three aforementioned aggressions, Russia has repeatedly demonstrated its military power. The military intervention in Syria stands out in terms of significance and demonstrated brutality and destructiveness. The devastated Aleppo and thousands of killed civilians in Syria were, until the continuation of the aggression in Ukraine in 2022, the most credible evidence of the demonstration of the brutality of Russian military power. Russia has presented its military power in other ways as well. Among them, several examples can be singled out: Armenia, the territory of the former SFRY, Kazakhstan.

There are well-known examples of the intensive activities of the Soviet intelligence service KGB in conducting special warfare during the so-called Cold War. The successor of that service, the Russian FSB, based on these experiences of using KGB methods, managed to modernize and perfect them and, it must be admitted, achieve enviable results. The continuation of Russian aggression against Ukraine has exposed only some of the most significant ones. Among them, the most significant are the extent of political corruption, influence on electoral processes in several important European countries as a result of Russian subversive activities that influenced the direction of the policies of these countries. This is completely obvious in terms of creating energy dependence on imports of Russian gas, oil and coal. For example, Germany's dependence on imports of Russian gas amounts to 40%, Austria's as much as 80%, etc. It is more than clear that Germany, as the economically leading country in Europe, could have met its energy needs in other ways. It did not heed the American warnings about the dangers of pursuing that policy, and contrary to them, it built Nord Stream 2 with Russia, which was supposed to increase even more the percentage of German dependence on Russian gas. It is known that the continuation of Russian aggression against Ukraine made it impossible to realize that plan. It is also known that this continuation of Russian aggression led to a turnaround in German policy towards Russia.

The examples of successful Russian military engagement mentioned in footnote 16, as well as the achieved results of hybrid action, were the foundations for creating the belief that the continuation of the aggression against Ukraine would be another successful military engagement that would "overshadow" everything that came before. Likewise, the starting point was that there would be no significant reaction from NATO and the EU, that it would be at a similar level as before. In doing so, Russian planners also counted on the previous disagreement of positions within NATO and the EU itself, as well as between the EU and the USA and in the EU-NATO relationship regarding the implementation of policy towards Russia. The scale of the global crisis caused by the continuation of Russian aggression has stimulated completely opposite - integration processes. NATO cohesion has been strengthened and its role as the greatest guarantee of security, currently most of the European members of Eastern Europe from Russian threats, has been affirmed. The greatest evidence of this affirmation is the accession of Finland and Sweden to NATO, which, as is known, has not yet been formally and legally completed.

It is important to emphasize that the Russian hybrid activity is also based on the postulates of the theory. It is developed in Russia, it is not even a little behind compared to the West. The development of Russian theoretical thought about the phenomenon of hybrid war is noticeable. It evolved from the initial resistance of the Russian military establishment to the use of the new term. In Russian military

terminology, the phrase non-linear military strategy is accepted. The wars in Iraq and Libya, as well as the so-called Arab revolutions influenced Russian military circles to adopt the concept of non-linear warfare.

The Chief of the General Staff of the Russian Armed Forces, General Valery Gerasimov, is considered the author of the concept of total war, the Russian new generation of war, which is named after him the Gerasimov Doctrine. This concept is similar in many elements to the concept of hybrid war and, in a conditional sense, can be considered its Russian version. It was developed by General Gerasimov in 2013, after which he published a 2,000-page document entitled The Importance of Science in Forecasting, part of which was published by the Russian weekly "Military-Industrial Courier" (Gerasimov, 2013). The work sets out new rules for Russian military action. It is rightly believed that with the publication of this work – the so-called Gerasimov Doctrine, Russian military strategy is evolving into a new approach that emphasizes the use of non-military methods to achieve strategic and political goals.

"The importance of non-military means in achieving political and strategic goals has increased and often exceeds the power of weapons in effectiveness," General Gerasimov emphasized in his work in 2013. Overcoming the constraints of limited financial resources, Russia has managed to create a strategy of strengthening non-military methods that have proven to be almost as effective as military ones. There are also opinions that relativize this new doctrine. They are based on the point of view that it is a sum of concepts arising from the Soviet strategy enriched with elements of total war and a new theory about the specific conditions of warfare. Essentially, these views derive from the definition of hybrid war, including this doctrine, as an evolved, modernized concept of special war and Soviet strategy. This calls into question whether the so-called The Gerasiml doctrine is an innovative theoretical concept. But, despite that, it is affirmed in practice, as the most important criterion for the valorization of the theory. The success of Russian activities, among other things, based on this doctrine, indicates that this relativization is not objective.

Andrej Koribko, a Russian journalist and publicist, contributed significantly to the affirmation of the phrase hybrid war. He called the colored revolutions in countries such as Ukraine, Libya, Egypt, Syria, some of which have turned into armed conflicts of non-state armed formations against the official armed forces of those countries, as a hybrid war conducted by the USA and certain European countries. In his book "Hybrid Wars: An Indirect Adaptive Approach to Regime Change" (Korybko, 2015) he listed the elements of such a hybrid war as: diplomacy, computer attacks, economic warfare, information warfare and propaganda, support for local groups, irregular armed forces (terrorism), regular armed forces and special units.

Academician Igor Panarain made the greatest contribution to the Russian theoretical foundation of hybrid war. His capital work is the book Hybrid War: Theory and Practice.[48] In this book, the objectives, reference areas, timetables and types of hybrid war are defined, systematized and considered. In addition, it initiates the creation of an institution for the implementation of hybrid war methods. This idea is recognizable in the last, 23rd chapter of the book - The technology of Russia's victory, subchapter Hybrid war matrix, or Why do we need an informative General Staff? The operationalization of academician Panarin's theoretical reflections presented in this chapter is not surprising, given that he is also a coordinating expert of the Analytical Council, an important advisory body of the President of the Russian Federation. This book is, conditionally speaking, an extension of the author's ideas published in the previous work Hybrid War against Russia (1816-2016). Academician Panarin is the author of the book Hybrid War and Geopolitics, also a significant work that considers the geopolitical aspect of hybrid war. The scope of the article does not allow the presentation of the works of other Russian authors. Among them, the book A.A. Bartoš stands out - Gray Zone: Theater of Hybrid Warfare.[49]

5. Conclusion

Looking at the previous approaches to defining hybrid war is extremely important. Three approaches can be observed in the definition so far: first, that it is an evolved concept of special war, second, that this syntagm is consistent, similar to the concepts of low-intensity conflict, fourth generation war, complex war, asymmetric war, including special war, and third, that it is a new concept of war. The article affirms the first approach. It is argued that the term hybrid war is the same as special war. Likewise, and that it has similarities with the other mentioned definitions of war, but that the greatest degree of agreement is with special war and has the same meaning. The question is also open - what are the reasons for the affirmation and indisputable primacy of the term hybrid war? It was pointed out that the initial reason should be sought in the domain of ideology and politics.

This paper does not claim to affirm the chosen approach as a solution to defining hybrid war. Considering the complexity and significance of the discussed topic, the article aims to initiate a discussion on the three mentioned approaches and to

[48] The book was translated into Serbian and published in 2019 by the Military Bookstore in Belgrade.

[49] Aleksandar Aleksandrovič Bartoš is also the author of the significant monographs "Conflicts of the 21st Century. Hybrid War and Colored Revolution" and "The Fog of Hybrid War. Uncertainties and Risks of the 21st Century".

direct further more complete research that would result in the acceptance or rejection of the proposed approach to defining hybrid war.

In addition, the article also points out the importance of considering the relationship between the theoretical and conceptual-doctrinal determination of hybrid war. Accordingly, the content of the provisions on hybrid war in the initial conceptual and doctrinal documents of NATO and the EU, the Strategic Concept of NATO and the Strategic Compass was analyzed. It is argued that these two documents are congruent regarding the view of hybrid warfare. In relation to the definition of the content of hybrid war, as indicated in the analysis, in both documents cyber action is not treated as part of hybrid action. It was pointed out that this omission is in contradiction with the theoretical definitions of hybrid war in which action in the cyber domain is an essential component of its definition.

Among other things, the question whether the affirmation of the theory and practice of hybrid war implies the need to redefine the previous theoretical concept of war was brought up to date. Likewise, the practice of applying Russian hybrid action in the preparation and execution of aggression against Ukraine was considered. On this example, which can tentatively be called a mini-case study, significant experiences and lessons can be identified. Critical questioning of the Russian hybrid action on this example leads to the conclusion that the reach of the effect of the hybrid action should not be overestimated.

The significance of the issues raised for the development and profiling of the theory and practice of hybrid war is unquestionable. It can be concluded that the theoretical and practical goal of the article has been achieved. From the theoretical aspect, the elements that can contribute to defining the concept of hybrid war are given. The practical aspect is significant, it indicates, as already mentioned, that the reach of hybrid war methods in practice should not be overestimated. It also aims to encourage experts, practitioners in the field of defense and security to study the basic postulates of hybrid war so that they can follow the development of the theory and practice of its application with greater understanding.

LITERATURE:

Author's works

1. Akrap, G. (2012). Specijalni rat 3. Večernji list, Zagreb.
2. Ahić,J., Alishapić, B. (2019): Horizontalno i vertikalno hibridno djelovanje i/ili rat/ studija slučaja Bosne i Hercegovine, Kriminalističke teme, br. 5/2019, https://krimteme.fkn.unsa.ba/index.php/kt/article/view/221/218
3. Ahmić, E., Dautbegović, A. i Korajlić, N. (2018): Pojam i determinante hibridnog ratovanja, Zbornik radova 11. Međunarodna znanstveno-stručna konferencija „Dani kriznog upravljanja 2018“, Veleučilište Velika Gorica, 2018., str. 83-88, file:///C:/Users/Admin/Downloads/967749.DKU-Radovi-2018%20(1).pdf
4. Arnel P., D., Lt Col Dave, A., Dr Nesic, A. and Krohley, N. (2020): Why We Need A Modern Theory of Special Warfare to Thrive in the Human Domain, https://wavellroom.com/2020/05/14/why-we-need-a-modern-theory-of-special-warfare-to-thrive-in-the-human-domain/
5.Brzica, N. (2018): Hibridno ratovanje i suvremeni sukobi - doktorski rad, Fakultet političkih znanosti, Zagreb, 2018, https://www.fpzg.unizg.hr/_download/repository/hibridno_ratovanje_i_suvremeni_sukobi_brzica.pdf
6. Cvrtila, Ž. (2017): HIbridni rat suvremeni naziv za već poznate oblike ratovanja, Zaštita, br. 12/2017, https://www.bib.irb.hr/1086183
7. Cvetković, N., Kovač, M. i Joksimović, B. (2019): Pojam hibridnog rata, Vojno delo, br. 7/2019, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo411/vd-411-2019-71-7-24-Cvetkovic.pdf
8. Gerasimov, V. (2013): Vrijednost znanosti je u predviđanju: Novi izazovi zahtijevaju ponovno promišljanje oblika i metoda provedbe borbenih operacija. VoyennoPromyshlennyy Kurier (VPK) (Military-Industrial Courier). http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf
9. Hibridno ratovanje – dilema koncepta savremenih sukoba, Tematski zbornik radova, Institut za strategijska istraživanja, Beograd, 2018., http://www.isi.mod.gov.rs/multimedia/dodaci/hr_tematski_zbornik_2_1555574872.pdf
10. Korybko, A., Hybrid Wars (2015): The Indirect Adaptive Approach to Regime Change, People’s Friendship University of Russia, Moscow, http://resistir.info/livros/hybrid_wars_updated.pdf
11. Kolobara,R (2019): Hibridne prijetnje u 21. stoljeću – teorija i istraživanje nazivlja u Bosni i Hercegovini, National security and the future, br. 1-2/2019, https://hrcak.srce.hr/file/337151

12. Maher, A. (2016): An Australian doctrinal concept for Special Warfare: Lessons and ConsiderationsThe Australian Army Research Centre (AARC) , https://researchcentre.army.gov.au/library/occasional-papers/australian-doctrinal-concept-special-warfare-lessons-and-considerations
13. Muhić, E. (2025): Psihološke operacije na društvenim mrežama – primjeri, tehnike, taktike i procedure, Zaštita i sigurnost, godina 5., broj 1/2025, 129-164 https://zisjournal.com/psiholoske-operacije-na-drustvenim-mrezama-primjeri-tehnike-taktike-i-procedure/
14. Mandić,I. (2016):Definiranje rata za 21. stoljeće, Polemos, br. 37/2016, https://hrcak.srce.hr/file/250352
15. Milošević, M., D. (2018): Pojmovno određenje fenomena hibridnog ratovanja, Vojno delo, br. 3/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo399/vd-399-2018-70-3-20-Milosevic.pdf
16. Milošević, M., D. (2018): Percepcija savremenih oružanih sukoba kao indikatora hibridnog koncepta rata, modeli prevencije i suprotstavljanja hibridnim pretnjama, Vojno delo, br. 5/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo401/vd-401-2018-70-5-19-Milosevic.pdf
17. Milenković, R., M. i Mitrović, M. (2019): Obojene revolucije u paradigmi hibridnog rata, Vojno delo, br. 6/2019, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo410/vd-410-2019-71-6-17-Milenkovic.pdf
18. Madden,D.,Hoffmann,D., Johnson, Krawchuk, T.,F., Nardulli,R.,B., Peters,E.,J., Robinson, L., Doll, A.: Toward Operational Art in Special Warfare - file:///C:/Users/Admin/Downloads/RAND_RR779%20(1).pdf
19. Pejić, I. (2019): Ruske vojne hibridne operacije u Ukrajini: prilagođavanje strategije i taktike savremenoj strukturi rata, Međunarodni problemi, br. 4/2019 (str. 423-446), http://www.doiserbia.nb.rs/img/doi/0025-8555/2019/0025-85551904423P.pdf
20. Prskalo, M. (2023.): *Suvremeni kibernetički rizici u upravljanju zračnim prometom*, Zaštita i sigurnost, godina 3., broj 2/2023, 132-143 https://zisjournal-com-647393.hostingersite.com/wp-content/uploads/2024/06/Godina_3.Broj_2.pdf
21. Petrović, R., J. (2021): Psihološki rat i vojne nauke, Baština, Priština-leposavić, sv. 55, 2021., https://scindeks-clanci.ceon.rs/data/pdf/0353-9008/2021/0353-90082155267P.pdf
22. Rančić, I. i Beriša, H. (2018): Hibridni rat – mit ili stvarnost (Rekonceptualizacija hibridnog rata), Vojno delo, br. 5/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo401/vd-401-2018-70-5-18-Rancic.pdf
23. Saković, R. i Terzić, R., M. (2018): Upotreba društvenih mreža u hibridnom ratovanju, Vojno delo, br. 7/2018,

http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo403/vd-403-2018-70-7-21-Sakovic.pdf
24. Vračar, S., M. (2017): Razmatranje adekvatnog teorijsko- -epistemološkog pristupa u istraživanju fenomena hibridnog ratovanja, Vojno delo, br. 7/2017, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo395/vd-395-2017-69-7-20-Vracar.pdf
23. Vuković,N. (2021): Konceptualizacija fenomena rata u savremenoj ruskoj vojnoj misli – doprinos generala Gerasimova, Međunarodni problemi, br. 2/2021 (str. 259-283), http://www.doiserbia.nb.rs/img/doi/0025-8555/2021/0025-85552102259V.pdf
25. Vračar, S.,M. i Tikhova, V.,V.(2018): Diskurzivni pristup fenomenu „hibridnog ratovanja“, Vojno delo, br. 3/2018, http://www.vojnodelo.mod.gov.rs/pdf_clanci/vojnodelo399/vd-399-2018-70-3-21-Vracar.pdf

Documents

1. Military Doctrine of the Russian Federation", 2014, https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf
2. Rezolucija Europskog parlamenta od 17. veljače 2022. o provedbi zajedničke sigurnosne i obrambene politike – godišnje izvješće za 2021. (2021/2183(INI)), 17. veljače 2022. – Strasbourg, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0040_HR.pdf
3. Strateški koncept, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
4. Strateški kompas za sigurnost i obranu - za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru i sigurnosti, Vijeće Europske unije, Bruxelles, 21. ožujka 2022., https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/hr/pdf
5. Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije, Visoki predstavnik unije za vanjske poslove i sigurnosnu politiku, Bruxelles, 06.04.2016., https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX:52016JC0018

Internet sources:

1. Hibrid - https://hr.wikipedia.org/wiki/Hibrid
2. Hibrid https://hr.wiktionary.org/wiki/hibrid
3. Hibridi https://www.enciklopedija.hr/natuknica.aspx?ID=25351
4. Hibridni rat https://hr.wikipedia.org/wiki/Hibridni_rat
5. Hibridni rat - https://ru.wikipedia.org/wiki/Гибридная_война

6. Prijevod 'hibridni rat' https://hr.glosbe.com/hr/en/Hibridni%20rat
7. Specijanje operacije - https://ru.wikipedia.org/wiki/Специальные_операции
8. Specijalni rat - https://sh.wikipedia.org/wiki/Specijalni_rat
9. Specijalni rat - https://www.enciklopedija.hr/natuknica.aspx?ID=57361
10. Special operations warfare - https://www.britannica.com/topic/special-operations-warfare11. Special Warfare, https://www.dvidshub.net/publication/372/special-warfare

INFORMISANJE I IZVJEŠTAVANJE U POLICIJSKIM AGENCIJAMA

DOI: *10.70329/2744-2403.2025.5.10.6*

Naučni članak

Doc. dr. Zoran Kovačević[50]
Doc. dr. Zoran Lakić[51]

Sažetak:

Izvještaji predstavljaju kompleksno izlaganje i prikaz rezultata i informacija analitičkog sagledavanja stanja bezbjednosti, pojava i događaja, preduzetih mjera i radnji, odnosno stepena realizacije programskih i planskih dokumenata iz rada službe.Pripadnici unutrašnjih poslova i rukovodioci nižeg nivoa imaju obavezu da predpostavljenog starješinu ili lice koje on ovlasti izvještavaju o događajima, pojavama, podacima i operativnim saznanjima, preduzetim mjerama i radnjama, ostvarenim rezultatima i postignutim efektima u obavljanju poslova iz svoje nadležnosti. U ovom radu obrađena je tema izvještavanja u policijskim agencijama, gdje su definisani pojam, ciljevi, vrste informisanja, izvori saznanja za krivična djela, na osnovu čega je izveden zaključak. U sklopu Informacije o stanju bezbjednosti u Bosni i Hercegovini za 2022. godinu koja je sačinjena u skladu sa Programom rada Ministarstva bezbjednosti BiH za 2023. godinu, te na osnovu raspoloživih podataka policijskih agencija BiH i u BiH i drugih nadležnih institucija, dostavljeni su statistički podaci o stanju opšteg kriminaliteta za pomenuti period kroz sistem informisanja i izvještavanja.

[50] Visoka poslovno tehnička škola Doboj. e-mail: zoran.kovacevic@dkpt.gov.ba
[51] Viktoria Internacionalni Univerzitet Mostar. e-mail: e-mail: zoran.lakic@viu.ba

Ključne riječi: *Izvještaj, informisanje, kriminalitet.*

1. Informisanje

1.1 Pojam, ciljevi i uslovi za informisanje

Informisanje predstavlja završnu funkciju u ciklusu procesa rukovođenja. To je komponenta kojoj rukovodni radnici moraju posvećivati punu pažnju. Zbog propusta na ovom planu, koji se najčešće odnosi na neblagovremeno informisanje, njihov rad se često ocjenjuje negativno, bez obzira na to koliko su im dobri operativni i drugi rezultati. Produkt takvog ponašanja je, nažalost, nedovoljno shvatanje značaja informisanja u procesu donošenja odluka, nemarnost, neposjedovanje adekvatne i ispravne tehnike za prenos informacija i drugi razlozi. Pod informisanjem se podrazumijeva razmjena obavještenja. Ta razmjena može se vršiti između subjekata u okviru jedne organizacione jedinice ili između te organizacije i njenog okruženja. Unutrašnji poslovi su poslovi državne bezbjednosti, poslovi javne bezbjednosti i drugi unutrašnji poslovi. (Talijan, M, 2001).

Osnovni ciljevi informisanja u organima unutrašnjih poslova su: da se blagovremeno otkrivaju, prate kriminalne i druge socijalno-patološke djelatnosti, da se na vrijeme, potpuno i tačno informišu sve organizacione jedinice i njihovi radnici o bezbjednosnim pojavama i događajima ugrožavanja, kako bi se blagovremeno mogle preduzeti mjere za njihovo suzbijanje, da se obezbjedi pravovremena i sadržajna informisanost nadležnih političkih subjekata, državnih organa, pravnih lica i građana, radi preduzimanja adekvatnih mjera iz njihove nadležnosti, koje mogu pozitivno uticati na jačanje opšteg stanja bezbjednosti. Sastavni dijelovi bezbjednosnih informacija su bezbjednosni podaci. Pod bezbjednosnim podatkom podrazumijeva se saopštenje o činjenicama koje se odnosi na bezbjednosnu pojavu. Da bi ovi podaci bili u potpunosti upotrebljivi, oni moraju biti: provjereni blagovremeni i tačni. Iz samog cilja bezbjednosnog informisanja vidljivo je koliko je ono bitno, jer se na osnovu njega ponekad donose sudbinske odluke za jedan narod, čije posljedice mogu biti katastrofalne ukoliko informacije, odnosno podaci, ne ispunjavaju uslove iz prethodnog pasusa.

Takođe i prijetnje koje nisu stvarne često nemaju dovoljno konkretnih informacija, što usmjerava bezbjednosne resurse u pogrešnom pravcu (Lakić, Kovačević, 2025). Da bi cjelokupni bezbjednosno-informacioni sistem agencija za sprovođenje zakona u BiH bio uspješan na području Bosne i Hercegovine, uslov je da mora biti jedinstven. To podrazumijeva: da se prikupljanje, selekcija, odnosno klasifikacija, obrada, terminologija, prezentovanje i korišćenje podataka

mora vršiti po jedinstvenog metodologiji, da su sve potrebne evidencije i obrasci utvrđeni po jedinstvenim principima, da se raspolaže jedinstvenim ili približno istim tehničkim sredstvima koja treba da obezbjede pohranjivanje podataka, brzo pronalaženje i davanje informacija iz baze podataka na korišćenje svim korisnicima sistema pod jednakim uslovima i da je bezbjednosni sistem informisanja jedinstveno normativno regulisan.

Policijske strukture moraju voditi računa o tome da javnost nije samo zainteresovana za događaje koji su se zbili iz oblasti sigurnosti, nego i kako radi policija u rješavanju i rasvjetljavanju onih kriminalnih problema, za koje je javnost posebno zainteresovana, te mjesto i ulogu građana u cilju pružanja odgovarajuće pomoći. (Masleša, R, 1999).

1.2 Vrste informisanja

Cjelokupno informisanje u organima unutrašnjih poslova može se posmatrati prema dva osnova:

1. Prema subjektima, odnosno korisnicima, koje može biti: a) interno, koje se vrši u okviru Ministarstva, bez obzira na nivo i b) eksterno, koje se vrši prema državnim organima, pravnim licima i građanima izvan Ministarstva unutrašnjih poslova.
2. Prema hitnosti, odnosno načinu, koje može biti: hitno, tekuće, povremeno, statističko. a) Hitno izvještavanje Hitno izvještavanje obavlja se depešom ili na drugi pogodan način za teža krivična djela i bezbjednosne događaje od kojih mogu nastati teže posljedice po bezbjednost, na način kako je to predviđeno Instrukcijom MUP-a o hitnom, tekućem, povremenom i statističkom izvještavanju.

b) Tekuće izvještavanje Tekuće izvještavanje vrši se dostavljanjem pisanih informacija o jednom ili više bezbjednosnih događaja ili pojava, kao i o mjerama i aktivnostima koje su s tim u vezi preduzete.

c) Povremeno izvještavanje Povremeno izvještavanje obavlja se dostavljanjem povremenih analiza, informacija i izvještaja o događajima i pojavama po linijama rada (javni red i mir, saobraćaj i dr.).

d) Statističko izvještavanje Statističko izvještavanje u policiji vrši se dostavljanjem popunjenih i kontrolisanih podataka prema utvrđenim obrascima. Statistički obrasci dostavljaju se redovno i periodično za određene bezbjednosne događaje i pojave, odnosno aktivnosti policije. (Gaćeša, D, 1998).

2. Izvori saznanja za krivična djela organizovanog kriminala

Do informacije da je izvršeno neko krivično djelo iz oblasti organizovanog kriminaliteta, veoma je teško doći uopšte, a posebno kod onih kriminalnih djelatnosti iz oblasti privrednog i finansijskog kriminaliteta, krijumčarenja i nedozvoljene trgovine, korupcije i pranja novca. Kada je riječ o organizovanom nasilničkom kriminalitetu i terorističkim aktivnostima, onda su posljedice krivičnih djela uglavnom vidne, pa se preduzimaju radnje i mjere s ciljem otkrivanja učinilaca. Zbog toga je veoma bitno da policija i drugi nadležni organi blagovremenom primjenom adekvatnih kriminalističko-taktičkih metoda usmjere svoju djelatnost na otkrivanje i razobličavanje svih oblika organizovanog kriminaliteta u onim oblastima gdje indicije ukazuju na vršenje takve kriminalne djelatnosti.

Takođe i ostale službe sigurnosti imaju važnu ulogu u očuvanju ustavnog poretka, zaštiti građana i borbi protiv savremenih prijetnji, uključujući terorizam, organizovani kriminal i druge oblike ugrožavanja javne sigurnosti (Nemanja, D, 2025). Otkrivanje ovih krivičnih djela zahtijeva složeniji i kvalitetniji pristup u odnosu na ona krivična djela koja vrše pojedinci ili neorganizovane kriminalne grupe, jer treba identifikovati kriminalnu organizaciju, njene veze i uporišta i u daljem postupku otkriti učinioca i obezbijediti dokaze. Uspješna aktivnost policije i drugih nadležnih organa u otkrivanju ovih krivičnih djela prevashodno podrazumijeva i odgovarajući nivo poznavanja suštine organizovanog kriminaliteta, budući da se organizovana kriminalna djelatnost upravo i konkretizuje kroz određena krivična djela privrednog, opšteg, ekološkog i političkog kriminaliteta. Zbog toga metodika otkrivanja krivičnih djela organizovanog kriminaliteta ima određene specifičnosti koje proizlaze iz nužnosti prilagođavanja postojećih kriminalističkih metoda svim bitnim karakteristikama ovih vidova organizovane kriminalne djelatnosti, odnosno svojstvima konkretnih krivičnih djela, kako bi se lakše došlo do saznanja o njihovom izvršenju.

U prvoj fazi otkrivanja, naročito ako je kriminalna organizacija uspostavila određenu vezu sa državnim, političkim i drugim organima, teško je od bilo kojeg izvora sa sigurnošću očekivati da ukaže na postojanje svih elemenata organizovanog kriminaliteta. Čim postoje indicije, organ unutrašnjih poslova, odnosno policija, treba odmah, kroz vidove svoje operativne djelatnosti, nastojati da dođe do svih bitnih saznanja koja kazuju da je izvršeno neko od ovih krivičnih djela. U tom smislu bitno je pratiti i otkrivati i ostalu kriminalnu djelatnost, naročito one oblike kriminaliteta za koje postoji sumnja da će se u daljem razvoju kretati ka organizovanom kriminalitetu, u koju svrhu je potrebno vršiti i odgovarajuću analizu otkrivenih krivičnih djela. Posebnu teškoću u otkrivanju

predstavljaju ona krivična djela organizovanog kriminaliteta gdje je već uspostavljena veza sa organima vlasti, državnim, političkim i drugim organima, jer se informacije dobro čuvaju, s obzirom na obostranu opasnost od krivičnog progona svih učesnika u lancu organizovane kriminalne djelatnosti. U postupku obezbeđenja dokaznog materijala od izuzetnog značaja su materijalni dokazi, s obzirom na to da su lični dokazi dosta rijetki i nepouzdani. (Kovačević, Z, 2017). Imajući u vidu sve rečeno, osnovni izvor saznanja za izvršena krivična djela organizovanog kriminaliteta jeste operativna djelatnost organa unutrašnjih poslova, odnosno policije. Pri otkrivanju ovih krivičnih djela informacije se ne mogu uspješno prikupiti samo na osnovu klasičnih izvora saznanja o izvršenom krivičnom djelu, već se moraju koristiti i specijalne istražne tehnike i drugi dozvoljeni, prethodno navedeni kriminalistički metodi.

Kriminalistička djelatnost treba da bude usmjerena i na kontrolu grupa i bandi koje su na putu da se razviju u organizovani kriminalitet. Pri otkrivanju ovih krivičnih djela policija primjenjuje kriminalističko-taktičke i kriminalističko-tehničke radnje i mjere kao i kod drugih krivičnih djela, i to: prikupljanjem prethodnih obavještenja, vođenjem informativnog razgovora, praćenjem, osmatranjem, provjerom, pregledom, uvidom u određenu dokumentaciju, provjerom alibija, utvrđivanjem identiteta, potražnom djelatnošću, kontrolom određenih kategorija lica, objekata i punktova, hemijskim klopkama, poligrafskim testiranjem i slično. Za uspješno otkrivanje krivičnih djela organizovanog kriminaliteta nužna je primjena drugih metoda koji su namjenski predviđeni za otkrivanje ovih krivičnih djela, kao što su specijalne istražne tehnike, kontrolisana isporuka, sklapanje simulovanih pravnih poslova, prikriveni istražitelj i svjedok saradnik. Međutim, s istim ciljem policija treba da koristi i posebne operativne metode, kao što su operativne veze, čije informacije, iako imaju isključivo operativni karakter, predstavljaju značajan doprinos i relevantne indicije za dalji operativni rad na otkrivanju konkretnog krivičnog djela.

U određenim situacijama pojedine radnje dokazivanja, kao što su pretresanje, privremeno oduzimanje predmeta, vještačenje i prepoznavanje, takođe mogu doprinijeti otkrivanju nekog od krivičnih djela iz organizovane kriminalne djelatnosti kao i njegovom daljem razjašnjavanju i dokazivanju. Do saznanja da je izvršeno neko od krivičnih djela organizovanog kriminaliteta policija može doći i u toku rada po kriminalističkoj obradi po nekom drugom krivičnom djelu, o čemu se obavještava nadležna jedinica koja preduzima adekvatne kriminalističke metode na daljem razjašnjavanju djela i otkrivanju učinilaca. Kao izvor saznanja mogu da posluže neke spoljne manifestacije, koje kao indicije mogu da ukažu na osnove sumnje da je bogatstvo nekih lica posljedica materijalne koristi od vršenja krivičnih djela organizovanog kriminaliteta.

Činjenica je da se jedan broj ljudi u našoj zemlji naglo obogatio što je promijenilo način njihovog života, a građane posebno iritiralo i kod njih stvorilo nezadovoljstvo i izazvalo sumnju u zakonit način sticanja tog bogatstva. Ovakve spoljne manifestacije mogu biti indicije, ali je bitno provjeriti i utvrditi da li su nastale bogaćenjem kroz kriminalnu djelatnost ili je ta imovina stečena na legalan način. Državni tužilac kroz svoja nova ovlašćenja, je mnogo više u situaciji da dođe do informacije o izvršenom nekom krivičnom djelu i da kriminalnu djelatnost policije usmjeri u pravcu otkrivanja i razjašnjavanja tog krivičnog djela, kao i cjelokupne kriminalne organizacije i posebno učinilaca krivičnog djela i da s tim ciljem preduzme odgovarajuće metode, prije svega radi obezbeđenja valjanih dokaza. Ostali organi nadležni za suzbijanje organizovanog kriminaliteta, naročito carinski i inspekcijski organi, takođe kroz svoju djelatnost mogu doći do saznanja da je izvršeno neko od ovih krivičnih djela i da u saradnji sa tužiocem i policijom preduzmu mjere na njegovom potpunom otkrivanju i utvrđivanju svih drugih bitnih činjenica. Ova saradnja je posebno značajna kada postoji sumnja da je kriminalna organizacija već uspostavila veze sa državnim i drugim relevantnim organima i time sebi obezbijedila odgovarajuću zaštitu, jer je policija, s obzirom na svoju stručnost i ovlašćenja u primjeni specijalnih metoda, najkompetentnija da utvrđuje i dokazuje postojanje jedne takve kriminalne sprege. U policijskoj organizaciji autoritet i odgovornost, a u skladu s visokim stupnjem formalizacije organizacijske strukture, normativno su formalizirani podzakonskim pravnim aktom (Krešimir, V, Slobodan, J, 2022).

Ostali izvori saznanja koji se pojavljuju kod drugih krivičnih djela, manje su izraženi kada je u pitanju otkrivanje krivičnih djela organizovanog kriminaliteta, što je i razumljivo s obzirom na sve prethodno iznete karakteristike ovih organizovanih oblika kriminalne djelatnosti. Međutim, ipak ne treba zapostaviti i značaj sredstava javnog informisanja, prijave preduzeća, organizacija, i nekih drugih pravnih lica, kao i anonimne i pseudonimne prijave, pri čemu ne treba apsolutno zapostaviti ni doprinos javnih pogovaranja. Dobijene informacije od navedenih subjekata mogu da ukažu na sumnju o postojanju pojedinih oblika organizovanog kriminaliteta u određenim sredinama, pa ih je potrebno stručno i adekvatnim kriminalističkim metodama provjeriti. Prijave građana takođe mogu biti izvor saznanja za izvršeno krivično djelo organizovanog kriminaliteta, ali se ono rijetko pojavljuje kada su u pitanju ovi vidovi kriminalne djelatnosti. To je i razumljivo jer građani teško dolaze do relevantnih saznanja o organizovanoj kriminalnoj djelatnosti, a ako raspolažu sa nekom informacijom, teško se odlučuju za neposredno prijavljivanje, upravo od straha da se u kasnijoj fazi krivičnog postupka pojave kao svjedoci, imajući u vidu poznate načine osvete i odmazde organizovanog kriminaliteta prema takvim licima i članovima njihove porodice. Logično se može pretpostaviti da će korišćenjem nove zakonske mjere zaštite svjedoka, do većeg izražaja doći i uloga građana kao izvor saznanja pri

otkrivanju i dokazivanju organizovanog kriminaliteta, i kao svjedoka u krivičnom postupku u predmetima po krivičnim djelima iz ove oblasti. (Bošković, M, 2003).

3. Analiza imovinskih delikata za 2022. godinu

Iz Informacije o stanju sigurnosti u Bosni i Hercegovini za 2022. godinu, vidljivo je da su imovinski delikti i dalje najzastupljeniji oblik opšteg kriminaliteta. Na osnovu podataka Ministarstva unutrašnjih poslova Republike Srpske broj evidentiranih krivičnih djela opšteg kriminaliteta (5.748 KD) je u padu za 2,9% u odnosu na uporednu godinu.

Tabela br.1. Statistički pokazatelji imovinskih delikata[52]

r.b..	Opšti kriminalitet	2022.	2021.	+ - %
1.	**Br evidentiranih KD opšteg kriminaliteta**	**5.748**	**5.922**	-2,9
1.1.	Broj krivičnih djela po poznatom počiniocu	3.113	2.927	6,4
1.2.	Broj krivičnih djela po NN počiniocu	2.635	2.995	-12,0
2.	Broj podnesenih izvještaja tužilaštvu	5.061	5.100	-0,8
3.	**Broj prijavljenih lica**	5.425	5.212	4,1
	- maloljetnici	153	142	7,7
	- povratnici	1.509	1.681	-10,2
4.	Broj rasvijetljenih KD po NN	1.920	2.227	-13,8
4.1.	od počinjenih u toku godine	1.789	2.063	-13,3
4.2.	iz prethodnih godina	131	164	-20,1
5.	Pričinjena materijalna šteta u KM	9.760.782	8.602.555	13,5
	Koeficijent ukupne rasvijetljenosti (%)	**85,6**	**84,7**	
	Koeficijent rasvijetljenosti po NN (%)	**69,4**	**70,5**	

Tužilaštvima je podneseno 5.061 izvještaja o počinjenim krivičnim djelima opšteg kriminaliteta (manje za 0,8%) i prijavljeno je 5.425 lica (više za 4,1%), od kojih su 153 maloljetnika i 1.509 povratnika. Broj maloljetnika je veći za 7,7%, a

[52] Informacija o stanju sigurnosti u Bosni i Hercegovini za 2022. godinu, Ministarstvo bezbjednosti BiH,
Sarajevo, 2023.

broj povratnika za 10,2% manji u odnosu na uporednu 2021. godinu. Od ukupnog broja počinjenih krivičnih djela opšteg kriminaliteta (5.748), policijski službenici su u 109 slučajeva lišili slobode počinioce u toku ili neposredno nakon izvršenog KD. Prema podacima Ministarstva unutrašnjih poslova Republike Srpske imovinska krivična djela (2.757 KD) su u padu za 10,4%. Od težih imovinskih KD smanjen je broj KD Teška krađa za 16,4%, dok je broj KD Razbojništava povećan 15 KD (ili za 71,4%). Broj KD u vezi sa otuđenjem vozila smanjen je za 17,9%. Koeficijent ukupne rasvijetljenosti KD u vezi sa otuđenjem motornih vozila iznosi 70,8%, a koeficijent po NN 67,4%.

4. Zaključak

Nakon sprovedenog istraživanja možemo reći da se putem djelatnosti izvještavanja i informisanja ostvaruje razmjena informacija kojima se daje «životna energija» sistemu unutrašnjih poslova kao ljudskim potrebama i tvorevinama. Imajući u vidu naprijed navedeno, a u cilju uspješnije borbe protiv krivičnih djela opšteg i organizovanog kriminaliteta, te stavljanja u funkciju određenih nedostataka čija će se funkcionalnost ubuduće dopunjavati i usavršavati, za početnu osnovu predlažem sljedeće okvirne smjernice rada:

- Sačiniti dijagram toka rasvjetljavanja krivičnog djela, radi preglednosti za postupanje u preduzimanju mjera i radnji i sa dijagramom obezbijediti sve dežurne službe u Policijskim upravama, odnosno policijskim stanicama.
- Da se dežurne službe policijskih stanica obezbjede tablicom pitanja, sačinjenom na osnovu devet zlatnih pitanja kriminalistike, za prikupljanje podataka prilikom zaprimanja prijave i prikupljanja podataka sa lica mjesta. Tablica pitanja da bi bila u funkciji treba biti pripremljena i na upotrebi u dežurnoj službi i da bude dovoljno iscrpna i tako sistematizovana da omogući da onaj koji prijavljuje događaj, odgovaranjem na postavljena pitanja daje što više podataka.
- Da se uspostavi brzi izlazak i postupanje na mjestu izvršenja krivičnog djela sa ciljem očuvanja nepromijenjenog stanja na licu mjesta, zaticanja očevidaca, pa i osumnjičenog, te da se uspostavi operativnost koja podrazumijeva dobru informisanost i vladanje situacijom (utvrditi da li se radi o krivičnom djelu i kakvom, slučaj - zades, prekršaj, disciplinska krivica, ili građansko-pravni delikt, ko je izvršilac, opis izvršioca u koliko je nepoznat, vrijeme izvršenja, na koji način je izvršeno, koja sredstva su upotrebljena za izvršenje, opis vozila ako je korišteno u izvršenju i udaljilo se sa lica mjesta, da li je bilo saučesnika i njihova uloga, zašto je krivično djelo izvršeno - motiv izvršenja, ako je koristoljublje - otuđeni predmeti i

opis, identitet žrtve ili oštećenog i koji objekat je napadnut), i to u što kraćem vremenu prenositi dežurnoj službi, da bi se ti operativni podaci koristili u sprovođenju mjera i radnji na terenu radi hvatanja izvršilaca.

O značaju brzog izlaska na lice mjesta, nepromijenjenog stanja na licu mjesta, koji tragovi se na licu mjesta mogu pronaći i operativnost na licu mjesta, neophodno je kroz vidove radnih sastanaka podsjećati policajce.

- Da se dežurne službe policijskih stanica obezbjede topografskim kartama opština sa adekvatnom razmjerom, radi preglednosti terena i vladanja situacijom prilikom preduzimanja operativno-taktičkih mjera i radnji na terenu.
- Da se sagleda stanje opremljenosti policije sa vozilom koje se može koristiti za potjerom motorizovanih kriminalaca, radio i GPS uređajima i baterijskim lampama i da se iznađe način za snabdijevanje nedostataka, te isto da se izdejstvuje za operativne radnike koji rade u grupi po predmetima težih krivičnih djela.
- Da se održi sastanak na kojem će učestvovati radnici iz Odjeljenja kriminalističke policije, policijskih stanica, policijskih stanica za bezbjednost saobraćaja i Jedinice za podršku sa zadatkom iznošenja propusta u radu, dogovora i planiranja za postupanje u određenim situacijama, podjele i razrade konkretnih zadataka.
- Da se sačini plan angažovanja drugih agencija za sprovođenje zakona u BiH. Da se vrši blagovremeno raspisivanje potrage i objave.
- Da se koriste sredstva javnog informisanja za obavljanje dobro odmjerene informacije o izvršiocu koja daje široke mogućnosti da se javljanjem očevidaca događaja prikupe podaci o traženom izvršiocu i daje mogućnost svim dobronamjernim građanima da jave gdje se izvršilac nalazi.

Efikasan rad u obavljanju ovih akcija kao i blagovremenom izvještavanju ostavlja veoma povoljan utisak kod građana na rad policije i moć pravne države.

LITERATURA

1. Bošković, M. (2003). Transnacionalni organizovani kriminalitet. Beograd: Policijska akademija.
2. Gaćeša, D. (1998). Policija - nadležnost, organizacija, rukovođenje. Banja Luka: Glas Srpske.
3. Informacija o stanju sigurnosti u Bosni i Hercegovini za 2022. godinu, Ministarstvo bezbjednosti BiH, Sarajevo, 2023.
4. Masleša, R. (1999). Policija organizacija i funkcionisanje u demokratskom društvu. Sarajevo: Fakultet kriminalističkih nauka.
5. Kovačević, Z. (2017). Kriminalistički aspekti istraživanja nedozvoljene proizvodnje i prometa opojnim drogama u Bosni i Hercegovini. Banja Luka: Nezavisni univerzitet.
6. Talijan, M. (2001). Rukovođenje unutrašnjim poslovima. Beograd: Viša škola unutrašnjih poslova.
7. Zakona o zaštiti tajnih podataka (¨Službeni glasnik BiH¨ broj 54/05 i 12/09).
8. Zaštita i sigurnost, godina 5., broj 1. (2025).
9. Zaštita i sigurnost, godina 2., broj 2. (2022).

INFORMATION AND REPORTING IN POLICE AGENCIES

DOI: *10.70329/2744-2403.2025.5.10.6*

Scientific Article

Doc. dr. Zoran Kovačević[53]
Doc. dr. Zoran Lakić[54]

Abstract:

Reports represent a complex presentation and display of results and information from analytical examination of the security situation, phenomena and events, measures and actions taken, i.e., the degree of implementation of program and planning documents from the service's work. Members of internal affairs and lower-level managers have the obligation to report to their superior officer or person authorized by them about events, phenomena, data and operational findings, measures and actions taken, achieved results and effects accomplished in performing duties within their jurisdiction. This paper addresses the topic of reporting in police agencies, where the concept, objectives, types of information, sources of knowledge about criminal offenses are defined, based on which a conclusion is drawn. Within the framework of the Information on the Security Situation in Bosnia and Herzegovina for 2022, which was prepared in accordance with the Work Program of the Ministry of Security of BiH for 2023, and based on available data from police agencies in BiH and other competent institutions, statistical data on the state of general crime for the mentioned period were provided through the information and reporting system.

Keywords*: Report, information, crime.*

[53] Higher Business Technical School Doboj, email: zoran.kovacevic@dkpt.gov.ba
[54] Victoria International University Mostar, email: zoran.lakic@viu.ba

1. Information

1.1 Concept, Objectives and Conditions for Information

Information represents the final function in the cycle of the management process. It is a component to which management personnel must pay full attention. Due to shortcomings in this area, which most often relate to untimely information, their work is often evaluated negatively, regardless of how good their operational and other results are. The product of such behavior is, unfortunately, insufficient understanding of the importance of information in the decision-making process, negligence, lack of adequate and correct techniques for information transfer and other reasons. Information is understood as the exchange of notifications. This exchange can take place between subjects within one organizational unit or between that organization and its environment.

Internal affairs include state security affairs, public security affairs and other internal affairs (Talijan, M., 2001).

The basic objectives of information in internal affairs bodies are:

- to timely detect and monitor criminal and other socio-pathological activities,
- to inform all organizational units and their employees in a timely, complete and accurate manner about security phenomena and threatening events, so that measures for their suppression can be taken in a timely manner,
- to ensure timely and substantive information to competent political subjects, state bodies, legal entities and citizens, in order to take adequate measures within their jurisdiction, which can positively influence the strengthening of the overall security situation.

Integral parts of security information are security data. Security data is understood as a notification about facts relating to a security phenomenon. For this data to be fully usable, it must be:

- verified
- timely and
- accurate.

From the very purpose of security information, it is evident how important it is, because decisions that are sometimes fateful for a nation are made based on it, the

consequences of which can be catastrophic if the information, i.e., data, does not meet the conditions from the previous paragraph. Also, threats that are not real often lack sufficient concrete information, which directs security resources in the wrong direction (Lakić, Kovačević, 2025).

For the entire security-information system of law enforcement agencies in BiH to be successful in the territory of Bosnia and Herzegovina, the condition is that it must be unified. This implies:

- that the collection, selection, i.e., classification, processing, terminology, presentation and use of data must be carried out according to a unified methodology,
- that all necessary records and forms are determined according to uniform principles,
- that unified or approximately the same technical means are available that should ensure data storage, quick finding and providing information from the database for use by all system users under equal conditions and
- that the security information system is uniformly normatively regulated.

Police structures must take into account that the public is not only interested in events that have occurred in the field of security, but also how the police work in solving and clarifying those criminal problems for which the public is particularly interested, as well as the place and role of citizens in providing appropriate assistance (Masleša, R., 1999).

1.2. Types of information

All information in internal affairs bodies can be viewed according to two bases:
1. According to subjects, i.e., users, which can be:
a) internal, which is carried out within the Ministry, regardless of level and
b) external, which is carried out to state bodies, legal entities and citizens outside the Ministry of Internal Affairs.
2. According to urgency, i.e., method, which can be:

- urgent,
- current,
- periodic,
- statistical.

a) Urgent reporting
Urgent reporting is carried out by telegram or in another suitable manner for more serious criminal offenses and security events from which more serious

consequences for security may arise, in the manner prescribed by the MUP Instruction on urgent, current, periodic and statistical reporting.
b) Current reporting
Current reporting is carried out by submitting written information about one or more security events or phenomena, as well as measures and activities taken in connection with them.
c) Periodic reporting
Periodic reporting is carried out by submitting periodic analyses, information and reports on events and phenomena by lines of work (public order and peace, traffic, etc.).
d) Statistical reporting
Statistical reporting in the police is carried out by submitting completed and controlled data according to established forms. Statistical forms are submitted regularly and periodically for certain security events and phenomena, i.e., police activities (Gaćeša, D., 1998).

2. Sources and knowledge about organizes crime offense

It is very difficult to obtain information that an organized crime offense has been committed at all, especially in the case of those criminal activities in the field of economic and financial crime, smuggling and illicit trade, corruption and money laundering. When it comes to organized violent crime and terrorist activities, then the consequences of criminal offenses are generally visible, so actions and measures are taken with the aim of detecting perpetrators. Therefore, it is very important that the police and other competent authorities, through the timely application of adequate criminal-tactical methods, direct their activities towards detecting and exposing all forms of organized crime in those areas where indications point to the commission of such criminal activity. Also, other security services have an important role in preserving the constitutional order, protecting citizens and fighting against modern threats, including terrorism, organized crime and other forms of endangering public security (Nemanja, D., 2025).

Detecting these criminal offenses requires a more complex and higher quality approach compared to those criminal offenses committed by individuals or unorganized criminal groups, because it is necessary to identify the criminal organization, its connections and strongholds and in further proceedings to detect the perpetrator and secure evidence. The successful activity of the police and other competent authorities in detecting these criminal offenses primarily implies an appropriate level of knowledge of the essence of organized crime, since organized criminal activity is precisely manifested through certain criminal offenses of economic, general, environmental and political crime. Therefore, the

methodology of detecting organized crime offenses has certain specificities that arise from the necessity of adapting existing criminalistic methods to all essential characteristics of these forms of organized criminal activity, i.e., the properties of specific criminal offenses, in order to more easily obtain knowledge about their commission.In the first phase of detection, especially if the criminal organization has established a certain connection with state, political and other bodies, it is difficult to expect with certainty from any source that it will indicate the existence of all elements of organized crime.

As soon as there are indications, the internal affairs body, i.e., the police, should immediately, through the forms of its operational activities, try to obtain all essential knowledge indicating that one of these criminal offenses has been committed. In this sense, it is important to monitor and detect other criminal activity as well, especially those forms of crime for which there is suspicion that they will move towards organized crime in further development, for which purpose it is necessary to carry out an appropriate analysis of detected criminal offenses.

A special difficulty in detection is represented by those organized crime offenses where a connection with government authorities, state, political and other bodies has already been established, because information is well guarded, given the mutual danger of criminal prosecution of all participants in the chain of organized criminal activity. In the procedure of securing evidentiary material, material evidence is of exceptional importance, given that personal evidence is quite rare and unreliable (Kovačević, Z., 2017).

Bearing in mind everything stated, the basic source of knowledge about committed organized crime offenses is the operational activity of internal affairs bodies, i.e., the police. When detecting these criminal offenses, information cannot be successfully collected only on the basis of classical sources of knowledge about a committed criminal offense, but special investigative techniques and other permitted, previously mentioned criminalistic methods must also be used. Criminalistic activity should also be directed at controlling groups and gangs that are on the path to developing into organized crime.

When detecting these criminal offenses, the police apply criminal-tactical and criminal-technical actions and measures as with other criminal offenses, namely: by collecting preliminary information, conducting informative interviews, tracking, observation, verification, examination, inspection of certain documentation, verification of alibis, identification, search activities, control of certain categories of persons, facilities and points, chemical traps, polygraph testing and the like.

For the successful detection of organized crime offenses, the application of other methods specifically intended for detecting these criminal offenses is necessary, such as special investigative techniques, controlled delivery, conclusion of simulated legal transactions, undercover investigator and cooperating witness. However, with the same goal, the police should also use special operational methods, such as operational connections, whose information, although exclusively operational in nature, represents a significant contribution and relevant indications for further operational work on detecting a specific criminal offense.

In certain situations, individual evidentiary actions, such as searches, temporary seizure of items, expert examination and identification, can also contribute to the detection of some of the criminal offenses from organized criminal activity as well as its further clarification and proving. The police can also obtain knowledge that one of the organized crime offenses has been committed during work on criminalistic processing of another criminal offense, about which the competent unit is informed, which takes adequate criminalistic methods for further clarification of the offense and detection of perpetrators.

Some external manifestations can serve as a source of knowledge, which as indications can point to grounds for suspicion that the wealth of certain persons is a consequence of material gain from committing organized crime offenses. The fact is that a number of people in our country became suddenly wealthy, which changed their way of life, and particularly irritated citizens and created dissatisfaction among them and caused suspicion about the legal manner of acquiring that wealth. Such external manifestations can be indications, but it is important to verify and determine whether they arose from enrichment through criminal activity or whether that property was acquired legally.

The state prosecutor, through his new powers, is much more in a position to obtain information about a committed criminal offense and to direct the criminal activity of the police towards detecting and clarifying that criminal offense, as well as the entire criminal organization and especially the perpetrators of the criminal offense, and with that aim to take appropriate methods, primarily to secure valid evidence. Other bodies competent to suppress organized crime, especially customs and inspection bodies, can also obtain knowledge through their activities that one of these criminal offenses has been committed and, in cooperation with the prosecutor and the police, take measures for its complete detection and determination of all other relevant facts.

This cooperation is particularly significant when there is suspicion that the criminal organization has already established connections with state and other relevant bodies and thus secured appropriate protection, because the police, given

their expertise and powers in applying special methods, are most competent to determine and prove the existence of such a criminal connection. In the police organization, authority and responsibility, in accordance with the high degree of formalization of the organizational structure, are normatively formalized by a by-law legal act (Krešimir, V., Slobodan, J., 2022).

Other sources of knowledge that appear in other criminal offenses are less pronounced when it comes to detecting organized crime offenses, which is understandable given all the previously stated characteristics of these organized forms of criminal activity. However, one should not neglect the importance of mass media, reports from enterprises, organizations, and some other legal entities, as well as anonymous and pseudonymous reports, and the contribution of public discussions should absolutely not be neglected either. Information obtained from the mentioned subjects can point to suspicion about the existence of certain forms of organized crime in certain environments, so it is necessary to verify them professionally and with adequate criminalistic methods. Citizens' reports can also be a source of knowledge about a committed organized crime offense, but it rarely appears when it comes to these forms of criminal activity.

This is understandable because citizens have difficulty obtaining relevant knowledge about organized criminal activity, and if they have some information, they have difficulty deciding to report directly, precisely out of fear of appearing as witnesses in the later stage of criminal proceedings, bearing in mind the known methods of revenge and retaliation of organized crime against such persons and members of their families. It can be logically assumed that by using the new legal measure of witness protection, the role of citizens as a source of knowledge in detecting and proving organized crime will become more prominent, as well as witnesses in criminal proceedings in cases involving criminal offenses from this area (Bošković, M., 2003).

3. Analysis of property offenses for 2022

From the Information on the Security Situation in Bosnia and Herzegovina for 2022, it is evident that property offenses continue to be the most prevalent form of general crime. Based on data from the Ministry of Internal Affairs of Republika Srpska, the number of registered general crime offenses (5,748 CO) is down by 2.9% compared to the comparison year.

Table No. 1. Statistical indicators of property crimes[55]

No.	General Crime	2022.	2021.	+ - %
1.	**Br evidentiranih KD opšteg kriminaliteta**	**5.748**	**5.922**	-2,9
1.1.	Number of registered general crime offenses	3.113	2.927	6,4
1.2.	Number of criminal offenses by known perpetrator	2.635	2.995	-12,0
2.	Number of criminal offenses by unknown perpetrator	5.061	5.100	-0,8
3.	Number of reports submitted to prosecutor's office	5.425	5.212	4,1
	Number of reported persons	153	142	7,7
	- minors	1.509	1.681	-10,2
4.	Number of solved offenses by unknown perpetrator	1.920	2.227	-13,8
4.1.	From those committed during the year	1.789	2.063	-13,3
4.2.	From previous years	131	164	-20,1
5.	Material damage caused in KM	9.760.782	8.602.555	13,5
	Overall clearance rate (%)	**85,6**	**84,7**	
	Clearance rate by unknown perpetrator (%)	**69,4**	**70,5**	

A total of 5,061 reports were submitted to prosecutor's offices about committed general crime offenses (less by 0.8%) and 5,425 persons were reported (more by 4.1%), of which 153 were minors and 1,509 repeat offenders. The number of minors is higher by 7.7%, and the number of repeat offenders is lower by 10.2% compared to the comparison year 2021. Of the total number of committed general crime offenses (5,748), police officers deprived perpetrators of their liberty in 109 cases during or immediately after the committed offense. According to data from the Ministry of Internal Affairs of Republika Srpska, property criminal offenses (2,757 CO) are down by 10.4%. Among more serious property offenses, the number of aggravated theft offenses decreased by 16.4%, while the number of robbery offenses increased by 15 CO (or by 71.4%). The number of offenses related to vehicle misappropriation decreased by 17.9%. The overall clearance rate for offenses related to motor vehicle misappropriation is 70.8%, and the clearance rate by unknown perpetrator is 67.4%.

[55] Information on the Security Situation in Bosnia and Herzegovina for 2022, Ministry of Security of BiH,
Sarajevo, 2023.

4. Conclusion

After the conducted research, we can say that through the activities of reporting and information, an exchange of information is achieved that gives "vital energy" to the system of internal affairs as human needs and creations.

Bearing in mind the above, and with the aim of a more successful fight against general and organized crime offenses, and putting certain shortcomings into function whose functionality will be supplemented and improved in the future, I propose the following framework work guidelines as an initial basis:

- Create a flowchart for clarifying criminal offenses, for the sake of clarity in proceeding with measures and actions, and provide all duty services in Police Administrations, i.e., police stations, with the diagram.
- That the duty services of police stations be provided with a table of questions, prepared on the basis of the nine golden questions of criminology, for collecting data when receiving a report and collecting data from the crime scene. For the table of questions to be functional, it should be prepared and used in the duty service and should be sufficiently comprehensive and systematized to enable the person reporting the event, by answering the questions posed, to provide as much data as possible.
- To establish quick departure and action at the place of commission of the criminal offense with the aim of preserving the unchanged state at the crime scene, finding eyewitnesses, and even the suspect, and to establish operability that implies good information and control of the situation (determine whether it is a criminal offense and what kind, case - mishap, misdemeanor, disciplinary offense, or civil-legal offense, who is the perpetrator, description of the perpetrator if unknown, time of commission, in what manner it was committed, what means were used for commission, vehicle description if it was used in commission and left the crime scene, whether there were accomplices and their role, why the criminal offense was committed - motive for commission, if it was for gain - misappropriated items and description, identity of the victim or injured party and which facility was attacked), and to transmit this operational data to the duty service in the shortest possible time, so that this operational data can be used in implementing measures and actions in the field to capture perpetrators.

About the importance of quick departure to the crime scene, unchanged state at the crime scene, what traces can be found at the crime scene and operability at the crime scene, it is necessary to remind police officers through forms of work meetings.

- That the duty services of police stations be provided with topographic maps of municipalities with adequate scale, for the sake of terrain clarity and control of the situation when taking operational-tactical measures and actions in the field.
- To review the state of police equipment with vehicles that can be used for pursuit of motorized criminals, radio and GPS devices and battery lamps, and to find a way to supply deficiencies, and to obtain the same for operational workers working in groups on cases of more serious criminal offenses.
- To hold a meeting in which workers from the Criminal Police Department, police stations, traffic safety police stations and Support Unit will participate with the task of presenting shortcomings in work, agreements and planning for action in certain situations, division and elaboration of specific tasks.
- To prepare a plan for engaging other law enforcement agencies in BiH.
- To carry out timely issuance of search warrants and announcements.
- To use mass media to provide well-measured information about the perpetrator that provides wide opportunities for collecting data about the wanted perpetrator by eyewitnesses reporting events and gives all well-intentioned citizens the opportunity to report where the perpetrator is located.

Efficient work in carrying out these actions as well as timely reporting leaves a very favorable impression among citizens about police work and the power of the rule of law.

LITERATURE

1. Bošković, M. (2003). Transnational Organized Crime. Belgrade: Police Academy.
2. Gaćeša, D. (1998). Police - Jurisdiction, Organization, Management. Banja Luka: Glas Srpske.
3. Information on the Security Situation in Bosnia and Herzegovina for 2022, Ministry of Security of BiH, Sarajevo, 2023.
4. Masleša, R. (1999). Police Organization and Functioning in a Democratic Society. Sarajevo: Faculty of Criminal Sciences.
5. Kovačević, Z. (2017). Criminalistic Aspects of Investigating Illicit Production and Trafficking of Narcotic Drugs in Bosnia and Herzegovina. Banja Luka: Independent University.
6. Talijan, M. (2001). Management of Internal Affairs. Belgrade: Higher School of Internal Affairs.
7. Law on Protection of Classified Information ("Official Gazette of BiH" No. 54/05 and 12/09).
8. Protection and Security, Volume 5, No. 1 (2025).
9. Protection and Security, Volume 2, No. 2 (2022).

ORGANIZACIJSKI MODELI KRIZNOG MENADŽMENTA: UZROCI I POSLJEDICE INSTITUCIONALNIH RIZIKA U BOSNI I HERCEGOVINI

DOI: *10.70329/2744-2403.2025.5.10.7*

Pregledni naučni članak

MsC Atina Perković PhD candidate

Sažetak:

Ovaj pregledni rad analizira organizacijske modele kriznog menadžmenta i institucionalne rizike u Bosni i Hercegovini (BiH), s ciljem identifikacije uzroka slabosti i njihovih posljedica na efikasnost odgovora u kriznim situacijama. Teorijski okvir rada obuhvata pojam i dimenzije kriznog menadžmenta, razliku između upravljanja rizicima i kriznog menadžmenta te ključne koncepte otpornosti, adaptivnosti i institucionalne koordinacije. Analizirani su centralizirani, decentralizirani i hibridni modeli kriznog menadžmenta, uz primjere iz međunarodne prakse (SAD, EU, Njemačka, Slovenija, Hrvatska). Poseban fokus stavljen je na specifičnosti BiH, uključujući složen ustavno-pravni okvir, fragmentirane nadležnosti i probleme koordinacije na državnom, entitetskom i lokalnom nivou. Studije slučaja poplava 2014., migrantske krize 2018–2021. i pandemije COVID-19 ilustriraju praktične izazove institucionalne neefikasnosti. Rezultati pokazuju da institucionalni rizici u BiH uzrokuju usporeno donošenje odluka, povećanu ranjivost stanovništva i infrastrukture, gubitak povjerenja građana te reputacijske rizike na međunarodnom planu. Na temelju uporedne analize s međunarodnim praksama, rad nudi preporuke za unapređenje organizacijskih modela kriznog menadžmenta u BiH. Ključne mjere uključuju jačanje koordinacijskih tijela, uspostavljanje integriranih informacionih sistema, edukaciju i profesionalizaciju kadrova te jačanje međunarodne i regionalne saradnje. Zaključuje se da institucionalne reforme u oblasti kriznog menadžmenta nisu samo tehničko pitanje, već i strateški prioritet za sigurnost, stabilnost i demokratsku konsolidaciju Bosne i Hercegovine.

Ključne riječi: Krizni menadžment; institucionalni rizici; Bosna i Hercegovina; koordinacija; otpornost; javne politike; međunarodna saradnja

1. Uvod

Krizni menadžment predstavlja planski i koordinirani proces kojim se institucije i organizacije pripremaju, odgovaraju i oporavljaju od kriznih situacija koje ugrožavaju stabilnost, sigurnost i funkcioniranje društva. Prema Mitroffu (2005), kriza je „neplanirani i potencijalno razoran događaj koji prijeti osnovnim ciljevima, resursima i egzistenciji organizacije ili zajednice". Upravljanje krizama obuhvata faze prevencije, pripreme, odgovora i oporavka, pri čemu se naglašava važnost institucionalne spremnosti i međusektorske koordinacije (Alexander, 2013). U savremenim društvima, obilježenim globalizacijom i povećanom kompleksnošću sigurnosnih izazova, krizni menadžment postaje ključan element nacionalne sigurnosti i javne politike. Značaj kriznog menadžmenta ogleda se u njegovoj sposobnosti da umanji posljedice prirodnih katastrofa, tehničko-tehnoloških nesreća, zdravstvenih prijetnji i društveno-političkih kriza. Posebno u državama sa složenim institucionalnim strukturama, poput Bosne i Hercegovine, efikasnost kriznog menadžmenta direktno zavisi od koordinacije između različitih nivoa vlasti i sposobnosti prevazilaženja institucionalnih slabosti (Perry & Quarantelli, 2005).

Ovaj članak ima za cilj da istraži organizacijske modele kriznog menadžmenta, s posebnim fokusom na uzroke i posljedice institucionalnih rizika u Bosni i Hercegovini. Analizom teorijskih modela i praksi iz međunarodnog okruženja nastoji se identificirati ključni faktori koji određuju efikasnost upravljanja krizama u složenim društveno-političkim sistemima. Metodološki pristup ovog članka temelji se na preglednoj analizi relevantne domaće i međunarodne literature. Korišteni su naučni članci, knjige, izvještaji međunarodnih organizacija i zakonski dokumenti kako bi se obuhvatila teorijska i praktična dimenzija kriznog menadžmenta. Pregledna analiza omogućava sintezu različitih istraživačkih nalaza i pruža uvid u dominantne trendove, izazove i preporuke u oblasti kriznog menadžmenta (Snyder, 2019). Fokus je stavljen na radove koji obrađuju institucionalne rizike, organizacijske modele i specifične primjere iz Bosne i Hercegovine i zemalja regije. Ovakav metodološki okvir omogućava da se članak pozicionira unutar postojećih teorijskih rasprava, ali i da ponudi praktične implikacije relevantne za institucionalne kapacitete kriznog menadžmenta u BiH.

2. Teorijski okvir kriznog menadžmenta

Krizni menadžment se definira kao planski i sistematski proces pripreme, odgovora i oporavka od događaja koji mogu ugroziti sigurnost ljudi, infrastrukturu ili funkcioniranje institucija (Boin et al., 2017). Osnovne dimenzije kriznog menadžmenta uključuju prevenciju, pripremu, odgovor i oporavak. Prevencija podrazumijeva identifikaciju i umanjenje potencijalnih rizika prije nego što prerastu u krizu, dok priprema obuhvata planiranje, edukaciju i testiranje kapaciteta. Odgovor je povezan s aktiviranjem operativnih resursa i donošenjem odluka u realnom vremenu, dok se oporavak odnosi na vraćanje sistema u funkcionalno stanje i izgradnju otpornosti za buduće krize (Coombs, 2015). Ove dimenzije čine ciklički proces u kojem se svaka faza nadovezuje na prethodnu. U literaturi se naglašava da je uspješnost kriznog menadžmenta određena ne samo formalnim planovima, već i fleksibilnošću institucija da odgovore na nepredviđene okolnosti (Comfort, 2007).

Iako se pojmovi upravljanja rizicima i kriznog menadžmenta često koriste naizmjenično, među njima postoji jasna razlika. Upravljanje rizicima fokusirano je na sistematičnu identifikaciju, procjenu i kontrolu potencijalnih prijetnji prije nego što prerastu u krizne situacije (Hopkin, 2018). Drugim riječima, riječ je o preventivnom procesu koji nastoji umanjiti vjerovatnoću i posljedice negativnih događaja. S druge strane, krizni menadžment se aktivira kada rizici eskaliraju i prerastu u događaje koji zahtijevaju hitnu reakciju (Bundy et al., 2017). Dok je upravljanje rizicima proaktivno i strateški usmjereno, krizni menadžment je reaktivan, s naglaskom na donošenje brzih odluka, koordinaciju resursa i komunikaciju u uvjetima nesigurnosti. U praksi, ovi procesi su komplementarni i čine dio šireg okvira sigurnosnog upravljanja.

U savremenim teorijskim raspravama o kriznom menadžmentu posebno se ističu tri koncepta: otpornost (resilience), adaptivnost i institucionalna koordinacija. Otpornost (resilience) odnosi se na sposobnost društvenih i institucionalnih sistema da izdrže šokove, brzo se oporave i nastave funkcionirati uprkos kriznim okolnostima. Boin i van Eeten (2013) ističu da otpornost podrazumijeva ne samo povratak u prvobitno stanje, nego i sposobnost učenja i jačanja kapaciteta nakon krize. Adaptivnost označava fleksibilnost institucija i organizacija da mijenjaju strategije, strukture i procese u skladu s novonastalim okolnostima. U uvjetima kompleksnih i višedimenzionalnih kriza, adaptivni kapacitet postaje ključna determinanta učinkovitog menadžmenta (Weick & Sutcliffe, 2015).

Adaptivne institucije sposobne su donositi odluke na temelju kontinuiranog učenja, evaluacije i prilagodbe. Institucionalna koordinacija je treći ključni koncept koji naglašava važnost međusobne saradnje različitih organizacija, nivoa vlasti i sektora. Prema Christensenu et al. (2016), krize često razotkrivaju fragmentiranost institucija i manjak komunikacijskih mehanizama. U složenim državnim strukturama, kao što je Bosna i Hercegovina, koordinacija postaje presudna za sinhronizirano djelovanje i smanjenje posljedica kriza. Integracija ovih koncepata u institucionalne modele kriznog menadžmenta omogućava izgradnju otpornijih i funkcionalnijih sistema, sposobnih da odgovore na izazove globaliziranog i nesigurnog okruženja. Bosna i Hercegovina je jedina država u regionu Jugoistočne Evrope koja nema usvojenu Strategiju pametne specijalizacije, iako je riječ o strateški važnom dokumentu koji kombinuje industrijske, obrazovne i inovacijske politike radi unapređenja otpornosti sistema na krizne situacije (Garaplija, 2022).

3. Organizacijski modeli kriznog menadžmenta

Centralizirani modeli kriznog menadžmenta zasnivaju se na hijerarhijskoj strukturi odlučivanja u kojoj dominira vertikalna linija komande i kontrole. Ovaj pristup karakterizira jasno definisana hijerarhija, koncentracija moći u centralnim institucijama i stroga podjela odgovornosti (Kapucu & Garayev, 2011). Prednost centraliziranog modela ogleda se u mogućnosti brzog donošenja odluka i mobilizacije resursa u kriznim situacijama koje zahtijevaju jedinstvenu koordinaciju. Međutim, slabost ovog modela jest njegova rigidnost i smanjena sposobnost adaptacije u kompleksnim krizama koje traže brze i inovativne odgovore (Christensen et al., 2016). Za razliku od centraliziranih struktura, decentralizirani modeli oslanjaju se na horizontalnu koordinaciju i saradnju različitih institucija, nivoa vlasti i sektora. U tim modelima, odgovornost za krizni menadžment raspoređena je na lokalne, regionalne i državne organe, uz uključivanje nevladinih organizacija, privatnog sektora i zajednica (Ansell et al., 2010).

Mrežni modeli posebno naglašavaju značaj umreženih aktera kroz zajedničke informacijske platforme, komunikacijske kanale i partnerske odnose. Prednosti ovog pristupa jesu fleksibilnost, inovativnost i mogućnost uključivanja različitih resursa. Ipak, slabost se ogleda u riziku fragmentacije i otežane koordinacije kada institucije nemaju jasno definisane nadležnosti ili kapacitete (Kapucu, 2009). Savremeni sistemi kriznog menadžmenta najčešće se temelje na hibridnim modelima koji kombinuju elemente centralizacije i decentralizacije. Hibridni modeli omogućavaju balans između snažne centralne koordinacije i fleksibilne

lokalne implementacije mjera. Prema Boin i 't Hart (2010), ovaj pristup omogućava bolje prilagođavanje različitim tipovima kriza, od prirodnih katastrofa do kompleksnih društveno-političkih prijetnji. U praksi, hibridni modeli se oslanjaju na centralne institucije koje postavljaju strategiju i okvir, dok lokalne zajednice i specijalizirane agencije imaju autonomiju u implementaciji. Takva kombinacija smanjuje rizik preopterećenja centralnih struktura i povećava otpornost sistema u cjelini. U Sjedinjenim Američkim Državama, krizni menadžment koordinira Federal Emergency Management Agency (FEMA), koja funkcioniše unutar centraliziranog okvira, ali u saradnji s državnim i lokalnim vlastima. FEMA razvija nacionalne planove i standarde, dok implementacija zavisi od partnerstva s lokalnim akterima (Sylves, 2019).

U Evropskoj uniji, Mehanizam civilne zaštite EU zasniva se na hibridnom modelu. Dok Evropska komisija pruža stratešku koordinaciju i resurse (npr. kroz rescEU kapacitete), države članice zadržavaju suverenitet u upravljanju krizama na svom teritoriju (European Commission, 2020). Ovaj model demonstrira balans između nadnacionalne koordinacije i nacionalne odgovornosti. Zemlje regije (npr. Hrvatska, Slovenija, Srbija) primjenjuju različite kombinacije modela. Hrvatska, kroz Državnu upravu za zaštitu i spašavanje (DUZS), sada integriranu u Ministarstvo unutarnjih poslova, koristi hibridni pristup s naglaskom na snažnu ulogu lokalnih zajednica (Pavić & Vlahinić-Dizdarević, 2018). Slovenija njeguje mrežni model saradnje između države i lokalnih zajednica, dok Srbija primjenjuje više centraliziran pristup kroz Sektor za vanredne situacije Ministarstva unutrašnjih poslova. Ovi primjeri pokazuju da savremeni krizni menadžment ne može biti u potpunosti centraliziran niti potpuno decentraliziran. Umjesto toga, najbolje rezultate donosi prilagodljivi, hibridni model koji kombinira efikasnost centralne koordinacije s fleksibilnošću lokalnog djelovanja.

4. Institucionalni rizici u kriznom menadžmentu

Institucionalni rizici u kriznom menadžmentu predstavljaju strukturne slabosti i ograničenja koja ometaju efikasno planiranje, donošenje odluka i provedbu mjera u kriznim situacijama. Oni se mogu klasificirati u nekoliko tipova. Pravni rizici nastaju iz nedostatka jasnog normativnog okvira ili postojanja kontradiktornih zakona i propisa. Kada pravni akti nisu usklađeni ili ne definiraju jasno nadležnosti, dolazi do pravne nesigurnosti i preklapanja odgovornosti (OECD, 2018). Politički rizici odnose se na nestabilnost političkog sistema, nedostatak konsenzusa među ključnim akterima i sklonost politizaciji odluka. U društvima s izraženim političkim podjelama, krizni menadžment često postaje talac političkih interesa (Boin et al., 2017). Organizacijski rizici uključuju nedovoljnu koordinaciju među institucijama, nejasnu podjelu odgovornosti i birokratsku

tromost. Ovi rizici dovode do situacija u kojima institucije djeluju izolirano umjesto u okviru integriranog sistema (Christensen et al., 2016). Resursni rizici obuhvataju nedostatak ljudskih, tehničkih i finansijskih kapaciteta. Legislativa koja tretira zaštitu kritične infrastrukture mora se kontinuirano unapređivati kako bi pratila sofisticiranost prijetnji i krivičnih djela usmjerenih na ključne sisteme i objekte (Garaplija, 2021). U kriznim situacijama ograničeni resursi često usporavaju reakciju i onemogućavaju adekvatnu zaštitu stanovništva i infrastrukture (Kapucu, 2009). Slabosti u institucionalnom okviru direktno utiču na proces donošenja odluka u krizama.

Kada pravni i organizacijski mehanizmi nisu jasno definisani, odluke se donose sporo, a njihova implementacija postaje nedosljedna (Comfort, 2007). Nedostatak koordinacije i povjerenja među institucijama dodatno produžava vrijeme reakcije, dok se resursi raspoređuju neefikasno. Također, institucionalne slabosti dovode do povećane ovisnosti o ad hoc rješenjima, što dugoročno slabi otpornost sistema. U kriznim situacijama gdje je potrebna hitna akcija, sporost i fragmentiranost odlučivanja može rezultirati ozbiljnim posljedicama po sigurnost građana i stabilnost društva (Perry & Quarantelli, 2005). U zemljama u tranziciji, poput Bosne i Hercegovine, institucionalne rizike dodatno pogoršavaju korupcija, politizacija i fragmentacija institucija.

Korupcija narušava transparentnost i pravednu raspodjelu resursa, stvarajući situacije u kojima odluke nisu motivirane javnim interesom, već privatnim ili stranačkim koristima (Transparency International, 2022). Politizacija kriznog menadžmenta dovodi do toga da ključne odluke zavise od političkih pregovora i interesa, umjesto od stručnih procjena i analiza rizika (’t Hart & Sundelius, 2013). To se posebno vidi u BiH, gdje složena političko-administrativna struktura često otežava donošenje jedinstvenih i koordiniranih odluka. Fragmentacija institucija predstavlja još jedan značajan problem.

Višeslojni sistem nadležnosti (državni, entitetski, kantonalni i općinski nivo) često stvara preklapanje ili praznine u odgovornosti. U takvom okruženju, krizni menadžment otežano funkcioniše jer različiti nivoi vlasti nemaju dovoljno razvijene mehanizme saradnje i razmjene informacija (Pavić & Vlahinić-Dizdarević, 2018). Sve navedeno pokazuje da institucionalni rizici nisu samo tehničko pitanje upravljanja krizama, već duboko političko i društveno pitanje koje određuje kapacitet jedne države da zaštiti svoje građane u vanrednim situacijama. Politizacija i etno-nacionalne podjele u BiH dodatno otežavaju funkcioniranje institucija u kriznim situacijama, pri čemu etno-nacionalne oligarhije nerijetko koriste krize za očuvanje vlastitog položaja (Garaplija & Korajlić, 2022).

5. Krizni menadžment u Bosni i Hercegovini

Bosna i Hercegovina posjeduje složen i višeslojan institucionalni okvir kriznog menadžmenta, oblikovan ustavno-pravnom strukturom države. Na državnom nivou, ključna institucija je Ministarstvo sigurnosti BiH, u čijem se okviru nalazi Sektor za zaštitu i spašavanje. On je zadužen za koordinaciju aktivnosti između entiteta, Brčko distrikta i međunarodnih partnera, ali njegove ovlasti su ograničene i često više koordinacijske nego izvršne (Ministarstvo sigurnosti BiH, 2017). Na entitetskom nivou, Republika Srpska ima Republičku upravu civilne zaštite, dok Federacija BiH djeluje kroz Federalnu upravu civilne zaštite i dodatno složeni sistem kantonalnih uprava civilne zaštite. Brčko distrikt Odjel za javnu sigurnost u kojem je i sektor zaštite i spašavanja.

Ovakva fragmentiranost znači da svaka administrativna jedinica ima svoje nadležnosti, zakone i procedure (Zakon o zaštiti i spašavanju ljudi i materijalnih dobara od prirodnih i drugih nesreća, 2017). Na lokalnom nivou, općine i gradovi imaju krizne štabove i jedinice civilne zaštite, ali njihovi kapaciteti variraju, zavisno od dostupnih resursa i političke volje. Ova višeslojnost institucionalnog okvira otežava jedinstveno planiranje i koordinaciju u krizama. Fragmentacija sistema kriznog menadžmenta u BiH ogleda se u podijeljenim nadležnostima, nedostatku vertikalne koordinacije i preklapanju zakonskih ovlasti. Dok entitetske i kantonalne institucije imaju operativne kapacitete, državni nivo često ostaje ograničen na komunikacijske i koordinacijske funkcije, bez direktne izvršne moći (Ejdus, 2017). Problemi koordinacije posebno dolaze do izražaja u situacijama kada je potrebna brza i sinhronizirana reakcija.

U praksi, odsustvo jedinstvene strategije dovodi do situacije u kojoj svaka administrativna jedinica primjenjuje različite procedure, što usporava odgovor i povećava ranjivost stanovništva (Bieber, 2020). Nedostatak integriranog informacionog sistema i zajedničkih planova dodatno otežava saradnju između različitih nivoa vlasti. Poplave koje su pogodile Bosnu i Hercegovinu u maju 2014. godine razotkrile su duboke slabosti institucionalnog okvira. Nedostatak koordinacije između državnog i entitetskog nivoa doveo je do sporog odgovora i neefikasne raspodjele resursa. Posebno se istaknula uloga lokalnih zajednica, koje su često bile prepuštene same sebi, dok je međunarodna pomoć stigla brže nego što su domaće institucije uspjele organizirati (UNDP, 2015). Analize su pokazale da je najveći izazov bio u nedostatku zajedničkog komandnog sistema i slaboj komunikaciji između entiteta. Tokom migrantske krize, BiH je postala tranzitna ruta za hiljade migranata, što je ponovo otkrilo institucionalne slabosti. Dok je Ministarstvo sigurnosti BiH imalo koordinacijsku ulogu, implementacija mjera bila je prepuštena entitetskim i lokalnim strukturama, koje nisu imale dovoljno

resursa niti jedinstvenu strategiju. Rezultat je bio neravnomjeran pristup, pri čemu su pojedini kantoni i općine odbijali preuzeti odgovornost za smještaj migranata, što je dodatno politiziralo krizu (Majetić, 2020). Ova situacija pokazala je koliko fragmentacija i politizacija mogu ugroziti sposobnost upravljanja transnacionalnim krizama. Pandemija COVID-19 još je jasnije demonstrirala slabosti kriznog menadžmenta u BiH. Umjesto jedinstvene nacionalne strategije, svaka administrativna jedinica donosila je vlastite mjere, što je rezultiralo konfuzijom i neujednačenim odgovorom. Entiteti, kantoni i općine uveli su različite restrikcije i protokole, dok je državni nivo imao minimalnu ulogu u koordinaciji i nabavci medicinske opreme (World Bank, 2021).

Pored toga, pandemija je otkrila značajan nedostatak povjerenja građana u institucije, što je smanjilo učinkovitost mjera javnog zdravlja. Specifičnosti kriznog menadžmenta u Bosni i Hercegovini proizlaze iz složene državne strukture, višeslojnog institucionalnog okvira i stalne fragmentacije nadležnosti. Studije slučaja pokazuju da krize razotkrivaju duboke slabosti sistema: odsustvo koordinacije, politizaciju odluka i zavisnost od međunarodne pomoći. Ovi izazovi jasno ukazuju na potrebu jačanja institucionalne saradnje, razvoja integriranih planova i izgradnje povjerenja u institucije kriznog menadžmenta. Dejtonski mirovni sporazum oblikovao je institucionalni okvir BiH na način koji često funkcionira kao svojevrsna 'društveno-politička luđačka košulja', sputavajući efikasno donošenje odluka u krizama (Garaplija & Korajlić, 2022).

6. Uzroci institucionalnih rizika u BiH

Jedan od ključnih uzroka institucionalnih rizika u Bosni i Hercegovini leži u njenom ustavno-pravnom okviru, koji je oblikovan Daytonskim mirovnim sporazumom iz 1995. godine. Ovaj okvir uspostavio je složenu i višeslojnu državnu strukturu s podijeljenim nadležnostima između državnog nivoa, dva entiteta, Brčko distrikta i, u slučaju Federacije BiH, dodatnih deset kantona (Bieber, 2020). Takva fragmentacija dovodi do nedostatka jedinstvene strategije i neujednačenog odgovora na krizne situacije.

U praksi, svaka administrativna jedinica ima vlastite propise, institucije i procedure, što stvara pravne praznine i preklapanja u nadležnostima (Ejdus, 2017). Posljedica je otežana koordinacija, naročito u krizama koje zahtijevaju brze, centralizirane odluke. Bosna i Hercegovina je obilježena dubokim političkim i etničkim podjelama koje značajno utiču na efikasnost kriznog menadžmenta. Političke elite često koriste krizne situacije kao instrument političke borbe, pri čemu odluke ne proizlaze iz stručnih analiza i potreba građana, već iz partikularnih interesa političkih stranaka (Keil & Kudlenko, 2015).

Nedostatak konsenzusa među ključnim političkim akterima dovodi do blokada u donošenju odluka, prolongiranja procesa i nedostatka jedinstvenog pristupa. Ovakvo stanje naročito je izraženo u krizama transnacionalnog karaktera (poput migrantske krize), gdje politički sukobi dodatno otežavaju institucionalni odgovor (Majetić, 2020). Pored političkih i pravnih izazova, značajan uzrok institucionalnih rizika u BiH jesu resursna ograničenja. Institucije nadležne za krizni menadžment suočavaju se s hroničnim nedostatkom finansijskih sredstava, tehničke opreme i specijaliziranih ljudskih resursa. Nedostatak kontinuiranog ulaganja u infrastrukturu civilne zaštite smanjuje kapacitete za pravovremeni odgovor na prirodne i društvene krize (UNDP, 2015).

Kadrovski problemi dodatno pogoršavaju situaciju. U mnogim institucijama prisutno je oslanjanje na politička imenovanja umjesto na profesionalne standarde, što rezultira smanjenom kompetentnošću i nedostatkom stručnih znanja potrebnih za upravljanje kompleksnim krizama (OSCE, 2020). Još jedan važan uzrok institucionalnih rizika u BiH je nedostatak strateške kulture kriznog menadžmenta. Pod strateškom kulturom podrazumijeva se usmjerenost institucija na dugoročno planiranje, prevenciju i razvoj otpornosti, a ne samo na reaktivno djelovanje kada kriza već nastupi (Boin et al., 2017). U BiH dominira reaktivan pristup krizama, pri čemu se mjere donose ad hoc, bez sistematskog oslanjanja na procjene rizika, scenarije i planove kontinuiteta. Nedostatak strategijske vizije jasno se pokazao tokom poplava 2014. i pandemije COVID-19, kada su institucije reagirale tek nakon izbijanja krize, bez adekvatno razvijenih preventivnih mehanizama (World Bank, 2021).

7. Posljedice institucionalnih rizika u BiH

Jedna od najočitijih posljedica institucionalnih rizika u Bosni i Hercegovini jest usporeno i nekoordinirano donošenje odluka tokom kriznih situacija. Zbog fragmentiranog sistema nadležnosti, odluke se često donose kroz višeslojne političke pregovore, što produžava vrijeme reakcije i smanjuje učinkovitost mjera (Christensen et al., 2016). Na primjeru poplava 2014. godine, različiti nivoi vlasti donosili su mjere bez zajedničkog plana, što je rezultiralo kašnjenjem u evakuaciji stanovništva i raspodjeli pomoći (UNDP, 2015). Nedostatak jedinstvenog komandnog sistema i sporost odlučivanja imaju direktan negativan utjecaj na brzinu i kvalitet odgovora na krizu. Institucionalne slabosti direktno povećavaju ranjivost stanovništva i infrastrukture.

Kada se odluke donose sporo i nekoordinirano, posljedice kriza su intenzivnije i dugotrajnije. Nedostatak adekvatnih preventivnih mjera, kao i slaba ulaganja u infrastrukturu otpornu na prirodne katastrofe, dovode do povećanog broja žrtava

i materijalnih šteta (Kapucu, 2009). Tokom pandemije COVID-19, razlike u mjerama između entiteta i kantona stvorile su konfuziju među građanima, povećale rizik od širenja virusa i dodatno opteretile zdravstveni sistem (World Bank, 2021). Neefikasan krizni menadžment uzrokuje gubitak povjerenja građana u institucije. Kada građani percipiraju da institucije ne djeluju u njihovom interesu ili da su odluke vođene političkim, a ne stručnim razlozima, dolazi do smanjenja legitimnosti vlasti (Perry & Quarantelli, 2005).

Povjerenje u institucije predstavlja ključan faktor u uspješnom provođenju kriznih mjera jer građani moraju biti spremni da ih prihvate i slijede. Tokom migrantske krize 2018–2021. godine, različiti stavovi lokalnih i državnih institucija doprinijeli su stvaranju osjećaja nesigurnosti među građanima i percepciji da vlasti nemaju kontrolu nad situacijom (Majetić, 2020). Institucionalni rizici ne utiču samo na unutrašnju stabilnost, već i na međunarodnu percepciju Bosne i Hercegovine.

Slabosti u kriznom menadžmentu dovode do reputacijskih rizika koji narušavaju kredibilitet države u očima međunarodnih partnera i investitora. U slučaju BiH, međunarodne organizacije i susjedne zemlje često su preuzimale vodeću ulogu u pružanju pomoći, što stvara percepciju nedovoljne sposobnosti države da samostalno upravlja krizama (Bieber, 2020). Takva reputacija može smanjiti povjerenje u institucije, otežati pristup međunarodnim fondovima i oslabiti položaj države u regionalnim i globalnim sigurnosnim aranžmanima. Posljedice institucionalnih rizika u Bosni i Hercegovini višestruke su: od usporenog i nekoordiniranog donošenja odluka, preko povećane ranjivosti građana i infrastrukture, do gubitka povjerenja u institucije i reputacijskih šteta na međunarodnoj sceni.

8. Uporedna analiza s međunarodnim praksama

Njemačka se često navodi kao primjer uspješnog modela kriznog menadžmenta koji se zasniva na kombinaciji centralizirane koordinacije i decentralizirane implementacije. Savezni ured za civilnu zaštitu i pomoć u katastrofama (BBK) koordinira strateške aktivnosti, dok savezne pokrajine (Länder) imaju značajnu autonomiju u provođenju mjera (BBK, 2016). Ovakav model omogućava balans između efikasne centralne koordinacije i fleksibilnosti lokalnog odgovora. Slovenija je razvila integrirani sistem civilne zaštite koji počiva na horizontalnoj koordinaciji između državnih institucija, lokalnih zajednica i volonterskih organizacija.

Posebno je važna uloga lokalnih jedinica, koje su ključne u prvoj reakciji na krize. Transparentna komunikacija s građanima dodatno povećava povjerenje u institucije i učinkovitost odgovora (Cindrič, 2019). Hrvatska, kroz Državnu upravu za zaštitu i spašavanje (DUZS), a danas integriranu u Ravnateljstvo civilne zaštite pri MUP-u, primjenjuje hibridni model koji naglašava ulogu lokalne samouprave, ali uz jasnu hijerarhiju komandovanja. Hrvatska je također kro DUZS bila mentor jačanja sistema civilne zaštite u BiH kroz EU projekt "EU4 Better Civil Protection in B&H". Poplave 2014. godine pokazale su potrebu za jačom centralnom koordinacijom, pa su reformske mjere dodatno osnažile vertikalnu integraciju sustava (Pavić & Vlahinić-Dizdarević, 2018).

Države u tranziciji često se suočavaju s izazovima sličnim Bosni i Hercegovini: slabim institucionalnim kapacitetima, politizacijom i nedostatkom resursa. Međutim, postoje primjeri uspješnih prilagodbi. Poljska je nakon 1990-ih reformirala sistem civilne zaštite uvođenjem jedinstvenog zakonodavnog okvira i nacionalne strategije sigurnosti, čime je osigurana veća koordinacija između lokalnog i državnog nivoa (Kowalski, 2015). Češka Republika razvila je sistem kriznog menadžmenta koji se oslanja na mrežnu saradnju između državnih institucija, lokalnih vlasti i nevladinog sektora, uz naglašenu ulogu preventivnog planiranja (Štěpánek, 2017).

Ovi primjeri pokazuju da tranzicijske države mogu postići značajne pomake kroz jasno normativno uređenje, profesionalizaciju kadrova i ulaganje u tehničke kapacitete. Za Bosnu i Hercegovinu, transfer znanja i dobrih praksi iz međunarodnog okruženja predstavlja ključan mehanizam za unapređenje kriznog menadžmenta. Pouke iz Njemačke i Slovenije ukazuju na važnost integriranog informacionog sistema, profesionalizacije kadrova i jasne raspodjele odgovornosti. Iskustvo Hrvatske pokazuje kako krize mogu biti katalizator za reformu i jačanje koordinacijskih tijela (Pavić & Vlahinić-Dizdarević, 2018). U kontekstu tranzicijskih država, BiH bi mogla profitirati od razvoja jedinstvenog zakonodavnog okvira na državnom nivou, koji bi precizno definirao nadležnosti i procedure za sve nivoe vlasti.

Također, uvođenje zajedničkih trening programa i regionalnih centara izvrsnosti doprinijelo bi jačanju otpornosti institucija. Transfer znanja može se ostvariti kroz saradnju s međunarodnim organizacijama (npr. EU Mehanizam civilne zaštite, UNDP, OSCE), bilateralne sporazume sa susjednim državama i uključivanje BiH u regionalne mreže kriznog menadžmenta. Time bi se smanjila institucionalna fragmentacija i povećala sposobnost zajedničkog djelovanja u krizama koje prelaze administrativne granice.

9. Preporuke za unapređenje organizacijskih modela u BiH

Prvi korak u unapređenju organizacijskih modela kriznog menadžmenta u Bosni i Hercegovini jeste jačanje koordinacijskih tijela na državnom nivou. S obzirom na fragmentiranu strukturu i višeslojni sistem vlasti, od ključne je važnosti uspostaviti centralizirano koordinacijsko tijelo s jasnim ovlastima za donošenje odluka u kriznim situacijama (Christensen et al., 2016). Takvo tijelo trebalo bi biti odgovorno za harmonizaciju entitetskih, kantonalnih i lokalnih planova, kao i za usklađivanje sa međunarodnim standardima. Jačanje međuinstitucionalne saradnje smanjilo bi rizik od preklapanja nadležnosti i doprinijelo efikasnijoj raspodjeli resursa (Kapucu, 2009). Efikasan krizni menadžment nezamisliv je bez razvijenog integriranog informacionog sistema koji omogućava pravovremenu razmjenu podataka između različitih institucija. U BiH trenutno ne postoji jedinstvena digitalna platforma koja povezuje državni, entitetski, kantonalni i lokalni nivo vlasti u kriznim situacijama (OSCE, 2020). Iskustva Njemačke i Slovenije pokazuju da zajednički informacioni sistemi značajno povećavaju brzinu donošenja odluka i preciznost operativnih mjera (BBK, 2016; Cindrič, 2019). Uvođenje takvog sistema u BiH doprinijelo bi boljem praćenju rizika, koordinaciji odgovora i transparentnosti prema građanima. Profesionalizacija kadrova predstavlja jedan od ključnih preduslova za jačanje otpornosti sistema.

Trenutno se u BiH krizni menadžment često oslanja na politički imenovane kadrove, dok su stručni kapaciteti nedovoljno razvijeni (OSCE, 2020). Preporučuje se uvođenje sistematične edukacije i certificiranih programa obuke, koji bi obuhvatali međunarodne standarde i dobre prakse (Weick & Sutcliffe, 2015). Također, potrebno je razviti akademske i stručne programe na univerzitetima i specijaliziranim centrima, čime bi se stvorila baza stručnjaka sposobnih za djelovanje u kompleksnim krizama. Međunarodne organizacije, poput Ujedinjenih naroda (UNDP, WHO), Evropske unije (EU Civil Protection Mechanism) i OSCE-a, već igraju važnu ulogu u jačanju kapaciteta BiH. Međutim, njihova podrška treba biti sistematičnije integrirana u domaće institucionalne strukture. BiH bi trebala aktivno koristiti mogućnosti koje pruža članstvo u međunarodnim mehanizmima civilne zaštite i kroz to osigurati pristup dodatnim resursima, znanju i obukama (European Commission, 2020). Regionalna saradnja, posebno sa zemljama Zapadnog Balkana, može biti ključna za zajednički odgovor na transnacionalne krize poput poplava, požara ili migrantskih kretanja. Stvaranje regionalnih centara izvrsnosti za krizni menadžment omogućilo bi razmjenu iskustava i bržu mobilizaciju resursa u hitnim slučajevima (Štěpánek, 2017).

10. Zaključak

Analiza organizacijskih modela kriznog menadžmenta i institucionalnih rizika u Bosni i Hercegovini pokazala je da složena državna struktura, pravna fragmentacija i političke podjele značajno otežavaju efikasan odgovor na krize. Dok teorijski okvir kriznog menadžmenta naglašava važnost otpornosti, adaptivnosti i koordinacije (Boin et al., 2017), praksa u BiH pokazuje da institucionalni rizici rezultiraju sporim i nekoordiniranim donošenjem odluka, povećanom ranjivošću stanovništva i gubitkom povjerenja građana u institucije (Christensen et al., 2016; Perry & Quarantelli, 2005). Kako pokazuju Garaplija i Korajlić (2022), institucionalni rizici u BiH ne predstavljaju isključivo tehnički izazov kriznog menadžmenta, nego reflektiraju duboku političku i društvenu krizu koja generira sigurnosne prijetnje i slabi otpornost države. Studije slučaja – poplave 2014., migrantska kriza i pandemija COVID-19 – ilustrirale su kako se institucionalne slabosti reflektiraju u realnim kriznim situacijama i dovode do zavisnosti od međunarodne pomoći (UNDP, 2015; World Bank, 2021). Teorijski doprinos rada ogleda se u sistematizaciji ključnih modela kriznog menadžmenta – centraliziranih, decentraliziranih i hibridnih – te njihovoj uporedbi s praksom u BiH. Naglašeno je da nijedan model sam po sebi nije dovoljan, već da je optimalno rješenje u hibridnim strukturama koje kombinuju prednosti centralizirane koordinacije i lokalne fleksibilnosti (Boin & 't Hart, 2010).

Praktični doprinos rada odnosi se na identifikaciju konkretnih slabosti u institucionalnom okviru BiH i davanje preporuka za njihovo prevazilaženje: jačanje koordinacijskih tijela, razvoj integriranih informacionih sistema, profesionalizacija kadrova i veće uključivanje međunarodnih i regionalnih mehanizama saradnje. Ove preporuke mogu poslužiti kao osnova za kreiranje novih javnih politika i strateških dokumenata u oblasti kriznog menadžmenta. Za buduća istraživanja posebno je važno analizirati percepciju građana o institucionalnoj efikasnosti, kao i ispitati ekonomske i socijalne posljedice slabog kriznog menadžmenta. Također, potrebno je provesti komparativna istraživanja unutar regije Zapadnog Balkana, kako bi se identifikirali modeli koji su se pokazali uspješnima u sličnim društveno-političkim kontekstima (Štěpánek, 2017). U domenu javnih politika, nužno je razviti nacionalnu strategiju kriznog menadžmenta koja bi bila obavezujuća za sve nivoe vlasti. Takva strategija trebala bi uključivati procjene rizika, planove kontinuiteta i integrirane vježbe koordinacije. Uspostavljanje ovakvog strateškog dokumenta ojačalo bi otpornost institucija, ali i povećalo povjerenje građana u sposobnost države da ih zaštiti u vanrednim situacijama.

LITERATURA

Autori:

1. Alexander, D. (2013) *Principles of emergency planning and management*. Dunedin Academic Press.
2. Ansell, C., Boin, A. and Keller, A. (2010) 'Managing transboundary crises: Identifying the building blocks of an effective response system', *Journal of Contingencies and Crisis Management*, 18(4), pp. 195–207. doi:10.1111/j.1468-5973.2010.00620.x.
3. Bieber, F. (2020) 'Bosnia and Herzegovina: Federalism and the limits of consociational democracy', *Nationalities Papers*, 48(4), pp. 625–642. doi:10.1017/nps.2019.121.
4. Boin, A. and 't Hart, P. (2010) 'Organising for effective emergency management: Lessons from research', *Australian Journal of Public Administration*, 69(4), pp. 357–371. doi:10.1111/j.1467-8500.2010.00694.x.
5. Boin, A. and van Eeten, M.J.G. (2013) 'The resilient organization', *Public Management Review*, 15(3), pp. 429–445. doi:10.1080/14719037.2013.769856.
6. Boin, A., 't Hart, P., Stern, E. and Sundelius, B. (2017) *The politics of crisis management: Public leadership under pressure*. 2nd edn. Cambridge University Press.
7. Bundy, J., Pfarrer, M.D., Short, C.E. and Coombs, W.T. (2017) 'Crises and crisis management: Integration, interpretation, and research development', *Journal of Management*, 43(6), pp. 1661–1692. doi:10.1177/0149206316680030.
8. Christensen, T., Lægreid, P. and Rykkja, L.H. (2016) 'Organizing for crisis management: Building governance capacity and legitimacy', *Public Administration Review*, 76(6), pp. 887–897. doi:10.1111/puar.12558.
9. Cindrič, M. (2019) 'Sistem civilne zaštite u Sloveniji: izazovi i perspektive', *Revija za sigurnost*, 21(1), pp. 45–58.
10. Comfort, L.K. (2007) 'Crisis management in hindsight: Cognition, communication, coordination, and control', *Public Administration Review*, 67(s1), pp. 189–197. doi:10.1111/j.1540-6210.2007.00827.x.
11. Coombs, W.T. (2015) *Ongoing crisis communication: Planning, managing, and responding*. 4th edn. Sage.

12. Ejdus, F. (2017) 'Crisis management in Western Balkans: The case of Bosnia and Herzegovina', *Journal of Regional Security*, 12(1), pp. 7–28.
13. Garaplija, E. and Korajlić, N. (2022) 'Društveno-političke krize kao inkubatori suvremenih sigurnosnih izazova i prijetnji po nacionalnu sigurnost – studija slučaja BiH', *Kriminalističke teme*, 22(1-2), pp. 5–28.
14. Hopkin, P. (2018) *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. 5th edn. Kogan Page.
15. Kapucu, N. (2009) 'Interorganizational coordination in complex environments of disasters: The evolution of intergovernmental response networks', *Journal of Homeland Security and Emergency Management*, 6(1). doi:10.2202/1547-7355.1498.
16. Kapucu, N. and Garayev, V. (2011) 'Designing, managing, and sustaining functionally collaborative emergency management networks', *The American Review of Public Administration*, 41(3), pp. 279–302. doi:10.1177/0275074010380456.
17. Keil, S. and Kudlenko, A. (2015) 'Bosnia and Herzegovina – Federalism and decentralization as a strategy for conflict management', *Federal Governance*, 12(1), pp. 27–47.
18. Kowalski, P. (2015) 'Reform of the Polish civil protection system: From fragmentation to integration', *Central European Journal of Public Policy*, 9(1), pp. 55–70.
19. Majetić, F. (2020) 'Migrantska kriza u Bosni i Hercegovini: izazovi i institucionalni odgovor', *Godišnjak Fakulteta političkih nauka*, 14(1), pp. 45–63.
20. Mitroff, I.I. (2005) *Why some companies emerge stronger and better from a crisis: 7 essential lessons for surviving disaster*. AMACOM.
21. Pavić, I. and Vlahinić-Dizdarević, N. (2018) 'Upravljanje rizicima i krizni menadžment u Hrvatskoj: institucionalni okvir i izazovi', *Ekonomska misao i praksa*, 27(1), pp. 315–334.
22. Perry, R.W. and Quarantelli, E.L. (2005) *What is a disaster? New answers to old questions*. Xlibris.
23. Snyder, H. (2019) 'Literature review as a research methodology: An overview and guidelines', *Journal of Business Research*, 104, pp. 333–339. doi:10.1016/j.jbusres.2019.07.039.
24. Sylves, R. (2019) *Disaster policy and politics: Emergency management and homeland security*. CQ Press.

25. Štěpánek, P. (2017) 'Crisis management in the Czech Republic: Current trends and challenges', *Journal of Security and Sustainability Issues*, 6(4), pp. 633–642.
26. 't Hart, P. and Sundelius, B. (2013) 'Crisis management revisited: Lessons from research', in Boin, A. (ed.) *The politics of crisis management*. Cambridge University Press, pp. 285–300.
27. Weick, K.E. and Sutcliffe, K.M. (2015) *Managing the unexpected: Sustained performance in a complex world*. 3rd edn. Wiley.
28. Garaplija E. *Strategija pametne specijalizacije u korelaciji sa upravljanjem rizicima od katastrofa na kritičnoj infrastrukturi – studija slučaja „INZA Group"*. Zaštita i sigurnost. 2022.
29. Garaplija E. *Krivično-pravna zaštita sistema kritične infrastrukture*. Zaštita i sigurnost. 2021.

Institucije:

1. BBK (2016) *Federal Office of Civil Protection and Disaster Assistance – Annual Report*. Federal Ministry of the Interior, Germany.
2. European Commission (2020) *The EU Civil Protection Mechanism*. Publications Office of the European Union.
3. Ministarstvo sigurnosti BiH (2017) *Izvještaj o radu Ministarstva sigurnosti BiH*. Sarajevo: Ministarstvo sigurnosti BiH.
4. OECD (2018) *OECD reviews of risk management policies: The changing face of strategic crisis management*. OECD Publishing.
5. OSCE (2020) *Assessment of emergency management capacities in Bosnia and Herzegovina*. OSCE Mission to Bosnia and Herzegovina.
6. Transparency International (2022) *Corruption perceptions index 2022*. Transparency International.
7. UNDP (2015) *Disaster risk reduction and recovery in Bosnia and Herzegovina: Lessons from the 2014 floods*. UNDP BiH.
8. World Bank (2021) *Bosnia and Herzegovina – COVID-19 response and recovery report*. World Bank Group.

Legislativa:

1. Zakon o zaštiti i spašavanju ljudi i materijalnih dobara od prirodnih i drugih nesreća (2017) *Službene novine Federacije BiH*, br. 39/03, 22/06, 43/10.

ORGANIZATIONAL MODELS OF CRISIS MANAGEMENT: CAUSES AND CONSEQUENCES OF INSTITUTIONAL RISKS IN BOSNIA AND HERZEGOVINA

DOI: *10.70329/2744-2403.2025.5.10.7*

Review scientific article

Atina Perković

Abstract:
This review paper analyzes organizational models of crisis management and institutional risks in Bosnia and Herzegovina (BiH), with the aim of identifying the root causes of systemic weaknesses and their consequences for the effectiveness of crisis response. The theoretical framework encompasses the concept and dimensions of crisis management, the distinction between risk management and crisis management, as well as the key concepts of resilience, adaptability, and institutional coordination. Centralized, decentralized, and hybrid crisis-management models are examined, with examples drawn from international practice (the United States, the European Union, Germany, Slovenia, and Croatia). Special attention is devoted to the specificities of BiH, including its complex constitutional and legal structure, fragmented jurisdictions, and persistent coordination challenges at the state, entity, and local levels. Case studies of the 2014 floods, the 2018–2021 migration crisis, and the COVID-19 pandemic illustrate the practical implications of institutional inefficiency. The findings indicate that institutional risks in BiH result in slow decision-making processes, increased vulnerability of the population and critical infrastructure, erosion of public trust, and reputational risks at the international level. Based on comparative analysis with international practices, the paper provides recommendations for improving organizational models of crisis management in BiH. Key measures include strengthening coordination bodies, establishing integrated information systems, enhancing training and professionalization of personnel, and fostering international and regional cooperation. The paper concludes that institutional reforms in the field of crisis management are not merely a technical requirement, but a strategic priority for the security, stability, and democratic consolidation of Bosnia and Herzegovina.

Keywords: *Crisis management; institutional risks; Bosnia and Herzegovina; coordination; resilience; public policy; international cooperation*

1. Introduction

Crisis management represents a planned and coordinated process through which institutions and organizations prepare for, respond to, and recover from crisis situations that threaten the stability, security, and functioning of society. According to Mitroff (2005), a crisis is "an unplanned and potentially devastating event that threatens the fundamental goals, resources, and existence of an organization or community." Crisis management encompasses the stages of prevention, preparedness, response, and recovery, emphasizing the importance of institutional readiness and cross-sectoral coordination (Alexander, 2013). In contemporary societies characterized by globalization and increasing complexity of security challenges, crisis management has become a key component of national security and public policy. The significance of crisis management lies in its ability to mitigate the consequences of natural disasters, technical and technological accidents, health threats, and socio-political crises. Particularly in states with complex institutional structures, such as Bosnia and Herzegovina, the effectiveness of crisis management directly depends on coordination among different levels of government and the capacity to overcome institutional weaknesses (Perry & Quarantelli, 2005).

The aim of this article is to explore organizational models of crisis management, with a particular focus on the causes and consequences of institutional risks in Bosnia and Herzegovina. Through the analysis of theoretical models and practices from the international context, the article seeks to identify key factors that determine the effectiveness of crisis governance in complex socio-political systems. The methodological approach is based on a review analysis of relevant domestic and international literature. Scholarly articles, books, reports of international organizations, and legal documents were used to encompass both the theoretical and practical dimensions of crisis management. Such a review approach enables the synthesis of various research findings and provides insight into dominant trends, challenges, and recommendations in the field of crisis management (Snyder, 2019). The focus is placed on works addressing institutional risks, organizational models, and specific examples from Bosnia and Herzegovina and countries in the region. This methodological framework allows the article to be positioned within existing theoretical debates while offering practical implications relevant to the institutional capacities of crisis management in BiH.

2. Theoretical Framework of Crisis Management

Crisis management is defined as a planned and systematic process of preparing for, responding to, and recovering from events that may threaten the safety of people, infrastructure, or the functioning of institutions (Boin et al., 2017). The core dimensions of crisis management include prevention, preparedness, response, and recovery. Prevention involves identifying and mitigating potential risks before they escalate into a crisis, while preparedness encompasses planning, training, and capacity testing. Response refers to the activation of operational resources and decision-making in real time, whereas recovery relates to restoring systems to a functional state and building resilience for future crises (Coombs, 2015). These dimensions constitute a cyclical process in which each phase builds upon the previous one. The literature emphasizes that the success of crisis management is determined not only by formal plans but also by the flexibility of institutions to respond to unforeseen circumstances (Comfort, 2007).

Although the terms *risk management* and *crisis management* are often used interchangeably, a clear distinction exists between them. Risk management focuses on the systematic identification, assessment, and control of potential threats before they escalate into crisis situations (Hopkin, 2018). In other words, it represents a preventive process aimed at reducing the likelihood and consequences of adverse events. Crisis management, by contrast, is activated when risks escalate and develop into events requiring an urgent response (Bundy et al., 2017). While risk management is proactive and strategically oriented, crisis management is reactive, emphasizing rapid decision-making, resource coordination, and communication under conditions of uncertainty. In practice, these processes are complementary and constitute part of a broader security management framework.

Contemporary theoretical debates on crisis management particularly highlight three concepts: resilience, adaptability, and institutional coordination. *Resilience* refers to the ability of social and institutional systems to withstand shocks, recover quickly, and continue functioning despite crisis conditions. Boin and van Eeten (2013) note that resilience entails not only returning to the initial state but also the capacity to learn and strengthen institutional capabilities after a crisis. *Adaptability* denotes the flexibility of institutions and organizations to adjust strategies, structures, and processes in accordance with emerging circumstances. In the context of complex and multidimensional crises, adaptive capacity becomes a key determinant of effective management (Weick & Sutcliffe, 2015). Adaptive

institutions are capable of making decisions based on continuous learning, evaluation, and adjustment.

Institutional coordination is the third central concept, emphasizing the importance of cooperation among various organizations, levels of government, and sectors. According to Christensen et al. (2016), crises often reveal institutional fragmentation and the absence of adequate communication mechanisms. In complex state structures such as Bosnia and Herzegovina, coordination becomes essential for synchronized action and minimizing the consequences of crises.

Integrating these concepts into institutional models of crisis management enables the development of more resilient and functional systems capable of responding to challenges in a globalized and uncertain environment. Notably, Bosnia and Herzegovina is the only country in the Southeast European region that has not adopted a Smart Specialization Strategy—an important strategic document that aligns industrial, educational, and innovation policies to strengthen systemic resilience to crisis situations (Garaplija, 2022).

4. Organizational Models of Crisis Management

Centralized crisis-management models are based on a hierarchical decision-making structure dominated by a vertical chain of command and control. This approach is characterized by a clearly defined hierarchy, concentration of authority in central institutions, and a strict division of responsibilities (Kapucu & Garayev, 2011). The advantage of a centralized model lies in its capacity for rapid decision-making and swift mobilization of resources in crisis situations that require unified coordination. However, its main weakness is rigidity and limited adaptability in complex crises that demand quick, innovative responses (Christensen et al., 2016).

In contrast to centralized structures, decentralized models rely on horizontal coordination and cooperation among various institutions, levels of government, and sectors. In such models, responsibility for crisis management is distributed across local, regional, and national authorities, with the inclusion of non-governmental organizations, the private sector, and community actors (Ansell et al., 2010). Network-based models, in particular, emphasize the importance of interconnected actors through shared information platforms, communication channels, and partnership relations. The advantages of this approach include flexibility, innovativeness, and the ability to mobilize diverse resources. Yet, its

main drawback is the risk of fragmentation and coordination difficulties when institutions lack clearly defined mandates or adequate capacities (Kapucu, 2009).

Modern crisis-management systems are most commonly based on hybrid models that combine elements of centralization and decentralization. Hybrid models allow a balance between strong central coordination and flexible local implementation of measures. According to Boin and 't Hart (2010), this approach enables more effective adaptation to different types of crises—from natural disasters to complex socio-political threats. In practice, hybrid models rely on central institutions that set overall strategy and frameworks, while local communities and specialized agencies retain autonomy in implementation. Such a combination reduces the risk of overburdening central structures and enhances the resilience of the system as a whole.

In the United States, crisis management is coordinated by the Federal Emergency Management Agency (FEMA), which operates within a centralized framework but in close cooperation with state and local authorities. FEMA develops national plans and standards, while implementation depends on partnerships with local actors (Sylves, 2019). In the European Union, the EU Civil Protection Mechanism is based on a hybrid model. While the European Commission provides strategic coordination and resources (e.g., through the rescEU capacities), member states retain sovereignty over crisis management on their own territory (European Commission, 2020). This model demonstrates a balance between supranational coordination and national responsibility.

Countries in the region (e.g., Croatia, Slovenia, Serbia) apply different combinations of these models. Croatia, through the former State Protection and Rescue Directorate (DUZS), now integrated within the Ministry of the Interior, employs a hybrid approach with an emphasis on the strong role of local communities (Pavić & Vlahinić-Dizdarević, 2018).

Slovenia maintains a network-based model of cooperation between the state and local communities, while Serbia applies a more centralized approach through the Sector for Emergency Management of the Ministry of the Interior. These examples illustrate that contemporary crisis management cannot be entirely centralized nor fully decentralized. Instead, the best outcomes are achieved through an adaptive, hybrid model that combines the efficiency of central coordination with the flexibility of local action.

5. Crisis Management in Bosnia and Herzegovina

Bosnia and Herzegovina possesses a complex and multilayered institutional framework for crisis management, shaped by the country's constitutional and legal structure. At the state level, the key institution is the Ministry of Security of BiH, within which the Sector for Protection and Rescue is responsible for coordinating activities among the entities, the Brčko District, and international partners. However, its competencies are limited and often primarily coordinative rather than executive (Ministry of Security of BiH, 2017). At the entity level, the Republic of Srpska operates through the Republic Civil Protection Administration, while the Federation of BiH functions through the Federal Civil Protection Administration and an additional network of cantonal civil protection administrations. In the Brčko District, these responsibilities fall under the Department of Public Safety, which encompasses the protection and rescue sector.

This fragmentation means that each administrative unit has its own competencies, laws, and procedures (Law on Protection and Rescue of People and Material Goods from Natural and Other Disasters, 2017). At the local level, municipalities and cities maintain crisis headquarters and civil protection units, but their capacities vary depending on available resources and political will. Such a multilayered institutional structure complicates unified planning and coordination in crisis situations. Fragmentation of the crisis-management system in BiH is reflected in divided mandates, insufficient vertical coordination, and overlapping legal authorities. While entity and cantonal institutions possess operational capacities, the state level often remains confined to communication and coordination functions without direct executive power (Ejdus, 2017). Coordination problems become particularly evident when rapid and synchronized action is required.

In practice, the absence of a unified strategy results in each administrative unit applying different procedures, slowing the response and increasing the vulnerability of the population (Bieber, 2020). The lack of an integrated information system and joint contingency plans further hampers cooperation between levels of government. The floods that struck Bosnia and Herzegovina in May 2014 exposed deep systemic deficiencies. The lack of coordination between the state and entity levels led to delayed responses and inefficient allocation of resources. Local communities were often left to manage crises independently, while international assistance arrived more quickly than domestic institutions were able to respond (UNDP, 2015). Analyses indicate that the major challenge

involved the absence of a unified command system and poor communication across the entities.

During the migration crisis, BiH became a transit route for thousands of migrants, once again revealing institutional weaknesses. While the Ministry of Security held a coordination role, implementation was left to entity and local structures that lacked sufficient resources and a unified strategy. The outcome was an uneven response, with some cantons and municipalities refusing to assume responsibility for migrant accommodation, further politicizing the crisis (Majetić, 2020). This situation underscored how fragmentation and politicization can undermine the ability to manage transnational crises.

The COVID-19 pandemic even more clearly exposed weaknesses in Bosnia and Herzegovina's crisis-management system. Instead of a unified national strategy, each administrative unit adopted its own measures, resulting in confusion and an inconsistent response. Entities, cantons, and municipalities introduced varying restrictions and protocols, while the state level played only a minimal role in coordination or procurement of medical equipment (World Bank, 2021). The pandemic also revealed a significant lack of public trust in institutions, which further reduced the effectiveness of public-health measures.

The specificities of crisis management in Bosnia and Herzegovina stem from its complex state structure, multilayered institutional framework, and persistent fragmentation of competencies. Case studies demonstrate that crises reveal profound systemic weaknesses: lack of coordination, politicization of decision-making, and reliance on international assistance. These challenges clearly point to the need for strengthened institutional cooperation, development of integrated plans, and rebuilding public trust in crisis-management institutions. The Dayton Peace Agreement shaped an institutional framework that often functions as a form of "socio-political straitjacket," constraining effective decision-making during crises (Garaplija & Korajlić, 2022).

6. Causes of Institutional Risks in Bosnia and Herzegovina

One of the primary causes of institutional risks in Bosnia and Herzegovina lies in its constitutional and legal framework, established by the 1995 Dayton Peace Agreement. This framework created a complex and multilayered state structure with divided competencies among the state level, the two entities, the Brčko District, and, in the case of the Federation of BiH, an additional ten cantons (Bieber, 2020). Such fragmentation results in the absence of a unified strategy and inconsistent responses to crisis situations.

In practice, each administrative unit maintains its own regulations, institutions, and procedures, creating legal gaps and overlapping jurisdictions (Ejdus, 2017). The consequence is hampered coordination, particularly in crises that require rapid, centralized decision-making. Bosnia and Herzegovina is also characterized by deep political and ethnic divisions that significantly affect the effectiveness of crisis management.

Political elites often instrumentalize crises as tools of political competition, meaning that decisions are not based on expert analyses or citizens' needs, but on the particular interests of political parties (Keil & Kudlenko, 2015). The lack of consensus among key political actors leads to decision-making deadlocks, prolonged processes, and the absence of a unified approach. This dynamic is especially pronounced in crises of a transnational nature—such as the migration crisis—where political conflict further complicates institutional response (Majetić, 2020).

Beyond political and legal challenges, resource limitations constitute a significant cause of institutional risks in BiH. Institutions responsible for crisis management face chronic shortages of financial resources, technical equipment, and specialized human resources. Insufficient long-term investment in civil protection infrastructure reduces the capacity for timely response to natural and societal crises (UNDP, 2015). Human resource issues further exacerbate the problem: many institutions rely on politically appointed personnel rather than professional standards, resulting in reduced competence and a lack of expertise necessary for managing complex crises (OSCE, 2020).

Another important cause of institutional risks in BiH is the absence of a strategic culture of crisis management. *Strategic culture* refers to the orientation of institutions toward long-term planning, prevention, and the development of resilience, rather than merely reactive action once a crisis has already occurred (Boin et al., 2017). In BiH, a reactive approach dominates, with measures being adopted ad hoc, without systematic reliance on risk assessments, scenarios, or continuity plans.

The lack of strategic vision was clearly evident during the 2014 floods and the COVID-19 pandemic, when institutions responded only after the crisis had already escalated, lacking adequately developed preventive mechanisms (World Bank, 2021).

7. Consequences of Institutional Risks in Bosnia and Herzegovina

One of the most evident consequences of institutional risks in Bosnia and Herzegovina is slow and uncoordinated decision-making during crisis situations. Owing to the fragmented system of competencies, decisions are often made through multilayered political negotiations, which prolongs response time and reduces the effectiveness of implemented measures (Christensen et al., 2016). During the 2014 floods, for example, different levels of government adopted measures without a unified plan, resulting in delays in evacuating the population and distributing aid (UNDP, 2015). The absence of a unified command system and slow decision-making directly undermine the speed and quality of crisis response.

Institutional weaknesses directly increase the vulnerability of the population and infrastructure. When decisions are made slowly and in an uncoordinated manner, the consequences of crises become more severe and long-lasting. Insufficient preventive measures, combined with weak investment in disaster-resilient infrastructure, lead to a higher number of casualties and greater material damage (Kapucu, 2009). During the COVID-19 pandemic, discrepancies in measures adopted by the entities and cantons created public confusion, increased the risk of virus transmission, and further strained the healthcare system (World Bank, 2021).

Ineffective crisis management contributes to the erosion of public trust in institutions. When citizens perceive that institutions do not act in their best interest or that decisions are driven by political rather than expert considerations, the legitimacy of authorities diminishes (Perry & Quarantelli, 2005). Public trust is a crucial factor in the successful implementation of crisis measures, as citizens must be willing to accept and comply with them. During the 2018–2021 migration crisis, diverging positions among local and state institutions fostered feelings of insecurity among citizens and reinforced perceptions that authorities lacked control over the situation (Majetić, 2020).

Institutional risks affect not only domestic stability but also the international perception of Bosnia and Herzegovina. Weaknesses in crisis management generate reputational risks that undermine the state's credibility in the eyes of international partners and investors. In BiH, international organizations and neighboring countries have frequently assumed leading roles in providing assistance, creating the perception that the country lacks sufficient capacity to independently manage crises (Bieber, 2020). Such a reputation can diminish institutional trust, complicate access to international funding, and weaken the state's position in regional and global security arrangements.

The consequences of institutional risks in Bosnia and Herzegovina are therefore multifaceted: slow and uncoordinated decision-making, increased vulnerability of citizens and infrastructure, loss of public trust in institutions, and reputational damage on the international stage.

8. Comparative Analysis with International Practices

Germany is frequently cited as an example of an effective crisis management model, combining centralized coordination with decentralized implementation. The Federal Office of Civil Protection and Disaster Assistance (BBK) coordinates strategic activities, while the federal states (Länder) retain significant autonomy in implementing measures (BBK, 2016). This model enables a balance between efficient central coordination and the flexibility of local responses.

Slovenia has developed an integrated civil protection system based on horizontal coordination among state institutions, local communities, and volunteer organizations. Local units play a critical role in initial crisis response, and transparent communication with citizens enhances public trust in institutions and overall response effectiveness (Cindrič, 2019).

Croatia, through the State Administration for Civil Protection (DUZS), now integrated into the Directorate for Civil Protection within the Ministry of the Interior, applies a hybrid model emphasizing local government involvement while maintaining a clear command hierarchy. DUZS has also acted as a mentor in strengthening Bosnia and Herzegovina's civil protection system through the EU project "EU4 Better Civil Protection in B&H." The 2014 floods highlighted the need for stronger central coordination, and subsequent reform measures further reinforced vertical integration of the system (Pavić & Vlahinić-Dizdarević, 2018).

Transitional states often face challenges similar to those in Bosnia and Herzegovina, such as weak institutional capacities, politicization, and resource constraints. However, there are examples of successful adaptation. Poland, after the 1990s, reformed its civil protection system by introducing a unified legislative framework and a national security strategy, ensuring greater coordination between local and state levels (Kowalski, 2015). The Czech Republic developed a crisis management system based on networked collaboration among state institutions, local authorities, and the NGO sector, with a strong emphasis on preventive planning (Štěpánek, 2017).

These examples demonstrate that transitional states can achieve significant progress through clear normative frameworks, professionalization of personnel, and investment in technical capacities. For Bosnia and Herzegovina, transferring

knowledge and best practices from international experiences is a crucial mechanism for improving crisis management. Lessons from Germany and Slovenia highlight the importance of an integrated information system, professionalized personnel, and clear allocation of responsibilities. Croatia's experience shows how crises can serve as catalysts for reform and strengthening coordination bodies (Pavić & Vlahinić-Dizdarević, 2018).

In the context of transitional states, Bosnia and Herzegovina could benefit from developing a unified legislative framework at the state level, precisely defining competencies and procedures across all levels of government. Additionally, implementing joint training programs and regional centers of excellence would strengthen institutional resilience. Knowledge transfer can be achieved through collaboration with international organizations (e.g., EU Civil Protection Mechanism, UNDP, OSCE), bilateral agreements with neighboring countries, and Bosnia and Herzegovina's participation in regional crisis management networks. This approach would reduce institutional fragmentation and enhance the capacity for coordinated action in crises that cross administrative boundaries.

9. Recommendations for Improving Organizational Models in Bosnia and Herzegovina

The first step in enhancing the organizational models of crisis management in Bosnia and Herzegovina is strengthening coordination bodies at the state level. Given the fragmented structure and multi-layered system of government, it is crucial to establish a centralized coordination body with clear decision-making authority during crises (Christensen et al., 2016). This body should be responsible for harmonizing entity, cantonal, and local plans, as well as ensuring alignment with international standards. Strengthening inter-institutional cooperation would reduce the risk of overlapping competencies and contribute to more efficient resource allocation (Kapucu, 2009).

Effective crisis management is impossible without a well-developed integrated information system that enables timely data exchange among institutions. Currently, Bosnia and Herzegovina lacks a unified digital platform connecting state, entity, cantonal, and local levels during crises (OSCE, 2020). Experiences from Germany and Slovenia show that shared information systems significantly improve decision-making speed and operational accuracy (BBK, 2016; Cindrič, 2019). Implementing such a system in Bosnia and Herzegovina would enhance risk monitoring, response coordination, and transparency toward citizens.

Professionalization of personnel is another key prerequisite for strengthening system resilience. Currently, crisis management in Bosnia and Herzegovina often

relies on politically appointed staff, while technical and professional capacities remain underdeveloped (OSCE, 2020). It is recommended to introduce systematic education and certified training programs incorporating international standards and best practices (Weick & Sutcliffe, 2015). Additionally, developing academic and professional programs at universities and specialized centers would create a pool of experts capable of operating in complex crises.

International organizations, such as the United Nations (UNDP, WHO), the European Union (EU Civil Protection Mechanism), and the OSCE, already play an important role in capacity building in Bosnia and Herzegovina. However, their support needs to be more systematically integrated into domestic institutional structures. Bosnia and Herzegovina should actively leverage opportunities provided by membership in international civil protection mechanisms to gain access to additional resources, knowledge, and training (European Commission, 2020).

Regional cooperation, particularly with Western Balkan countries, can be crucial for a coordinated response to transnational crises such as floods, fires, or migration flows. Establishing regional centers of excellence for crisis management would enable the exchange of experiences and faster mobilization of resources in emergencies (Štěpánek, 2017).

These recommendations collectively aim to reduce institutional fragmentation, enhance operational efficiency, and build resilient, adaptive, and professionalized crisis management structures in Bosnia and Herzegovina.

10. Conclusion

The analysis of organizational models of crisis management and institutional risks in Bosnia and Herzegovina demonstrates that the country's complex state structure, legal fragmentation, and political divisions significantly hinder effective crisis response. While the theoretical framework of crisis management emphasizes the importance of resilience, adaptability, and coordination (Boin et al., 2017), the practical reality in Bosnia and Herzegovina shows that institutional risks result in slow and uncoordinated decision-making, increased vulnerability of the population, and a loss of public trust in institutions (Christensen et al., 2016; Perry & Quarantelli, 2005). As highlighted by Garaplija and Korajlić (2022), institutional risks in Bosnia and Herzegovina are not merely technical challenges in crisis management but reflect a deep political and social crisis that generates security threats and weakens state resilience.

Case studies – including the 2014 floods, the migration crisis, and the COVID-19 pandemic – illustrate how institutional weaknesses manifest in real crisis situations, leading to reliance on international assistance (UNDP, 2015; World Bank, 2021). The theoretical contribution of this study lies in the systematization of key crisis management models – centralized, decentralized, and hybrid – and their comparison with practice in Bosnia and Herzegovina. It is emphasized that no single model is sufficient on its own; the optimal solution lies in hybrid structures that combine the advantages of centralized coordination with local flexibility (Boin & 't Hart, 2010).

The practical contribution of this work pertains to identifying concrete weaknesses in Bosnia and Herzegovina's institutional framework and providing recommendations for overcoming them: strengthening coordination bodies, developing integrated information systems, professionalizing personnel, and enhancing the use of international and regional cooperation mechanisms. These recommendations can serve as a basis for creating new public policies and strategic documents in the field of crisis management.

For future research, it is particularly important to analyze citizens' perceptions of institutional effectiveness and examine the economic and social consequences of weak crisis management. Comparative studies within the Western Balkans are also necessary to identify models that have proven successful in similar socio-political contexts (Štěpánek, 2017). In the domain of public policy, it is crucial to develop a national crisis management strategy that is binding for all levels of government. Such a strategy should include risk assessments, continuity plans, and integrated coordination exercises. Establishing this strategic document would strengthen institutional resilience and increase public trust in the state's capacity to protect citizens during emergencies.

LITERATURE

Autorhs:

30. Alexander, D. (2013) *Principles of emergency planning and management*. Dunedin Academic Press.
31. Ansell, C., Boin, A. and Keller, A. (2010) 'Managing transboundary crises: Identifying the building blocks of an effective response system', *Journal of Contingencies and Crisis Management*, 18(4), pp. 195–207. doi:10.1111/j.1468-5973.2010.00620.x.
32. Bieber, F. (2020) 'Bosnia and Herzegovina: Federalism and the limits of consociational democracy', *Nationalities Papers*, 48(4), pp. 625–642. doi:10.1017/nps.2019.121.
33. Boin, A. and 't Hart, P. (2010) 'Organising for effective emergency management: Lessons from research', *Australian Journal of Public Administration*, 69(4), pp. 357–371. doi:10.1111/j.1467-8500.2010.00694.x.
34. Boin, A. and van Eeten, M.J.G. (2013) 'The resilient organization', *Public Management Review*, 15(3), pp. 429–445. doi:10.1080/14719037.2013.769856.
35. Boin, A., 't Hart, P., Stern, E. and Sundelius, B. (2017) *The politics of crisis management: Public leadership under pressure*. 2nd edn. Cambridge University Press.
36. Bundy, J., Pfarrer, M.D., Short, C.E. and Coombs, W.T. (2017) 'Crises and crisis management: Integration, interpretation, and research development', *Journal of Management*, 43(6), pp. 1661–1692. doi:10.1177/0149206316680030.
37. Christensen, T., Lægreid, P. and Rykkja, L.H. (2016) 'Organizing for crisis management: Building governance capacity and legitimacy', *Public Administration Review*, 76(6), pp. 887–897. doi:10.1111/puar.12558.
38. Cindrič, M. (2019) 'Sistem civilne zaštite u Sloveniji: izazovi i perspektive', *Revija za sigurnost*, 21(1), pp. 45–58.
39. Comfort, L.K. (2007) 'Crisis management in hindsight: Cognition, communication, coordination, and control', *Public Administration Review*, 67(s1), pp. 189–197. doi:10.1111/j.1540-6210.2007.00827.x.
40. Coombs, W.T. (2015) *Ongoing crisis communication: Planning, managing, and responding*. 4th edn. Sage.

41. Ejdus, F. (2017) 'Crisis management in Western Balkans: The case of Bosnia and Herzegovina', *Journal of Regional Security*, 12(1), pp. 7–28.
42. Garaplija, E. and Korajlić, N. (2022) 'Društveno-političke krize kao inkubatori suvremenih sigurnosnih izazova i prijetnji po nacionalnu sigurnost – studija slučaja BiH', *Kriminalističke teme*, 22(1-2), pp. 5–28.
43. Hopkin, P. (2018) *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. 5th edn. Kogan Page.
44. Kapucu, N. (2009) 'Interorganizational coordination in complex environments of disasters: The evolution of intergovernmental response networks', *Journal of Homeland Security and Emergency Management*, 6(1). doi:10.2202/1547-7355.1498.
45. Kapucu, N. and Garayev, V. (2011) 'Designing, managing, and sustaining functionally collaborative emergency management networks', *The American Review of Public Administration*, 41(3), pp. 279–302. doi:10.1177/0275074010380456.
46. Keil, S. and Kudlenko, A. (2015) 'Bosnia and Herzegovina – Federalism and decentralization as a strategy for conflict management', *Federal Governance*, 12(1), pp. 27–47.
47. Kowalski, P. (2015) 'Reform of the Polish civil protection system: From fragmentation to integration', *Central European Journal of Public Policy*, 9(1), pp. 55–70.
48. Majetić, F. (2020) 'Migrantska kriza u Bosni i Hercegovini: izazovi i institucionalni odgovor', *Godišnjak Fakulteta političkih nauka*, 14(1), pp. 45–63.
49. Mitroff, I.I. (2005) *Why some companies emerge stronger and better from a crisis: 7 essential lessons for surviving disaster*. AMACOM.
50. Pavić, I. and Vlahinić-Dizdarević, N. (2018) 'Upravljanje rizicima i krizni menadžment u Hrvatskoj: institucionalni okvir i izazovi', *Ekonomska misao i praksa*, 27(1), pp. 315–334.
51. Perry, R.W. and Quarantelli, E.L. (2005) *What is a disaster? New answers to old questions*. Xlibris.
52. Snyder, H. (2019) 'Literature review as a research methodology: An overview and guidelines', *Journal of Business Research*, 104, pp. 333–339. doi:10.1016/j.jbusres.2019.07.039.
53. Sylves, R. (2019) *Disaster policy and politics: Emergency management and homeland security*. CQ Press.

54. Štěpánek, P. (2017) 'Crisis management in the Czech Republic: Current trends and challenges', *Journal of Security and Sustainability Issues*, 6(4), pp. 633–642.
55. 't Hart, P. and Sundelius, B. (2013) 'Crisis management revisited: Lessons from research', in Boin, A. (ed.) *The politics of crisis management*. Cambridge University Press, pp. 285–300.
56. Weick, K.E. and Sutcliffe, K.M. (2015) *Managing the unexpected: Sustained performance in a complex world*. 3rd edn. Wiley.
57. Garaplija E. *Strategija pametne specijalizacije u korelaciji sa upravljanjem rizicima od katastrofa na kritičnoj infrastrukturi – studija slučaja „INZA Group"*. Zaštita i sigurnost. 2022.
58. Garaplija E. *Krivično-pravna zaštita sistema kritične infrastrukture*. Zaštita i sigurnost. 2021.

Institutions:

9. BBK (2016) *Federal Office of Civil Protection and Disaster Assistance – Annual Report*. Federal Ministry of the Interior, Germany.
10. European Commission (2020) *The EU Civil Protection Mechanism*. Publications Office of the European Union.
11. Ministarstvo sigurnosti BiH (2017) *Izvještaj o radu Ministarstva sigurnosti BiH*. Sarajevo: Ministarstvo sigurnosti BiH.
12. OECD (2018) *OECD reviews of risk management policies: The changing face of strategic crisis management*. OECD Publishing.
13. OSCE (2020) *Assessment of emergency management capacities in Bosnia and Herzegovina*. OSCE Mission to Bosnia and Herzegovina.
14. Transparency International (2022) *Corruption perceptions index 2022*. Transparency International.
15. UNDP (2015) *Disaster risk reduction and recovery in Bosnia and Herzegovina: Lessons from the 2014 floods*. UNDP BiH.
16. World Bank (2021) *Bosnia and Herzegovina – COVID-19 response and recovery report*. World Bank Group.

Legislation:

2. Zakon o zaštiti i spašavanju ljudi i materijalnih dobara od prirodnih i drugih nesreća (2017) *Službene novine Federacije BiH*, br. 39/03, 22/06, 43/10.

ONLINE SEKSUALNA EKSPLOATACIJA DJECE: METODE POČINILACA I ODGOVORI SIGURNOSNIH AGENCIJA

DOI: *10.70329/2744-2403.2025.5.10.8*

Pregledni rad

Aldina Bjelić, MA[56]

Sažetak:

Online seksualna eksploatacija djece predstavlja jedan od najbrže rastućih oblika cyber kriminala, potaknut dinamičnim razvojem digitalnih tehnologija, globalnom povezanosti i širokom dostupnošću komunikacijskih platformi. Počinioci koriste raznovrsne metode kojima ciljaju ranjivu populaciju djece, uključujući grooming, sextortion, socijalni inženjering, kreiranje lažnih identiteta i distribuciju materijala seksualnog zlostavljanja putem enkriptiranih kanala, peer-to-peer mreža i darknet servisa. Tehnološki faktori poput end-to-end enkripcije, kriptovaluta, anonimizacijskih mreža i generativne umjetne inteligencije dodatno otežavaju detekciju i omogućavaju počiniocima visok stepen operativne sigurnosti. Sigurnosne agencije odgovaraju razvojem specijaliziranih timova, jačanjem digitalno-forenzičkih kapaciteta, međunarodnom saradnjom i oslanjanjem na OSINT i SOCMINT metode u identifikaciji počinilaca i praćenju kriminalnih mreža. Ipak, izazovi poput nedostatka kadra, tehničkih barijera, fragmentiranih nadležnosti i brzine tehnoloških promjena i dalje ograničavaju efikasnost institucionalnog odgovora. Pravne i političke mjere, uključujući Budimpeštansku konvenciju i Lanzarote konvenciju, pružaju okvir za djelovanje, ali u praksi ostaje značajan jaz između normativnih zahtjeva i operativnih mogućnosti. Rad naglašava da borba protiv online seksualne eksploatacije djece zahtijeva kombinaciju preventivnih mjera, tehnoloških inovacija, multisektorske saradnje i jačanja kapaciteta sigurnosnih institucija. Zaštita djece u digitalnom prostoru predstavlja ne samo pravni i društveni prioritet nego i ključni faktor ukupne sigurnosne stabilnosti.

Ključne riječi*: cyber kriminal, grooming, sextortion, darknet, OSINT*

[56] aldinabjelic@hotmail.com

1. Uvod

Online seksualna eksploatacija djece predstavlja jedan od najsloženijih i najbrže rastućih izazova savremenog digitalnog okruženja. Razvoj informacijsko-komunikacijskih tehnologija, široka dostupnost interneta i masovna upotreba pametnih telefona otvorili su nove prostore interakcije u kojima djeca provode sve veći dio svakodnevnog života. U takvom ambijentu, tradicionalni obrasci viktimizacije poprimaju nove digitalne dimenzije, a počinioci koriste specifične tehnike prilagođene online okruženju kako bi identifikovali, manipulirali i eksploatisali djecu. Ovaj fenomen dobija na ozbiljnosti jer internet omogućava širok spektar anonimnih i teško detektabilnih aktivnosti koje nadilaze geografske granice i izmiču tradicionalnim oblicima nadzora i kontrole. Istovremeno, globalni porast slučajeva online seksualne eksploatacije djece ukazuje na rastući jaz između brzog tehnološkog napretka i institucionalne sposobnosti da se na adekvatan način zaštiti najranjivija populacija. Sigurnosne i druge agencije suočene su s izazovima poput enkriptiranih komunikacijskih kanala, decentraliziranih mreža, kriptovaluta i generativne umjetne inteligencije, koji dodatno otežavaju identifikaciju počinilaca i procesuiranje krivičnih djela. Iako postoje međunarodni standardi, pravni okviri i specijalizirane jedinice koje se bave ovim oblikom kriminala, njihova efikasnost često zavisi od tehničke opremljenosti, kapaciteta za digitalnu forenziku i nivoa međunarodne saradnje. Uzimajući u obzir navedene okolnosti, cilj ovog preglednog rada je sistematizirati savremene spoznaje o metodama koje online počinioci najčešće koriste, analizirati institucionalne i sigurnosne odgovore, te ukazati na ključne izazove koji oblikuju mogućnosti efikasne prevencije i represije. Namjera je ponuditi jasan i sveobuhvatan pregled literature i praksi koje mogu poslužiti stručnjacima, istraživačima i donositeljima odluka u unapređenju politika zaštite djece u digitalnom prostoru.

2. Definisanje cyber eskploatacije djece

Cyber eksploatacija djece predstavlja skup kriminalnih radnji koje uključuju korištenje informaciono-komunikacijskih tehnologija radi seksualnog iskorištavanja maloljetnih osoba, distribucije ili proizvodnje materijala seksualnog zlostavljanja, manipulacije, iznude ili drugih oblika nedozvoljenog postupanja nad djecom. Prema Lanzarote konvenciji Vijeća Evrope (2007), seksualno iskorištavanje djece obuhvata sve radnje u kojima se dijete koristi u svrhu seksualnog zadovoljstva druge osobe, bez obzira na to odvija li se čin u fizičkom ili digitalnom prostoru. Digitalni prostor omogućava da se ove radnje odvijaju bez fizičkog kontakta, pri čemu počinioci koriste anonimnost, tehničku zaštitu i globalnu dostupnost interneta kako bi izbjegli nadzor i odgovornost. Internet tehnologija omogućava spajanje udaljenih, širenje vijesti i informacija, ali se u navedenom krije i mogućnost manipulacije umom i načinom razmišljanja

svakog misaonog bića (Muhić, 2025).U savremenoj literaturi i praksi najčešće se koristi termin online seksualna eksploatacija djece, odnosno *Online Child Sexual Exploitation*, koji prema izvještajima Europola (2025) obuhvata grooming, sextortion, regrutaciju djece za seksualne aktivnosti putem interneta i distribuciju materijala seksualnog zlostavljanja djece. S tim u vezi, poseban akcenat stavlja se na CSAM (Child Sexual Abuse Material), odnosno materijal koji vizualno prikazuje seksualno zlostavljanje djeteta. Interpol i ECPAT (2018) predlažu sve češću upotrebu termina CSEM (Child Sexual Exploitation Material), naglašavajući da fokus nije samo na prikazu zlostavljanja, nego na eksploataciji koja stoji iza nastanka takvog sadržaja.

Jedan od najznačajnijih elemenata cyber eksploatacije je grooming, proces manipulativne izgradnje povjerenja između počinioca i djeteta. Whittle i saradnici (2014) definišu grooming kao ciljanu, faznu i psihološki usmjerenu strategiju kojom počinilac stvara emocionalnu vezu sa žrtvom, pripremajući je na seksualiziranu komunikaciju ili susret. Grooming se danas dominantno odvija na društvenim mrežama, online igrama i chat aplikacijama, gdje počinilac može nesmetano komunicirati, bez neposrednog nadzora odraslih. Sextortion predstavlja drugi ključni modalitet eksploatacije, a Wolak i saradnici (2018) definiraju ga kao oblik iznude u kojem počinilac zahtijeva dodatne seksualne sadržaje, novac ili druge koristi, prijeteći objavljivanjem stvarnog ili manipuliranog materijala koji prikazuje dijete u seksualiziranom kontekstu. Ovaj oblik kriminala postaje sve prisutniji zbog mogućnosti obrade slika i videa, uključujući deepfake tehnologiju, koju UNODC (2015) identifikuju kao rastući izazov za identifikaciju žrtava i dokazni postupak. Razumijevanje cyber eksploatacije djece zahtijeva poznavanje tehnoloških faktora koji omogućavaju da počinioci djeluju uz minimalan rizik. Izvještaji Europola i Interpola pokazuju da enkriptirane aplikacije, anonimne mreže poput Tora, kriptovalute i peer-to-peer sistemi omogućavaju visok stepen digitalne sigurnosti počinioca, dok istovremeno otežavaju istrage sigurnosnih agencija. UNODC upozorava i na porast sintetičkih vizualnih materijala generiranih umjetnom inteligencijom, koji se koriste u svrhe manipulacije, ucjene ili distribucije, čime se dodatno zamagljuju granice između stvarnog i kreiranog sadržaja. Stoga se cyber eksploatacija djece može jasno definisati tek kada se posmatra kroz tri međusobno povezana aspekta - krivična ponašanja koja se manifestuju u digitalnom prostoru, tehnološka sredstva koja omogućavaju anonimnost i širenje materijala, te psihološko-manipulativne strategije kojima se počinioci služe u komunikaciji sa žrtvama. Tek kombinacija ovih elemenata omogućava adekvatno prepoznavanje rizika, pravilnu kategorizaciju pojavnih oblika i izgradnju institucionalnih mehanizama za prevenciju i suzbijanje ovog oblika kriminaliteta.

3. Metode počinilaca online seksualne eksploatacije djece

Metode koje počinioci koriste u online seksualnoj eksploataciji djece kontinuirano se razvijaju paralelno s razvojem komunikacijskih tehnologija, digitalnih platformi i novih mogućnosti za prikrivanje identiteta. Za razliku od tradicionalnih oblika zlostavljanja, koji zahtijevaju fizičku prisutnost i direktan kontakt, online okruženje omogućava počiniocima da djeluju transnacionalno, anonimno i uz minimalne rizike otkrivanja. Europol u svojim IOCTA izvještajima (2022-2025) naglašava da je najveća prijetnja upravo dinamičnost metoda, koje se brzo prilagođavaju promjenama sigurnosnih protokola i nadzornih mehanizama.

3.1. Grooming kao centralni obrazac ponašanja

Grooming predstavlja jedan od najkompleksnijih i najopasnijih oblika online manipulacije djece, a njegovo razumijevanje zahtijeva analizu dinamičnih i međusobno povezanih faza kroz koje počinitelji nastoje ostvariti psihološku kontrolu nad djetetom. Tipologija koju je razvila O'Connell (2003) jedna je od najutjecajnijih i najdetaljnijih u ranoj fazi istraživanja ovog fenomena, te predstavlja temelj za savremene modele koji objašnjavaju kako se komunikacijski obrasci, manipulativne strategije i tehnološki faktori uklapaju u proces eksploatacije. Ipak, kasniji radovi pokazuju da se grooming ne odvija uvijek linearno te da počinitelji znatno ubrzavaju pojedine faze. Zbog toga je danas nužno posmatrati grooming kao fluidan, prilagodljiv i višedimenzionalan proces koji se oblikuje u skladu s motivacijom počinitelja, karakteristikama djeteta i specifičnostima digitalnog okruženja. O'Connell (2003) je dala naredne faze groominga koje je potrebno razmotriti zarad efikasnijeg shvatanja problema u vezi sa istraživanjem ove vrste krivičnog djela, a samim time i procesuiranjem.

Faza formiranja prijateljstva

Prema O'Connell (2003), proces najčešće počinje fazom uspostavljanja prijateljstva, u kojoj počinitelj ulazi u prvi kontakt s djetetom, bilo predstavljajući se kao vršnjak, bilo otvoreno kao odrasla osoba. Cilj je procijeniti djetetovu otvorenost za komunikaciju i uspostaviti osnovni osjećaj poznanstva. U ovoj fazi počinitelj postavlja uvodna pitanja o dobi, interesima, školskim obavezama ili hobijima, te često traži fotografije djeteta kako bi potvrdio njegov identitet ili provjerio odgovara li fizički njegovim preferencijama. Dumitriu, Dudu i Nanău (2024) napominju da se već u ovoj fazi može prepoznati selekcija žrtve, jer počinitelji biraju djecu koja pokazuju znake ranjivosti ili potrebe za potvrdom.

Faza formiranja veze

Ova faza predstavlja produbljivanje prvog kontakta i stvaranje emocionalne bliskosti. Počinitelj se predstavlja kao podrška, povjerljiv sagovornik ili „najbolji prijatelj", a razgovori se šire na teme koje uključuju porodične odnose, školske

probleme, uspjehe, nesigurnosti i svakodnevne izazove (O'Connell, 2003). Cilj ove faze je stvaranje privida emocionalne sigurnosti. Prema Whittle i drugim (2013), počinitelji tokom ove faze aktivno prate emocionalna stanja djeteta kako bi prepoznali trenutke ranjivosti i iskoristili ih za jačanje veze. Cano, Fernandez i Alani (2014) ističu da ova faza odgovara prvoj etapi Olsonove teorije luring komunikacije, poznatoj kao *Deceptive Trust Development*, u kojoj počinitelj namjerno stvara atmosferu povjerenja i zajedničke identifikacije.

Faza procjene rizika

Nakon uspostavljanja osnovnog odnosa, počinitelji prelaze na procjenu rizika otkrivanja. O'Connell (2003) pokazuje da počinitelji postavljaju pitanja poput: „Ko sve koristi računar?", „Jesu li roditelji trenutno kod kuće?", „Da li imaš telefon koji koristiš samo ti?", s ciljem da utvrde stepen nadzora i sigurnost daljnje komunikacije. Ova faza je ključna jer određuje intenzitet i smjer narednih postupaka. Chiang i Grant (2017) napominju da suvremeni groomeri često ne čekaju duže razdoblje da bi procijenili rizik, već tu fazu obavljaju u ranim minutama razgovora, što omogućava brzu procjenu mogućnosti manipulacije i izbjegavanje nadzora.

Faza eksluzivnosti

U ovoj fazi počinitelj uvodi narative o posebnom odnosu, međusobnoj tajnosti i emocionalnoj povezanosti. Tipični izrazi uključuju tvrdnje da dijete može vjerovati samo njemu, da ga odrasli ne razumiju ili da su njih dvoje „posebni" i „povezani na način koji drugi ne mogu razumjeti". Cilj je izolirati dijete od drugih izvora podrške i stvoriti odnos zavisnosti. Prema Dumitriu i saradniciima (2024), ova faza odgovara mehanizmima izolacije i psihološke kontrole, koji se pojavljuju i kod offline zlostavljanja. Ova faza također priprema dijete za normalizaciju seksualizirane komunikacije tako što pojačava osjećaj lojalnosti i emocionalne obaveze prema počinitelju.

Seksualna faza

Nakon što je postignut određeni stepen povjerenja i izolacije, počinitelj prelazi na postepeno ili naglo seksualiziranje komunikacije. Pitanja koja uvode seksualne teme mogu biti vrlo suptilna („jesi li imao/la simpatiju?"), ali i direktna („da li se diraš?"). Također, počinitelj može tražiti eksplicitne slike, predlagati upotrebu kamere ili detaljno opisivati seksualna ponašanja. Chiang i Grant (2017) ukazuju da savremeni groomeri često uvode seksualni sadržaj znatno ranije nego što O'Connell-ov model sugerira, ponekad već u prvim minutama komunikacije, što predstavlja veliki izazov za tradicionalne modele detekcije. Kloess, Hamilton-Giachritsis i Beech (2017) dodatno razlikuju groomere koji koriste *indirektni pristup*, postepeno povećanje seksualizacije od onih koji koriste *direktni pristup*, bez prethodne emocionalne pripreme.

Faza izvođenja seksualnih fantazija

O'Connell (2003) dodaje završnu fazu u kojoj počinitelj pokušava navesti dijete na seksualno eksplicitne radnje, bilo online ili offline. To uključuje vođenje djeteta kroz simulirane seksualne scenarije, izvođenje eksplicitnih radnji pred kamerom ili predlaganje fizičkog susreta. Chiang i Grant (2017) potvrđuju da se u suvremenim slučajevima ova faza može pojaviti veoma rano, zbog ubrzane dinamike komunikacije i činjenice da počinitelji često djeluju iz pedofilskih zajednica na darknetu gdje se razmjenjuje znanje i "savjeti" o optimalnim strategijama eksploatacije.

Dinamičnost, preklapanja i ubrzavanje faza

Iako je O'Connell-in model bio pionirski i ostaje najdetaljniji opis faznog pristupa, moderni empirički radovi (Chiang & Grant, 2017; Kloess et al., 2017) pokazuju da se grooming u savremenom online okruženju odvija mnogo brže i da faze nisu ni približno linearne.
Studije otkrivaju da:

- sve faze mogu nastupiti unutar prvog sata komunikacije
- seksualizacija može biti prisutna već u prvim porukama
- faze se često preklapaju
- groomeri mogu preskakati čitave faze ako procijene da je dijete ranjivo
- digitalne platforme omogućavaju brzu eskalaciju, naročito uz enkriptirane aplikacije

Dumitriu i saradnici (2024) potvrđuju da grooming treba posmatrati kao adaptivni proces koji zavisi od motivacije počinitelja, ranjivosti žrtve i konteksta komunikacije, a ne kao fiksni slijed koraka.

3.2. Online seksualna iznuda

Online seksualna iznuda predstavlja jedan od najagresivnijih i najštetnijih oblika tehnologijom posredovane seksualne eksploatacije djece, a u posljednjoj deceniji dobila je status prioritetne prijetnje u izvještajima Europola i međunarodnih organizacija. Iako se u javnom diskursu dugo poistovjećivala s groomingom ili širim kategorijama online seksualnog nasilja, današnja istraživanja jasno ukazuju da se radi o zasebnom i izrazito destruktivnom obrascu ponašanja. Najjednostavnije rečeno, sextortion uključuje situaciju u kojoj počinitelj prijeti da će objaviti, distribuirati ili poslati seksualno eksplicitne slike ili videozapise djeteta ako ono ne ispuni određene zahtjeve, bilo seksualne, emocionalne ili materijalne prirode. Ta osnovna struktura prisile čini temelj fenomena koji, prema nalazima Finkelhora i saradnika (2020), pogađa oko 3,5% mladih prije

punoljetstva, pri čemu je stvarna prevalencija vjerovatno znatno veća zbog izuzetno niskog nivoa prijavljivanja.

Za razliku od groominga, koji se dominantno temelji na stvaranju emocionalne bliskosti i postepenom urušavanju granica, online seksualna iznuda počiva na naglom i radikalnom narušavanju ravnoteže moći u trenutku kada počinitelj dođe u posjed seksualnog materijala djeteta. Açar (2016) ovaj oblik eksploatacije definira kroz tri ključna elementa, a to su digitalni prostor kao okruženje djelovanja, posjedovanje kompromitirajućeg materijala i upotrebu tog materijala kao sredstva ucjene. Tek kada su ta tri elementa ispunjena, može se govoriti o sextortion-u kao specifičnoj formi online seksualnog nasilja. Ova formulacija posebno je korisna jer razgraničava seksualnu iznudu od groominga, sextinga, cyberbullyinga i drugih digitalnih rizika. Istraživanja ukazuju da inicijalni materijal najčešće nastaje kroz dobrovoljno slanje slika u kontekstu romantičnog odnosa, prijateljstva ili očekivane intimnosti. Wolak i saradnici (2018) pokazuju da je 75% maloljetnih žrtava svjesno poslalo prvi materijal, ali pod pritiskom ili emocionalnom manipulacijom, dok više od 60% počinitelja dolazi iz kruga poznanika, vršnjaka ili bivših partnera. Ovi nalazi ozbiljno narušavaju stereotip o „strancu-predatoru“ i ukazuju da se veliki broj incidenata odvija unutar postojećih odnosa moći među adolescentima. Istovremeno, suvremeni oblici iznude sve češće uključuju i nepoznate počinioce, uključujući kriminalne grupe koje putem lažnih profila iniciraju razmjenu intimnih slika, brzo eskaliraju komunikaciju i potom zahtijevaju novac, dodatne eksplicitne materijale ili druge oblike poslušnosti (Ray & Henry, 2024).

Modaliteti pribavljanja materijala uveliko variraju, ali se u literaturi mogu prepoznati tri dominantna obrasca (Açar, 2016). Prvi se odnosi na iznudu unutar postojećih odnosa, najčešće među adolescentima, gdje intimne fotografije postaju alat kontrole nakon sukoba ili prekida. Drugi se povezuje s predatorskim ponašanjem u kojem se grooming tehnike koriste samo kao početna faza za pribavljanje vizualnog materijala, nakon čega slijedi brza eskalacija prijetnji. Treći obrazac uključuje tehnički sofisticirane metode, poput hakovanja računa ili kamera, iako se u praksi javljaju znatno rjeđe nego što se pretpostavlja, jer zahtijevaju znanja koja većina počinitelja nema (Açar, 2016). Ipak, IoT uređaji i funkcija „live streaminga“ otvaraju nove rizike, posebno u kontekstu praksi snimanja bez pristanka. Dinamika iznude posebno je opasna zbog činjenice da prijetnje ne služe samo kao sredstvo kontrole, već i kao faktor psihološke destabilizacije žrtve. Tipično, počinitelj prijeti javnim objavljivanjem materijala, slanjem roditeljima, prijateljima ili nastavnicima, kreiranjem lažnih profila ili slanjem materijala školskim zajednicama. Studije pokazuju da mnogi počinioci prijetnje ponavljaju kroz mjesece i da, u slučajevima maloljetnih žrtava, nerijetko potiču djecu na samopovređivanje ili samoubistvo kako bi dodatno učvrstili kontrolu (Wolak et al., 2018). Upravo takve eskalacije ukazuju da sextortion nije samo digitalni fenomen, već oblik psihološkog i emocionalnog nasilja sa

ozbiljnim posljedicama po mentalno zdravlje žrtve. Psihološke posljedice seksualne iznude izrazito su teške, a literatura potvrđuje trajne efekte poput depresije, intenzivne anksioznosti, osjećaja krivnje i srama, povlačenja iz socijalnih kontakata i ozbiljnih samodestruktivnih misli (Ray & Henry, 2024). Zabilježeni su slučajevi u kojima su djeca promijenila školu, prekinula obrazovanje ili pokušala samoubistvo kako bi pobjegla od prijetnji koje nisu znala kako zaustaviti. Ključno je što većina žrtava ne traži pomoć jer polovina maloljetnika u studiji Wolaka i saradnika (2018) nikada nije prijavila incident, iz straha od osude, nevjerice, reakcije roditelja ili gubitka reputacije. Time se stvara začarani krug u kojem se iznuda nastavlja upravo zato što je nevidljiva.

3.3. Proizvodnja i distribucija CSAM: tehnološki infrastruktura, kriminalne dinamie i izazovi za istrage

Savremena proizvodnja i distribucija materijala seksualnog zlostavljanja djece (CSAM) odvija se u digitalnom prostoru koji karakterišu brzina, anonimnost i globalni domet. Tehnološki napredak posljednjih dvadeset godina fundamentalno je promijenio kriminalne procese, čineći nastanak i širenje CSAM jednostavnijim i operativno sigurnijim za počinitelje. Lee i saradnici (2020) naglašavaju da današnje online okruženje spaja tri ključne dimenzije relevantne za razumijevanje fenomena su zakonski okvir, distribucijske kanale i tehničke mehanizme detekcije. Ove dimenzije oblikuju cjelokupnu infrastrukturu u kojoj počinitelji djeluju, a ujedno postavljaju jasna ograničenja pred istražne organe. Kriminalni proces počinje u fazi proizvodnje, koja se danas odvija u širokom rasponu kontekstaod direktnog kontaktnog zlostavljanja u intrafamilijarnim okvirima, do potpunog online iskorištavanja putem web kamera i digitalnih uređaja. Sistematski pregled Calea i suradnika (2021) pokazuje da se značajan dio CSAM proizvodi u okruženjima gdje počinitelj ima neposredan pristup djetetu. U više od polovine slučajeva počinitelj je član porodice žrtve ili blizak poznanik, što potvrđuju i nalazii Gewirtz-Meydan i saradnika (2018) koji ukazuju da su porodica, bliski partneri roditelja i osobe iz neposrednog okruženja najčešći proizvođači sadržaja. Paralelno, sve je više slučajeva u kojima se CSAM producira isključivo online, bez fizičkog kontakta, putem direktnog nagovaranja djece da pred kamerom izvode seksualizirane radnje (McManus, Long, Alison, & Almond, 2015). Ovaj oblik predstavlja relativno novu kategoriju digitalnih zločina, potaknutu ekspanzijom aplikacija sa video-komunikacijom i niskom procjenom rizika kod počinitelja.

Distribucija CSAM materijala zauzima centralno mjesto u savremenom ekosistemu seksualne eksploatacije djece, a odvija se kroz tri dominantna kanala: otvoreni web, P2P mreže i dark web. Na otvorenom webu CSAM se pojavljuje u dva konteksta: u direktnim kontaktima počinitelja i djece putem društvenih mreža, i u formi nestrukturiranih, privremeno dostupnih materijala koji izmiču

moderaciji. Cale i saradnici (2021) ističu da je upravo otvoreni web prostor u kojem se odvija najveći dio početnih kontakata između djece i počinitelja, posebno na platformama kao što su Facebook, Instagram, Snapchat i različite aplikacije za razmjenu videa. U tom segmentu dominiraju fenomeni grominga, seksualiziranog uvjeravanja i prikupljanja inicijalnih fotografija koje kasnije prelaze u kriminalne mreže. Ova interakcija pokazuje stalnu povezanost između proizvodnje i distribucije kroz sadržaj nastao tokom grominga koji je često je polazna tačka za širu razmjenu. P2P mreže predstavljaju drugi sloj distribucije i omogućavaju globalno dijeljenje velikih datoteka bez centralnog posrednika. Bissias i saradnici (2016) procjenjuju da je u određenom trenutku više od 800.000 korisnika na globalnom nivou učestvovalo u dijeljenju CSAM na P2P mrežama, dok Bouhours i Broadhurst (2011) ukazuju da se značajan dio razmjene dešava lokalno i u jezičkim i kulturnim grupama povezanih korisnika. Ove mreže posebno karakterišu ogromni volumeni podataka, česta razmjena višegodišnjeg sadržaja, te fragmentiranost datoteka koja otežava identifikaciju originalnog materijala. Policijske agencije u brojnim zemljama izvještavaju o tome da P2P mreže generiraju obim rada koji nadmašuje njihove tehničke i kadrovske kapacitete, što potvrđuje i Johansson (2019) u svojoj studiji o švedskom policijskom kontekstu.

Najorganiziraniji i najopasniji sloj distribucije razvija se na dark webu. Ngo, Gajula, Thorpe i McKeever (2024) analizirali su više od 353.000 objava na osam dark web foruma i identificirali preko 10.000 aktivnih CSAM autora koji koriste ove platforme za razmjenu materijala, komunikaciju, savjetovanje o metodama izbjegavanja detekcije i stvaranje zatvorenih zajednica. Autori bilježe i specifične kriminalne obrasce kao što su razmjena ekskluzivnih materijala, korištenje kodiranog žargona, primjenu sofisticiranih operativnih sigurnosnih mjera i jasno strukturirane hijerarhije u kojima se status stiče obimom doprinosa. Ove strukture predstavljaju digitalni ekvivalent organiziranih kriminalnih mreža i značajno otežavaju infiltraciju i prikupljanje dokaza. Istraživanja takođe pokazuju da su platforme kao što su Tor i I2P glavni pristupni kanali, uz dodatno korištenje enkripcije, kriptovaluta i decentraliziranih hosting servisa koji dodatno otežavaju rad istražnih agencija.

Sve ove dinamike stvaraju ozbiljne operativne izazove za istrage. Leclerc i saradnici (2022) navode da policijski istražitelji širom svijeta ističu nedostatak specijalizirane obuke, tehničkih resursa i analitičke podrške kao najveće prepreke efikasnom procesuiranju slučajeva. Problemi se kreću od tehničke zastarjelosti opreme i nedostatka digitalnih forenzičara, do nedovoljne saradnje s globalnim društvenim mrežama i pravnih ograničenja koja usporavaju pristup podacima. Johansson (2019) dodatno ukazuje da mnoge policijske organizacije tretiraju CSAM kao kriminal nižeg prioriteta, što dovodi do preopterećenosti istražitelja, dugih zastoja u procedurama i slabog institucionalnog odgovora u odnosu na obim štete.

3.4. Tehnike identifikacije žrtava i počinitelja

Identifikacija žrtava i počinitelja u slučajevima online seksualnog zlostavljanja djece predstavlja ključnu kariku između "digitalnog traga" i klasičnog krivičnog postupka. Pritom se isprepliću tri ravni- forenzička analiza vizuelnog sadržaja, automatizirane tehnike detekcije i klasifikacije CSAM-a, te operativno-istražne metode usmjerene na traganje za konkretnim osobama iza ekrana. Savremena literatura pokazuje da nijedna od ovih komponenti nije dovoljna sama za sebe, već da se najveći učinak postiže kombiniranjem više pristupa, uz jasno definisanu institucionalnu podjelu uloga i odgovornosti.

3.4.1. Forenzička analiza i klasifikacija slikovnog materijala

Osnovni preduvjet za identifikaciju žrtava i počinitelja jeste uopće prepoznati da određeni materijal predstavlja seksualnu zloupotrebu djece te ga konzistentno razvrstati u zakonske kategorije. Kloess i saradnici pokazuju da čak i iskusni policijski analitičari imaju značajne poteškoće pri procjeni dvije ključne dimenzije, da li je prikazana osoba dijete i da li je sadržaj "nedozvoljen" odnosno "indecentan" u smislu zakona (Kloess, Woodhams, Whittle, Grant, & Hamilton-Giachritsis, 2017). Posebno problematične su tzv. "granične slike"odnosno adolescenti u ranijim stadijima puberteta, djelimična golotinja, ili situacije u kojima kontekst može imati i "nevinu" interpretaciju. Inter-rater analize pokazuju da se kod takvih snimaka javlja veći stepen neslaganja između kodera, što direktno utiče na dosljednost krivičnog gonjenja i procjenu težine djela. Radi smanjenja subjektivnosti uvedene su skale tipa COPINE i kasnije jednostavniji sistemi kategorizacije (A, B, C), koje razdvajaju penetrativne radnje, nepenetrativne seksualne aktivnosti i "erotsko poziranje" (Taylor, Holland, & Quayle, 2001). Međutim, upravo kategorija C ("erotsko poziranje") pokazuje koliko je normativna granica fluidna. Analitičari priznaju da se u praksi često "drže sigurnog terena" i fokusiraju na očigledno teške materijale, dok dio nižeg nivoa ostaje u zoni neodlučnosti. To ima neposrednu posljedicu na identifikaciju žrtava, odnosno djeca čije se slike formalno ne prepoznaju kao CSAM ostaju izvan spektra proaktivnih istraga i međunarodnih baza.

Poseban izazov predstavlja procjena starosti. Istraživanja pokazuju da čak ni medicinski stručnjaci nisu značajno bolji od laika u razlikovanju kasnih adolescenata od punoljetnih osoba na osnovu fotografija, upravo zbog velike varijabilnosti u tempu pubertetskog razvoja (Cattaneo, i dr., 2009). U digitalnom kontekstu dodatno otežavaju etničke razlike u tjelesnoj građi, promjene u indeksu tjelesne mase i globalna priroda CSAM-a. U operativnom smislu to znači da procjena starosti mora biti kombinirana sa drugim indikatorima – kontekstom scene, metapodacima, nazivom fajla, jezikom i kulturnim obilježjima okruženja – umjesto da se oslanja na vizuelni utisak.

3.4.2. Hash baze, P2P monitoring i web-crawleri kao temelji identifikacije

Na tehničkoj razini, većina savremenih sistema borbe protiv CSAM-a počiva na hash bazama poznatog materijala. PhotoDNA i slične tehnologije generišu "otiske" slika, omogućavajući prepoznavanje već ranije identifikovanih snimaka čak i kada su djelimično izmijenjeni (Edwards, Christensen, Rayment-McHugh, & Jones, 2021). Time se postižu dva cilja, a to su broj digitalnih artefakata koje analitičar mora ručno pregledati drastično se smanjuje, a istovremeno se omogućava da se ista žrtva prati kroz različite kolekcije počinitelja i preko više platformi, što je presudno za njen fizički pronalazak. Nadzor P2P mreža i specijalizirani alati poput iCOP-a idu korak dalje, kombinirajući hash pretragu sa analizom naziva fajlova i saobraćaja kroz mrežu (Peersman, Schulze, Rashid, Brennan, & Fischer, 2016). Studije pokazuju da mali broj "čvorišta" generiše nesrazmjerno veliki dio prometa CSAM-a, te da bi uklanjanje samo vrha distribucijske piramide moglo smanjiti dostupnost materijala na pojedinim mrežama za 30–40% (Wolak, Liberatore, & Levine, 2014). Sa stanovišta identifikacije počinitelja, praćenje IP-adresa, obrazaca dijeljenja i listi "sjemenskih" fajlova omogućava profiliranje najaktivnijih distributera, koji su ujedno i najvjerovatniji producenti ili administratori zatvorenih zajednica, dakle akteri sa najvećim "operativnim značajem".

Web-crawleri primijenjeni na "clear web" i, u ograničenoj mjeri, na darknet, automatski prate linkove s već poznatih CSAM domena i mapiraju mrežu povezanih stranica (Westlake, Bouchard, & Frank, 2012). Primjer projekata poput Project Arachnid[57] pokazuje da je moguće procesuirati stotine miliona stranica i identificirati desetine hiljada unikatnih CSAM slika u kratkom vremenu, što policiji otvara mogućnost da gađa sajtove sa najvećom "centralnošću" i tako razbija infrastrukturu distribucije. Istovremeno, svaki put kad se poznata slika pojavi na novoj lokaciji, generiše se trag koji može voditi ka novim počiniteljima i eventualno novim informacijama o identitetu žrtve.

3.4.3. Metapodaci, nazivi fajlova i analiza darkneta

Noviji radovi sve više ističu vrijednost metapodataka i tekstualnih tragova kao izvora za identifikaciju kako CSAM sadržaja, tako i aktera koji njime upravljaju. Studija Pereire i saradnika (2024) pokazuje da su klasifikacijski modeli zasnovani isključivo na nazivima fajlova i putanjama (file paths) u stanju da postignu visok stepen tačnosti, upravo zato što počinitelji razvijaju specifičan, prepoznatljiv vokabular i kodirani jezik u imenovanju sadržaja. P2P pretrage se ionako u velikoj mjeri zasnivaju na tekstualnom pretraživanju naziva fajlova, pa je prelazak na automatiziranu analizu tih obrazaca logičan korak.

[57] Projekt Arachnid je nastau u Australiji i predstavlja specifičan skup alata usmjeren na žrtve online seksualne eksploatacije i namijenjen je borbi protiv širenja materijala o seksualnom zlostavljanju djece (CSAM) na internetu. Pokrenut je 2017. godine i objedinjuje automatizirane metode otkrivanja CSAM-a.

Ngo i saradnici razvijaju sistem za detekciju CSAM-a na dark web forumima baziran na mašinskom učenju, koji na korpusu od preko 353.000 objava uspijeva da identifikuje oko 63.000 CSAM-relevantnih objava i preko 10.500 "kreatora" CSAM sadržaja (Ngo et al., 2024). Analiza metapodataka tih postova daje nekoliko važnih uvida: dominantne teme i preferencije pojedinih autora, tipične starosne skupine i nacionalnosti žrtava koje se spominju, te platforme koje se najčešće koriste za pribavljanje i razmjenu materijala (Omegle, YouTube, Skype, Instagram, Telegram). Za potrebe identifikacije počinitelja, ovakvi obrasci služe kao osnova za ciljanje najaktivnijih i najopasnijih aktera, kao i za prepoznavanje novih žarišnih tačaka na "surface" platformama gdje se žrtve regrutiraju ili gdje se CSAM inicijalno proizvodi (npr. live streaming preko VoIP aplikacija, web-kamera i društvenih mreža).

Metapodaci u širem smislu kao EXIF podaci fotografije, vremenske oznake, geolokacija, verzija softvera, jezik sistema dopunjuju ovu sliku. Iako su počinitelji sve svjesniji potrebe da "čiste" metapodatke, analiza milijuna fajlova i mrežnih interakcija ipak omogućava statističko profiliranje tipičnih konfiguracija, vremenskih obrazaca i tehnoloških sredstava koja koriste određene grupe. To ne daje automatski "ime i prezime", ali sužava operativni prostor i usmjerava klasične istražne radnje.

3.4.4. Automatizirano otkrivanje, AI i forenzički workflow

Pregled literature o automatiziranom otkrivanju CSAM-a ukazuje na jasnu konvergenciju, najefikasniji sistemi kombinuju više modaliteta – hash vrijednosti, vizuelne karakteristike slike, tekstualne signale u nazivima fajlova i metapodacima umjesto da se oslanjaju na jedan indikator (Edwards et al., 2021). Duboke neuronske mreže postižu najbolje rezultate pri detekciji do tada neviđenog CSAM-a, posebno kada se višestruki deskriptori slike i videa spajaju u jedinstveni klasifikator (Lee, Ermakova, Ververis, & Fabian, 2020). Vitorino i drugi (2018) pokazuju da CNN modeli istrenirani na velikim policijskim datasetima mogu vrlo efikasno razlikovati CSAM od adult pornografije, dok radovi o kombiniranju detekcije pornografije i procjene dobi dodatno sužavaju fokus na potencijalne žrtve (Vitorino et al., 2018; Lee et al., 2020).

Međutim, Pereira i saradnici (2024) naglašavaju da se modeli moraju testirati u realističnim scenarijima, uključujući potpuno benigne "out-of-sample" setove i situacije u kojima počinitelji namjerno mijenjaju tekstualne obrasce (adversarial examples tipa "Lo7ita", "b4", slično). Visoka stopa lažno pozitivnih nalaza može praktično blokirati implementaciju sistema u platformama sa milijardama korisnika, a sa stanovišta policije stvara dodatni operativni teret. Istraživanje Sanchez i saradnika (2019), zasnovano na anketi istražitelja, pokazuje da su praktičari veoma osjetljivi na pitanje lažno pozitivnih nalaza; većina ih smatra veću stopu FP ozbiljnijim problemom od propuštenih slučajeva, upravo zato što FP direktno opterećuju ograničene resurse. Istovremeno, Sancher i saradnic

(2019) ukazuju da mnogi praktičari nisu dovoljno upoznati sa osnovama data science i AI, iako već rade sa alatima koji te tehnike koriste. To stvara raskorak između mogućnosti tehnologije i načina na koji se zaista koristi u praksi.

S tehničke strane, razvijeni su brojni alati za trijažu i filtriranje od jednostavnih sistema za detekciju golotinje na nivou piksela, preko specijaliziranih "field triage" alata, do kompleksnih sistema koji automatski rangiraju uređaje i medije prema vjerovatnoći da sadrže relevantne dokaze (Marturana & Tacconi, 2013). Sa stanovišta identifikacije žrtava i počinitelja, njihova vrijednost leži u tome što kratkoročno oslobađaju istražitelje od pregledavanja ogromnih količina benignog materijala, čime se brže dolazi do "čistog" CSAM-a u kojem je moguće prepoznati konkretna lica, prostore i obrasce ponašanja.

3.4.5. Identifikacija žrtava i počinitelja

Iako većina navedenih tehnologija primarno služi detekciji i klasifikaciji sadržaja, one su istovremeno temelj za identifikaciju žrtava i počinitelja u užem smislu. U praksi se to odvija kroz nekoliko komplementarnih koraka. Prvo, hash baze i automatizirana vizuelna detekcija omogućavaju izdvajanje materijala koji sadrži do tada neidentifikovane žrtve, što postaje prioritet za specijalizirane timove za "victim identification" (Edwards et al., 2021; Johansson, 2019). Drugo, procjena dobi, spoljašnjih obilježja, jezika u pozadini i kulturnih artefakata (odjeća, arhitektura, tehnika) pomaže u geografskoj i demografskoj atribuciji žrtve, iako Kloess i drugi (2017) jasno pokazuju da procjena starosti ostaje izvor ozbiljne nesigurnosti, posebno kod adolescenata. Treće, u sve većoj mjeri koriste se tehnike poput prepoznavanja lica, poređenja prostorija, namještaja i "mikro-okruženja" između različitih slučajeva i prijava, što omogućava da se ista žrtva ili isti počinitelj povežu kroz više istraga i jurisdikcija (Edwards et al., 2021). U širem, kriminološkom smislu, studije o "crime commission processes" ukazuju da producenti CSAM-a često spajaju online i offline dimenziju pri čemu kombiniraju kontaktno zlostavljanje sa snimanjem i digitalnom distribucijom. Tu se ključne odluke donose na temelju procjene rizika detekcije, dostupnosti djece i tehničkih mogućnosti (Cale et al., 2021). Upravo razumijevanje tih procesa pomaže policiji da prioritizira profil počinitelja koji je vjerovatnije istovremeno i online distributer i offline zlostavljač.

Identifikacija počinitelja zavisi i od "klasičnih" digitalnih tragova: IP adresa, logova, naloga na društvenim mrežama, komunikacije u P2P i darknet okruženju, kao i od načina na koji se te informacije integriraju sa rezultatima OSINT, HUMINT, SIGINT i tradicionalnih istražnih radnji. U istraživanju OKG i njihovih članova koriste se otvoreni izvori kao što su društvene mreže na kojima akteri mogu ostaviti značajan broj podataka i informacija, kao što su fotografije, video snimke, objave i tako dalje (Muhić, 2024). Johansson pokazuje da je, na primjer, u Švedskoj jedan od ključnih problema nedostatak obaveze ISP-ova da čuvaju IP logove, što direktno otežava identifikaciju počinitelja čak i kada je

CSAM sadržaj otkriven (Johansson, 2019). Slično tome, Leclerc i saradnici (2022) ističu da policijski istražitelji kao ključne vještine navode kombinaciju "social engineering" komunikacijskih sposobnosti, dobrog poznavanja IT tehnologija i razumijevanja profila seksualnih prestupnika. Drugim riječima, ni najnapredniji algoritmi ne mogu zamijeniti vještinu istražitelja da iskoristi digitalne tragove za razvijanje operativnih hipoteza i njihovo testiranje kroz ispitivanja, nadzor i druge mjere.

3.4.6. Ljudski faktor: kapaciteti, opterećenje i zaštita istražitelja

Većina navedenih tehnika podrazumijeva intenzivan rad specijaliziranih policijskih timova i digitalnih forenzičara. Više studija potvrđuje da je riječ o profesionalnoj populaciji izložene visokom riziku sekundarne traumatizacije, hroničnog stresa i "burnouta", upravo zbog kontinuiranog kontakta sa ekstremno uznemirujućim sadržajem (Burns, Morley, Bradshaw, & Domene, 2008; Seigfried-Spellar, 2017; Sanchez, Grajeda, Baggili, & Hall, 2019). Istražitvači u Leclercovoj studiji navode kao ključne probleme enorman obim podataka, nedostatak osoblja i tehničkih resursa, te ograničeno razumijevanje fenomena CSAM-a u menadžmentu vlastitih institucija (Leclerc et al., 2022). Johansson dolazi do sličnih nalaza za Švedsku gdje različite policijske regije rade po različitim procedurama, digitalno forenzičko osoblje je "usko grlo", a CSAM se u praksi često tretira kao "niskoprioritetni" kriminalitet (Johansson, 2019). Sanchez i saradnici (2019) pokazuju da istražitelji prepoznaju veliku vrijednost filtriranja i trijažnih tehnologija. To se radi prvenstveno da bi smanjili vlastitu izloženost i ubrzali rad ali da istovremeno relativno malo koriste alate zasnovane na naprednim AI tehnikama, dijelom i zato što ih nedovoljno razumiju (Sanchez, Grajeda, Baggili, & Hall, 2019). Efektivno korištenje tehnika identifikacije žrtava i počinitelja stoga zahtijeva ne samo nabavku tehnoloških rješenja, nego i ulaganje u sistematsku obuku, superviziju, psihološku podršku i jasne protokole rada, kako bi se omogućilo da ljudi koji rade najteže zadatke ostanu funkcionalni i profesionalno održivi.

4. Institucionalni, operativni i pravni odgovori na online seksualnu eksploataciju djece

4.1. Nacionalni i međunarodni pravni okvir

Savremeni međunarodni pravni okvir koji regulira online seksualnu eksploataciju djece razvijao se u vremenu koje nije poznavalo današnji obim, dinamiku i tehnološke mogućnosti digitalne proizvodnje i distribucije materijala seksualnog zlostavljanja djece. Uprkos velikoj normativnoj gustoći i širokom prihvatanju najvažnijih međunarodnih instrumenata, uočljiva je strukturalna napetost između formalnih obaveza država i njihovih stvarnih kapaciteta da adekvatno odgovore na fenomen koji se transformira brže nego što zakonodavstvo može reagirati. Prema Global Status Report on Preventing Violence Against Children (WHO,

2020), većina država ima relativno razvijen normativni okvir zaštite djece, ali manje od polovine posjeduje funkcionalne mehanizme provedbe. U digitalnom okruženju, gdje se CSAM distribuira kroz anonimne mreže, peer-to-peer sisteme, šifrirane komunikacijske kanale i platforme zasnovane na generativnoj umjetnoj inteligenciji, ta disproporcija između normativnog i operativnog postaje još izraženija. Razumijevanje međunarodnog i evropskog pravnog okvira time postaje ključno za identifikaciju uzroka neuspjeha istraga, sporosti u identifikaciji žrtava i ograničenog dometa kaznenih mehanizama. Konvencija o pravima djeteta iz 1990. godine predstavlja temeljni međunarodni instrument zaštite djece, ali je nastala u historijskom kontekstu u kojem internet tek počinje ulaziti u širu društvenu upotrebu. Zbog toga CRC nije sadržavala specifične odredbe koje bi prepoznale digitalno okruženje kao primarni prostor viktimizacije, niti je predviđala fenomene kao što su virtualni CSAM, deepfake tehnologije, vizualne manipulacije ili anonimna globalna tržišta distribuirana putem darkneta. Njena najveća snaga leži u uspostavljanju principa najboljeg interesa djeteta, obaveze preventivnog djelovanja i unapređenja dječijeg razvoja, ali upravo ti principi ostaju nedovoljno operacionalizirani u digitalnom kontekstu. Dodatni Protokol o prodaji djece, dječjoj prostituciji i dječjoj pornografiji (OPSC) predstavlja pokušaj dopune tih praznina, ali analiza Maxwella (2022) jasno pokazuje da OPSC ostaje primarno fokusiran na kriminalizaciju, dok su preventivne mjere formulirane široko, sugestivno i bez jasnih minimalnih standarda koje bi države morale ispuniti. Takav pristup dovodi do situacije u kojoj države uglavnom ispunjavaju formalne obaveze kriminalizacije, dok sistemske preventivne politike ostaju rudimentarne ili se uopće ne razvijaju.

Budimpeštanska konvencija Vijeća Evrope iz 2001. godine predstavlja prvi sveobuhvatni međunarodni instrument koji adresira računalno posredovane oblike kriminaliteta, uključujući i proizvodnju, distribuciju i posjedovanje „child pornography“ u smislu člana 9. Ona je postavila arhitekturu međunarodne policijske i pravosudne saradnje, ali je ubrzo postalo jasno da njezina efikasnost trpi zbog nekoliko ključnih faktora. Transnacionalni karakter CSAM kriminaliteta otežava primjenu teritorijalnih pravila nadležnosti, pa istrage koje uključuju servere, počinioce i žrtve u različitim državama završavaju u dugotrajnim procedurama međusobnog pravnog pomaganja. Uz to, države različito definiraju šta se smatra nezakonitim sadržajem, osobito u pogledu virtualnih, realističnih i AI-generisanih prikaza djece, što otežava koordinirano djelovanje i razmjenu dokaza (Sorbán, 2024). Razlike u propisima o obaveznom čuvanju IP logova dodatno usložnjavaju situaciju, budući da se u nekim jurisdikcijama podaci čuvaju nekoliko mjeseci, dok se u drugim čuvaju godinama, što u praksi određuje granice uspješne digitalne istrage (Kasper & Laurits, 2016).

Lanzarote konvencija iz 2007. godine unijela je kvalitativni iskorak kriminalizacijom grooming ponašanja putem informacionih tehnologija i uspostavljanjem obaveze država da poduzmu sve odgovarajuće mjere radi zaštite

djece od seksualne eksploatacije na internetu. Ipak, kao i svi instrumenti Vijeća Evrope, Lanzarote konvencija pati od odsustva mehanizama sankcioniranja država koje ne implementiraju svoje obaveze. Njena fleksibilna normativna struktura dopušta različita tumačenja, posebno u vezi s virtualnim i AI-manipulisanim prikazima, što stvara dodatne pravne praznine u kontekstu generativne umjetne inteligencije i naprednih alata za vizualnu manipulaciju dječijih slika (Parti & Szabó, 2024). Uprkos tome što uvodi ključne konceptualne inovacije, Lansarote konvencija nije predvidjela mogućnost stvaranja potpuno fiktivnih, hiperealističnih prikaza djece, pa njena primjena u slučajevima AI-generisanog materijala ostaje nedovoljno razrađena.

Na regionalnom nivou, najvažniji instrument predstavlja Direktiva 2011/93/EU o borbi protiv seksualnog zlostavljanja djece, koja obavezuje države članice da kriminaliziraju sve oblike online seksualne eksploatacije, uključujući grooming, posjedovanje, distribuciju, stvaranje i podsticanje stvaranja CSAM-a. Direktiva predviđa i proaktivne istrage koje ne zavise od prijave žrtve, proširenu ekstrateritorijalnu nadležnost, mjere podrške žrtvama od najranije faze postupka te specijalizirane operativne mehanizme. Ipak, kao instrument minimalne harmonizacije, ona dopušta državama da njene odredbe transponuju na različite načine, što je u praksi proizvelo duboke razlike u definicijama, procedurama i sankcijama. Ta fragmentacija otežava koordinaciju istraga, razmjenu dokaza, saradnju sa Europolom i sprovođenje zajedničkih operacija, posebno u slučajevima koji uključuju peer-to-peer sisteme, razmjene putem enkriptiranih aplikacija ili AI-generisane sadržaje (Huemer, 2024). Dodatni problem leži u tome što Direktiva ne sadrži detaljne smjernice u vezi s izazovima koje donosi generativna umjetna inteligencija, ne dotiče se realističnih avatar-prikaza djece u metaverzumskim okruženjima i ne nudi rješenja za situacije u kojima E2EE komunikacija onemogućava pristup dokazima. Najnoviji pokušaj uspostavljanja snažnijeg evropskog pravnog okvira predstavlja Prijedlog regulacije *COM (2022) 209 final*, koji predviđa obavezu internetskih platformi da detektuju, uklanjaju i prijavljuju CSAM, kao i identifikaciju grooming komunikacija kroz automatizirane sisteme. Regulacija, međutim, otvara ozbiljna pitanja balansa između zaštite djece i zaštite privatnosti, budući da njezina implementacija u praksi zahtijeva nadzor nad korisničkim komunikacijama koji je u suprotnosti sa standardima enkriptirane privatne komunikacije i načelima GDPR-a (Rezende, 2024). Evropske organizacije za zaštitu privatnosti upozoravaju da bi široko nadgledanje moglo stvoriti presedan za masovno nadziranje građana, dok evropske policijske i tužilačke institucije tvrde da je bez takvih mehanizama nemoguće pratiti eksponencijalni rast digitalne eksploatacije djece.

Sve ove razine pravne regulacije ukazuju na duboko ukorijenjen problem: postojeći pravni instrumenti nastali su u vremenu analognog kriminaliteta i ne uspijevaju u potpunosti odgovoriti na digitalne fenomene koji uključuju globalnu distribuciju, brisanje tragova, E2EE komunikacije, upotrebu kriptovaluta i

generativnu umjetnu inteligenciju. Razlike u definicijama, kapacitetima i primjeni prava između država stavljaju djecu u neravnopravan položaj, dok operativne prepreke poput varijabilnog čuvanja IP logova, spore međunarodne pravne pomoći i ograničenog pristupa digitalnim dokazima, često rezultiraju neuspjelim istragama ili nemogućnošću identifikacije žrtava. Time postaje jasno da je, uprkos široko ratificiranim instrumentima i formalno visokim standardima zaštite, pravni okvir i dalje nedovoljno usklađen sa stvarnim zahtjevima digitalnog okruženja i da zahtijeva duboku, strukturnu reformu kako bi mogao odgovoriti na rastući fenomen online seksualne eksploatacije djece.

4.2. Organizacijski modeli i kapaciteti policije i tužilaštava

Iako međunarodni i evropski pravni okvir postavlja minimalne standarde kriminalizacije i međudržavne saradnje, stvarni domet zaštite djece u digitalnom prostoru zavisi prvenstveno od organizacijskih modela, kapaciteta, resursa i operativnih procedura nacionalnih policijskih i tužilačkih institucija. Online seksualna eksploatacija djece se ne može adekvatno procesuirati u sistemima čije institucionalne arhitekture pripadaju periodu prije masovne digitalizacije, niti u organizacijama koje i dalje tretiraju digitalni kriminalitet kao periferan oblik delinkvencije. Empirijski podaci, kao i komparativne studije (Sanchez et al., 2019; Johansson, 2019), pokazuju da se većina nacionalnih sistema suočava s hroničnim nedostatkom specijaliziranih jedinica, fragmentiranim procedurama, nedovoljno obučenim kadrom i visokim emocionalnim troškovima koji dugotrajni rad s CSAM materijalom ostavlja na istražitelje. Ove slabosti imaju direktne posljedice: veliki broj slučajeva ostaje neistražen, prepoznate žrtve ostaju neidentifikovane, a predmeti u tužilaštvima kasne mjesecima ili godinama.

U većini država, organizacijski odgovor zasniva se na specijaliziranim jedinicama za cyber kriminal, digitalnu forenziku i seksualne delikte, no stvarni obim njihovih ovlasti i kapaciteta značajno varira. Strukturalno, policijske agencije najčešće primjenjuju model u kojem se digitalne istrage odvijaju u tri komponente - analitičkoj, operativnoj i forenzičkoj. Analitičke jedinice prikupljaju i obrađuju prijave, analiziraju OSINT i SOCMINT tragove, mapiraju P2P mreže i prate trendove distribucije. Operativne jedinice sprovode undercover aktivnosti u online okruženju, iniciraju prikrivene komunikacije sa osumnjičenim osobama i sakupljaju materijalne tragove u realnom vremenu. Forenzičke jedinice preuzimaju zaplijenjene uređaje, analiziraju metapodatke, koriste hash-baze i specijalizirane algoritme za identifikaciju sadržaja, te izlučuju dokaze koji će biti korišteni u krivičnim postupcima. Međutim, u praksi su ove tri funkcije često dislocirane, nedovoljno koordinirane i zavisne od individualnog entuzijazma i ekspertize malog broja službenika, što predstavlja ozbiljno ograničenje u slučajevima u kojima brzina, tehnološko znanje i međusektorska komunikacija određuju ishod istrage.

Poseban izazov predstavlja preopterećenost policijskih i tužilačkih kapaciteta. Studija Sanchez i saradnika (2019) pokazuje da istražitelji u CSAM predmetima rade pod značajnim psihološkim pritiskom, izloženi su sekundarnoj viktimizaciji i čestim simptomima burnouta, što dovodi do visoke fluktuacije, smanjenog učinka i gubitka institucionalne memorije. U mnogim državama, broj prijava višestruko nadmašuje broj raspoloživog osoblja. NCMEC je samo u 2023. godini primio 35,9 miliona prijava (National Centre for Missing & Exploited Children, 2023), dok Europol i Interpol bilježe stalni porast materijala koji se distribuiraju u fragmentima preko enkriptiranih chat aplikacija, cloud servisa i dark web foruma. Policijske i tužilačke institucije ne mogu pratiti taj obim, što rezultira selektivnim prioritiziranjem, često na štetu slučajeva koji uključuju online grooming ili materijal bez neposrednog fizičkog zlostavljanja, ali sa dugoročnim psihološkim posljedicama po djecu. U takvom modelu, CSAM se u mnogim državama tretira kao krivično djelo „nižeg prioriteta“, što direktno utječe na brzinu i kvalitet istraga.

Tehnička infrastruktura predstavlja dodatnu dimenziju institucionalnih ograničenja. Analiza terabajta materijala sa zaplijenjenih uređaja zahtijeva napredne alate, ogromne kapacitete skladištenja i specijalizirane SQL ili AI-pokretane sisteme koji omogućavaju klasifikaciju sadržaja, prepoznavanje žrtava i povezivanje slučajeva iz različitih jurisdikcija. U mnogim državama ti sistemi nisu standardizirani; koristi se heterogena kombinacija zastarjelih softvera, komercijalnih alata i open-source rješenja koja nisu interoperabilna (Johansson, 2019). Nedostatak standardizacije otežava forenzičku analizu, usporava istrage i umanjuje kvalitet dokaza koji se prezentiraju tužilaštvima. Uz to, policijske agencije u državama sa ograničenim resursima često nemaju ni osnovne kapacitete za dešifriranje uređaja, analizu enkriptovanih komunikacija ili rad sa P2P monitoring alatima, što stvara vidljivi jaz između tehnoloških mogućnosti počinilaca i kapaciteta institucija da im se suprotstave.

Uloga međunarodnih institucija, kao što su NCMEC, Europol i Interpol, postaje ključna u prevazilaženju ovih jazova, ali istovremeno otkriva slabosti nacionalnih sistema. Europolov EC3, Interpolova ICSE baza i NCMEC-ova CyberTipline pružaju neophodne alate za identifikaciju žrtava i usklađivanje globalnih evidencija, ali njihova efikasnost zavisi od brzine i kvaliteta nacionalnih odgovora. Države koje nemaju razvijene kapacitete za proaktivno skeniranje, prepoznavanje hash podudarnosti ili analizu metapodataka ostaju izvan globalnih tokova podataka, što znači da žrtve iz tih jurisdikcija ostaju neidentifikovane, a počinioci neprocesuirani. U tom smislu, međunarodna infrastruktura može samo djelimično kompenzirati nacionalne slabosti; ona ne može nadomjestiti nedostatak specijaliziranih kadrova, jasnih procedura, adekvatnog finansiranja ili političke volje za prioritetno tretiranje online seksualne eksploatacije djece.

4.3. Operativne strategije i modeli saradnje u suprotstavljanju online seksualnoj eksploataciji djece

Operativni odgovor na online seksualnu eksploataciju djece razvija se u složenom prostoru u kojem se isprepliću tehnološke inovacije, transnacionalni kriminalni ekosistemi i institucionalne razlike između država. Dok pravni okvir definiše obaveze, a organizacijski kapaciteti određuju šta je praktično izvodivo, operativne strategije predstavljaju konačan, najdinamičniji sloj institucionalnog djelovanja, onaj u kojem se norme i kapaciteti moraju pretvoriti u konkretne istrage, identifikaciju žrtava i razbijanje mreža počinilaca. Online seksualna eksploatacija djece karakterizira se izrazitom fluidnošću: počinioci koriste raznolike platforme, brzo migriraju između servisa, kombiniraju legitimne i anonimne kanale komunikacije, a sve češće koriste i generativne AI alate. U takvom okruženju, tradicionalni reaktivni modeli policijskog rada pokazuju se nedovoljnim, pa se države sve više oslanjaju na proaktivne, inteligentne i međunarodno koordinirane strategije.

Operativne strategije zasnivaju se na tri ključna pristupa a to su proaktivno otkrivanje, tehničko-forenzička analitika i međunarodna saradnja. Proaktivne strategije uključuju sistematsko praćenje online prostora, korištenje undercover identiteta u komunikaciji sa osumnjičenim osobama, identifikaciju obrazaca grooming ponašanja i analizu otvorenih i polu-zatvorenih mrežnih prostora. OSINT i SOCMINT metode u tom kontekstu postaju nezamjenjive. Policijske jedinice prikupljaju informacije iz javnih profila, digitalnih tragova, društvenih mreža, otvorenih P2P hubova i kriptoforuma, te koriste algoritamske alate za prepoznavanje rizičnih interakcija. Edwards i saradnici (2021) naglašavaju da P2P monitoring nije samo tehnički proces otkrivanja distribucije CSAM-a, nego i taktička strategija infiltracije zatvorenih mreža u kojima počinioci dijele materijale i informacije o novim modusima izbjegavanja nadzora. Uspjeh ovakvih operacija zavisi od iskustva istražitelja, njihove sposobnosti da prepoznaju obrasce ponašanja u fragmentiranom digitalnom okruženju i kapaciteta da simultano prate više kanala komunikacije. Drugi sloj operativnih strategija čini tehničko-forenzička analitika. Materijali prikupljeni kroz proaktivne operacije, zapljene uređaja ili prijave korisnika prolaze kroz složene faze digitalne obrade kao što su hash-matching, analizu metapodataka, geolokacijsku procjenu, vizuelnu klasifikaciju i identifikaciju potencijalnih žrtava. Automatizirani sistemi i algoritamska rješenja igraju ključnu ulogu u brzini obrade materijala, ali njihova efikasnost zavisi od kvaliteta nacionalnih baza podataka i mogućnosti pristupa međunarodnim platformama. Projekti poput kanadskog Project Arachnid, koji automatski skenira internet i detektira CSAM sadržaj u realnom vremenu, pokazali su se kao primjer dobre prakse, ali njihova primjena zavisi od regulatorne i tehničke infrastrukture u pojedinim državama. Australski modeli ACIC-a, koji povezuju obavještajne podatke s operativnim timovima i automatiziranim sistemima za praćenje mreža, dodatno ilustriraju kako centralizirani i tehnološki

sofisticirani pristupi mogu nadomjestiti nacionalne nedostatke u kadrovskim kapacitetima. Treći strateški sloj predstavlja međunarodna saradnja, bez koje je ozbiljna borba protiv online seksualne eksploatacije nemoguća. Većina CSAM sadržaja distribuira se preko servera koji se nalaze u drugim državama, a počinioci vrlo često koriste VPN-ove, proxy-je i enkriptirane komunikacije kako bi prikrili lokaciju, što istrage automatski uvodi u transnacionalnu domenu. Europolova Evropska cybercrime jedinica (EC3) koordinira operacije između članica EU, dok Europolove analitičke platforme omogućavaju identifikaciju obrazaca i povezivanje razbacanih fragmenata materijala. Interpolova ICSE baza podataka, koja sadrži identifikovane i neidentifikovane žrtve, ključni je alat koji omogućava da se pojedinačni slučajevi povežu u širi operativni mozaik. NCMEC-ova CyberTipline predstavlja međunarodni mehanizam koji može inicirati istrage u desetinama država za nekoliko sati, ali njegova efikasnost uveliko zavisi od toga koliko brzo i pouzdano nacionalne policijske institucije mogu reagirati na proslijeđene informacije.

Ipak, međunarodna saradnja suočava se s brojnim izazovima. Različiti standardi dokazivanja među državama, spor odziv internet provajdera na zahtjeve za dostavu podataka, pravne razlike u definiranju CSAM-a i enkripcija sadržaja koja onemogućava pristup podacima predstavljaju ozbiljna ograničenja. U mnogim slučajevima, čak i kada je identifikacija počinitelja moguća, pravni standardi dokazivanja u jednoj državi sprečavaju korištenje dokaza prikupljenih u drugoj, što dovodi do nesrazmjerno velikog broja neprocesuiranih predmeta. U slučajevima gdje se koriste kriptovalute za naplatu pristupa livestream zlostavljanju, istrage postaju dodatno složene, jer zahtijevaju kombinaciju digitalne forenzike, finansijskog praćenja i međunarodnog pravnog pomaganja, što mnoge države ne mogu brzo ili efikasno provesti.

5. Zaključak

Online seksualna eksploatacija djece danas se razvija u prostoru u kojem su ubrzane tehnološke promjene, globalna dostupnost digitalnih platformi i sofisticirane metode prikrivanja stvorile kriminalni ekosistem koji nadilazi kapacitete tradicionalnog pravnog i institucionalnog odgovora. Fenomen CSAM-a prestao je biti ograničen na lokalne granice ili pojedinačne aktere; on se oblikuje kao transnacionalna, dinamična i tehnološki potpomognuta prijetnja koja neprestano erodira postojeće modele zaštite djece. U takvom okruženju postaje jasno da normativni instrumenti, ma koliko dobro koncipirani, ne mogu ispuniti svoju svrhu ukoliko nisu praćeni odgovarajućim operativnim sposobnostima, tehničkim kapacitetima i stvarnom političkom voljom da se ovaj oblik nasilja prepozna kao prioritet sigurnosne agende.

Srž problema nije samo u nedosljednostima zakona, već u činjenici da se digitalni rizici razvijaju brže nego što pravni sistemi mogu reagovati. Generativna umjetna inteligencija, realistične vizualne manipulacije dječjih slika, enkripcija komunikacija i anonimne mreže potkopavaju tradicionalne metode kriminalističkog rada i zahtijevaju pristupe koji integrišu forenzičku analitiku, proaktivno nadziranje, međunarodnu koordinaciju i interdisciplinarno znanje. Bez takve integracije, istrage ostaju reaktivne, fragmentirane i spore, dok počinioci koriste prednosti digitalnog okruženja da bi izbjegli identifikaciju i pravne posljedice. Institucionalni odgovor, posebno u policiji i tužilaštvima, suočava se s teretom za koji mnogi sistemi nisu dizajnirani. Preopterećenost istražitelja, nedostatak specijalizirane obuke, psihološki pritisci dugotrajnog izlaganja CSAM materijalu i ograničena tehnička infrastruktura čine da se značajan broj predmeta nikada ne procesuira, a veliki broj žrtava ostaje neidentifikovan.

Ova strukturalna ograničenja stvaraju začarani krug jer što je sistem slabiji, to su počinioci hrabriji, a djeca izloženija, dok digitalno okruženje proizvodi nove oblike rizika brže nego što institucije uspijevaju izgraditi otpornost. Iz tih razloga, borba protiv online seksualne eksploatacije djece ne može se oslanjati isključivo na krivičnopravni odgovor, koliko god on bio neophodan. Potrebna je transformacija paradigme od reaktivnih modela koji intervenišu nakon nastanka štete, prema preventivnim, proaktivnim i tehnološki potpomognutim mehanizmima koji smanjuju dostupnost materijala, otežavaju pristup potencijalnim žrtvama, prepoznaju rizična ponašanja prije nego što eskaliraju i stvaraju digitalna okruženja u kojima su djeca manje ranjiva. U tom smislu, prevencija ne predstavlja dopunski segment sistema, nego njegov osnovni zaštitni okvir.

Kao zaključak pregleda navedene teorije, uviđa se da zaštita djece u digitalnom okruženju zahtijeva stabilan spoj tri elementa, a to su normativne jasnoće, operativne sposobnosti i međunarodne solidarnosti. Nijedan od ta tri elementa ne može djelovati samostalno. Međunarodni instrumenti moraju biti usklađeni s tehnološkom realnošću, institucije moraju biti finansijski i kadrovski ojačane, a saradnja između država mora biti brža, sadržajnija i oslobođena birokratskih barijera koje trenutno omogućavaju počiniocima da koriste geografske razlike kao zaštitni štit. Samo u sistemu koji prepoznaje da je sigurnost djece neraskidivo vezana za tehničke, političke i pravne kapacitete savremenih društava moguće je govoriti o stvarnoj, a ne deklarativnoj zaštiti njihovih prava.

LITERATURA

Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, 110–126.

Basave, A. E., Fernandez, M., & Alani, H. (2014). Detecting Child Grooming Behaviour Patterns on Social Media. *Lecture Notes in Computer Science*.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect*, 185–199.

Bouhours, B., & Broadhurst, R. (2011). *On-line Child Sex Offenders: Report on a Sample of Peer to Peer Offenders Arrested between July 2010-June 2011.* Canberra: Australian National University.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology*, 20–31.

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends and Issues in Crime and Criminal Justice*.

Cattaneo, C., Ritz-Timme, S., Gabriel, P., Gibelli, D., Giudici, E., Pasquale Poppa, D. N., . . . Grandi, M. (2009). The difficult issue of age assessment on pedo-pornographic material. *Forensic Science International*, 21-24.

Council of Europe. (2007). *Council of Europe Convention on the Protection of Children against Sexual.* Lanzarote: Council of Europe.

Dumitriu, C.-G., Dudu, A., & Nanău, I.-A. (2024). SYSTEMATIC REVIEW: GROOMING BEHAVIOR IN CASES OF CHILD SEXUAL ABUSE: STAGES OF THE PROCESS, RELATION DYNAMICS AND PREVENTION. *Anthropological Researches and Studies*, 268-292.

Edwards, G., Christensen, L. S., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends & issuesin crime and criminal justice*.

Europol. (2025). *Internet Organised Crime Threat Assessment.* Europol.

Finkelhor, D., Turner, H., & Colburn, D. (2020). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA Netw Open*. doi:doi:10.1001/jamanetworkopen.2022.34471

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect*, 238–248.

Grant, T., & Chiang, E. (2017). Online grooming: moves and strategies. *Language and Law*, 103-141.

Huemer, M.-A. (2024). *Revision of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.* European Parliamentary Research Service.

Interpol & ECPAT. (2018). *owards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material.* ECPAT.

Johansson, C. (2019). *Combating online child sexual abuse material. An explorative study of Swedish police investigations.* Malmo: Faculty of Health and Society.

Kasper, A., & Laurits, E. (2016). Challenges in Collecting Digital Evidence: A Legal Perspective. *The Future of Law and eTechnologies*, 195–233.

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2017). Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms. *Sexual Abuse*, 73-96.

Kloess, J. A., Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2017). The Challenges of Identifying and Classifying Child Sexual Abuse Material. *Sexual Abuse*, 173-196.

Leclerc, B., Cale, J., Holt, T., & Drew, J. (2022). Child Sexual Abuse Material Online: The Perspective of Online Investigators on Training and Support Get access Arrow. *Policing: A Journal of Policy and Practice*.

Lee, H.-E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*.

Marturana, F., & Tacconi, S. (2013). A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation*, 193-204.

Maxwell, F. (2022). Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age. *The International Journal of Children's Rights*.

McManus, M. A., Long, M. L., Alison, L., & Almond, L. (2015). Factors associated with contact child sexual abuse in a sample of indecent image offenders. *Journal of Sexual Aggression*, 368–384.

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, 4*(2), 314-338.

Muhić, E. (2025). Psihološke operacije na društvenim mrežama - primjeri, tehnike, taktike i procedure. *Zaštita i sigurnost, 5*(1). doi:https://doi.org/10.70329/2744-2403.2025.5.9.7

National Centre for Missing & Exploited Children. (2023). *CyberTipline 2023 Report.* NCMEC.

Ngo, V. M., Gajula, R., Thorpe, C., & Mckeever, S. (2024). Discovering child sexual abuse material creators' behaviors and preferences on the dark web. *Child Abuse & Neglect*.

O'Connell, R. (2003). *A Typology of Child Cybersexploitation and Online Grooming Practices.* Cyberspace Research Unit, University of Central Lancashire.

Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws* .

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, 50–64.

Pereira, M., Dodhia, R., Anderson, H., & Brown, R. (2024). Metadata-Based Detection of Child Sexual Abuse Material. *IEEE Transactions on Dependable and Secure Computing*, 3153-3164.

Ray, A., & Henry, N. (2024). Sextortion: A Scoping Review. *Trauma, Violence, & Abuse*, 138-155.

Rezende, I. N. (2024). The proposed regulation to fight online child sexual abuse: An appraisal of privacy, data protection and criminal justice issues. *International Review of Law Computers & Technology*, 369–390.

Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). *Digital Investigation*, 124-142.

Seigfried-Spellar, K. C. (2017). Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations. *Journal of Police and Criminal Psychology*, 215–226.

Sorbán, K. (2024). Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations . *Belügyi Szemle*, 133-151.

Taylor, M., Holland, G., & Quayle, E. (2001). Typology of paedophile picture collections. *The Police Journal*, 97-107.

UNODC. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.* New York: UN.

Vitorino, P., Avila, S., Perez, M., & Rocha, A. (2018). Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, 303-313.

Westlake, B., Bouchard, M., & Frank, R. (2012). Comparing methods for detecting child exploitation content online. *European Intelligence and Security Informatics Conference*, (str. 153-163). Odense.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). In Their Own Words: Young Peoples' Vulnerabilities to Being Groomed and Sexually Abused Online. *Psychology, 5*(10). doi:http://dx.doi.org/10.1016/j.avb.2012.09.003

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Colling, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 62-70.

WHO. (2020). *Global status report on preventing violence against children.* Geneva: WHO.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72–79.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72-79.

Wolak, J., Liberatore, M., & Levine, B. N. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect*, 347–356.

ONLINE SEXUAL EXPLOITATION OF CHILDREN: OFFENDER METHODS AND SECURITY AGENCY RESPONSES

DOI: *10.70329/2744-2403.2025.5.10.8*

Review article

Aldina Bjelić, MA[58]

Abstract

Online sexual exploitation of children is one of the fastest-growing forms of cybercrime, driven by the rapid development of digital technologies, global connectivity and the wide availability of communication platforms. Offenders use different methods to target vulnerable children, including grooming, sextortion, social engineering, creating fake identities and distributing child sexual abuse material through encrypted channels, peer-to-peer networks and darknet services. Technological factors such as end-to-end encryption, cryptocurrencies, anonymisation networks and generative artificial intelligence further complicate detection and give offenders a high level of operational security. Security agencies respond by developing specialised teams, strengthening digital forensic capacities, improving international cooperation and relying on OSINT and SOCMINT methods to identify offenders and track criminal networks. However, challenges such as lack of staff, technical barriers, fragmented jurisdictions and the speed of technological change continue to limit the effectiveness of the institutional response. Legal and political measures, including the Budapest Convention and the Lanzarote Convention, provide a framework for action, but in practice there is still a significant gap between normative requirements and operational capabilities. The paper emphasises that combating online sexual exploitation of children requires a combination of preventive measures, technological innovation, multisectoral cooperation and stronger capacities of security institutions. Protecting children in the digital environment is not only a legal and social priority but also an important factor of overall security stability.

Keywords: *cybercrime, grooming, sextortion, darknet, OSINT*

[58] aldinabjelic@hotmail.com

1. Introduction

Online sexual exploitation of children is one of the most complex and fastest-growing challenges of the modern digital environment. The development of information and communication technologies, the wide availability of the internet and the mass use of smartphones have created new spaces of interaction where children spend an increasing part of their everyday lives. In this setting, traditional patterns of victimisation take on new digital dimensions, and offenders use specific techniques adapted to the online environment to identify, manipulate and exploit children. This phenomenon is becoming more serious because the internet enables a wide range of anonymous and hard-to-detect activities that cross geographical borders and escape traditional forms of oversight and control. At the same time, the global rise in cases of online sexual exploitation of children shows a growing gap between rapid technological progress and the ability of institutions to adequately protect the most vulnerable population. Security and other agencies face challenges such as encrypted communication channels, decentralised networks, cryptocurrencies and generative artificial intelligence, which further complicate the identification of offenders and the prosecution of criminal acts. Although international standards, legal frameworks and specialised units dealing with this form of crime already exist, their effectiveness often depends on technical equipment, digital forensic capacity and the level of international cooperation. Considering these circumstances, the aim of this review paper is to systematise current knowledge about the methods most commonly used by online offenders, analyse institutional and security responses, and highlight the key challenges that shape the possibilities for effective prevention and repression. The intention is to offer a clear and comprehensive overview of literature and practices that can help professionals, researchers and decision-makers improve child-protection policies in the digital environment.

2. Defining Cyber Exploitation of Children

Cyber exploitation of children refers to a set of criminal acts that involve the use of information and communication technologies for the sexual exploitation of minors, the distribution or production of child sexual abuse material, manipulation, extortion or other forms of unlawful behaviour against children. According to the Lanzarote Convention of the Council of Europe (2007), sexual exploitation of children includes all actions in which a child is used for the sexual satisfaction of another person, regardless of whether the act takes place in a physical or digital space. The digital environment allows these actions to occur without physical contact, while offenders use anonymity, technical protection and

the global availability of the internet to avoid monitoring and responsibility. Internet technology enables connecting distant users and spreading news and information, but it also carries the possibility of influencing the mind and ways of thinking of every human being (Muhić, 2025). In contemporary literature and practice, the term most commonly used is online sexual exploitation of children, or Online Child Sexual Exploitation, which according to Europol reports (2025) includes grooming, sextortion, recruitment of children for sexual activities via the internet and the distribution of child sexual abuse material. In this regard, special emphasis is placed on CSAM (Child Sexual Abuse Material), which visually depicts the sexual abuse of a child. Interpol and ECPAT (2018) increasingly propose the use of the term CSEM (Child Sexual Exploitation Material), emphasising that the focus is not only on the visual representation of abuse but also on the exploitation behind the creation of such content. One of the most important elements of cyber exploitation is grooming, the manipulative process of building trust between the offender and the child. Whittle et al. (2014) define grooming as a targeted, step-by-step and psychologically driven strategy in which the offender creates an emotional bond with the victim, preparing them for sexualised communication or contact. Grooming today mostly takes place on social networks, online games and chat applications, where the offender can communicate freely, without direct supervision by adults. Sextortion represents another key modality of exploitation, and Wolak et al. (2018) describe it as a form of extortion in which the offender demands additional sexual content, money or other benefits, threatening to publish real or manipulated material showing the child in a sexualised context. This form of crime is becoming more common due to the possibility of editing images and videos, including deepfake technology, which UNODC (2015) identifies as a growing challenge for victim identification and evidence procedures. Understanding cyber exploitation of children requires awareness of the technological factors that allow offenders to act with minimal risk. Reports by Europol and Interpol show that encrypted applications, anonymous networks such as Tor, cryptocurrencies and peer-to-peer systems provide a high level of digital security for offenders, while at the same time making investigations by security agencies more difficult. UNODC also warns about the rise of synthetic visual materials generated by artificial intelligence, which are used for manipulation, blackmail or distribution, further blurring the line between real and created content. Therefore, cyber exploitation of children can be clearly defined only when observed through three interconnected aspects- the criminal behaviours manifested in the digital environment, the technological tools that enable anonymity and the spread of material, and the psychological–manipulative strategies used by offenders in communication with victims. Only the combination of these elements allows proper recognition of risks, accurate categorisation of forms of exploitation and the development of institutional mechanisms for preventing and combating this type of crime.

3. Methods Used by Offenders in Online Sexual Exploitation of Children

The methods used by offenders in online sexual exploitation of children continually develop in parallel with the evolution of communication technologies, digital platforms and new possibilities for hiding identity. Unlike traditional forms of abuse, which require physical presence and direct contact, the online environment allows offenders to act transnationally, anonymously and with minimal risk of detection. Europol's IOCTA reports (2022–2025) emphasise that the greatest threat lies in the dynamic nature of these methods, which quickly adapt to changes in security protocols and monitoring mechanisms.

3.1 Grooming as a Central Behavioural Pattern

Grooming is one of the most complex and dangerous forms of online manipulation of children, and understanding it requires an analysis of the dynamic and interconnected stages through which offenders seek to achieve psychological control over the child. The typology developed by O'Connell (2003) is one of the most influential and detailed early models and serves as the basis for modern explanations of how communication patterns, manipulative strategies and technological factors fit into the process of exploitation. However, later studies show that grooming does not always follow a linear order and that offenders often speed up certain phases. For this reason, grooming today must be viewed as a fluid, adaptable and multidimensional process shaped by the offender's motivation, the child's characteristics and the specifics of the digital environment. O'Connell (2003) outlined several grooming stages that are important to consider for better understanding and investigating this type of crime.

Friendship-forming stage

According to O'Connell (2003), the process usually begins with the establishment of friendship, where the offender initiates the first contact with the child, either by pretending to be a peer or openly presenting themselves as an adult. The goal is to assess the child's willingness to communicate and to create a basic sense of familiarity. In this stage, the offender asks introductory questions about age, interests, school obligations or hobbies and may request photos of the child to confirm identity or check physical appearance. Dumitriu, Dudu and Nanău (2024) note that already in this stage it is possible to detect victim selection, since offenders target children who show signs of vulnerability or a need for approval.

Bond-forming stage

This stage represents the deepening of initial contact and the creation of emotional closeness. The offender presents themselves as support, a trustworthy listener or a "best friend", and the conversation expands to topics such as family relations,

school problems, successes, insecurities and everyday challenges (O'Connell, 2003). The goal is to create an illusion of emotional safety. According to Whittle et al. (2013), offenders actively monitor the child's emotional states in this phase to identify moments of vulnerability that can be used to strengthen the connection. Cano, Fernandez and Alani (2014) point out that this stage corresponds to the first part of Olson's theory of luring communication, known as Deceptive Trust Development, in which the offender intentionally creates an atmosphere of trust and shared identity.

Risk assessment stage

After establishing the basic relationship, offenders move to assessing the risk of being discovered. O'Connell (2003) explains that offenders ask questions such as "Who uses the computer?", "Are your parents at home right now?" or "Do you have a phone that only you use?" to determine the level of supervision and the safety of continued communication. This stage is essential because it influences the intensity and direction of the next actions. Chiang and Grant (2017) note that modern groomers often assess risk much earlier, sometimes within the first minutes of conversation, allowing quick evaluation of manipulation potential and avoidance of oversight.

Exclusivity stage

In this phase, the offender introduces narratives about a special relationship, shared secrets and emotional connection. Typical expressions include claims that the child can trust only them, that adults don't understand them, or that the two of them are "special" and "connected in a way others cannot understand". The goal is to isolate the child from other sources of support and create dependency. According to Dumitriu et al. (2024), this stage reflects mechanisms of isolation and psychological control similar to those found in offline abuse. This stage also prepares the child for the normalisation of sexualised communication by strengthening feelings of loyalty and emotional obligation.

Sexual stage

Once a certain level of trust and isolation is achieved, the offender gradually or suddenly introduces sexual content. Questions can range from subtle ("do you have a crush?") to direct ("do you touch yourself?"). Offenders may also request explicit images, suggest using a camera or describe sexual behaviour. Chiang and Grant (2017) show that modern groomers often introduce sexual content much earlier than O'Connell's model suggests, sometimes within minutes, which presents a major challenge for traditional detection tools. Kloess, Hamilton-Giachritsis and Beech (2017) distinguish between groomers who use an indirect approach, gradually increasing sexualisation, and those who use a direct approach without emotional preparation.

Fantasy enactment stage

O'Connell (2003) identifies a final stage in which the offender tries to involve the child in sexually explicit actions, either online or offline. This includes guiding the child through simulated sexual scenarios, performing explicit acts on camera or suggesting a physical meeting. Chiang and Grant (2017) confirm that this stage may appear very early in modern cases due to the fast pace of communication and the fact that many offenders operate within pedophile communities on the darknet, where knowledge and "tips" on effective exploitation strategies are shared.

Dynamic, overlapping and accelerated phases

Although O'Connell's model was pioneering and remains the most detailed staged approach, modern empirical studies (Chiang & Grant, 2017; Kloess et al., 2017) show that grooming in the contemporary online environment occurs much faster and that the stages are far from linear. Research shows that:
• all stages can occur within the first hour of communication
• sexualisation can appear in the first messages
• stages often overlap
• groomers may skip entire stages if the child appears vulnerable
• digital platforms enable fast escalation, especially when using encrypted apps

Dumitriu et al. (2024) confirm that grooming should be viewed as an adaptive process influenced by the offender's motivation, the victim's vulnerability and the communication context, and not as a fixed sequence of steps.

3.2 Online Sexual Extortion

Online sexual extortion is one of the most aggressive and harmful forms of technology-mediated sexual exploitation of children, and in the last decade it has become a priority threat in Europol reports and international organisations. Although public discourse often equated it with grooming or broader categories of online sexual violence, current research shows that it is a separate and highly destructive behavioural pattern. In simple terms, sextortion occurs when an offender threatens to publish, distribute or send sexually explicit images or videos of a child if the child does not meet certain demands, whether sexual, emotional or material. This basic structure of coercion forms the core of a phenomenon that, according to findings by Finkelhor et al. (2020), affects around 3.5% of youth before adulthood, while the real prevalence is likely much higher due to very low reporting rates.

Unlike grooming, which relies mostly on creating emotional closeness and gradually weakening boundaries, online sexual extortion is based on a sudden and

radical shift in power once the offender gains possession of sexual material involving the child. Açar (2016) defines this form of exploitation through three key elements, first, the digital environment as the setting of the act, second, possession of compromising material and the third, use of that material as a tool of blackmail. Only when all three elements are present can we speak of sextortion as a specific form of online sexual violence. This formulation is particularly useful because it distinguishes sexual extortion from grooming, sexting, cyberbullying and other digital risks. Research shows that the initial material is most often created through voluntarily sent images in the context of a romantic relationship, friendship or expected intimacy. Wolak et al. (2018) find that 75% of minor victims knowingly sent the first material but under pressure or emotional manipulation, and more than 60% of offenders came from the victim's circle of acquaintances, peers or former partners. These findings challenge the stereotype of the "stranger predator" and show that many incidents occur within existing adolescent power dynamics. At the same time, modern extortion increasingly involves unknown offenders, including criminal groups that use fake profiles to initiate the exchange of intimate images, escalate communication quickly and later demand money, more explicit material or other forms of obedience (Ray & Henry, 2024).

The methods of obtaining material vary, but three dominant patterns appear in the literature (Açar, 2016). The first concerns extortion within existing relationships, usually among adolescents, where intimate photos become a tool of control after conflict or a breakup. The second involves predatory behaviour in which grooming techniques are used only as an initial step to obtain visual material, followed by a quick escalation of threats. The third includes technically sophisticated methods, such as hacking accounts or cameras, although these are much less common in practice because they require knowledge that most offenders do not have (Açar, 2016). However, IoT devices and live-streaming functions introduce new risks, especially in the context of recording without consent. The dynamics of extortion are particularly dangerous because threats serve not only as a means of control but also as a factor of psychological destabilisation. Typically, the offender threatens to publish the material, send it to parents, friends or teachers, create fake profiles or distribute it within school communities. Studies show that many offenders repeat threats for months and that, in cases involving minors, they sometimes encourage self-harm or suicide to strengthen their control (Wolak et al., 2018). These escalations demonstrate that sextortion is not only a digital phenomenon but a form of psychological and emotional violence with severe consequences for the victim's mental health. The psychological consequences of sexual extortion are severe, and the literature reports long-term effects such as depression, strong anxiety, guilt, shame, withdrawal from social contact and serious self-destructive thoughts (Ray & Henry, 2024). There are documented cases in which children changed schools,

stopped education or attempted suicide to escape threats they did not know how to stop. Crucially, most victims do not seek help because half of minors in Wolak et al.'s (2018) study never reported the incident, fearing judgement, disbelief, parental reactions or damage to reputation. This creates a vicious cycle in which extortion continues precisely because it remains invisible.

3.3 Production and Distribution of CSAM: Technological Infrastructure, Criminal Dynamics and Challenges for Investigation

The modern production and distribution of child sexual abuse material (CSAM) takes place in a digital environment characterised by speed, anonymity and global reach. Technological development over the past twenty years has fundamentally changed criminal processes, making the creation and spread of CSAM easier and operationally safer for offenders. Lee et al. (2020) emphasise that today's online environment combines three key dimensions important for understanding this phenomenon, the legal framework, distribution channels and technical detection mechanisms. These dimensions shape the entire infrastructure in which offenders operate and, at the same time, set clear limitations for investigative bodies. The criminal process begins with the production phase, which now occurs in a wide range of contexts from direct contact abuse within intrafamilial settings to fully online exploitation through webcams and digital devices. The systematic review by Cale et al. (2021) shows that a significant portion of CSAM is produced in environments where the offender has direct access to the child. In more than half of cases, the offender is a family member or close acquaintance of the victim. This is confirmed by findings from Gewirtz-Meydan et al. (2018), which show that family members, partners of parents and individuals in the child's immediate environment are the most common producers of such content. At the same time, there is a growing number of cases in which CSAM is produced exclusively online, without physical contact, through direct persuasion of children to perform sexualised acts in front of a camera (McManus, Long, Alison, & Almond, 2015). This form represents a relatively new category of digital crime, encouraged by the expansion of video-communication apps and offenders' low perception of risk.

The distribution of CSAM is central within the modern ecosystem of child sexual exploitation and takes place through three dominant channels. Firsth is the open web, then P2P networks and finaly, the dark web. On the open web, CSAM appears in two contexts, in direct offender-child interactions through social networks, and in the form of unstructured, temporarily available material that escapes moderation. Cale et al. (2021) note that the open web is where most initial contacts between children and offenders occur, especially on platforms such as Facebook, Instagram, Snapchat and various video-sharing applications. Grooming, sexualised persuasion and the collection of initial photos dominate this segment, and this content often becomes the starting point for broader distribution

within criminal networks. This shows a constant connection between production and distribution because material created during grooming frequently becomes part of wider circulation. P2P networks form the second layer of distribution and enable global sharing of large files without a central intermediary. Bissias et al. (2016) estimate that at a certain point more than 800,000 users worldwide participated in sharing CSAM on P2P networks, while Bouhours and Broadhurst (2011) highlight that much of the exchange occurs locally within language and cultural groups of connected users. These networks are characterised by huge data volumes, frequent sharing of long-term archived material and fragmentation of files, all of which make the identification of original content more difficult. Police agencies in many countries report that P2P networks generate workloads that exceed their technical and staffing capacities, a finding also confirmed by Johansson (2019) in the Swedish policing context.

The most organised and dangerous layer of distribution is found on the dark web. Ngo, Gajula, Thorpe and McKeever (2024) analysed more than 353,000 posts on eight dark web forums and identified over 10,000 active CSAM contributors who use these platforms for material exchange, communication, advice on avoiding detection and the creation of closed communities. The authors note specific criminal patterns, exchange of exclusive content, coded jargon, advanced operational security practices and structured hierarchies in which status is built through volume of contribution. These structures represent the digital equivalent of organised criminal networks and significantly hinder infiltration and evidence collection. Research also shows that platforms such as Tor and I2P are the main access channels, supported by encryption, cryptocurrencies and decentralised hosting services that further complicate investigative work.

All these dynamics generate serious operational challenges for investigations. Leclerc et al. (2022) report that investigators around the world highlight the lack of specialised training, technical resources and analytical support as the biggest obstacles to effective case processing. Problems range from outdated equipment and a shortage of digital forensic experts to weak cooperation with global social networks and legal barriers that slow access to data. Johansson (2019) further notes that many police organisations still treat CSAM as a lower-priority offence, resulting in overloaded investigators, lengthy procedural delays and an institutional response that remains weak compared to the scale of harm.

3.4. Techniques for Identifying Victims and Offenders

Identifying victims and offenders in cases of online child sexual abuse represents the key link between the “digital trace” and the traditional criminal justice process. Three layers interact in this process: forensic analysis of visual content,

automated detection and classification techniques for CSAM, and operational-investigative methods aimed at tracing the real individuals behind the screen. Modern literature shows that none of these components is sufficient on its own. The greatest effect is achieved by combining several approaches, supported by a clearly defined institutional division of roles and responsibilities.

3.4.1. Forensic Analysis and Classification of Visual Material

A basic precondition for identifying victims and offenders is the ability to recognise that certain material involves child sexual abuse and to consistently classify it according to legal categories. Kloess et al. show that even experienced police analysts have significant difficulty evaluating two key dimensions whether the person shown is a child, and whether the content is "illegal" or "indecent" in a legal sense (Kloess, Woodhams, Whittle, Grant, & Hamilton-Giachritsis, 2017). Particularly challenging are so-called "borderline images", such as early pubescent adolescents, partial nudity or situations where context may be interpreted as "innocent". Inter-rater analyses show higher disagreement among coders on such material, which directly affects the consistency of prosecution and assessment of offence severity. To reduce subjectivity, classification tools such as the COPINE scale and later simplified categories (A, B, C) were introduced, separating penetrative acts, non-penetrative sexual activities and "erotic posing" (Taylor, Holland, & Quayle, 2001). However, category C ("erotic posing") illustrates how fluid the normative boundary is. Analysts often admit they prefer to focus on clearly severe material, while lower-level cases remain in a zone of uncertainty. This has a direct impact on victim identification, as children whose images are not formally recognised as CSAM remain outside proactive investigations and international databases.

Age estimation presents a particular challenge. Research shows that even medical experts are not significantly better than laypersons at distinguishing older adolescents from adults on the basis of photographs, due to high variability in pubertal development (Cattaneo et al., 2009). In the digital context this challenge is heightened by ethnic differences in body structure, changes in body mass index and the global nature of CSAM. In practical terms this means that age assessment must be combined with other indicators such as scene context, metadata, file names, language and cultural elements of the environment, rather than relying solely on visual impression.

3.4.2. Hash Databases, P2P Monitoring and Web Crawlers as Foundations of Identification

On the technical level, most modern CSAM-detection systems rely on hash databases of known material. PhotoDNA and similar technologies generate "fingerprints" of images, allowing recognition of previously identified files even when they have been partially altered (Edwards, Christensen, Rayment-McHugh, & Jones, 2021). This achieves two goals. First, the number of digital artefacts

requiring manual review is drastically reduced, and investigators can track the same victim across different offender collections and platforms, which is crucial for physical rescue. Monitoring of P2P networks and specialised tools such as iCOP go further by combining hash searches with analysis of file names and network traffic (Peersman, Schulze, Rashid, Brennan, & Fischer, 2016). Studies show that a small number of "nodes" produce a disproportionately large share of CSAM traffic, and that removing only the top of the distribution pyramid could reduce material availability on certain networks by 30–40% (Wolak, Liberatore, & Levine, 2014). From the perspective of offender identification, tracking IP addresses, sharing patterns and "seed file" lists allows profiling of the most active distributors, who are often the main producers or administrators of closed communities, meaning actors with the highest "operational significance".

Web crawlers applied to the clear web and, to a limited extent, to the darknet automatically track links from known CSAM domains and map networks of connected pages (Westlake, Bouchard, & Frank, 2012). Initiatives such as Project Arachnid demonstrate that it is possible to process hundreds of millions of pages and identify tens of thousands of unique CSAM images in a short period of time, giving police the capability to target sites with the highest "centrality" and disrupt distribution infrastructure. At the same time, every instance in which a known image appears at a new location generates a trace that may lead to new offenders and potentially new information about the identity of the victim.

3.4.3. Metadata, File Names and Darknet Analysis

Newer studies increasingly highlight the value of metadata and textual traces as sources for identifying both CSAM content and the actors involved in its distribution. Research by Pereira et al. shows that classification models based solely on file names and file paths can achieve a high level of accuracy because offenders tend to develop specific, recognisable vocabulary and coded language when naming their files (Pereira, Dodhia, Anderson, & Brown, 2024). P2P searches already rely heavily on textual searches of file names, so moving towards automated analysis of these patterns is a logical next step.

Ngo et al. developed a machine-learning system for detecting CSAM on dark web forums, which, on a corpus of over 350,000 posts, successfully identified around 63,000 CSAM-relevant entries and more than 10,500 "creators" of CSAM content (Ngo et al., 2024). Analysis of metadata from these posts offers several key insights: dominant themes and preferences of certain authors, typical age groups and nationalities of victims mentioned, and platforms most commonly used for obtaining and exchanging material (Omegle, YouTube, Skype, Instagram, Telegram). For the purpose of offender identification, such patterns serve as a basis for targeting the most active and dangerous individuals, as well as for identifying new hotspots on "surface" platforms where victims are recruited or

where CSAM is initially produced (e.g., live streaming via VoIP applications, webcams and social networks).

Metadata in a broader sense – such as EXIF data, timestamps, geolocation, software version and system language – further enrich the analytical picture. Although offenders are increasingly aware of the need to "clean" metadata, the analysis of millions of files and network interactions still allows statistical profiling of typical configurations, time patterns and technological tools used by certain groups. This does not automatically provide a specific identity, but it narrows the operational field and guides traditional investigative work.

3.4.4. Automated Detection, AI and Forensic Workflow

The review of literature on automated CSAM detection shows a clear convergence. The most effective systems combine multiple modalities – hash values, visual characteristics of images, textual signals in file names and metadata – instead of relying on a single indicator (Edwards et al., 2021). Deep neural networks achieve the best results when detecting previously unseen CSAM, especially when multiple image and video descriptors are merged into a unified classifier (Lee, Ermakova, Ververis, & Fabian, 2020). Vitorino et al. (2018) show that CNN models trained on large police datasets can effectively distinguish CSAM from adult pornography, while studies combining pornography detection and age estimation further narrow the focus on potential child victims (Vitorino et al., 2018; Lee et al., 2020). However, Pereira et al. emphasise that models must be tested in realistic scenarios, including fully benign "out-of-sample" sets and situations in which offenders intentionally modify textual patterns (adversarial examples such as "Lo7ita", "b4", and similar) (Pereira et al., 2024). A high rate of false positives can practically block the implementation of such systems on platforms with billions of users, and for police work it creates additional operational burden. The practitioner survey by Sanchez et al. shows that investigators are highly sensitive to false positives; most consider a high FP rate a more serious problem than missed cases precisely because FP findings directly overwhelm limited resources (Sanchez, Grajeda, Baggili, & Hall, 2019). At the same time, Sanchez et al. (2019) note that many practitioners are not sufficiently familiar with data science and AI basics, even though they already work with tools that rely on these techniques. This creates a gap between technological potential and actual practical use.From a technical standpoint, many tools for triage and filtering have been developed – from simple pixel-level nudity detectors, through specialised field-triage tools, to complex systems that automatically rank devices and storage media by the likelihood of containing relevant evidence (Marturana & Tacconi, 2013). In terms of identifying victims and offenders, their value lies in reducing the time investigators spend reviewing large amounts of benign material, allowing them to reach "clean" CSAM faster, where concrete faces, environments and behavioural patterns can be recognised.

3.4.5. Identification of Victims and Offenders

Although most of the technologies mentioned above primarily serve to detect and classify content, they also form the foundation for identifying victims and offenders in a narrower sense. In practice, this process unfolds through several complementary steps. First, hash databases and automated visual detection help isolate material that contains previously unidentified victims, which then becomes a priority for specialised "victim identification" teams (Edwards et al., 2021; Johansson, 2019). Second, estimating age, external characteristics, background language and cultural artefacts (such as clothing, architecture or household items) helps to geographically and demographically attribute the victim, although Kloess et al. (2017) clearly show that age estimation remains a major source of uncertainty, especially with adolescents. Third, investigative teams increasingly use techniques such as facial recognition, comparison of rooms, furniture and "micro-environments" across different cases and reports, which makes it possible to link the same victim or offender across multiple investigations and jurisdictions (Edwards et al., 2021). In a broader criminological sense, studies on crime commission processes show that CSAM producers often merge online and offline dimensions, combining contact abuse with recording and digital distribution. Key decisions in these cases depend on the offender's assessment of detection risk, access to children and technical capacity (Cale et al., 2021). Understanding these processes helps police prioritise offenders who are likely to be both online distributors and offline abusers.

Offender identification also depends on traditional digital traces such as IP addresses, logs, social media accounts, communication within P2P and darknet environments and the way these elements are integrated with OSINT, HUMINT, SIGINT and classic investigative methods. In the investigation of organised criminal groups and their members, open sources such as social networks provide a large amount of relevant information, including photographs, videos, posts and similar content (Muhić, 2024). Johansson shows that in Sweden, for example, one major challenge is the lack of an obligation for ISPs to store IP logs, which directly complicates offender identification even when CSAM content has been detected (Johansson, 2019). Similarly, Leclerc et al. (2022) report that police investigators highlight a mix of "social engineering" communication skills, strong IT literacy and understanding of sexual offender profiles as key competencies. In other words, even the most advanced algorithms cannot replace the investigator's ability to turn digital traces into operational hypotheses and test them through interviews, surveillance and other measures.

3.4.6. The Human Factor: Capacities, Workload and Investigator Protection

Most of the techniques described above require intensive work by specialised police teams and digital forensic analysts. Multiple studies confirm that this professional group faces a high risk of secondary trauma, chronic stress and burnout due to ongoing exposure to extremely disturbing content (Burns, Morley,

Bradshaw, & Domene, 2008; Seigfried-Spellar, 2017; Sanchez, Grajeda, Baggili, & Hall, 2019). Investigators in Leclerc's study identify several key problems such as enormous data volumes, lack of personnel and technical resources and limited understanding of the CSAM phenomenon among the management of their own institutions (Leclerc et al., 2022). Johansson reports similar findings in Sweden: different police regions follow different procedures, digital forensic staff represent a major "bottleneck" and CSAM is often treated as a "low-priority" crime in practice (Johansson, 2019). Sanchez et al. (2019) show that investigators recognise the high value of filtering and triage technologies, mainly because they reduce exposure to harmful material and speed up the workflow. At the same time, investigators report relatively limited use of advanced AI-based tools, partly because they do not fully understand how such tools work (Sanchez, Grajeda, Baggili, & Hall, 2019). Effective implementation of techniques for identifying victims and offenders therefore requires more than simply procuring technological solutions. It also demands investment in systematic training, supervision, psychological support and clear operational protocols to ensure that the personnel who perform the most difficult tasks remain functional and professionally sustainable.

4. Institutional, Operational and Legal Responses to Online Sexual Exploitation of Children

4.1. National and International Legal Framework

The modern international legal framework regulating online sexual exploitation of children was developed in a period that did not anticipate today's scale, speed and technological capabilities of digital production and distribution of child sexual abuse material. Despite strong normative density and wide adoption of key international instruments, there is a visible structural tension between the formal obligations of states and their actual capacities to respond adequately to a phenomenon that evolves faster than legislation can adapt. According to the *Global Status Report on Preventing Violence Against Children* (WHO, 2020), most states have relatively developed normative frameworks for child protection, but fewer than half possess effective implementation mechanisms. In the digital environment, where CSAM is distributed through anonymous networks, peer-to-peer systems, encrypted communication channels and platforms based on generative artificial intelligence, this gap between normative commitments and operational capacity becomes even more pronounced. Understanding the international and European legal framework is therefore essential for identifying the root causes of investigative failures, delays in victim identification and the limited reach of criminal justice mechanisms. The *Convention on the Rights of the Child* (CRC) of 1990 is the foundational international instrument for child protection, yet it was created in a historical context in which the internet was only

beginning to enter wider use. For that reason, the CRC does not contain specific provisions recognising the digital environment as a primary space of victimisation, nor does it address phenomena such as virtual CSAM, deepfake technologies, visual manipulation or anonymous global markets operating through the darknet. Its greatest strength lies in establishing principles such as the best interests of the child, the obligation to take preventive action and the promotion of child development. However, these principles remain insufficiently operationalised in the digital context. The *Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography* (OPSC) represents an attempt to fill these gaps, but Maxwell's analysis (2022) shows that the OPSC remains primarily focused on criminalisation, while preventive measures are formulated broadly, suggestively and without clear minimum standards that states must meet. This approach leads to a situation in which states mostly fulfil their formal criminalisation obligations, while systemic preventive policies remain underdeveloped or entirely absent.

The Budapest Convention of the Council of Europe (2001) is the first comprehensive international instrument addressing computer-mediated crime, including the production, distribution and possession of "child pornography" under Article 9. It established the architecture for international police and judicial cooperation, but its effectiveness has been limited by several structural factors. The transnational nature of CSAM-related crime complicates the application of territorial jurisdiction, meaning that cases involving servers, offenders and victims in different countries often end up in lengthy mutual legal assistance procedures. In addition, states define illegal content differently, especially in relation to virtual, realistic or AI-generated depictions of children, which complicates coordinated action and evidence exchange (Sorbán, 2024). Differences in regulations on mandatory retention of IP logs further burden investigations, since some jurisdictions store logs for only a few months while others keep them for years, which in practice determines the outer limits of successful digital investigations (Kasper & Laurits, 2016).

The Lanzarote Convention (2007) introduced a qualitative shift by criminalising grooming behaviour via information technologies and establishing the obligation of states to take all appropriate measures to protect children from online sexual exploitation. However, as with all Council of Europe instruments, the Lanzarote Convention lacks mechanisms to sanction states that fail to implement their obligations. Its flexible normative structure allows different interpretations, especially regarding virtual and AI-manipulated depictions, which creates additional legal gaps in the context of generative AI and advanced image-manipulation tools (Parti & Szabó, 2024). Although it introduced important conceptual innovations, the Lanzarote Convention did not anticipate the creation of fully fictional, hyper-realistic depictions of children. As a result, its application to AI-generated content remains under-developed.

At the regional level, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children is the most important instrument. It obliges EU Member States to criminalise all forms of online sexual exploitation, including grooming, possession, distribution, creation and facilitation of CSAM. The Directive also provides for proactive investigations that do not depend on a victim's report, extended extraterritorial jurisdiction, victim-support measures from the earliest stages of proceedings and specialised operational mechanisms. However, as a minimum-harmonisation instrument, it allows Member States to transpose its provisions differently, which has resulted in deep differences in definitions, procedures and sanctions. This fragmentation hinders investigative coordination, evidence exchange, cooperation with Europol and the implementation of joint operations, particularly in cases involving peer-to-peer systems, encrypted applications or AI-generated content (Huemer, 2024). An additional problem is that the Directive does not provide detailed guidance on the challenges posed by generative AI, does not address realistic child-like avatars in metaverse environments and does not offer solutions for situations in which end-to-end encryption prevents access to evidence. The most recent attempt to create a stronger European legal framework is the draft Regulation COM (2022) 209 final, which would require internet platforms to detect, remove and report CSAM, as well as identify grooming communication through automated systems. The Regulation, however, raises serious questions about the balance between child protection and privacy, since its practical implementation would require monitoring user communications in ways that conflict with standards of encrypted private communication and the principles of the GDPR (Rezende, 2024). European privacy-protection organisations warn that such large-scale monitoring could set a precedent for mass surveillance, while police and prosecution bodies argue that without these mechanisms it is impossible to address the exponential growth of online child exploitation.

All these layers of legal regulation point to a deeply rooted problem which is the existing legal instruments were created in an era of analogue crime and are not fully capable of responding to digital phenomena that involve global distribution, trace deletion, E2EE communication, the use of cryptocurrencies and generative artificial intelligence. Differences in definitions, capacities and legal implementation across states place children in an unequal position, while operational barriers such as inconsistent IP-log retention, slow international legal assistance and limited access to digital evidence often result in failed investigations or an inability to identify victims. This makes it clear that, despite widely ratified instruments and formally high protection standards, the legal framework remains insufficiently aligned with the real demands of the digital environment. A deep, structural reform is required if the system is to respond effectively to the growing phenomenon of online sexual exploitation of children.

4.2. Organisational Models and Capacities of Police and Prosecution Services

Although the international and European legal framework sets minimum standards for criminalisation and interstate cooperation, the actual level of child protection in the digital environment depends primarily on the organisational models, capacities, resources and operational procedures of national police and prosecutorial institutions. Online sexual exploitation of children cannot be effectively addressed within systems whose institutional architecture belongs to the period before mass digitalisation, nor within organisations that still treat digital crime as a peripheral form of offending. Empirical data and comparative studies (Sanchez et al., 2019; Johansson, 2019) show that most national systems face chronic shortages of specialised units, fragmented procedures, insufficiently trained staff and the high emotional burden that prolonged exposure to CSAM material places on investigators. These weaknesses have direct consequences. Many cases remain uninvestigated, identified victims remain unidentified in practice and prosecutorial files are delayed for months or even years.

In most countries, the organisational response relies on specialised cybercrime, digital forensics and sexual offences units, yet the real scope of their mandates and capacities varies significantly. Structurally, police agencies usually apply a model in which digital investigations unfold across three components- analytical, operational and forensic. Analytical units collect and process reports, analyse OSINT and SOCMINT traces, map P2P networks and track distribution trends. Operational units conduct undercover activities in online environments, initiate covert communication with suspects and collect real-time material traces. Forensic units handle seized devices, analyse metadata, use hash databases and specialised algorithms to identify content and extract evidence for criminal proceedings. However, in practice these three functions are often separated, poorly coordinated and dependent on the individual motivation and expertise of a small number of officers. This represents a major limitation in cases where speed, technological knowledge and inter-sectoral communication determine the outcome of the investigation.

The overburdening of police and prosecutorial capacities represents a particularly acute challenge. The study by Sanchez et al. (2019) shows that investigators working on CSAM cases operate under significant psychological pressure, are exposed to secondary victimisation and frequently experience symptoms of burnout. This leads to high staff turnover, reduced efficiency and a loss of institutional memory. In many countries, the number of reports far exceeds available personnel. In 2023 alone, NCMEC received 35.9 million reports (National Center for Missing & Exploited Children, 2023), while Europol and Interpol continue to record a constant rise in material distributed in fragments across encrypted chat applications, cloud services and dark web forums. Police and prosecutorial bodies cannot keep up with this volume, resulting in selective prioritisation, often at the expense of cases involving online grooming or material

without immediate physical abuse, but with significant long-term psychological consequences for children. In such systems, CSAM is treated in many states as a "lower-priority" offence, which directly affects the speed and quality of investigations.

Technical infrastructure adds another dimension to institutional limitations. Processing terabytes of data from seized devices requires advanced tools, large storage capacities and specialised SQL or AI-driven systems capable of classifying content, identifying victims and linking cases across jurisdictions. In many countries, these systems are not standardised; instead, a heterogeneous mix of outdated software, commercial tools and open-source solutions is used, often without interoperability (Johansson, 2019). The lack of standardisation complicates forensic analysis, slows down investigations and undermines the quality of evidence presented to prosecutors. In addition, police agencies in resource-limited states often lack even basic capacities for device decryption, analysis of encrypted communications or work with P2P monitoring tools, creating a visible gap between the technological capabilities of offenders and the institutional capacity to counter them.

The role of international institutions such as NCMEC, Europol and Interpol is therefore crucial in bridging some of these gaps, but their work also exposes weaknesses within national systems. Europol's EC3, Interpol's ICSE database and NCMEC's CyberTipline provide essential tools for victim identification and coordination of global records, yet their effectiveness depends on the speed and quality of national responses. States without developed capacities for proactive scanning, hash-matching or metadata analysis remain outside global information flows, leaving victims in those jurisdictions unidentified and offenders unprosecuted. In this sense, international infrastructure can only partially compensate for national weaknesses; it cannot replace the absence of specialised staff, clear procedures, adequate funding or the political will to treat online sexual exploitation of children as a priority issue.

4.3. Operational Strategies and Models of Cooperation in Countering Online Sexual Exploitation of Children

Operational responses to online sexual exploitation of children develop within a complex environment where technological innovation, transnational criminal ecosystems and institutional differences between states intersect. While legal frameworks define obligations and organisational capacities determine what is practically feasible, operational strategies represent the final and most dynamic layer of institutional action, the point where norms and capacities must be translated into real investigations, victim identification and the dismantling of offender networks. Online child exploitation is marked by extreme fluidity. Offenders use diverse platforms, move rapidly between services, combine

legitimate and anonymous communication channels and increasingly rely on generative AI tools. In such an environment, traditional reactive policing models have proven insufficient, pushing states toward proactive, intelligence-led and internationally coordinated strategies.

Operational strategies rest on three core approaches such as proactive detection, technical-forensic analytics and international cooperation. Proactive strategies involve systematic monitoring of online spaces, the use of undercover identities when communicating with suspects, the identification of grooming patterns and the analysis of open and semi-closed online environments. OSINT and SOCMINT methods become indispensable in this context. Police units gather information from public profiles, digital traces, social networks, open P2P hubs and crypto forums, and use algorithmic tools to detect risky interactions. Edwards et al. (2021) emphasise that P2P monitoring is not only a technical mechanism for detecting CSAM distribution but also a tactical strategy for infiltrating closed networks where offenders share material and information on new methods of evading detection. The success of such operations depends on investigator experience, their ability to recognise behavioural patterns in fragmented digital environments and their capacity to monitor multiple communication channels at once. The second layer of operational strategies is technical-forensic analytics. Material obtained through proactive operations, device seizures or user reports passes through complex stages of digital processing, hash matching, metadata analysis, geolocation assessment, visual classification and the identification of potential victims. Automated systems and algorithmic tools are crucial for processing speed, but their effectiveness depends on the quality of national databases and access to international platforms. Projects such as Canada's Project Arachnid, which automatically scans the internet and detects CSAM content in real time, have proven valuable models, although their implementation depends on national regulatory and technical infrastructures. Australia's ACIC models, which integrate intelligence data with operational teams and automated network-monitoring systems, further demonstrate how centralised and technologically advanced approaches can compensate for shortages in national staffing capacities. The third strategic layer is international cooperation, without which a serious fight against online sexual exploitation is impossible. Most CSAM is hosted or distributed via servers located in other countries, and offenders frequently use VPNs, proxies and encrypted communications to obscure their location, automatically turning investigations into transnational cases. Europol's European Cybercrime Centre (EC3) coordinates operations among EU member states, and Europol's analytical platforms help identify patterns and connect scattered fragments of material. Interpol's ICSE database, containing identified and unidentified victims, is a crucial tool enabling individual cases to be linked into a broader operational picture. NCMEC's CyberTipline can trigger investigations in

dozens of countries within hours, but its effectiveness depends heavily on the speed and reliability of national police responses.

However, international cooperation faces numerous obstacles. Differences in evidentiary standards between states, slow responses from internet service providers to data requests, legal differences in CSAM definitions and content encryption all pose significant limitations. In many cases, even when an offender can be identified, evidentiary standards in one jurisdiction prevent the use of material collected in another, resulting in a disproportionate number of unprosecuted cases. In situations where cryptocurrencies are used to pay for access to livestreamed abuse, investigations become even more complex, requiring a combination of digital forensics, financial tracking and mutual legal assistance, processes that many states cannot carry out quickly or effectively.

5. CONCLUSION

Online sexual exploitation of children is developing in an environment where rapid technological change, global access to digital platforms and sophisticated methods of concealment have created a criminal ecosystem that exceeds the capacities of traditional legal and institutional responses. The CSAM phenomenon is no longer limited to local boundaries or isolated offenders; it has evolved into a transnational, dynamic and technologically enabled threat that continually erodes existing models of child protection. In such a context, it becomes evident that normative instruments, no matter how well designed, cannot achieve their purpose unless accompanied by adequate operational abilities, technical capabilities and real political will to recognise this form of violence as a priority security concern.

The core problem does not lie only in inconsistencies within the law, but in the fact that digital risks evolve faster than legal systems can respond. Generative artificial intelligence, realistic visual manipulation of child images, encrypted communication and anonymous networks undermine traditional investigative methods and require approaches that integrate forensic analytics, proactive monitoring, international coordination and interdisciplinary knowledge. Without such integration, investigations remain reactive, fragmented and slow, while offenders exploit the advantages of the digital environment to avoid identification and legal consequences.

The institutional response, particularly within police and prosecution services, faces a burden for which many systems were never designed. Overworked investigators, a lack of specialised training, the psychological pressures of long-

term exposure to CSAM material and limited technical infrastructure result in a large number of cases never being processed and many victims remaining unidentified. These structural limitations create a vicious cycle, the weaker the system, the bolder the offenders and the more exposed the children, while the digital environment produces new forms of risk faster than institutions can build resilience.

For these reasons, the fight against online sexual exploitation of children cannot rely solely on the criminal justice response, although it remains indispensable. What is needed is a shift in paradigm from reactive models that intervene only after harm occurs, toward preventive, proactive and technologically supported mechanisms that reduce material availability, restrict access to potential victims, recognise risky behaviours before they escalate and create digital environments in which children are less vulnerable. In this sense, prevention is not a supplementary component of the system but its primary protective framework.

P As a conclusion of the reviewed theory, it becomes clear that protecting children in the digital environment requires a stable combination of three elements: normative clarity, operational capability and international solidarity. None of these elements can function on its own. International instruments must be aligned with technological realities, institutions must be strengthened in terms of funding and staffing, and cooperation between states must be faster, more substantial and free of bureaucratic barriers that currently allow offenders to use geographical differences as a protective shield. Only in a system that recognises that child safety is closely linked to the technical, political and legal capacities of modern societies can we speak of real, and not merely declarative, protection of children's rights.

LITERATURE

Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, 110–126.

Basave, A. E., Fernandez, M., & Alani, H. (2014). Detecting Child Grooming Behaviour Patterns on Social Media. *Lecture Notes in Computer Science*.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect*, 185–199.

Bouhours, B., & Broadhurst, R. (2011). *On-line Child Sex Offenders: Report on a Sample of Peer to Peer Offenders Arrested between July 2010-June 2011.* Canberra: Australian National University.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology*, 20–31.

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends and Issues in Crime and Criminal Justice*.

Cattaneo, C., Ritz-Timme, S., Gabriel, P., Gibelli, D., Giudici, E., Pasquale Poppa, D. N., . . . Grandi, M. (2009). The difficult issue of age assessment on pedo-pornographic material. *Forensic Science International*, 21-24.

Council of Europe. (2007). *Council of Europe Convention on the Protection of Children against Sexual.* Lanzarote: Council of Europe.

Dumitriu, C.-G., Dudu, A., & Nanău, I.-A. (2024). SYSTEMATIC REVIEW: GROOMING BEHAVIOR IN CASES OF CHILD SEXUAL ABUSE: STAGES OF THE PROCESS, RELATION DYNAMICS AND PREVENTION. *Anthropological Researches and Studies*, 268-292.

Edwards, G., Christensen, L. S., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends & issuesin crime and criminal justice*.

Europol. (2025). *Internet Organised Crime Threat Assessment.* Europol.

Finkelhor, D., Turner, H., & Colburn, D. (2020). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA Netw Open*. doi:doi:10.1001/jamanetworkopen.2022.34471

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect*, 238–248.

Grant, T., & Chiang, E. (2017). Online grooming: moves and strategies. *Language and Law*, 103-141.

Huemer, M.-A. (2024). *Revision of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.* European Parliamentary Research Service.

Interpol & ECPAT. (2018). *owards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material.* ECPAT.

Johansson, C. (2019). *Combating online child sexual abuse material. An explorative study of Swedish police investigations.* Malmo: Faculty of Health and Society.

Kasper, A., & Laurits, E. (2016). Challenges in Collecting Digital Evidence: A Legal Perspective. *The Future of Law and eTechnologies*, 195–233.

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2017). Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms. *Sexual Abuse*, 73-96.

Kloess, J. A., Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2017). The Challenges of Identifying and Classifying Child Sexual Abuse Material. *Sexual Abuse*, 173-196.

Leclerc, B., Cale, J., Holt, T., & Drew, J. (2022). Child Sexual Abuse Material Online: The Perspective of Online Investigators on Training and Support Get access Arrow. *Policing: A Journal of Policy and Practice*.

Lee, H.-E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*.

Marturana, F., & Tacconi, S. (2013). A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation*, 193-204.

Maxwell, F. (2022). Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age. *The International Journal of Children's Rights*.

McManus, M. A., Long, M. L., Alison, L., & Almond, L. (2015). Factors associated with contact child sexual abuse in a sample of indecent image offenders. *Journal of Sexual Aggression*, 368–384.

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, 4*(2), 314-338.

Muhić, E. (2025). Psihološke operacije na društvenim mrežama - primjeri, tehnike, taktike i procedure. *Zaštita i sigurnost, 5*(1). doi:https://doi.org/10.70329/2744-2403.2025.5.9.7

National Centre for Missing & Exploited Children. (2023). *CyberTipline 2023 Report.* NCMEC.

Ngo, V. M., Gajula, R., Thorpe, C., & Mckeever, S. (2024). Discovering child sexual abuse material creators' behaviors and preferences on the dark web. *Child Abuse & Neglect*.

O'Connell, R. (2003). *A Typology of Child Cybersexploitation and Online Grooming Practices.* Cyberspace Research Unit, University of Central Lancashire.

Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws* .

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, 50–64.

Pereira, M., Dodhia, R., Anderson, H., & Brown, R. (2024). Metadata-Based Detection of Child Sexual Abuse Material. *IEEE Transactions on Dependable and Secure Computing*, 3153-3164.

Ray, A., & Henry, N. (2024). Sextortion: A Scoping Review. *Trauma, Violence, & Abuse*, 138-155.

Rezende, I. N. (2024). The proposed regulation to fight online child sexual abuse: An appraisal of privacy, data protection and criminal justice issues. *International Review of Law Computers & Technology*, 369–390.

Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). *Digital Investigation*, 124-142.

Seigfried-Spellar, K. C. (2017). Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations. *Journal of Police and Criminal Psychology*, 215–226.

Sorbán, K. (2024). Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations . *Belügyi Szemle*, 133-151.

Taylor, M., Holland, G., & Quayle, E. (2001). Typology of paedophile picture collections. *The Police Journal*, 97-107.

UNODC. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.* New York: UN.

Vitorino, P., Avila, S., Perez, M., & Rocha, A. (2018). Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, 303-313.

Westlake, B., Bouchard, M., & Frank, R. (2012). Comparing methods for detecting child exploitation content online. *European Intelligence and Security Informatics Conference*, (str. 153-163). Odense.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). In Their Own Words: Young Peoples' Vulnerabilities to Being Groomed and Sexually Abused Online. *Psychology, 5*(10). doi:http://dx.doi.org/10.1016/j.avb.2012.09.003

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Colling, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 62-70.

WHO. (2020). *Global status report on preventing violence against children.* Geneva: WHO.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72–79.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72-79.

Wolak, J., Liberatore, M., & Levine, B. N. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect*, 347–356.

UTJECAJ BIRD STRIKE DOGAĐAJA NA SIGURNOST ZRAČNOG PROMETA S OSVRTOM NA BOSNU I HERCEGOVINU

***DOI**: 10.70329/2744-2403.2025.5.10.9*

Izvorni naučni članak

Lejla Nikšić, dr.sc.[59]
Marija Prskalo, mag. ing. el.[60]

Sažetak
Bird strike događaji predstavljaju jedan od stalnih sigurnosnih izazova u civilnom zrakoplovstvu, jer sudari zrakoplova s pticama mogu ugroziti sigurnost leta, operativnu pouzdanost i troškovnu učinkovitost zračnog prometa. Fenomen je globalno prisutan, a učestalost incidenata najveća je u neposrednoj blizini aerodroma i pri niskim visinama, gdje na njegovo pojavljivanje utječu migracijski obrasci ptica, sezonske klimatske varijacije i lokalni ekološki čimbenici. Razumijevanje i praćenje bird strike događaja ključno je za planiranje sigurnosnih mjera i učinkovito upravljanje rizikom. Cilj istraživanja je sagledati globalne i lokalne trendove, prikazati regulatorni okvir i sustave upravljanja sigurnošću, te istaknuti značaj preventivnih mjera u svakodnevnoj praksi. Poseban fokus stavljen je na pregled i analizu podataka o zabilježenim incidentima u Bosni i Hercegovini. To omogućuje uvid u učestalost, tipologiju i razine rizika incidenata te u provedbu preventivnih mjera i koordinaciju nadležnih tijela. Takav integrirani pristup omogućuje sustavno razumijevanje problema, podržava primjenu najboljih međunarodnih praksi i doprinosi jačanju sigurnosne kulture u zračnom prometu, pri čemu lokalni kontekst zahtijeva specifične mjere prilagođene okolišu i operativnim uvjetima.

Ključne riječi: *bird strike, sigurnost zračnog prometa, upravljanje rizicima, Bosna i Hercegovina.*

[59] E-mail: lejla.niksic@fsk.unsa.ba
[60] E-mail: marija.prskalo@bhansa.gov.ba

1. Uvod

Sigurnost zračnog prometa predstavlja temeljni prioritet civilnog zrakoplovstva i ključni je čimbenik održivosti i učinkovitosti globalnog zrakoplovnog sustava. Povećanje opsega zračnog prometa i rast složenosti operacija nameću potrebu za sustavnim, aktivnim pristupom upravljanju sigurnosnim rizicima.
Sustav upravljanja sigurnošću u zračnoj plovidbi (Safety Management System - SMS) čini osnovni okvir za nadzor i unapređenje sigurnosti. Temelji se na jasno definiranim pravilima i procedurama, a provodi se kroz suradnju regulatornih tijela, zračnih prijevoznika, aerodroma, proizvođača zrakoplova i drugih dionika. Zajedničkim aktivnostima, kontinuiranom edukacijom osoblja i praćenjem sigurnosnih pokazatelja postiže se stalno unapređenje sigurnosne kulture u zrakoplovstvu (Prskalo, 2024).

Unutar ovog sustava, sudari zrakoplova s pticama predstavljaju specifičan i kompleksan sigurnosni izazov s izraženim operativnim, tehničkim i ekonomskim posljedicama. Takvi incidenti mogu oštetiti ključne zrakoplovne sustave, ugroziti sigurnost leta i izazvati značajne troškove održavanja te kašnjenja letova. Njihova učestalost i ozbiljnost ovise o kombinaciji prirodnih, tehničkih i operativnih čimbenika, uključujući migracijske obrasce ptica, lokalne uvjete okoliša te stupanj implementacije preventivnih mjera.

Ovaj rad analizira bird strike događaje u kontekstu SMS-a u civilnom zrakoplovstvu, s posebnim naglaskom na Bosnu i Hercegovinu. Metodološki okvir uključuje detaljnu analizu dostupnih statističkih podataka i izvješća o incidentima, pregled relevantne nacionalne i međunarodne regulative, te analizu najboljih praksi i standarda u upravljanju rizicima od sudara zrakoplova s pticama. U okviru istraživanja provedena je deskriptivna statistička analiza prijavljenih bird strike događaja u razdoblju 2017-2024. godine, kojom su obuhvaćene sezonske i prostorne varijacije, distribucija događaja prema fazi leta i vrsti ptica, te trendna analiza učestalosti incidenata po aerodromima. Rezultati su dopunjeni stručnim kritičkim osvrtom s ciljem prepoznavanja mogućih uzroka uočenih obrazaca i procjene učinkovitosti postojećih mjera prevencije.
Takav integrirani pristup omogućuje sustavno razumijevanje uzročno-posljedičnih veza i pruža znanstvenu osnovu za procjenu učinkovitosti postojećih sigurnosnih mehanizama u zrakoplovnom sustavu.
Cilj rada je pružiti cjelovit pregled aktualnog stanja, identificirati ključne čimbenike rizika te predložiti znanstveno utemeljene mjere za unapređenje SMS-a u zračnom prometu Bosne i Hercegovine.

2. Povijest i razvoj bird strike fenomena

Bird strike, odnosno sudar zrakoplova s pticama, predstavlja jedan od najozbiljnijih prirodnih rizika u civilnom zrakoplovstvu i globalni je fenomen. U međunarodnoj terminologiji često se koristi i pojam wildlife hazard, kojim se označava svaki rizik koje divlje životinje predstavljaju za sigurnost zračnog prometa. Takvi incidenti mogu se dogoditi u bilo kojoj fazi leta, ali su najčešći tijekom polijetanja i slijetanja, kada zrakoplov prolazi kroz područja s najvećom aktivnošću ptica u neposrednoj blizini aerodroma, uglavnom u dnevnim satima. Prvi zabilježeni bird strike dogodio se 1908. godine, kada je Orville Wright udario u pticu. Godine 1912., Calbraith Perry Rodgers postao je prva smrtna žrtva takvog incidenta nakon što je njegov Wright Flyer zapleo galeba i pao u more (ICAO, 2012).

Rani zrakoplovi, zbog krhke konstrukcije i slabih motora, bili su vrlo osjetljivi na oštećenja, iako je spora brzina omogućavala djelomično izbjegavanje sudara. Kako su konstrukcija i materijali napredovali, letjelice su postajale čvršće i otpornije, što je smanjilo učestalost teških posljedica sudara s pticama. Ipak, unatoč napretku u konstrukciji, incidenti nisu postali rijetki, što ukazuje na trajnu ranjivost zrakoplova na bird strike događaje. Posebno su ugroženi dijelovi zrakoplova koji su izloženi izravnim udarcima, poput kokpita, vjetrobrana, motora i okolnih strukturnih elemenata. U nekim slučajevima sudari su bili dovoljno ozbiljni da su dovodili do ozljeda članova posade ili narušavali kontrolu nad letjelicom. Ovi incidenti jasno pokazuju da, iako su suvremeni zrakoplovi znatno otporniji nego ranije verzije, bird strike i dalje predstavlja ozbiljan sigurnosni izazov za civilno zrakoplovstvo, zahtijevajući stalnu pozornost i primjenu preventivnih mjera.

Primjerice, Eastern Air Lines Flight 375 (1960) udario je u jato čvoraka pri polijetanju iz bostonske zračne luke Logan, što je dovelo do gubitka snage u tri od četiri motora i pogibije 62 od 72 osobe (Eastern Airlines, 1960). Također, nesreća United Airlines Flight 297 (1962) bila je posljedica sudara s jatom labudova na visini od 6.000 stopa, pri čemu je jedan labud prošao u horizontalni stabilizator, oslabio strukturnu cjelovitost i doveo do gubitka kontrole nad zrakoplovom s pogibijom svih putnika i posade (Civil Aeronautics Board, 1963). Primjeri ovih događaja ukazuju na ranjivost zrakoplova na sudare s velikim pticama, posebice u kritičnim fazama leta, i doveli su do podizanja kriterija otpornosti horizontalnih stabilizatora na udar ptica. Učestalost i posljedice sudara zrakoplova s pticama potaknule su razvoj sustavnog pristupa upravljanju ovim rizikom na globalnoj razini.

3. Pregled regulative i smjernica za upravljanje bird strike rizikom

Povijesni incidenti jasno su ukazali na ozbiljnost rizika koji bird strike predstavlja za sigurnost zrakoplova, što je potaknulo međunarodnu zajednicu na uspostavu sustavnih smjernica i standarda. Međunarodna organizacija civilnog zrakoplovstva (International Civil Aviation Organization - ICAO) ima ključnu ulogu u postavljanju globalnih standarda i preporuka vezanih uz sigurnost zračnog prometa, uključujući i upravljanje rizikom od udara ptica. Kao specijalizirana agencija Ujedinjenih naroda, ICAO djeluje kroz uspostavljanje međunarodnih standarda i preporučenih praksi koji se primjenjuju u državama članicama, a čine osnovu za nacionalne propise i operativne procedure.

Temeljni dokument koji se bavi ovom problematikom je Annex 14-Aerodromes, Volume I: Aerodrome Design and Operations, u kojem je definiran okvir za smanjenje rizika od sudara zrakoplova s divljim životinjama, prvenstveno pticama. ICAO (2018) naglašava da prisutnost ptica i drugih životinja na ili u blizini aerodroma predstavlja ozbiljnu prijetnju sigurnosti letova te propisuje obvezu država članica da uspostave sustavne procedure za praćenje i upravljanje ovim rizikom.

Prema Annexu 14, svaka država treba razviti nacionalni sustav evidentiranja i prijavljivanja udara divljih životinja te prikupljanja podataka o njihovoj prisutnosti na aerodromu i u okolnom području. Ključni element je kontinuirana procjena rizika koju provodi stručno osposobljeno osoblje, uz redovito izvješćivanjeprema međunarodnoj bazi podataka ICAO Bird Strike Information System (IBIS) (ICAO, 2018). Ovaj sustav omogućuje globalnu analizu i razmjenu informacija o incidentima, što olakšava prepoznavanje trendova i donošenje učinkovitih mjera prevencije.

Prema podacima IBIS (2023), u razdoblju 2016.-2021. zabilježeno je 273.343 udara divljih životinja u 194 države i teritorija, pri čemu ptice čine najveći udio ovih incidenata. Ovi podaci naglašavaju važnost sustavnog praćenja prisutnosti divljih životinja na i oko aerodroma, procjene rizika te implementacije dobro organiziranih programa kontrole divljih životinja, s posebnim fokusom na ptice, kako bi se smanjili operativni rizici i povećala sigurnost zračnog prometa.
ICAO preporučuje provođenje preventivnih mjera za smanjenje rizika od sudara s divljim životinjama, uključujući kontrolu okoliša, uklanjanje izvora hrane i sprječavanje stvaranja staništa koja bi mogla privući ptice (ICAO, 2013). Dodatne tehničke smjernice sadržane su u Airport Services Manualu (Doc 9137, Part 3), koji detaljno opisuje metode identifikacije i odvraćanja ptica u području aerodroma.

U cjelini, Annex 14 postavlja sustavan i sveobuhvatan okvir za upravljanje rizikom od udara ptica, koji kombinira nadzor, izvješćivanje i preventivno djelovanje te čini osnovu za razvoj nacionalnih programa i procedura sigurnosti. Na europskoj razini, upravljanje rizikom od udara ptica i drugih divljih životinja temelji se na propisima Europske unije i standardima koje provodi Europska agencija za sigurnost zračnog prometa (European Union Aviation Safety Agency - EASA). Europska regulativa u potpunosti preuzima načela ICAO-a, ali ih nadopunjuje detaljnijim operativnim zahtjevima i obveznim procedurama.

Države članice Europske unije obvezne su uspostaviti nacionalne sustave za evidentiranje i izvješćivanje o incidentima, kontinuirano prikupljati informacije o prisutnosti životinja koje mogu ugroziti sigurnost operacija te provoditi redovitu procjenu rizika koju izrađuje stručno ovlašteno osoblje (EK, 2014).
Poseban naglasak stavljen je na razvoj i održavanje snažne sigurnosne kulture, budući da je dokazano kako organizacije koje potiču visoku razinu sigurnosne svijesti imaju nižu stopu incidenata i učinkovitiji sustav unutarnjeg nadzora (Prskalo i Šahić, 2024).

Temeljni pravni akt u ovom području je Uredba Komisije (EU) br. 139/2014 o zahtjevima za aerodrome, poznata i kao dio tzv. Easy Access Rules for Aerodromes. Uz nju, EASA objavljuje prateće dokumente AMC i GM (Acceptable Means of Compliance i Guidance Material), koji nude praktične smjernice za dokazivanje usklađenosti sa zahtjevima propisanim Uredbom.
Kronološki gledano, europski regulatorni okvir razvijao se paralelno s ICAO smjernicama, uz periodična ažuriranja AMC i GM materijala, čime je uspostavljen koherentan sustav koji osigurava visoku razinu sigurnosti, ali i fleksibilnost u primjeni prema lokalnim uvjetima i vrstama ptica koje predstavljaju prijetnju zračnom prometu.

U Sjedinjenim Američkim Državama, nadležnost za upravljanje rizikom od udara ptica pripada Federalnoj upravi za zrakoplovstvo (Federal Aviation Administration - FAA). FAA je među prvim tijelima koja je razvila sustavan pristup ovoj problematici, a njezine smjernice danas se koriste kao međunarodni referentni standard.

Temeljni dokument u ovom području je Advisory Circular (AC) 150/5200-33C-Hazardous Wildlife Attractants on or Near Airports, koji definira postupke za identifikaciju i upravljanje izvorima koji mogu privući divlje životinje u blizinu aerodroma. Sudari s pticama i drugim životinjama predstavljaju značajan sigurnosni i ekonomski rizik, a učinkovitost mjera ovisi o lokalnim uvjetima, prostornom planiranju i koordiniranom djelovanju nadležnih tijela (FAA, 2020).
Dodatno, AC 150/5200-32C-Reporting Wildlife Aircraft Strikes propisuje obvezu prijavljivanja svih sudara s divljim životinjama, neovisno o razini štete, u

National Wildlife Strike Database - jednu od najopsežnijih baza podataka te vrste. Prema FAA (2020), oko 97 % svih zabilježenih udara uključuje ptice, a najčešće pogođene vrste su divlje patke, guske, galebovi i grabljivice. Iako samo manji udio incidenata uzrokuje ozbiljnu štetu, ekonomske posljedice su značajne.

Ptice i druge divlje životinje važan su ekološki i gospodarski resurs, ali mogu predstavljati ozbiljan rizik za sigurnost zračnog prometa. Od 1990. do 2024., u SAD-u je prijavljeno ukupno 319.047 udara divljih životinja, pri čemu su ptice činile najveći udio incidenata. Većina udara ptica događa se tijekom dana i u fazi prilaza aerodromu, a visina udara značajno utječe na opasnost - udari iznad 150 metara češće uzrokuju štetu. Ukupno je 88 udara rezultiralo uništenjem zrakoplova, a procijenjeni godišnji trošak za civilno zrakoplovstvo SAD-a u 2024. iznosio je 473 milijuna USD i 74.268 sati zastoja zrakoplova. (FAA, 2024).
Međunarodni regulatorni okvir (ICAO, EASA, FAA) zasniva se na konceptu upravljanja sigurnosnim rizicima SMS-a, koji zahtijeva proaktivno prepoznavanje i kontrolu prijetnji.

Slično tome, analiza ATC-povezanih avionskih nesreća pokazuje da ljudski, proceduralni i komunikacijski faktori mogu imati značajan utjecaj na sigurnost zrakoplovstva, što dodatno potvrđuje važnost proaktivnog pristupa u upravljanju rizicima, kao što je slučaj i kod problema bird strike događaja (Nikšić & Öztürk, 2023).

4. Upravljanje bird strike događajima u Bosni i Hercegovini

U Bosni i Hercegovini, aerodromi i nadležna tijela djeluju u skladu s međunarodnim standardima ICAO-a i EASA-e, kroz implementaciju okvira SMS-a i procedura za praćenje, izvješćivanje i prevenciju događaja. Svi događaji koji mogu ugroziti sigurnost zrakoplova, putnika ili posade klasificirani su prema smjernicama Direkcije za civilno zrakoplovstvo Bosne i Hercegovine (BHDCA), koja donosi regulativu u oblasti zračnog prometa Bosne i Hercegovine.

U skladu s BHDCA (2021), svi događaji koji imaju utjecaj na sigurnost leta kategoriziraju se prema vrsti aktivnosti i području na kojem su se dogodili. Bird strike, odnosno sudar zrakoplova s pticama, može se svrstati u više kategorija ovisno o okolnostima događaja i njegovim posljedicama.

Većina bird strike incidenata klasificirana je kao događaji vezani za aerodrome i zemaljske usluge, budući da se većina sudara događa u neposrednoj blizini aerodroma, gdje ptice pronalaze hranu, vodu i sklonište.

U slučajevima kada sudar uzrokuje fizičko oštećenje zrakoplova (npr. motora, radarske kupole, trupa ili elipse), događaj se može klasificirati i kao događaj povezan s tehničkim uvjetima, održavanjem i popravkom zrakoplova, budući da oštećenje može utjecati na strukturalnu čvrstoću ili performanse letjelice. Ako se incident dogodi tijekom polijetanja ili slijetanja, može biti obuhvaćen i kategorijom događaja vezanih za provođenje operacija zrakoplovom, osobito ako je imao utjecaj na sigurnost leta.

Manji, ponavljajući sudari koji ne uzrokuju značajnije posljedice, ali ukazuju na potencijalni rizik, mogu se evidentirati unutar skupine ostalih događaja, jer se smatraju faktorom koji dugoročno može utjecati na sigurnost operacija.
Ovakva kategorizacija omogućuje učinkovitije praćenje, izvješćivanje i planiranje preventivnih mjera na razini aerodroma i zrakoplovnih operacija, u skladu s međunarodnim standardima i praksom koju primjenjuje ICAO.

Tablica 1. Podjela ozbiljnosti zrakoplovnih incidenata (Izvor: ESSAR 2)

OZBILJNOST	**A**	**Ozbiljan incident**	**A1**	**A2**	**A3**	**A4**	**A5**
	B	**Glavni incident**	**B1**	**B2**	**B3**	**B4**	**B5**
	C	**Bitni incident**	**C1**	**C2**	**C3**	**C4**	**C5**
	D	**Nedefinirani**	**D1**	**D2**	**D3**	**D4**	**D5**
	E	**Bez utjecaja na sigurnost**	**E1**	**E2**	**E3**	**E4**	**E5**
			1	**2**	**3**	**4**	**5**
			Vrlo učestalo	**Učestalo**	**Povremeno**	**Rijetko**	**Vrlo rijetko**
			UČESTALOST				

Tablica 2. Definiranje učestalosti nesreća/incidenata zrakoplova (Izvor: ESSAR 2)

UČESTALOST	**DEFINICIJA**
Vrlo rijetko	Nikada tijekom životnog vijeka sustava.
Rijetko	Samo nekoliko zabilježenih sličnih slučajeva u odnosu na veliki obim prometa ili bez zabilježenih slučajeva u odnosu na mali obim prometa.
Povremeno	Nekoliko zabilježenih sličnih ugrožavanja sigurnosti, nesreća i ozbiljnih nezgoda - više od jednog puta na istom mjestu.
Učestalo	Već ranije zabilježen značajan broj sličnih ugrožavanja sigurnosti, nesreća i ozbiljnih nezgoda - značajan broj ponavljanja na istom mjestu.
Vrlo učestalo	Vrlo veliki broj već ranije zabilježenih sličnih ugrožavanja sigurnosti, nesreća i ozbiljnih nezgoda - vrlo veliki broj ponavljanja na istom mjestu.

4.1. Studije slučaja

Bird strike predstavlja jedan od najčešćih sigurnosnih incidenata u civilnom zrakoplovstvu. Iako većina takvih događaja ne uzrokuje izravnu štetu ni ugrožava sigurnost leta, njihova evidencija i analiza ključni su za upravljanje rizikom unutar SMS-a. BHDCA sustavno bilježi ovakve događaje i procjenjuje ih prema ICAO matrici rizika, omogućujući preciznu klasifikaciju i razvoj preventivnih mjera. Prikazuju se tri zabilježena slučaja, s fokusom na različite kategorije rizika te pripadajuće preporuke za preventivne mjere i upravljanje rizikom.

Studija slučaja 1
Prema BHDCA (2021), dana 6.9.2021. godine tijekom zaustavljanja zrakoplova došlo je do sudara s pticom (jastreb). Nije zabilježeno oštećenje zrakoplova niti je sigurnost leta bila ugrožena. Stručno osoblje aerodroma obavijestilo je BHDCA, pregledalo uzletno-sletnu stazu i pronašlo pticu u jednom komadu. Prema ICAO matrici rizika, događaj je klasificiran kao 3E - niska vjerojatnost i zanemarive posljedice.
Preporuke:

- Nastaviti s redovitim nadzorom područja aerodroma.
- Održavati područje bez izvora hrane i vode koji mogu privući ptice.
- U razdobljima migracija pojačati dnevne inspekcije.
- Naglasak na praćenje i edukaciju osoblja.

Studija slučaja 2
Prema BHDCA (2024), dana 2.6.2024. godine zrakoplov je tijekom slijetanja, pri brzini od približno 150 čvorova, udario u pticu. Nije došlo do oštećenja zrakoplova, ali događaj je zabilježen i analiziran. Kategorija 4D označava rijetko ponavljanje događaja s manjim utjecajem. Takvi incidenti zahtijevaju praćenje trendova i aktivne mjere jer se događaju relativno često.
Preporuke:

- Sustavno provođenje programa kontrole ptica prema internim procedurama SMS-a.
- U vegetacijskom razdoblju provoditi aktivne metode rastjerivanja (plinski topovi, vozila sa sirenama, dresirani jastrebovi).
- Uključiti statističko praćenje i analizu sezonskih uzoraka (učestalost po mjesecima).
- Uspostaviti bazu podataka o bird strike događajima radi procjene trendova i učinkovitosti mjera.

Studija slučaja 3
Prema BHDCA (2025), dana 25.7.2025. godine kapetan zrakoplova prijavio je mogući sudar s pticom tijekom prilaza za slijetanje. Pregledom piste pronađena je uginula ptica, no zrakoplov nije pretrpio nikakvu štetu te je nastavio let. Prema

ICAO matrici rizika, događaj je ocijenjen kao 4E - povremena pojava s potpuno zanemarivim posljedicama, bez utjecaja na sigurnost.
Preporuke:

- Pojačati mjere rastjerivanja tijekom kritičnih faza leta (prilaz i slijetanje).
- Uvesti laserske uređaje kao suvremeno i ekološki prihvatljivo sredstvo rastjerivanja ptica.
- Redovito pregledavati vegetaciju i površine koje mogu privlačiti ptice.
- Uvesti obavezno dnevno izvješćivanje o prisutnosti faune na području aerodroma.

Stručni kritički osvrt
Sustav prijavljivanja i analize bird strike događaja u Bosni i Hercegovini funkcionira u skladu s ICAO standardima i nacionalnim propisima.
Kategorije 3E, 4D i 4E ukazuju na niske razine rizika, no njihova pojava zahtijeva stalno aktivno djelovanje. Analiza prikazanih slučajeva sudara zrakoplova s pticama u Bosni i Hercegovini pokazuje da, iako se radi o događajima niskog rizika, sustavno praćenje i procjena tih incidenata predstavljaju ključni element u funkcionalnom SMS-a. Različite kategorije rizika odražavaju varijabilnost vjerojatnosti pojave i potencijalnih posljedica, što naglašava potrebu za individualiziranim pristupom u planiranju preventivnih mjera. Primijećena učestalost incidenata u fazama prilaza i slijetanja ukazuje na kritične točke u operacijama aerodroma koje zahtijevaju pojačan nadzor i pravovremene preventivne intervencije. Strateški pristup, koji uključuje kombinaciju tehničkih, bioloških i edukativnih mjera, zajedno s uspostavom baze podataka i sustavnim analizama trendova, omogućuje ne samo smanjenje učestalosti incidenata, već i povećanje operativne otpornosti aerodroma.
Zaključno, ovi primjeri potvrđuju da aktivno upravljanje rizikom, predstavlja učinkovit okvir za očuvanje sigurnosti letenja i kontinuirani razvoj sigurnosne kulture u Bosni i Hercegovini.

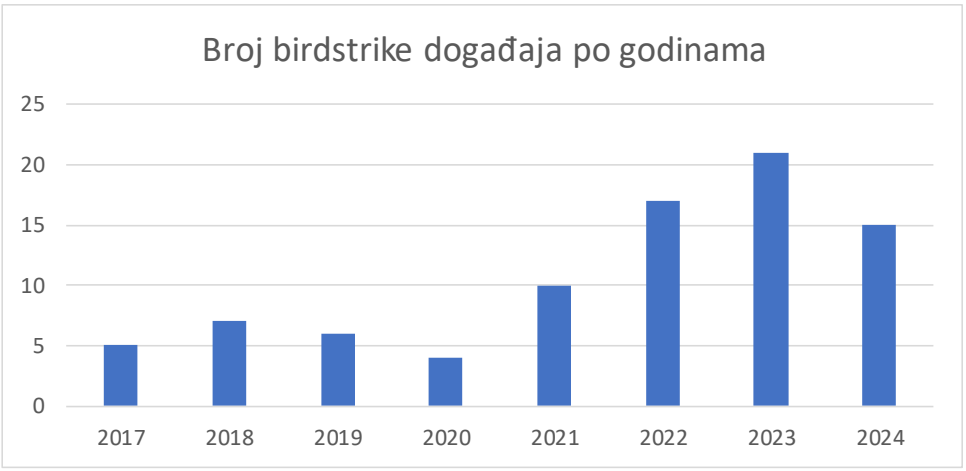
5. Statistička analiza podataka

Analiza bird strike događaja u Bosni i Hercegovini provedena je na temelju dostupnih izvješća Agencije za pružanje usluga u zračnoj plovidbi Bosne i Hercegovine (BHANSA) u razdoblju od 2017. do 2024. godine.
Cilj statističke obrade je kvantitativno prikazati učestalost i karakteristike bird strike događaja u zračnom prostoru Bosne i Hercegovine, identificirati prostorne i sezonske obrasce te utvrditi faze leta i vrste ptica najčešće uključene u ove incidente koji utječu na sigurnost zračnog prometa.

5.1. Deskriptivna analiza

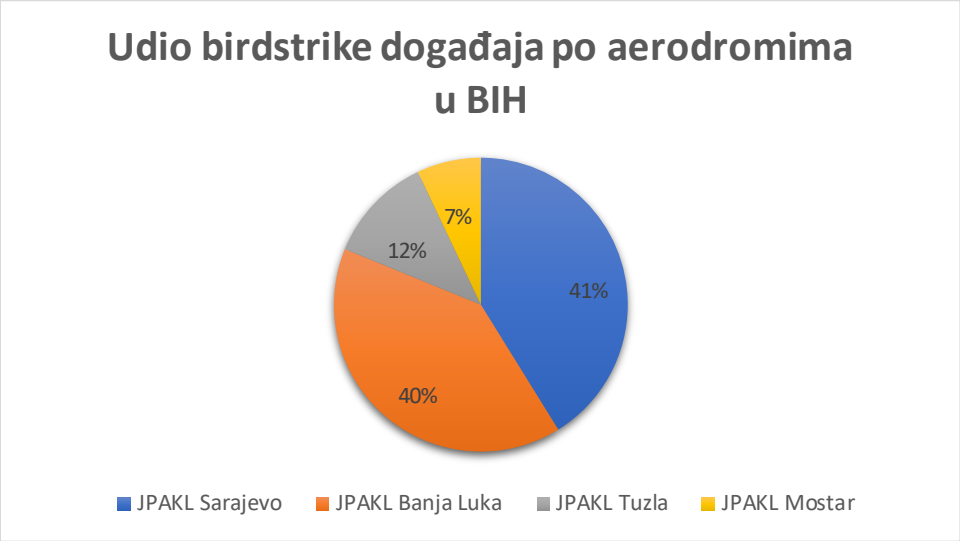
U analiziranom razdoblju zabilježeno je ukupno 84 bird strike događaja na četiri međunarodna aerodroma u Bosni i Hercegovini (Sarajevo, Banja Luka, Tuzla i Mostar). Najveći broj događaja zabilježen je na aerodromima Sarajevo i Banja Luka, što je u skladu s obimom prometa i lokalnim ekološkim uslovima koji pogoduju prisustvu ptica. Najmanji broj događaja prijavljen je 2020. godine (4 događaja), što se može dovesti u vezu sa smanjenim intenzitetom zračnog prometa tokom pandemije COVID-19, dok je najveći broj registrovan 2023. godine (21 događaj).

Promatrajući trend, primjetan je postepeni rast broja prijavljenih incidenata nakon 2021. godine, što se može tumačiti povećanjem obima operacija, ali i unapređenjem sistema prijavljivanja i praćenja događaja unutar SMS-a.



Grafikon 1. Broj bird strike događaja po godinama (2017–2024) (Izvor: BHANSA)

Analiza prema aerodromima pokazuje da se najveći broj incidenata dogodio na aerodromima Sarajevo (35) i Banja Luka (34), dok su aerodromi Tuzla (10) i Mostar (6) imali znatno manji broj zabilježenih slučajeva (Grafikon 2). Ovakva raspodjela u skladu je s obimom prometa - aerodromi s većim brojem operacija imaju i veću vjerojatnost pojave sudara s pticama.



Grafikon 2. Udio bird strike događaja po aerodromima (2017–2024) (Izvor: BHANSA)

Distribucija prema fazi leta

Analiza pokazuje da se bird strike događaji najčešće dešavaju u kritičnim fazama leta, pri polijetanju (27,4%) i slijetanju (27,4%), dok je 10,7% zabilježeno u fazama zaustavljanja i taksiranja. Kod 34,5% slučajeva faza leta nije jasno naznačena u izvještajima, što ukazuje na potrebu za dosljednijim opisom okolnosti pri prijavljivanju događaja.

Ovakva distribucija u potpunosti je u skladu s međunarodnim podacima (ICAO, 2018; FAA, 2024), prema kojima se većina bird strike incidenata događa u niskim visinama, tokom poletno-sletnih operacija, kada je vjerovatnoća susreta s pticama najveća. Sličan obrazac prisutan je i kod drugih kategorija sigurnosnih događaja i avionskih nesreća, gdje se najveći broj incidenata također javlja upravo u kritičnim fazama leta - polijetanju i slijetanju (Nikšić & Öztürk, 2022).

Distribucija prema vrsti ptica

U najvećem broju slučajeva (67,9%) vrsta ptice nije navedena u izvještajima. Od poznatih slučajeva, u 22,6% se navodi „nepoznata ptica“, dok su u manjem broju zabilježene konkretne vrste: vrabac (3%), jastreb (3%), orao (3%), te po 2% za svraku i sovu. Ovakva struktura pokazuje da, iako većina incidenata ne uključuje teže posljedice, postoji potreba za sistematičnijom identifikacijom ptica i saradnjom s ornitolozima, što bi doprinijelo boljoj procjeni rizika i planiranju preventivnih mjera.

Recentna istraživanja pokazuju da integracija DNA barcodinga i terenskih istraživanja omogućava precizniju identifikaciju vrsta ptica koje najčešće uzrokuju sudare s avionima, čime se mogu unaprijediti mjere prevencije i smanjenje rizika od incidenata (Chen et al., 2025).

Dodatno, procjena relativnog rizika i sezonskih razlika između vrsta ptica može pomoći u prioritetnom fokusiranju mjera upravljanja staništima i operacijama na aerodromima, posebno tokom migracijskih perioda kada je rizik od sudara najveći (Ross et al., 2025).

Sezonski i prostorni obrasci

Analiza datuma pokazuje izraženu sezonsku varijaciju; većina događaja javlja se tokom proljeća i ljeta (maj–avgust), u periodima povećane aktivnosti ptica i migracija grabljivica. Ovakav sezonski obrazac u skladu je s očekivanjima, budući da se u toplijim mjesecima bilježi povećano kretanje ptica, ali i intenzivniji zračni promet (Kelly, 2024; Tal et al., 2024).

Prostorna raspodjela pokazuje da su Sarajevo i Banja Luka glavni centri pojave ovih incidenata, što je povezano s većim obimom prometa, ali i s okolišnim faktorima koji pogoduju prisustvu ptica u zoni aerodroma. Iako Sarajevo ostvaruje znatno veći broj letnih operacija, broj bird strike događaja u Banjoj Luci gotovo je jednak, što može ukazivati na nekoliko mogućih uzroka:

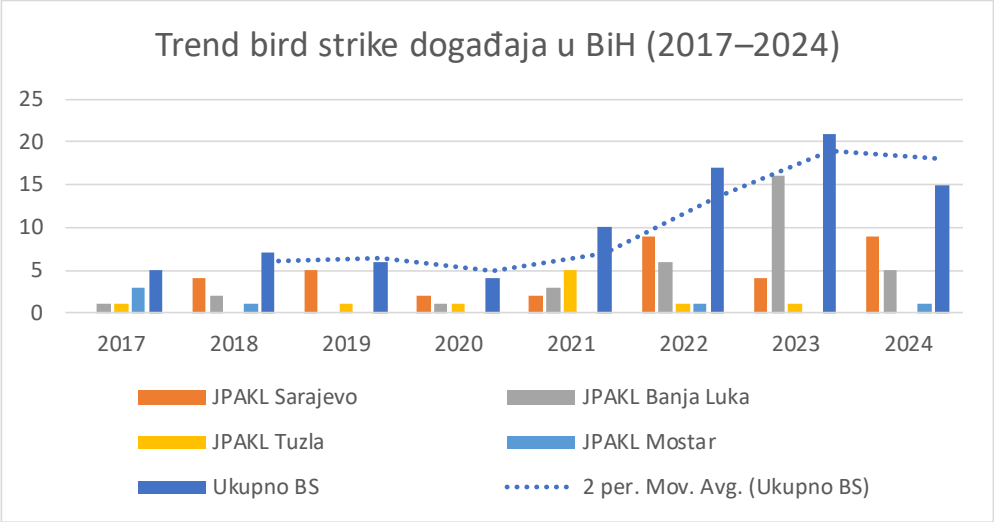
a) povoljnije prostorne i ekološke uslove za prisustvo ptica (npr. blizina šumskih i poljoprivrednih površina),
b) položaj aerodroma unutar mogućeg migracijskog koridora, ili
c) potrebu za mogućim unapređenjem postojećih mjera kontrole i rastjerivanja ptica koje se provode na aerodromu Banja Luka.

Ovakva opažanja upućuju na potrebu za detaljnijom analizom lokalnih biotičkih i prostorno-ekoloških faktora, kao i za periodičnim vrednovanjem učinkovitosti postojećih programa upravljanja faunom (wildlife management) na aerodromima u Bosni i Hercegovini.

5.2. Trendna analiza

Analiza vremenskog kretanja broja bird strike događaja u periodu 2017–2024. godine omogućava uvid u dinamiku pojave incidenata kroz duži vremenski horizont.

U prvom dijelu posmatranog razdoblja (2017–2020.) bilježi se relativno nizak i stabilan broj događaja, dok nakon 2021. godine dolazi do značajnog porasta prijava, što ukazuje na promjenu u učestalosti ovih incidenata. Ovakav rast može biti rezultat kombinovanog uticaja povećanja obima zračnih operacija nakon pandemijskog perioda, poboljšanja u sistemu evidentiranja događaja, ali i promjena u ekološkim uslovima koji utiču na prisustvo ptica u blizini aerodroma.



Grafikon 3. Trend bird stike događaja u BIH (2017-2024) (Izvor: BHANSA)

Rezultati prikazani na Grafikonu 3. pokazuju da se broj bird strike događaja u Bosni i Hercegovini kontinuirano povećavao nakon 2021. godine, s najvišim vrijednostima zabilježenim tokom 2022. i 2023. godine.
Primjena dvogodišnjeg pokretnog prosjeka jasno potvrđuje uzlazni trend, što ukazuje na potrebu kontinuiranog praćenja i evaluacije rizika.
Usporedba među aerodromima pokazuje da Sarajevo i Banja Luka prednjače po broju zabilježenih događaja, dok aerodromi Tuzla i Mostar bilježe manji broj incidenata. Zanimljivo je, međutim, da Banja Luka, unatoč znatno manjem obimu zračnih operacija, bilježi gotovo isti broj incidenata kao i Sarajevo. Ovakav odnos može upućivati na to da je područje aerodroma Banja Luka prostorno pogodnije za prisustvo ptica, da se nalazi na migracijskom koridoru, ili da mjere kontrole faune nisu jednako učinkovite kao na drugim aerodromima. S druge strane, aerodromi Tuzla i Mostar bilježe manji broj događaja, što može biti povezano s manjim brojem letova, ali i lokalnim ekološkim uslovima koji manje pogoduju koncentraciji ptica.

Stručni kritički osvrt

Provedena analiza pokazuje da su bird strike događaji u zračnom prostoru Bosne i Hercegovine uglavnom niskog rizika, ali da njihova učestalost pokazuje uzlazni trend u posljednjih nekoliko godina. Ovaj trend ne mora nužno ukazivati na pogoršanje sigurnosnih uslova, već može odražavati bolju evidenciju i svijest o važnosti prijavljivanja incidenata u okviru SMS-a.
S druge strane, disproporcija između obima zračnih operacija i broja bird strike događaja, posebno u slučaju aerodroma Banja Luka, zahtijeva dodatnu pažnju. Ovakva pojava može ukazivati na specifične lokalne ekološke faktore, prisustvo ptica duž migracijskih koridora ili nedovoljnu učinkovitost postojećih mjera

kontrole faune. Preporučljivo je da se u narednom razdoblju provede detaljnija procjena rizika po aerodromima, s naglaskom na prostorne i sezonske varijacije, kako bi se utvrdili stvarni uzroci povećane učestalosti događaja. Nadalje, visok udio slučajeva u kojima vrsta ptice nije identificirana (gotovo 68%) ograničava mogućnost precizne procjene rizika i planiranja ciljano usmjerenih mjera. To naglašava potrebu za standardizacijom obrasca prijave bird strike događaja i jačanjem suradnje s ornitološkim stručnjacima radi poboljšanja identifikacije vrsta i razumijevanja njihovih migracijskih navika. Konačno, iako analizirani događaji u većini slučajeva nisu rezultirali ozbiljnim posljedicama po sigurnost letenja, činjenica da se najveći broj incidenata javlja u fazama polijetanja i slijetanja ukazuje na trajnu izloženost ključnih faza leta povećanom riziku. Zato je važno da aerodromi u BiH nastave s kontinuiranim praćenjem, evaluacijom učinkovitosti i unapređenjem mjera upravljanja faunom, u skladu s međunarodnim smjernicama (ICAO Annex 14, Doc 9137 – Airport Services Manual, Part 3). Dobijeni rezultati predstavljaju osnovu za formuliranje zaključaka i preporuka usmjerenih na unapređenje sigurnosti zračnog prometa i učinkovitije upravljanje rizikom od sudara zrakoplova s pticama.

6. Zaključak

Analiza bird strike događaja u zračnom prostoru Bosne i Hercegovine pokazala je da, iako se većina incidenata klasificira kao niskog rizika, njihova učestalost pokazuje uzlazni trend u posljednjih nekoliko godina. Ovaj porast može odražavati kombinovani uticaj povećanog broja letnih operacija, promjena u migracijskim obrascima ptica i poboljšanja u sistemu prijavljivanja incidenata.
Najveći broj događaja zabilježen je na aerodromima Sarajevo i Banja Luka. Iako Sarajevo ima znatno veći promet, Banja Luka bilježi gotovo jednaku učestalost bird strike incidenata, što može ukazivati na lokalne ekološke faktore, blizinu područja pogodnih za okupljanje ptica ili razlike u provođenju mjera kontrole faune. Rezultati analize po fazama leta pokazuju da su najrizičnije faze polijetanje i slijetanje, što je u skladu s globalnim trendovima. Veći broj slučajeva u toplijem dijelu godine potvrđuje sezonsku varijaciju povezana s aktivnošću i migracijom ptica. Međutim, značajan udio prijava s neidentifikovanom vrstom ptica ukazuje na potrebu poboljšanja evidencije i saradnje s ornitološkim stručnjacima.
Dalji napredak u upravljanju rizikom od bird strike događaja zahtijeva sistemski pristup: objedinjavanje podataka, standardizaciju prijavljivanja, procjenu rizika po aerodromima i kontinuiranu evaluaciju učinkovitosti mjera upravljanja faunom. Posebnu pažnju treba posvetiti razvoju integrisanih strategija koje kombinuju tehničke, biološke i edukativne mjere.Zaključno, bird strike događaji, iako u većini slučajeva ne predstavljaju visok sigurnosni rizik, ostaju relevantan faktor koji zahtijeva trajnu analitičku pažnju i koordinisano djelovanje svih aktera u sistemu zrakoplovne sigurnosti Bosne i Hercegovine.

Popis grafikona i tablica

Popis literature

1. Chen, W., Sun, C., Zhang, J., Li, J., Chang, Q., Li, P., & Hu, C.(2025) "Avian collision risks at airports: Integrating DNA barcoding, species traits, and phylogenetic analyses to inform mitigation strategies." Global Ecology and Conservation 62(2025): e03829.
2. Civil Aeronautics Board (1963) Investigation of Aircraft Accident: United Air Lines Flight 297, Vickers-Armstrongs Viscount, N 7430, near Ellicott City, Maryland, November 23, 1962. Report No. 1-0034.
3. Direkcija za civilno zrakoplovstvo Bosne i Hercegovine (2021) Izvještaj o događajima koji su uticali na bezbjednost letenja u Bosni i Hercegovini. Banja Luka: BHDCA.
4. Direkcija za civilno zrakoplovstvo. (2021-2025). Izvještaji o sudarima zrakoplova s pticama (bird strike) u Bosni i Hercegovini. Banja Luka: BHDCA. Dostupno na: http://www.bhdca.gov.ba/index.php/hr/doc/bezbjedonosne-informacije [9.10.2025.]
5. Eastern Airlines (1960) Investigation of Aircraft Accident: Eastern Airlines, Boston, Massachusetts: 1960-10-04. Civil Aeronautics Board. Report No. 1-0043.
6. Eurocontrol (2011) Reporting and Assessment of Safety Occurrences in ATM - ESSAR 2. Brussels: Eurocontrol.
7. Europska komisija (2014) Uredba Komisije (EU) br. 139/2014 od 12. veljače 2014. o utvrđivanju zahtjeva i upravnih postupaka u vezi s aerodromima u skladu s Uredbom (EZ) br. 216/2008 Europskog parlamenta i Vijeća. Službeni list Europske unije, L 44/1.
8. FAA (2024) Wildlife Strikes to Civil Aircraft in the United States 1990 - 2024. Serial Report Number 31, Washington, DC
9. ICAO (2013) Airport Services Manual, Part 3: Wildlife Control and Reduction. Montreal: ICAO.
10. ICAO (2018) Annex 14 to the Convention on International Civil Aviation, Aerodromes - Volume I: Aerodrome Design and Operations. 8th ed. Montreal: International Civil Aviation Organization.

11. ICAO (2018) Safety Report, Montreal: ICAO
12. International Civil Aviation Organization (2023) Electronic Bulletin EB 2023/30: 2016-2021 Wildlife Strike Analyses (IBIS). Montreal: ICAO.
13. International Civil Aviation Organization (ICAO) (2012) Airport Services Manual: Part 3-Wildlife Control and Reduction. 4th edn. Montreal: ICAO.
14. Kelly, T.A. (2024) „Seasonal Variation in Birdstrike Rate for Two North American Seasonal Variation in Birdstrike Rate for Two North American Raptors: Turkey Vulture (cathartes Aura) and Red-tailed Hawk Raptors: Turkey Vulture (cathartes Aura) and Red-tailed Hawk (buteo Jamaicensis)“, Journal of Raptor Research, 33(1), str: 59-62.
15. Nikšić, L. & Ozturk, E.A. (2022) „US./Europe Comparison Of ATC-Related Accidents And Incidents“, International Journal for Traffic and Transport Engineering, 12(2), pp 155 - 169 DOI: http://dx.doi.org/10.7708/ijtte2022.12(2).01
16. Nikšić, L. & Ozturk, E.A. (2023) „Analysis of ATC-related aviation accidents and incidents“, Aircraft Engineering and Aerospace Technology, 95(6), pp 890-898 https://doi.org/10.1108/AEAT-03-2022-0078
17. Pravilnik o izvještavanju o događajima. (2015/2017) „Službeni glasnik BiH“, br. 57/15 i 88/17. BHDCA.
18. Prskalo, M. & Šahić, A. (2024) „Utjecaj ljudskih čimbenika na sigurnost zračnog prometa“, Zaštita i sigurnost, 1, str. 174–203. DOI: 10.70329/2744-2403.2024.1.7.177.
19. Prskalo, M. (2024) „Suvremeni kibernetički rizici u upravljanju zračnim prometom“, Zaštita i sigurnost, 3(2), str. 132–143.
20. Ross, C. D., M. Schank, M. J. Begier, B. F. Blackwell, and T. L. DeVault. (2025) „Assessing relative hazard, risk, and seasonal differences of Wildlife-aircraft collisions“, Wildlife Society Bulletin, 49(3), DOI https://doi.org/10.1002/wsb.1609
21. Tal, T., Jansen, D., Jansen, E., Green, A.W., Hoekstra, E., Heetkamp, M., T'jollyn, F., Engelen, D., Hoekstra, B., Kaasiku, T. And Wansteelant, W.M.G. (2024) „Full-season spring migration counts reveal seasonal contrasts in raptor migration through the eastern Black Sea flyway“, bioRxiv, 2024-08
22. U.S. Department of Transportation, Federal Aviation Administration (2020) Advisory Circular: Hazardous Wildlife Attractants on or near Airports. AC No. 150/5200-33C, 21 February.
23. U.S. Department of Transportation, Federal Aviation Administration (2024) Advisory Circular: Reporting Wildlife Aircraft Strikes. AC No. 150/5200-32C, 31 July.
24. US FAA (2024) Wildlife Strikes to Civil Aircraft in the United States 1990–2024. Washington, DC: Federal Aviation Administration.

THE IMPACT OF BIRD STRIKE INCIDENTS ON AVIATION SAFETY WITH REFERENCE TO BOSNIA AND HERZEGOVINA

***DOI**: 10.70329/2744-2403.2025.5.10.9*

Original Scientific Article

Lejla Nikšić, PhD.[61]
Marija Prskalo, M. Eng.[62]

Abstract
Bird strike incidents represent a persistent safety challenge in civil aviation, as collisions between aircraft and birds can compromise flight safety, operational reliability, and cost efficiency of air transport. This phenomenon is globally widespread, with the highest frequency of incidents occurring in the vicinity of airports and at low altitudes, where its occurrence is influenced by bird migration patterns, seasonal climatic variations, and local ecological factors. Understanding and monitoring bird strike incidents are essential for planning safety measures and for effective risk management. The objective of this research is to examine global and local trends, present the regulatory framework and safety management systems, and emphasize the importance of preventive measures in daily operations. Special attention is given to the review and analysis of reported bird strike incidents in Bosnia and Herzegovina, providing insight into the frequency, typology, and risk levels of such incidents, as well as the implementation of preventive actions and coordination among competent authorities. This integrated approach enables a systematic understanding of the problem, supports the application of international best practices, and contributes to strengthening the safety culture in aviation, while recognizing that the local context requires specific measures adapted to environmental and operational conditions.

***Keywords:** bird strike, aviation safety, risk management, Bosnia and Herzegovina*

[61] E-mail: lejla.niksic@fsk.unsa.ba
[62] E-mail: marija.prskalo@bhansa.gov.ba

1. Introduction

Aviation safety represents a fundamental priority of civil aviation and is a key factor for the sustainability and efficiency of the global air transport system. The increasing scope of air traffic and the growing complexity of operations necessitate a systematic and proactive approach to managing safety risks.
The Safety Management System (SMS) forms the essential framework for monitoring and improving safety in air navigation. It is based on clearly defined rules and procedures and implemented through cooperation among regulatory authorities, air carriers, airports, aircraft manufacturers, and other stakeholders. Through joint activities, continuous staff training, and the monitoring of safety indicators, a continuous improvement of the safety culture in aviation is achieved (Prskalo, 2024).

Within this system, bird strikes represent a specific and complex safety challenge with significant operational, technical, and economic consequences. Such incidents can damage critical aircraft systems, endanger flight safety, and lead to substantial maintenance costs and flight delays. Their frequency and severity depend on a combination of natural, technical, and operational factors, including bird migration patterns, local environmental conditions, and the degree of implementation of preventive measures.

This paper analyses bird strike incidents within the context of the SMS, with a special focus on Bosnia and Herzegovina. The methodological framework includes a detailed analysis of available statistical data and incident reports, a review of relevant national and international regulations, and an evaluation of best practices and standards in managing bird strike risks.

The research includes a descriptive statistical analysis of reported bird strike events for the period 2017–2024, covering seasonal and spatial variations, distribution of events by flight phase and bird species, and trend analysis of incident frequency across airports. The results are supplemented with a professional critical review aimed at identifying potential causes of observed patterns and assessing the effectiveness of existing preventive measures.
This integrated approach enables a systematic understanding of cause-and-effect relationships and provides a scientific basis for evaluating the effectiveness of existing safety mechanisms within the aviation system. The objective of this paper is to provide a comprehensive overview of the current situation, identify key risk factors, and propose scientifically grounded measures to improve the SMS in the aviation sector of Bosnia and Herzegovina.

2. History and Development of the Bird Strike Phenomenon

Bird strike, or aircraft collision with birds, represents one of the most serious natural hazards in civil aviation and is a global phenomenon. In international terminology, the term wildlife hazard is often used to denote any risk posed by wild animals to the safety of air operations. Such incidents can occur during any phase of flight, but they are most common during take-off and landing, when aircraft pass through areas of highest bird activity in the immediate vicinity of airports, mostly during daylight hours. The first recorded bird strike occurred in 1908, when Orville Wright struck a bird. In 1912, Calbraith Perry Rodgers became the first fatal victim of such an incident after his Wright Flyer became entangled with a seagull and crashed into the sea (ICAO, 2012).

Early aircraft, due to their fragile structures and weak engines, were highly susceptible to damage, although their low speeds allowed partial avoidance of collisions. As aircraft structures and materials advanced, airplanes became stronger and more resistant, which reduced the frequency of severe consequences resulting from bird collisions. Nevertheless, despite technological progress, these incidents have not become rare, indicating the persistent vulnerability of aircraft to bird strike events. Parts of the aircraft that are particularly exposed to direct impact, such as the cockpit, windshield, engines, and adjacent structural components, remain especially at risk. In some cases, collisions have been severe enough to cause crew injuries or impair aircraft control. These incidents clearly demonstrate that, although modern aircraft are significantly more resilient than earlier models, bird strikes still pose a serious safety challenge to civil aviation, requiring continuous attention and the implementation of preventive measures.

For instance, Eastern Air Lines Flight 375 (1960) struck a flock of starlings during take-off from Boston Logan Airport, resulting in the loss of power in three out of four engines and the deaths of 62 of the 72 occupants (Eastern Airlines, 1960). Likewise, the United Airlines Flight 297 (1962) accident resulted from a collision with a flock of swans at an altitude of 6,000 feet, where one swan penetrated the horizontal stabilizer, weakened its structural integrity, and caused loss of aircraft control, leading to the deaths of all passengers and crew (Civil Aeronautics Board, 1963).These examples illustrate the vulnerability of aircraft to collisions with large birds, particularly during critical phases of flight, and led to the establishment of higher design standards for the bird strike resistance of horizontal stabilizers. The frequency and consequences of aircraft-bird collisions have prompted the development of a systematic, global approach to managing this hazard.

3. Overview of Regulations and Guidelines for Managing Bird Strike Risk

Historical incidents have clearly demonstrated the severity of the risk that bird strikes pose to aircraft safety, prompting the international community to establish systematic guidelines and standards.

The International Civil Aviation Organization (ICAO) plays a key role in setting global standards and recommendations related to aviation safety, including the management of bird strike hazards. As a specialized agency of the United Nations, ICAO operates through the development of international standards and recommended practices applied by member states, which form the basis for national regulations and operational procedures.

The fundamental document addressing this issue is Annex 14 - Aerodromes, Volume I: Aerodrome Design and Operations, which defines the framework for reducing the risk of aircraft collisions with wildlife, primarily birds. ICAO (2018) emphasizes that the presence of birds and other animals on or in the vicinity of aerodromes represents a serious threat to flight safety, and requires member states to establish systematic procedures for monitoring and managing this risk.

According to Annex 14, each state should develop a national system for recording and reporting wildlife strikes and for collecting data on their presence at and around aerodromes. A key element is the continuous risk assessment carried out by professionally trained personnel, with regular reporting to the international database ICAO Bird Strike Information System (IBIS) (ICAO, 2018). This system enables global analysis and information exchange on incidents, facilitating the identification of trends and the adoption of effective preventive measures.

According to IBIS data (2023), during the period 2016–2021 a total of 273,343 wildlife strikes were recorded across 194 states and territories, with birds representing the majority of these incidents. These data highlight the importance of systematic monitoring of wildlife presence on and around aerodromes, risk assessment, and the implementation of well-organized wildlife control programs, with a particular focus on birds in order, to reduce operational risks and enhance aviation safety.

ICAO recommends the implementation of preventive measures aimed at mitigating the risk of wildlife collisions, including environmental control, removal of food sources, and elimination of habitats that may attract birds (ICAO, 2013). Additional technical guidance is provided in the Airport Services Manual (Doc 9137, Part 3), which describes in detail the methods for identifying and dispersing birds in the aerodrome environment.

Overall, Annex 14 establishes a systematic and comprehensive framework for managing the risk of bird strikes, combining monitoring, reporting, and preventive actions, and serving as the foundation for the development of national safety programs and procedures.

At the European level, the management of risks related to bird and other wildlife strikes is based on European Union regulations and the standards implemented by the European Union Aviation Safety Agency (EASA). European regulations fully adopt the principles of ICAO but complement them with more detailed operational requirements and mandatory procedures.

EU member states are required to establish national systems for recording and reporting wildlife strike incidents, to continuously collect data on the presence of animals that may endanger operational safety, and to conduct regular risk assessments prepared by professionally qualified personnel (EC, 2014).

Particular emphasis is placed on the development and maintenance of a strong safety culture, as research has shown that organizations promoting a high level of safety awareness have lower incident rates and more effective internal oversight systems (Prskalo and Šahić, 2024).

The key legal act in this area is Commission Regulation (EU) No. 139/2014 on Aerodrome Requirements, also known as part of the Easy Access Rules for Aerodromes. In addition, EASA publishes accompanying documents Acceptable Means of Compliance (AMC) and Guidance Material (GM) which provide practical guidance for demonstrating compliance with the requirements established by the Regulation.

Chronologically, the European regulatory framework has evolved in parallel with ICAO guidance, with periodic updates of the AMC and GM materials, thereby establishing a coherent system that ensures a high level of safety while maintaining flexibility in application according to local conditions and the bird species that pose threats to aviation operations.

In the United States, responsibility for managing the risk of bird strikes lies with the Federal Aviation Administration (FAA). The FAA was among the first authorities to develop a systematic approach to this issue, and its guidance documents are now used as international reference standards.

The principal document in this field is Advisory Circular (AC) 150/5200-33C-Hazardous Wildlife Attractants on or Near Airports, which defines procedures for identifying and managing sources that may attract wildlife near aerodromes. Collisions with birds and other animals represent a significant safety and economic risk, and the effectiveness of mitigation measures depends on local conditions, spatial planning, and coordinated action among the competent authorities (FAA, 2020).

Additionally, Advisory Circular (AC) 150/5200-32C - Reporting Wildlife Aircraft Strikes establishes the requirement to report all wildlife collisions, regardless of the level of damage, to the National Wildlife Strike Database, one of the most comprehensive databases of its kind. According to FAA (2020), approximately 97% of all recorded strikes involve birds, with the most frequently affected species being wild ducks, geese, gulls, and raptors. Although only a small proportion of incidents result in significant damage, the economic consequences are substantial.

Birds and other wildlife represent an important ecological and economic resource, yet they can pose a serious safety risk to aviation operations. Between 1990 and 2024, a total of 319,047 wildlife strikes were reported in the United States, with birds accounting for the majority of these incidents. Most bird strikes occur during daylight hours and in the approach phase of flight, while altitude has a significant influence on the level of risk - strikes occurring above 150 meters are more likely to cause damage. In total, 88 strikes resulted in the destruction of aircraft, and the estimated annual cost to U.S. civil aviation in 2024 amounted to USD 473 million and 74,268 aircraft downtime hours (FAA, 2024).
The international regulatory framework (ICAO, EASA, FAA) is based on the concept of SMS risk management, which requires the proactive identification and control of hazards. Similarly, the analysis of air traffic control (ATC)-related aircraft accidents has shown that human, procedural, and communication factors can have a significant impact on aviation safety, further underscoring the importance of a proactive approach to risk management, as is the case with the bird strike phenomenon (Nikšić & Öztürk, 2023).

4. Management of Bird Strike Incidents in Bosnia and Herzegovina

In Bosnia and Herzegovina, aerodromes and the competent authorities operate in accordance with the international standards of ICAO and EASA, through the implementation of the SMS framework and procedures for monitoring, reporting, and preventing safety-related occurrences. All occurrences that may endanger the safety of aircraft, passengers, or crew are classified in accordance with the guidelines of the Civil Aviation Authority of Bosnia and Herzegovina (BHDCA), which issues regulations governing the field of civil aviation in the country.

According to BHDCA (2021), all occurrences affecting flight safety are categorized based on the type of activity and the area in which they occurred. A bird strike, or collision between an aircraft and birds, may fall into several categories depending on the circumstances of the event and its consequences.
Most bird strike incidents are classified as aerodrome and ground services–related events, since the majority of collisions occur in the immediate vicinity of aerodromes, where birds find sources of food, water, and shelter.

In cases where a collision causes physical damage to the aircraft (e.g., to the engine, radar dome, fuselage, or wing leading edge), the event may also be categorized as technical conditions, maintenance, and repair–related, as such damage can affect the structural integrity or performance of the aircraft. If the incident occurs during take-off or landing, it may additionally fall under aircraft operations–related events, particularly when it has an impact on flight safety.

Minor or recurring collisions that do not cause significant consequences but indicate a potential risk can be recorded within the "other events" category, as they are considered a factor that may influence operational safety in the long term. This categorization enables more effective monitoring, reporting, and planning of preventive measures at both the aerodrome and operational levels, in line with international standards and ICAO-recommended practices.

Table 1. Classification of Aviation Incident Severity (Source: ESSAR 2)

SEVERITY	**A**	**Serious Incident**	**A1**	**A2**	**A3**	**A4**	**A5**
	B	**Major Incident**	**B1**	**B2**	**B3**	**B4**	**B5**
	C	**Significant Incident**	**C1**	**C2**	**C3**	**C4**	**C5**
	D	**Undefined**	**D1**	**D2**	**D3**	**D4**	**D5**
	E	**No Safety Impact**	**E1**	**E2**	**E3**	**E4**	**E5**
			1	**2**	**3**	**4**	**5**
			Very Frequent	**Frequent**	**Occasional**	**Rare**	**Very Rare**
			FREQUENCY				

Table 2. Definition of Aircraft Accident/Incident Frequency (Source: ESSAR 2)

FREQUENCY	DEFINITION
Very Rare	Never observed during the system's operational lifetime.
Rare	Only a few similar cases recorded in relation to high traffic volume, or none recorded in relation to low traffic volume.
Occasional	Several similar safety threats, accidents, or serious incidents recorded - more than once at the same location.
Frequent	A significant number of similar safety threats, accidents, or serious incidents previously recorded - repeated occurrences at the same location.
Very Frequent	A very high number of similar safety threats, accidents, or serious incidents previously recorded - very frequent repetition at the same location.

4.1. Case Studies

Bird strikes represent one of the most common safety incidents in civil aviation. Although the majority of such events do not cause direct damage or compromise flight safety, their recording and analysis are essential for risk management within the SMS. The BHDCA systematically records these events and assesses them using the ICAO risk matrix, enabling accurate classification and the development of preventive measures.

Three recorded cases are presented, focusing on different risk categories and the corresponding recommendations for preventive actions and risk management.

Case Study 1

According to BHDCA (2021), on 6 September 2021, a bird strike occurred while the aircraft was taxiing (hawk). No damage to the aircraft was reported, and flight safety was not compromised. Airport personnel notified BHDCA, inspected the runway, and found the bird intact. According to the ICAO risk matrix, the incident was classified as 3E - low probability and negligible consequences.

Recommendations:

- Continue regular monitoring of the airport area.
- Maintain the area free of food and water sources that could attract birds.
- Increase daily inspections during migration periods.
- Emphasize monitoring and staff training.

Case Study 2

According to BHDCA (2024), on 2 June 2024, an aircraft struck a bird during landing at approximately 150 knots. No damage occurred, but the incident was recorded and analysed. Category 4D indicates a rarely recurring incident with minor impact. Such incidents require trend monitoring and proactive measures as they occur relatively frequently.

Recommendations:

- Systematic implementation of bird control programs according to internal SMS procedures.
- Use active dispersal methods during vegetative periods (pyrotechnics, vehicle-mounted sirens, trained hawks).
- Include statistical monitoring and analysis of seasonal patterns (frequency by month).
- Establish a bird strike database to assess trends and the effectiveness of measures.

Case Study 3

According to BHDCA (2025), on 25 July 2025, the aircraft captain reported a possible bird strike during approach for landing. Inspection of the runway revealed a dead bird, but the aircraft sustained no damage and continued the flight. According to the ICAO risk matrix, the incident was assessed as 4E - occasional occurrence with completely negligible consequences, no impact on flight safety.

Recommendations:

- Strengthen dispersal measures during critical flight phases (approach and landing).

- Introduce laser devices as a modern and environmentally friendly bird deterrent.
- Regularly inspect vegetation and surfaces that may attract birds.
- Implement mandatory daily reporting on wildlife presence at the airport.

Expert Critical Review

The bird strike reporting and analysis system in Bosnia and Herzegovina operates in accordance with ICAO standards and national regulations. Categories 3E, 4D, and 4E indicate low-risk levels, yet their occurrence requires continuous active management. Analysis of the presented bird strike incidents in Bosnia and Herzegovina demonstrates that, although they are low-risk events, systematic monitoring and assessment of these incidents are key elements within an effective SMS.

The different risk categories reflect variability in the probability of occurrence and potential consequences, highlighting the need for a tailored approach in planning preventive measures. Observed incident frequency during approach and landing phases indicates critical points in airport operations that require enhanced monitoring and timely preventive interventions.

A strategic approach combining technical, biological, and educational measures, together with the establishment of a database and systematic trend analyses, enables not only the reduction of incident frequency but also the enhancement of airport operational resilience.

In conclusion, these examples confirm that active risk management provides an effective framework for maintaining flight safety and continuously developing a safety culture in Bosnia and Herzegovina.

5. Statistical Data Analysis

The analysis of bird strike incidents in Bosnia and Herzegovina was conducted based on available reports from the Bosnia and Herzegovina Air Navigation Services Agency (BHANSA) for the period 2017–2024.

The aim of the statistical processing is to quantitatively present the frequency and characteristics of bird strike incidents in the airspace of Bosnia and Herzegovina, identify spatial and seasonal patterns, and determine the flight phases and bird species most frequently involved in these incidents that affect aviation safety.

5.1. Descriptive Analysis

During the analyzed period, a total of 84 bird strike events were recorded at four international airports in Bosnia and Herzegovina (Sarajevo, Banja Luka, Tuzla, and Mostar). The highest number of incidents occurred at Sarajevo and Banja Luka airports, which corresponds to their traffic volume and local ecological conditions that favor the presence of birds. The lowest number of events was

reported in 2020 (four incidents), likely due to the reduced air traffic intensity during the COVID-19 pandemic, while the highest number was recorded in 2023 (21 incidents). Observing the overall trend, a gradual increase in reported incidents has been evident since 2021, which may be attributed both to the growth in flight operations and to improvements in the reporting and monitoring system within the SMS.

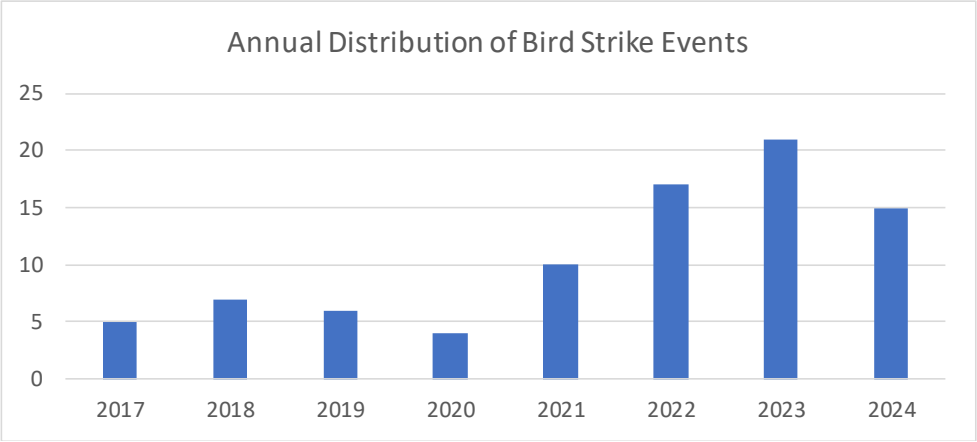


Figure 1. Annual Distribution of Bird Strike Events (2017–2024) (Source: BHANSA)

The analysis by airport shows that the highest number of incidents occurred at Sarajevo (35) and Banja Luka (34) airports, while Tuzla (10) and Mostar (6) recorded significantly fewer cases (Figure 2).
This distribution corresponds to the volume of air traffic - airports with a higher number of operations generally have a greater likelihood of bird strike occurrences.

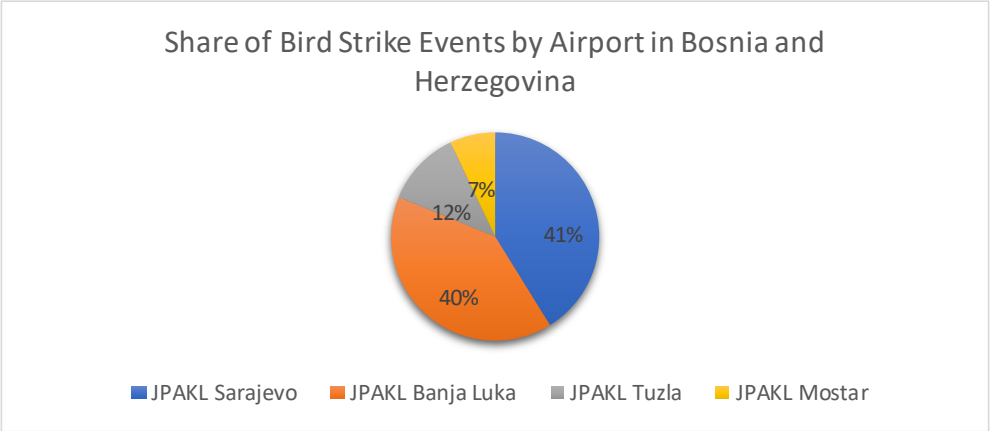


Figure 2. Share of Bird Strike Events by Airport in Bosnia and Herzegovina (2017-2024) (Source: BHANSA)

Distribution by Flight Phase

The analysis shows that bird strike events most frequently occur during the critical phases of flight - take-off (27.4%) and landing (27.4%) - while 10.7% were recorded during taxiing and deceleration phases.
In 34.5% of cases, the flight phase was not clearly indicated in the reports, highlighting the need for a more consistent description of circumstances when reporting such events.
This distribution is fully consistent with international data (ICAO, 2018; FAA, 2024), according to which most bird strike incidents occur at low altitudes, during take-off and landing operations, when the likelihood of bird encounters is highest. A similar pattern has been observed for other categories of safety events and aviation accidents, where the majority of incidents also occur during these critical flight phases - take-off and landing (Nikšić & Öztürk, 2022).

Distribution by Bird Species

In the largest number of (67.9%), the bird species was not specified in the reports. Of the known cases, 22.6% are reported as "unknown bird", while in a smaller number, specific species were recorded: sparrow (3%), hawk (3%), eagle (3%), and 2% each for magpie and owl. Such a structure indicates that, although the majority of incidents do not involve severe consequences, there is a need for a more systematic identification of birds and collaboration with ornithologists, which would contribute to a better assessment of risk and planning of preventive measures. Recent research shows that the integration of DNA barcoding and field surveys enables a more precise identification of bird species that most frequently cause collisions with aircraft, which can improve preventive measures and reduce the risk of incidents (Chen et al., 2025). Additionally, the assessment of relative risk and seasonal differences between bird species can assist in the prioritized focusing of habitat management measures and airport operations, particularly during migration periods when the risk of collisions is highest (Ross et al., 2025).

Seasonal and Spatial Patterns

Analysis of dates shows a pronounced seasonal variation; the majority of events occur during spring and summer (May–August), periods of increased bird activity and raptor migrations. Such a seasonal pattern is consistent with expectations, as warmer months are associated with increased bird movements as well as higher air traffic intensity (Kelly, 2024; Tal et al., 2024).
Spatial distribution indicates that Sarajevo and Banja Luka are the main centres for these incidents, which is related both to higher traffic volume and environmental factors that favour bird presence in the airport vicinity.

Although Sarajevo experiences a significantly higher number of flight operations, the number of bird strike events in Banja Luka is almost equal, which may point to several possible causes:
a) more favourable spatial and ecological conditions for bird presence (e.g., proximity to forests and agricultural areas),
b) the location of the airport within a potential migratory corridor, or
c) the need for potential improvement of existing bird control and dispersal measures implemented at Banja Luka Airport.
These observations indicate the need for a more detailed analysis of local biotic and spatial-ecological factors, as well as for periodic evaluation of the effectiveness of existing wildlife management programs at airports in Bosnia and Herzegovina.

5.2. Trend Analysis

Analysis of the temporal progression of the number of bird strike events in the period 2017–2024 allows insight into the dynamics of incident occurrence over a longer time horizon.
In the first part of the observed period (2017–2020), a relatively low and stable number of events is recorded, whereas after 2021 there is a significant increase in reports, indicating a change in the frequency of these incidents.
Such an increase may result from the combined influence of the growth in air traffic volume following the pandemic period, improvements in the event recording system, as well as changes in ecological conditions that affect the presence of birds in the vicinity of airports.

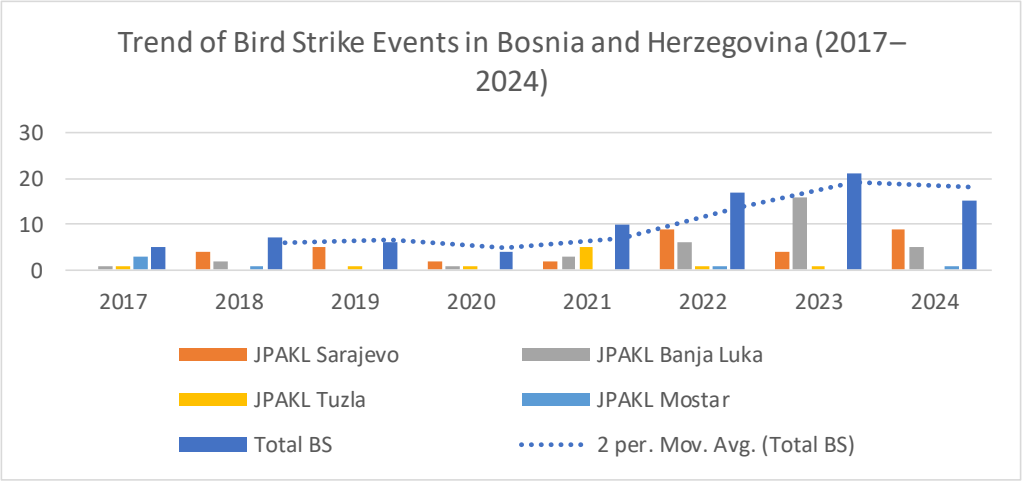


Figure 3. Trend of Bird Strike Events in Bosnia and Herzegovina (2017–2024) (Source: BHANSA)

The results presented in Figure 3 show that the number of bird strike events in Bosnia and Herzegovina continuously increased after 2021, with the highest values recorded during 2022 and 2023.
The application of a two-year moving average clearly confirms the upward trend, indicating the need for continuous monitoring and risk evaluation.
Comparison among airports shows that Sarajevo and Banja Luka lead in the number of recorded events, whereas Tuzla and Mostar airports record a smaller number of incidents. Interestingly, however, Banja Luka, despite a significantly lower volume of air traffic, records almost the same number of incidents as Sarajevo. Such a pattern may suggest that the area surrounding Banja Luka Airport is spatially more favourable for bird presence, that it is located within a migratory corridor, or that wildlife control measures are not as effective as at other airports. On the other hand, Tuzla and Mostar airports record fewer events, which may be associated with a smaller number of flights, as well as local ecological conditions that are less favourable for bird concentration.

Expert Critical Review

The conducted analysis shows that bird strike events in the airspace of Bosnia and Herzegovina are generally of low risk, but their frequency demonstrates an upward trend over the past several years. This trend does not necessarily indicate a deterioration of safety conditions, but may reflect improved record-keeping and awareness of the importance of reporting incidents within the framework of the SMS.
On the other hand, the disproportion between the volume of air traffic and the number of bird strike events, particularly in the case of Banja Luka Airport, requires additional attention. Such a phenomenon may point to specific local ecological factors, the presence of birds along migratory corridors, or insufficient effectiveness of existing wildlife control measures. It is advisable that a more detailed risk assessment be conducted at airports in the forthcoming period, with an emphasis on spatial and seasonal variations, in order to determine the actual causes of the increased frequency of events.
Furthermore, the high proportion of cases in which the bird species is not identified (almost 68%) limits the possibility of precise risk assessment and planning of targeted measures. This highlights the need for standardization of the bird strike reporting form and strengthening cooperation with ornithological experts to improve species identification and understanding of their migratory habits.
Finally, although the analysed events in most cases did not result in serious consequences for flight safety, the fact that the highest number of incidents occurs during take-off and landing phases indicates a continued exposure of critical flight stages to increased risk. Therefore, it is important that airports in Bosnia and

Herzegovina continue with continuous monitoring, evaluation of effectiveness, and improvement of wildlife management measures, in accordance with international guidelines (ICAO Annex 14, Doc 9137 – Airport Services Manual, Part 3).

The obtained results provide a basis for formulating conclusions and recommendations aimed at enhancing air traffic safety and more effective management of the risk of aircraft-bird collisions.

6. Conclusion

The analysis of bird strike events in the airspace of Bosnia and Herzegovina has shown that, although the majority of incidents are classified as low risk, their frequency demonstrates an upward trend over the past several years. This increase may reflect the combined influence of a growing number of flight operations, changes in bird migration patterns, and improvements in the incident reporting system.
The highest number of events was recorded at Sarajevo and Banja Luka airports. Although Sarajevo experiences significantly higher traffic, Banja Luka records almost the same frequency of bird strike incidents, which may indicate local ecological factors, proximity to areas favourable for bird congregation, or differences in the implementation of wildlife control measures. Analysis by flight phases shows that the riskiest stages are take-off and landing, which is consistent with global trends. A higher number of cases during the warmer part of the year confirms the seasonal variation associated with bird activity and migration. However, a significant proportion of reports with unidentified bird species highlights the need for improved record-keeping and cooperation with ornithological experts.

Further advancement in the management of bird strike risk requires a systemic approach: data integration, standardization of reporting, airport-specific risk assessment, and continuous evaluation of the effectiveness of wildlife management measures. Particular attention should be given to the development of integrated strategies that combine technical, biological, and educational measures.

In conclusion, bird strike events, although in most cases not representing a high safety risk, remain a relevant factor requiring continuous analytical attention and coordinated action by all actors within the aviation safety system of Bosnia and Herzegovina.

List of Figures and Tables

References

25. Chen, W., Sun, C., Zhang, J., Li, J., Chang, Q., Li, P., & Hu, C.(2025) "Avian collision risks at airports: Integrating DNA barcoding, species traits, and phylogenetic analyses to inform mitigation strategies." Global Ecology and Conservation 62(2025): e03829.
26. Civil Aeronautics Board (1963) *Investigation of Aircraft Accident: United Air Lines Flight 297, Vickers-Armstrongs Viscount, N 7430, near Ellicott City, Maryland, November 23, 1962.* Report No. 1-0034.
27. Direkcija za civilno zrakoplovstvo Bosne i Hercegovine (2021) *Izvještaj o događajima koji su uticali na bezbjednost letenja u Bosni i Hercegovini*. Banja Luka: BHDCA.
28. Direkcija za civilno zrakoplovstvo. (2021-2025). *Izvještaji o sudarima zrakoplova s pticama (bird strike) u Bosni i Hercegovini*. Banja Luka: BHDCA. Dostupno na: http://www.bhdca.gov.ba/index.php/hr/doc/bezbjedonosne-informacije [9.10.2025.]
29. Eastern Airlines (1960) *Investigation of Aircraft Accident: Eastern Airlines, Boston, Massachusetts: 1960-10-04.* Civil Aeronautics Board. Report No. 1-0043.
30. Eurocontrol (2011) *Reporting and Assessment of Safety Occurrences in ATM - ESSAR 2*. Brussels: Eurocontrol.
31. Europska komisija (2014) *Uredba Komisije (EU) br. 139/2014 od 12. veljače 2014. o utvrđivanju zahtjeva i upravnih postupaka u vezi s aerodromima u skladu s Uredbom (EZ) br. 216/2008 Europskog parlamenta i Vijeća. Službeni list Europske unije*, L 44/1.

32. FAA (2024) Wildlife Strikes to Civil Aircraft in the United States 1990 - 2024. Serial Report Number 31, Washington, DC

33. ICAO (2013) *Airport Services Manual, Part 3: Wildlife Control and Reduction*. Montreal: ICAO.

34. ICAO (2018) *Annex 14 to the Convention on International Civil Aviation, Aerodromes - Volume I: Aerodrome Design and Operations*. 8th ed. Montreal: International Civil Aviation Organization.

35. ICAO (2018) Safety Report, Montreal: ICAO

36. International Civil Aviation Organization (2023) *Electronic Bulletin EB 2023/30: 2016-2021 Wildlife Strike Analyses (IBIS)*. Montreal: ICAO.

37. International Civil Aviation Organization (ICAO) (2012) *Airport Services Manual: Part 3-Wildlife Control and Reduction*. 4th edn. Montreal: ICAO.

38. Kelly, T.A. (2024) „Seasonal Variation in Birdstrike Rate for Two North American Seasonal Variation in Birdstrike Rate for Two North American Raptors: Turkey Vulture (cathartes Aura) and Red-tailed Hawk Raptors: Turkey Vulture (cathartes Aura) and Red-tailed Hawk (buteo Jamaicensis)“, Journal of Raptor Research, 33(1), str: 59-62.

39. Nikšić, L. & Ozturk, E.A. (2022) „US./Europe Comparison Of ATC-Related Accidents And Incidents“, International Journal for Traffic and Transport Engineering, 12(2), pp 155 - 169 DOI: http://dx.doi.org/10.7708/ijtte2022.12(2).01

40. Nikšić, L. & Ozturk, E.A. (2023) „Analysis of ATC-related aviation accidents and incidents“, Aircraft Engineering and Aerospace Technology, 95(6), pp 890-898 https://doi.org/10.1108/AEAT-03-2022-0078

41. Pravilnik o izvještavanju o događajima. (2015/2017) „Službeni glasnik BiH“, br. 57/15 i 88/17. BHDCA.

42. Prskalo, M. & Šahić, A. (2024) „Utjecaj ljudskih čimbenika na sigurnost zračnog prometa“, *Zaštita i sigurnost*, 1, str. 174–203. DOI: 10.70329/2744-2403.2024.1.7.177.

43. Prskalo, M. (2024) „Suvremeni kibernetički rizici u upravljanju zračnim prometom“, *Zaštita i sigurnost*, 3(2), str. 132–143.

44. Ross, C. D., M. Schank, M. J. Begier, B. F. Blackwell, and T. L. DeVault. (2025) „Assessing relative hazard, risk, and seasonal

differences of Wildlife-aircraft collisions“, Wildlife Society Bulletin, 49(3), DOI https://doi.org/10.1002/wsb.1609

45. Tal, T., Jansen, D., Jansen, E., Green, A.W., Hoekstra, E., Heetkamp, M., T'jollyn, F., Engelen, D., Hoekstra, B., Kaasiku, T. And Wansteelant, W.M.G. (2024) „Full-season spring migration counts reveal seasonal contrasts in raptor migration through the eastern Black Sea flyway“, bioRxiv, 2024-08
46. U.S. Department of Transportation, Federal Aviation Administration (2020) *Advisory Circular: Hazardous Wildlife Attractants on or near Airports*. AC No. 150/5200-33C, 21 February.
47. U.S. Department of Transportation, Federal Aviation Administration (2024) *Advisory Circular: Reporting Wildlife Aircraft Strikes*. AC No. 150/5200-32C, 31 July.
48. US FAA (2024) *Wildlife Strikes to Civil Aircraft in the United States 1990–2024*. Washington, DC: Federal Aviation Administrators

ULOGA OBAVJEŠTAJNIH SLUŽBI U SPROVOĐENJU AKTIVNIH MJERA KAO OBLIKA POLITIČKOG NASILJA

DOI: *10.70329/2744-2403.2025.5.10.10*

Izvorni naučni rad

Dr. Emir Muhić[63]

Sažetak

Rad analizira ulogu obavještajnih službi u provođenju aktivnih mjera kao specifičnog oblika političkog nasilja koje djeluje u sferi percepcije, informacija i kognitivne manipulacije, a ne u domenu fizičke sile. Aktivne mjere predstavljaju sofisticirano političko oružje kojim države, putem svojih obavještajnih i propagandnih kapaciteta, utiču na društveno-političku arhitekturu protivnika kroz prikrivene, poricljive i dugoročno usmjerene operacije. Metode poput dezinformacijskih kampanja, infiltracije političkih struktura, kompromitovanja lidera, induciranja društvenih tenzija i fragmentacije identiteta stvaraju alternativni politički realitet koji pogoduje ostvarivanju strateških ciljeva agresivnog aktera. Istraživanje naglašava da su aktivne mjere latentne, teško dokazive i čvrsto uklopljene u savremene oblike specijalnog rata, što doprinosi njihovoj efikasnosti i nedovoljnom razumijevanju u akademskim, institucionalnim i političkim krugovima. Poseban akcenat stavljen je na potrebu izgradnje otpornih institucionalnih mehanizama, medijske pismenosti i strateške komunikacije kao ključnih elemenata odbrane od prikrivenog političkog nasilja koje narušava suverenitet, društvenu koheziju i stabilnost savremenih država.

Ključne riječi: *obavještajne službe, aktivne mjere, političko nasilje, specijalni rat, dezinformacije, hibridno djelovanje.*

[63] emirmuhic@fkn.unsa.ba

1. Uvod

Nekonvencionalni ratovi koji odbacuju primjenu otvorenog oružanog sukoba i upotrebe legalnih i legitimnih državnih armija nalažu upotrebu sredstava kojima se na liminalnom nivou podriva suverenitet i integritet protivnika, državnog ili nedržavnog aktera. Konvencionalni, oružani ratovi su ekonomski i resursno neisplativi, te politički nepogodni, što implicira korištenje drugih načina za ugrožavanje, kontrolu ili uništavanje protivnika. Kao jedna od uspješnih metoda specijalnog rata, koja se po nalogu državnog vrha provode od strane obavještajnih službi, i koja stvara značajne posljedice na nacionalnu i međunarodnu sigurnost su aktivne mjere. Aktivne mjere u svojoj osnovi predstavljaju političko oružje, alat kojim se ostvaruju od državnih rukovodioca propisani ciljevi. Kao takve, aktivne mjere pripadaju sistemu specijalnog rata, pri čemu su veoma efikasno i efektivno oružje ili alat kojim se kreira specifično političko okruženje i društveno-politički i kulturološki narativ. Aktivnim mjerama se kreira „novi realitet" potreban za daljnje ostvarivanje strateških ciljeva. Same aktivne mjere predstavljaju „dokazano" političko oružje koje od dvadesetih godina prošlog stoljeća kontinuirano kreira i stvara specifične društveno-političke odnose pogodne državnom rukovodstvu.

Značajna problematika aktivnih mjera se ogleda u nedovoljnom rauzumijevanju istih od strane akademske zajednice, te uskogrudno posmatranje istog u domenu dezinformacija i lažnih vijesti. Aktivne mjere se trebaju posmatrati kao širok spektar metoda i mjera koje poduzimaju obavještajne službe, a kojima se utječe na političke donosioce odluka i politiku države koja se njima tretira. Kao predmet ovog istraživanja se nameće operativna uloga obavještajnih službi na provođenje aktivnih mjera u svrhu destabilizacije ciljane države. Neophodno je adekvatnije razumjeti *modus operandi* obavještajnih službi koje provode aktivne mjere kao oblik političkog nasilja. Značajan problem predstavlja sama priroda aktivnih mjera koje su latentne, nevidljive, teško dokazive i sofisticirane, pri čemu konspirativnost djelovanja obavještajnih službi dodatno uslovljava istraživanje istih. Pitanja poput mjera, načina provođenja, ciljeva, metoda, tehnika i drugog koje se odnosi na operativne aktivnosti obavještajnih službi su nepoznanica koja se mora demistificirati kako bi bilo moguće kreirati programe i sisteme rezilijentnosti.

2. Definisanje aktivnih mjera i političkog nasilja

Aktivne mjere predstavljaju veoma efikasno i efektivno oružje agresivnih političkih aktera u borbi za političku moć ili resurse na regionalnom ili globalnom nivou. One svoj početak vežu za boljševičku kontraobavještajnu operaciju „Povjerenje" iz 1921. godine usmjerenu protiv izbjeglih monarhista (Rid, 2019), te svoju kontinuiranu primjenu imaju u periodu Hladnog rata (Galeotti, 2019) u

kojem su dominirale nekonvencionalne mjere političkog, diplomatskog i vojnog sukoba[64] Sovjeta i Zapada. Fraza „aktivne mjere" ima svoje korijene iz vremena sovjetskog KGB-a koja u sebi uključuje dezinformacijske kampanje, pokušaje političkog utjecaja i djelovanja *proxy* grupa i partija Sovjetskog saveza (Kux, 1985). Rid (2019) definiše aktivne mjere kao strateške aktivnosti koje obavještajne službe koriste za manipulaciju, dezinformaciju i podrivanje političkih procesa s ciljem postizanja geopolitičkih ciljeva. One su ključni alat političkog ratovanja, koji prevazilazi klasičnu špijunažu i uključuje ofanzivne operacije usmjerene na formiranje političkih, društvenih i ekonomskih odluka u targetiranim državama.

Zbog svoje ofanzivne prirode, aktivnim mjerama se postiže dezorganizacija, destabilizacija i demoralizacija protivnika, odnosno političke zajednice, organizacije, korporacije ili pojedinca, i usko su povezane sa ideološkom subverzijom o kojoj je govorio KGB-ov defektor Yuri Bezmenov. Galeotti (2019) navodi da su aktivne mjere termin koji je Sovjetski Savez koristio od 1950-ih godina kako bi opisao širok spektar prikrivenih i poricljivih operacija političkog utjecaja i subverzije u koji spadaju aktivnosti poput osnivanja front / proxy organizacija, podršku prijateljskim političkim sistemima, organizovanju lokalnih nemira i širenju dezinformacija i tako dalje. Radin, Demus i Marcinek (2020) aktivne mjere vide kao prikrivene i poricljive operacije političkog utjecaja i subverzije, koje obuhvataju korupciju i dezinformacije, pa sve do otvorenih atentata, pa čak i sponzorstva državnih udara. Aktivne mjere su usko povezane sa konceptom specijalnog rata koji se definiše kao koordinisana politička, ekonomska, psihološko-propagandna, obavještajno-subverzivna i vojna aktivnost provedena da se ostvari utjecaj i intrevniše na teritoriji druge države pri čemu je upotreba konvencionalne vojne sile krajnja opcija (Muhić, 2025). Specijalni rat koristi aktivne mjere kao sredstvo za postizanje strateškog i operativnog cilja kroz niz kampanja i operacija u dužem vremenskom periodu. Kako je priroda specijalnog rata dugoročna i ciklična (Muhić, 2025), tako su i operacije prolongirane, kontinuirane i naslanjaju se jedna na drugu u koordinaciji sa drugim mjerama, aktivnostima i akterima koji ih izvode.

Suštinski, aktivne mjere se ostvaruju putem medija i sistema informisanja, političkog rada, obrazovanja, fizičkog nasilja i drugih adekvatnih načina kojima je moguće direktno utjecati na targetirano društvo, naciju ili zajednicu, kako bi se utjecalo na političke donosioce odluka. Trenutačno u akademskoj zajednici regiona ne postoji prepoznavanje termina „aktivne mjere", te ista neadekvatno upotrebljva termin „dezinformacija" za aktivnosti koje imaju cilj utjecati na

[64] U navedenom sukobu Sovjeta i Zapada, osnovni cilj je bio poraziti neprijatelja bez dikretne upotrebe vojne sile, već uz pomoć nekinetičkih, nekonvencionalnih i asimetričnih mjera kojima se direktno napadao um targetirane skupine. Kada se govori o upotrebi vojne sile, tada se misli na proxy ratove (Koreja, Vijetnam, Afganistan) u kojima su akteri nudili svoje usluge savjetnika ili vojno pomagali stranu koja se bori protiv njihovog ideološkog protivnika.

donošenje odluka. Također ne postoji prepoznavanje i razlikovanje načina na koji se postiže dominacija u informativnom prostoru kroz operacije utjecaja, psihološke operacije i informacione operacije pri čemu se različiti modaliteti etiketiraju jednostavno kao dezinformacija. Kako Rid (2019) navodi, aktivne mjere uvijek u sebi uključuju upotrebu dezinformacija, ali one nisu jedini element. Ponekad su projekti osmišljeni kako bi olakšali određenu političku odluku kroz stvaranje „povoljnog" okruženja koje određenu zajednicu, grupu ili vladu dovodi do navedene političke odluke. Isto se čini aktivnim propagiranjem činjenica koje navedenoj grupi idu u prilog, te nanose reputacijsku ili drugu štetu neprijateljskom akteru. Gotov nevidljivo usmjeravanje ka specifičnom cilju predstavlja *modus operandi* kojim se ostvaruje pobjeda nad protivnikom bez ulaska u otvoreni, konvencionalni sukob.

Također, aktivne mjere aktivne mjere nisu spontane laži političara, već metodični rezultat velikih birokratija. Izjave mnogih političkih aktera iako one izgledaju sasvim proste, jednostavne i beznačajne u sebi nose poruku koja je usmjerena prema određenoj skupini ili služe za kreiranje budućeg narativa zasnovanog na izjavi. To nisu samo izjave političkih aktera, već specifični revizionistički narativi nepolitičkih ili pseudopolitičkih aktera kojima se nastoje mijenjati historijske činjenice i fakti. Plasiranjem specivičnih informacija u eter, stvara se sidrište za izgradnju lažnih narativa koji će u budućnosti služiti kao podrška strateškom cilju. Za ostvarenje istog je potrebna kritična masa građana koja će svjesno ili nesvjesno pristati na laž.

Aktivne mjere su u svojoj osnovi političko oružje zasnovano na pisanim ili govornim aktima političkih i drugih državno-važnih aktera, koji za cilj imaju mijenjanje trenutačnog društveno-političkog stanja. One predstavljaju sofisticiran oblik političkog nasilja jer djeluju bez upotrebe fizičke sile, ali s ciljem prisilnog oblikovanja političkih odluka, stavova i ponašanja targetiranih grupa, zajednica i društava. Ove metode i aktivnosti se koriste u simbiozi sa djelovanjem obavještajnih službi koje služe kao potpora političkom ili drugom akteru, bilo u pribavljanju informacija ili u širenju istih. U savremenom kibernetičkom okruženju, širenje informacija i dezinformacija, misinformacija i malinformacija postalo je glavno sredstvo za stvaranje nasilne političke dominacije koja ne djeluje kroz fizičku destrukciju, već kroz eroziju povjerenja, delegitimizaciju institucija i ograničavanje slobodne političke volje. Takvo djelovanje proizvodi sistemsku asimetriju moći i onemogućava funkcionisanje demokratskih i liberalnih principa upravljanja. Aktivne mjere stoga predstavljaju specifičan oblik političkog nasilja koje se, iako nenasilno u fizičkom smislu, ostvaruje kroz prisilu u sferi odlučivanja, oblikovanja percepcije i stvaranja operativnog okruženja u kojem targetirana zajednica donosi odluke protiv vlastitih interesa. Političko nasilje u ovom kontekstu ne podrazumijeva isključivo upotrebu sile, već svako djelovanje kojem je cilj potkopavanje sposobnosti države ili društva da suvereno upravlja vlastitim političkim procesima, čime se direktno utiče na raspodjelu

moći. U tom smislu, aktivne mjere funkcionišu kao „tihi koercijski aparat" kojim agresivni akter nameće vlastite narative i interpretacije stvarnosti, istovremeno ograničavajući manevarski prostor legitimnim političkim akterima unutar ciljanog društva. Političko nasilje koje nastaje primjenom aktivnih mjera proizvodi tri ključna efekta: prvo, ono narušava vertikalnu legitimnost vlasti kroz eroziju povjerenja u institucije, pri čemu svaka izmišljena kriza ili fabricirani narativ postaje katalizator političke nestabilnosti; kao drugo, ono razara horizontalnu koheziju društva stvaranjem dubokih simboličkih podjela, identitetskih konflikata i permamentne sumnje među društvenim grupama koje više ne dijele zajednički okvir istine; i treće, ono vrši kognitivnu okupaciju, jer ciljano društvo počinje internalizirati narative koji su kreirani izvan njegovih granica. Takva okupacija predstavlja najnapredniji i najopasniji oblik političkog nasilja, budući da se postiže bez fizičke prisile, bez vojnih efektiva i bez vidljivog konflikta, ali s daleko većim dugoročnim posljedicama u pogledu razgradnje političkog suvereniteta.

3. Aktivne mjere i obavještajne službe

Aktivne mjere kao političko oružje zasnovane su primarno na nenasilnom djelovanju koje kao posljedicu mogu imati fizičko nasilje. Ruski general-major Vladimirov napisao je da se „savremeni ratovi vode na nivou svijesti i ideja" i da „savremeno čovječanstvo postoji u stanju permanentnog rata", u kojem se „neprestano nalazi između faza stvarne oružane borbe i stalne pripreme za nju" (Galeotti, 2021). Sovjetski KGB, detašman D nastojao da ugrozi i uništi SAD kroz sofisticirane obavještajne, primarno nenasilne operacije zasnovane na dezinformacijama. Bivši pripadnik KGB-a, general-potpukovnik Oleg Kalugin, nazvao je subverziju i aktivne mjere „srcem i dušom sovjetske obavještajne službe", dakle „subverzija, a ne prikupljanje podataka" (CNN, 2000). Navedene operacije su se zasnivale na specifičnim vanjsko-političkim aktivnostima Sovjetskog saveza kroz „bijele", „sive" ili „crne" operacije (Kux, 1985). Prema Kuxu (1985), „bijele" operacije su bile normalne diplomatske, trgovinske ili humanitarne aktivnosti, „sive" operacije su u sebi uključivale rad ilegalnih komunističkih grupacija na zapadu i „crne" operacije su bile zapravo tajne operacije djelovanja agenata u širenju dezinformacija, laži, širenja plagijata, krivotvorina i tako dalje. U modernom vremenu, gotovo pa da ne postoji razlika između „bijelih", „sivih" i „crnih" operacija, niti je moguće razlikovati aktere koji iste provode zbog zasićenosti informativnog prostora i propagandnog djelovanja kojim se one skrivaju. Anarhizam na međunarodnom nivou, uslovio je konstantnu borbu država za prijesto hegemona koji pripada SAD-u (Donnelly, 2006). Međutim, dešavanja na geopolitičkom nivou uveliko prijete trenutnoj postavci i odnosima, te su na sceni ponovno „bijele", „sive" i „crne" operacije za razliku od onih konvencionalnih, vojnih. Ove operacije omogućavaju kontinuirano provođenje političkog nasilja nad različitim akterima i ostvarivanje strateških

ciljeva bez otvorenih konfrontacija i konvencionalnog rata koji bi mogao proizvesti katastrofalne posljedice kao što je nuklearna razmjena projetkila, rušenje monternog sistema, masovni cyber napadi na kritičnu infrastrukturu i tako dalje. Akteri poput obavještajnih službi primjenjuju aktivne mjere koje omogućavaju liminalnu dimenziju rata kako to navodi Kilcullen (2020). Liminalna dimenzija rata prema Kilcullenu je stanje u kome nema otovrenog oružanog sukoba, ali su primjetne obavještajne aktivnosti. Sveobuhvatnost primjene aktivnih mjera i političko-društveno utjecaja je bila značajna u vremenu Hladnog rata kada je sovjetski KGB provodio mnoštvo dezinfromacionih operacija poput operacije „Denver" koja je za cilj imala okriviti vojsku SAD-a za kreiranje virusa HIV-a i AIDS-a (Kramer, 2019), te subverzivnih operacija „Pandora" koja je za cilj imala izazivanje međurasnih nereda na teritoriji SAD-a (Andrew & Mitrokhin, 2000). Period nakon raspada Sovjetskog saveza je stvorio drugačiju klimu društveno-političkih odnosa, te je pojava religijskog radikalizma, ekstremizma i terorizma uzrokovala veću upotrebu kinetičkih nad nekinetičkim mjerama i operacijama.

Period nakon terorističkih napada 11. septembra 2001. godine je fokus stavio na kinetičko djelovanje (invazija na Irak, Afganistan), pri čemu aktivne mjere kao samostalno sredstvno nisu bile adekvatne i primjerene i nalagale su upotrebu vojnih efektiva. Period tzv. Arapskog proljeća kao niza insurgencija na Bliskom istoku, pojava ISIL-a, te ruska okupacija Krima, ukazali su na značaj aktivnih mjera i provođenja političkog nasilja prema protivnicima. Operativno djelovanje obavještajnih službi za račun agresivnih političkih aktera, omogućilo je pokretanje društveno-političkih procesa kao što su pobune, insurgencije i građanski ratovi. Važnost aktivnih mjera se ogleda u pozicijama i snagama aktera koji ih primjenjuju i aktera prema kojima su primjenjene.

Razlog zašto se aktivne mjere nisu primjenjivale u vrijeme takozvanog „globalnog rata protiv terorizma", ogleda se u tome što su protivnički akteri – terorističke organizacije / insurgenti / pobunjenici[65] na Bliskom istoku bili ranjivi i pogodni za vojno djelovanje, te su isti akteri bili značajno inferiorni u pogledu tehnološkog, ekonomskog, društveno-političkog i kultrološkog aspekta. Zbog navedenih okolnosti, nije bilo potrebe primjenjivati aktivne mjere prema

[65] Specičnost sukoba sa raznim grupama koje su imale zajednički imenitelj borbu protiv koalicionih snaga se ogleda u tome da nisu sve bile odane Al-Kaidi i njenim podružnicama. Određene frakcije su bile odane Sadamu Huseinu ili mudžahedinskim ili talibanskim vođama i za cilj su imale borbu protiv strane sile koja je došla na njihov teritorij. U konstekstu GWOT-a potrebno je razlikovati domicilne aktere na području Iraka i Afganistana, ciljeve i svrhu njihove borbe, te strane borce okupljene oko Osame bin Ladena u Al-Kaidu. Ideja da su svi koji pružaju otpor američkoj vojsci i koalicionim snagama samo teroristi je eklatantan primjer nepozvanja geopolitičkih i internih odnosa. Navedenim nepoznavanjem osnažuju se neokolonizatorske ideje i valoriziraju zločini koji su počinjeni proitv muslimana-arapa u svrhu održanja ideje „sukoba civilizacija", pri čemu sukob nije bio na teritoriji SAD-a ili Europe, već teritoriji „kulturološkog" neprijatelja.

targetiranim akterima. Također, specifične kontra-insurgencijske strategije (COIN)[66] su se pokazale kao neuspješne u Iraku i Afganistanu, pri čemu je smrt civila označena kao kolateralna šteta služila kao radikalizirajući i regrutirajući element za pobunjenike kao što su Talibani, šitske i sunijske milicije u Iraku i terorističke grupe poput Al-Kaide koja je obećavala osvetu.

S druge strane, kada je riječ o velikim globalnim i regionalnim silama poput Rusije, Kine, Irana i Sjeverne Koreje koje Kilcullen (2020) naziva „zmajevima" i organizirnim kriminalnim grupama, terorističkim organizacijama i kartelima koje navedeni autor naziva „zmijama", aktivne mjere predstavljaju pogodno oružje za njihovo ugrožavanje, ometanje, destabilizaciju, kontrolu, pobjeđivanje ili uništavanje.

Primjenom aktivnih mjera ulazi se u domen specijalnog rata koji je zasnovan na djelovanju obavještajnih službi kroz tajne, konspirativne i maliciozne aktivnosti kojima se napada društvo i nacija bez primjene oružane sile. Sam specijalni rat kao sredstvo i način borbe za strateške ciljeve koji kreiraju državne politike i provode obavještajne službe omogućava da se na globalnom nivou provodi utjecaj na specifične skupine koje predstavljaju prijetnju nacionalnom sistemu sigurnosti. One isto tako mogu služiti kao element za postizanje lokalne ili regionalne dominacije nasuprot tehnološki i društveno-politički inferiornijih aktera.

Današnje strategije i doktrine su usmjerene ka nevidljivoj okupaciji i kontroli protivničkog stanovništva kroz primjenu raznih aktivnosti i mjera utjecaja na političkom, ekonomskom, obrazovnom, kultrnom i drugom nivou. Pripadnici kopenhagenške škole poput Barry Buzana su fokus stavili na pet sektora sigurnosti (Buzan, 1983), te su navedeni sektori dobili i istoimene prijetnje, ali danas u modernom dobu desila se diverzifikacija i širenje sektora. Samim time se poseban aspekt treba posvetiti kibernetičkom i obrazovnom sektoru koji se mogu definisati kao *novum* u sigurnosnim studijama.

Navedena dva *nova* sektora su pogodna za aktivne mjere. Prvi sektor, kibernetički, koristi se za širenje, odnosno diseminaciju misinfromacija, dezinformacija i malinformacija kao i za info-kinetičke napade, dok se posljednji, obrazovni, koristi za indoktrinaciju društva kroz kompromitirani školski i obrazovni sistem. U ovom slučaju riječ je o mješavini već pomenutih „bijelih", „sivih" i „crnih" operacija, te su svi državno-politički i sigurnosno-obavještajni nivoi uključeni u njih.

[66] Counter insurgency – skupine političko-društvenih, vojnih i ekonomskih mjera koje se koriste za suzbijanje pobunjeničkih, gerilskih, insurgencijskih, partizanskih pokreta, njihovih ciljeva i podrške koju imaju unutar lokalnog stanovništva.

4. Subverzivne aktivnosti i političko nasilje obavještajnih službi

Obavještajne službe kao državi podređen organ koji ima sposobnosti za izvođenje specijalnih operacija kinetičke i nekinetičke prirode, predstavlja adekvatnog aktera u izvodđenju aktivnih mjera. Kao što je u vrijeme bloklvske podjele dvadesetog stoljeća sovjetski KGB provodio svoje aktivnosti zarad uspostavljanja nove ideološke orjentacije stanovništva SAD-a, te umanjivanja utjecaj SAD-a u svijetu, danas isto čine mnoge obavještajne službe. Ostvarivanje strateških ciljeva agresivnog aktera koji teži postati hegemon, nalaže kontinuirano obavještajno tretiranje protivnika i neutralnih aktera. Njihovim obavještajnim tretiranjem stvaraju se pogodni uvjeti za političke, diplomatske i ekonomske benefite koji su rezultat ometanja, uništavanja ili ugrožavanja protivnika, te indoktrinacije neutralnih aktera. Obavještajne službe izvode *de facto* sabotažu političko-društvenog uređenja kroz sljedeće aktivnosti:

- Širenje dezinformacija, misinformacija i malinformacija,
- Aktivno ofanzivno propagandno djelovanje,
- Pružanje podrške političkoj opoziciji,
- Sabotiranju izbornog procesa,
- Izazivanje klime straha i nesigurnosti u ciljanom društvu,
- Pravno, ekonomsko i diplomatsko podrivanje nezavisnosti, suvereniteta i integriteta,
- Osnivanju subverzivnih ideološki odanih organizacija,
- Finansiranju kriminalnih i terorističkih organizacija,
- Organiziranju, podstrekvianju i izvođenju atentata i političkih ubistava,
- Podstrekivanju na građanski nemir, neposluh i nasilje.

Da bi se navedene aktivnosti jasnije sistematizovale i razumjele u kontekstu savremenog političkog nasilja, u nastavku je prikazana tipologija subverzivnih mjera (Tabela 1), njihovi instrumenti, ciljevi i očekivane posljedice.

Tabela 1 Tipologija subverzivnih aktivnosti obavještajnih službi

Kategorija subverzivne aktivnosti	**Operativni instrumenti**	**Primarni cilj**	**Posljedice po targetiranu državu**
1. Informacione operacije	Dezinformacije, misinformacije, malinformacije, bot mreže, deepfake sadržaji, kontrola medija, psiho-operacije	Kognitivna destabilizacija populacije	Polarizacija, pad povjerenja u institucije, masovna konfuzija, delegitimizacija vlasti
2. Propagandno djelovanje	Sistematske kampanje, amplifikacija narativa kroz influensere, mreže „korisnih idiota“,	Uspostavljanje alternativne stvarnosti i ideološke dominacije	Normalizacija ekstremnih stavova, sužavanje javnog prostora, promjena političkih preferencija

	akademska ili kulturna podrška		
3. Političko infiltriranje	Podrška opozicionim grupama, finansiranje partija, podrška protestnim pokretima, ubacivanje agenata u političke strukture	Slabljenje vladajućih struktura i stvaranje unutrašnjeg haosa	Slom političke stabilnosti, mobilizacija nezadovoljstva, pad legitimiteta institucija
4. Izborno sabotiranje	Manipulacija biračkim spiskovima, curenje kompromitiranih podataka, financiranje kampanja, cyber napadi	Narativ da su izbori nelegitimni ili manipulirani	Delegitimizacija izbornog procesa, masovni protesti, institucionalni kolaps
5. Oslabljivanje države kroz pravni i ekonomski pritisak („lawfare“)	Tužbe, sankcije, blokade, specijalni trgovinski režimi, manipulacija međunarodnim institucijama	Prisiljavanje države da mijenja političke odluke	Ekonomsku štetu, gubitak suvereniteta, pravni haos, politička ucjenjivost
6. Osnivanje subverzivnih organizacija	Kreiranje NVO, think-tankova, pokreta, vjerskih ili kulturnih grupa lojalnih stranoj sili	Dugoročna indoktrinacija i kontrola društva	Transformacija političke kulture, „meko“ preuzimanje institucija
7. Podržavanje kriminalnih i terorističkih mreža	Finansiranje, obuka, logistika, krijumčarenje oružja	Slabljenje države iznutra stvaranjem paralelne moći	Erozija monopola sile, povećanje nasilja, delegitimizacija organa reda
8. Organizacija atentata i političkih ubistava	Plaćeni atentatori, prikrivene operacije, korištenje kriminalnih struktura	Eliminacija ključnih aktera koji predstavljaju prepreku interesima stranog aktera	Politički šok, vakuum moći, zastrašivanje opozicije i društva
9. Društvena destabilizacija	Podsticanje nemira, radikalizacije, identitarnih sukoba, pozivanje na secesiju	Kreiranje uslova za političko nasilje i raspad sistema	Građanski sukobi, masovne podjele, uslovi za intervenciju „zaštitne sile“

Navedene aktivnosti omogućavaju agresivnoj obavještajnoj službi stvaranje operativnog okruženja pogodnog za značajnije strateške poteze kao što su preuzimanje monteranog sistema, iskorištavanja ili uništavanja kritične infrastrukture, diplomatsko zasjenjivanje i odstranjivanje iz međunarodnih

tokova, otuđenje ili iskorištavanje resursa, kontrola zračne, vodene ili kopnene granice, kontrola ili nadzor telekomunikacija i tako dalje. Prvenstveno, aktivne mjere kao oblik političkog nasilja, prevazilaze fizičke okvire nasilja i prelaze u kognitivnu sferu utjecaja na targetirane nacije, društva i grupe. Obavještajne službe uz pomoć svojih kadrovskih, tehničkih i tehnoloških kapaciteta, nastoje aktivno provoditi radnje kojima se targetirano stanovništvo stavlja u stanje straha, anksioznosti i panike. Nepostojanje aktivnih kontramjera države žrtve i njenih organa (obavještajne službe, obrazovnih institucija i tako dalje) ili općenito prepoznavanja aktivnih mjera koje provodi agresivna obavještajna služba, predstavlja političko-ideološku okupaciju. Ova okupacija ne spada u tradicionalne okupacije koje se vrše uz pomoć oružanih snaga i vojno-policijskog prisustva i provođenja kontra-insurgencijskih operacija, već se okupacija provodi kontrolom narativa, stavova, mišljenja, ponašanja i kreiranja događaja koji ih uslovljavaju. Provođenje kontramjera predstavlja veoma sofisticiranu aktivnost u ovom slučaju, pri čemu značajno otežavajući faktor predstavlja infiltracija neprijateljskih agenata, korištenje korisnih idiota[67], finansiranju opozicije i drugog.

U činjenju političkog nasilja, radnje poput širenja dezinformacija, utjecaja / opstrukcije izbornih / političkih procesa, predstavljaju ključan element za održavanje potrebnog nivoa represije koji će stvoriti značajne političko-društvene probleme. Eskalacija političko-društvenih problema dovodi do podjela, segmentacije i atomizacije društva i nacije, te kreira operativno okruženje potrebno za prelazak na aktivnosti poput pozivanja na secesiju i njenog ostvarivanja ili izazivanja unutrašnjih sukoba koji mogu eskalirati u otvoreni oružani rat. Agresivne obavještajne službe aktivnim, tajnim i prikrivenim djelovanjem unutar političkog, ekonomskog i društvenog sistema postižu mnogo veće uspjehe nego što bi se to ostvarilo konvencionalnim ratom i upotrebom vojne sile. Korištenjem dezinformacija, propagande, kontroliranog i ciljanog fizičkog nasilja, upotrebe prava i zakona za opstrukcije političkih procesa, kao i fokusom na identitarne politike koje stvaraju podjele i produbljuju sukobe.

5. Aktivne mjere i ideološka subverzija

Djelovanje državnih elemenata ne može biti uspješno bez sistematskog oslabljivanja neprijatelja, što se provodi uz pomoć ideološke subverzije. O navedenom je govorio bivši operativac KGB-a Yuri Bezmenov, koji je u svojim intervjuima često naglašavao četiri faze kroz koje je potrebno provesti jedno društvo da bi ono bilo podložno stranom utjecaju. Bezmenov je navedene četiri faze klasifikovao kao demoralizaciju, destabilizaciju, krizu i normalizaciju, te je

[67] Hladnoratovski termin koji se koristio za ideološke i istinske sljedbenike komunizma i socijalizma u SAD-u koji su iskorištavani od sovjetskog KGB-a za različite vrste aktivnosti – proteste, govore, napade i tako dalje.

cilj svake od navedene faze bio neprimjetno slabljenje društvenih veza i izazivanje straha, netrpeljivosti, nepovjerenja i mržnje (Bezmenov, 1985). Bezmenov (1985) na sljedeći način objašnjava navedene faze: a) *Demoralizacija: Za ovaj korak u procesu potrebno je 15 – 20 godina. Toliko je vremena potrebno da se odgoji jedna generacija. Na tom putu pomažu mediji i učitelji koji su postali simpatični (svjesno ili nesvjesno) teoretskim uzrocima subvertirajuće nacije.* b) *Destabilizacija: Nakon prethodne faze, ovo je razdoblje od dvije do pet godina za promjenu vanjskih odnosa, obrane i ekonomije ciljne zemlje.* c) *Kriza: Potrebno je oko šest sedmica haosa kao značajne društveno – političke prekretnice.* d) *Normalizacija: Ova faza mijenja mišljenje o tome kako status quo izgleda.* Bezmenovljev opis ove faze također uključuje vojno preuzimanje države, odnosno širokogrudno prihvatanje neprijateljske vojske kao oslobodilačke. Prema riječima Bezmenova, aktivne mjere su korištene za slabljenje američkog društva kroz propagiranje antizapadnih ideja poput anarhizma, komunizma, socijalizma, marksizma i ostalih lijevo orijentiranih *-izama*. Na taj način se nastojalo izazvati niz sukoba u američkom društvu na osnovu rasnih, etničkih, klasnih i seksualnih osnova. Također, u navedenoj ideološkoj subverziji kao jednom od alata aktivnih mjera, primjetna je i simbiotička upotreba drugih metoda i aktivnosti specijalnog rata poput propagande, sabotaža, diverzija, atentata i političkih ubistava i tako dalje. Osnovni cilj navedene ideološke subverzije je slabljenje države i nacije, ali se isto ne može ostvariti bez ostalih mjera, metoda i aktivnosti koje čine specifičan sistem djelovanja unutar specijalnog rata.

U provođenju aktivnih mjera, kroz koje se ostvaruje slabljenje napadnute države i nacije, osnovu napada čini dezinformacija. Navedena dezinformacija je sastavni dio ostalih aktivnosti, bilo da je u ulozi osnovnog ili dopunskog elementa. Međutim, kada je riječ o ideološkoj subverziji kao jednoj od metoda napada na društvo i državu, dezinformacije kao osnova aktivnih mjera se nalaze u prvom redu. Razlog za navedeno je moć kojom se mijenja realitet i objektivna stvarnost koja proizilazi iz manipulacije infromacijom. Kao potvrdu navedenog imamo ponovno u izjavi Bezmenova koji iznosi podatak da samo 15% resursa ide u špijunske aktivnosti, dok ostalih 85% je alocirano u aktivne mjere, odnosno ideološku subverziju koja je za cilj imala mijenjanje percepcije stvarnosti amerikanaca koji iako imaju informacije iz prve ruke *šta se dešava,* ipak ne poduzimaju ništa za odbranu države, nacije, društva, zajednice i porodice (1985). Danas, ukoliko posmatramo obavještjane aktivnosti globalnih i regionalnih sila, uviđamo značaj kontrole medijskog prostora, naročito na društvenim mrežama i širenja narativa. Na primjer, Izrael u toku provođenja genocida u Gazi koristi influencere i društvene mreže za širenje propagande i izvođenje psiholoških operacija pri čemu su navedeni infulenseri plaćeni u iznosima od 7 hiljada američkih dolara (Middle East Eye, 2025). Društvene mreže igraju ključnu ulogu u savremenim psihološkim operacijama, omogućavajući brzo širenje dezinformacija i manipulaciju percepcijom ciljane publike (Muhić, 2025).

Hasbara, odnosno javna diplomatija Izraela, je usmjerena na formiranje stavova i mišljenja širih društvenih masa u pravcu opravdavanja ubijanja semitskog, odnosno arapskog i muslimanskog stanovništva. Isto ima za cilj da kroz medijske kampanje prikaže arape i muslimane kao prijetnju Europi, a Izrael kao branu koja štiti kršćanstvo. U ovim narativima se protežu Huntingtonove ideje o sukobu civilizacija i nekopatibilnosti Islama sa europskim vrijednostima[68]. Amplifikacija dehumanzirajućih poruka se odvija preko plaćenih influensera, korisnih idiota i zvaničnih državnih kanala. Trenutno ove operacije nemaju značajnijeg uspijeha zbog odsustva cenzure na društvenim mrežama kao što je X koja je dominantna za širenje političkih poruka. Na ovoj mreži je moguće uživo vidjeti genocid, zvjerstva i zločine protiv čovječnosti koje provodi izraelska država i vojska, pri čemu hasbara nema utjecaj, već stvara kontraefekat, a infuenseri koji propagiraju ove poruke bivaju etiketirani kao izraelski plaćenici.

U slučajevima informacijske dominacije i održanja tog stanja, potrebno je plasirati dovoljan broj dezinformacija i malinformacija u društvo, pri čemu njihova diseminacija mora biti kontinuirana i mnogobrojna. Dezinformacijama se mijenja sadržaj jer agenti provokatori plasiraju određene informacije u političko-društveni eter, lažiraju se izvori i osnažuju se aktivne operacije napada na štićene elemente države. U primjeru aktivnih mjera, širenje dezinformacija poput onih u KGB-ovim operacijama „Pandora“ i „Denver“, oslabljuje se napadnuto društvo, te se kidaju kohezivne veze istog. Isto se može upotrijebiti i na globalnom nivou kada je cilj da se određena nacija ili država etiketira kao globalna prijetnja. Primjer za navedeno se nalazi u lažnoj informaciji da Irak ima oružje za masovno uništenje koje je došlo od nepouzdanog izvora. Međutim, istinitim informacijama se također može utjecati, pa su tako sovjeti 60-ih godina printali letke na engleskom i francuskom koji govore o rasnoj diskriminaciji afro-amerikanaca i diseminirali ih u državama afrike koje su imale prisne veze sa bivšim kolonizatorima, Englezima i Francuzima (Andrew & Mitrokhin, 2000; Rid, 2019). Kroz istinu i činjenice, sovjetski KGB je nastojao da stvori nove ideološke okvire koji bi se suprostavili saradnji sa europljanima i bivšim kolonizatorima, te

[68] U ovom slučaju bitne su Huntingtonove teze o sukobu istoka i zapada, te najavi novih krstaških ratova, koje su se prvo očitovale u agresiji na Republiku Bosnu i Hercegovinu od Jugoslovenske narodne armije, a kasnije i takozvane vojske Republike srpske. Potvrdu za isto su dala i dva djela „Crno janje i sivi soko“ Rebbece West i „Balkanski duhovi“ Roberta Kaplana koji navode da je region prepun „zle krvi“ i da je potrebna katarza kroz etnički sukob u kome represovani pravoslavci traže odmazdu za osmansku vladavinu. Ova djela su bila obavezno štivo američki donosioca odluka koji su na osnovu njih prepustili sprskom agresoru da čini ratne zločine i genocid. Također, sukobi na Bliskom istoku kojima je prethodio teroristički napad 11. septembra 2001. godine su osnažili ideju nesklada između istoka i zapada, pri čemu su Huntingtonove teze bile gotovo proročanske. Započeo se novi krstaški rat hiljadama kilometara od judeo-kršćanskog svijeta opravdan tezom da terorizam arapa koji su nedavno zbacili jarm britanskog i francuskog kolonijalizma prijeti cijelom svijetu. Milioni ubijenih muslimana na Bliskom istoku, kao i stotine hiljada ubijenih palestinaca su dokaz da državno sponzorirana propaganda i aktivne mjere mogu promijeniti narativ te žrtvu prikazati kao zločinca.

okrenuli se prema socijalizmu koji ne vidi rasu, etnicitet i druge biološko-kulturološke različitosti. Danas kada se dezinformacije veoma jednostavno mogu raskrinkati, agresivni akteri koji provode aktivne mjere jednostavno kroz amplifikaciju istine i činjenica mogu postići značajan uspijeh, pri čemu je teško proizvesti kontranarativ i obrazložiti razloge za određene događaje. Iznošenje istine se planira u skladu sa drugim mjerama - propagandom, dezinformacijom, obmanom, plagijatom i tako dalje koji služe da se istina prikaže u sasvim drugom svjetlu.

6. Moderne tehnologije i aktivne mjere

Razvoj interneta i društvenih mreža je omogućio brzo širenje informacija, međutim, kada su informacije kompromitirane, maliciozne i fabrikovane, one u tom slučaju postaju političko oružje. Vijesti o ratovima, terorističkim napadima, političkim kampanjama i političkoj represiji, često imaju dvostruku ulogu, prva je da informira stanovništvo, a druga je da izazove određene osjećaje u društvu ili specifičnim društvenim skupinama koje je potrebno demoralizirati ili radikalizirati shodno strateškom cilju. Tehnologije poput interneta i društvenih mreža omogućile su da se novi front prenese u kognitivnu oblast odnosno ljudski mozak, pri čemu ljudski um postaju novo bojište. Društvene mreže poput X-a, Facebooka, Instagrama, Tik Toka, Reddita, 4Chana i sličnih, postaju mjesta na kojima se bore politički akteri, svaki sa ciljem kao što je radikalizacija ili demoralizacija.

Fenomen hibridnog rata koji je populariziran 2010. godine, navodi da je to sistem u kojem se koriste nekonvencionalne metode i sredstva u cilju podčinjavanja protivnika, pri čemu je dominantno odsustvo konvencionalne oružane sile. Military Balance Međunarodnog instituta za strateške studije (2015) opisao je ruski hibridni rat kao "upotrebu vojnih i nevojnih alata u integriranoj kampanji osmišljenoj za postizanje iznenađenja, preuzimanje inicijative i stjecanje psihološke kao i fizičke prednosti, korištenjem diplomatskih sredstava; sofisticirane i brze informacijske, elektroničke i kibernetičke operacije; tajno i povremeno otvoreno vojno i obavještajno djelovanje; i ekonomski pritisak". Dakle, novitet u ratovanju je upravo korištenje nevojnih efektiva koji dominiraju u cyber i informacionom prostoru. Širenjem i razvojem cyber prostora kao nove domene ljudskog života, omogućeno je obavještajno djelovanje i prikupljanje podataka i informacija (Muhić, 2024), a na osnovu toga i aktivno djelovanje.

Neki zapadni promatrači pokušali su shvatiti jesu li ruske metode na aneksiranom Krimu 2014. godine bile samo primjena takozvane Gerasimovljeve doktrine jer, u stvarnosti, Rusija formalno ne priznaje zapadni koncept hibridnog ratovanja, iako postoje ograničeni akademski spisi o tumačenju prevedenom kao *gibridnaya voyna* (Fridman, 2017). Dok se zapadni koncept uglavnom fokusira na vojne aktivnosti za postizanje sinergijskih učinaka, ruski pandan uključuje sve sfere

javnog života (Jasper, 2020). Shodno tome, rusi nisu provodili hibrirdni rat, već obavještajne aktivnosti koje pripadaju domenu aktivnih mjera i političkog nasilja. Upotreba „malih zelenih“[69] kako ih je nazvala zapadna štampa, je klasična jobaveštajna akcija upotrebe specijalnih jedinica bez oznaka kako bi se ostvario adekvatan nivo plauzabilnog negiranja. Na taj način, koordinacijom obavještanih, sigurnosnih, vojnih i političkih elementata, stvara se specifično okruženje u kojem protivnik i njegovi saveznici ne mogu reagovati brzo i na adekvatan način, te se strateški cilj postiže bez značajnijih gubitaka, bilo ljudskih ili političkih. Ove vrste akcija su bile prisutne i u prošlosti, kada je američka CIA koristila vlastite specijalne jedinice bez oznaka u raznim konfliktnim zonama, od Vijetnama, Paname pa sve do Afganistana, Iraka, Libije i Sirije.

Danas kada je ruska invazija na Ukrajinu u širokom zamahu, aktivne mjere, odnsno određeni nekinetički i nekonvencionalni aspekti rata se još uvijek primjenjuju poput trolovskih ili botovskih aktivnosti na društvenim mrežama. Trolovi i botovi kao „vojnici“ hibridnog rata imaju za cilj da određene narative poput ukrajinskog nacizma prošire i usidre u umove širom svijeta. Na taj način se omogućava daljnje vođenje rata i činjenje raznih zločina koji će biti opravdani dehumanizacijom ukrajinaca jer im je pripisana etiketa „nacista“.

Revizionizam i fabrikacija stvarnosti predstavlja jedan od primarnih zadataka trolova i botova na društvenim mrežama koji svoju snagu nalaze u brojnosti. Brojnost navedenih trolova i botova omogućava da se specifični narativ prikaže kao narativ društva jer je proširen i ima mnogo afirmacija u obliku likea, retweeta, upvotea ili plusa na domaćem portalu. Rat u ovom slučaju postaje hibridan, te prelazi i u domen kibernetičkog prostora koji je pogodan za druge oblike djelovanja poput hakerskih napada. Napasti preciznim projektilima ili raketama štab neprijatelja donosi mnogo benefita, međutim oni su skupi i zahtjevaju mnogo obavještajnog rada i aktivnosti, međutim hakerski napad mogu da se izvedu uvijek, bilo kada i bilo gdje, te da se pored uništenja infrasturkture pribave i štićene informacije koje neprijatelj ima. Evolucija rata je omogućila da on bude sveprisutan, širok i obiman. Aktivne mjere kao političko sredstvo djeluju sinergijski i sa pseudo-kinetičkim udarima unutar kibernetičkog svijeta.

[69] „Mali zeleni“, odnosno „little green men“ bili su maskirani ruski vojnici i pripadnici Spetsnaza koji su bez bez oznaka 2014. djelovali u Krimu prije i za vrijeme aneksije, čime im je Moskva osigurala međunarodnu „plauzibilno negiranje“ u učešću. Isto je omogućilo ruskoj diplomatiji da pregovara, vrši pritisak, obmanjuje, te provede sve strateški važne ciljeve na Krimu, dok je Zapad nastojao da pruži adekvatan politički odgovor, koji se na kraju nije ni desio.

7. Primjeri aktivnih mjera u savremenom političkog i geopolitičkom kruženju

7.1 Savremena reinterpretacija aktivnih mjera

Savremene aktivne mjere više se ne ispoljavaju kao striktno tajne operacije pod direktnom kontrolom jedne obavještajne službe, nego kao složen skup političkih, informacijskih i institucionalnih aktivnosti koje ciljaju na destabilizaciju protivnika ili kreiranje povoljnog političkog ishoda. Iako termin potječe iz sovjetskog doktrinarnog korpusa, njegove savremene varijante doživjele su značajnu transformaciju zahvaljujući digitalnoj tehnologiji, globalnoj međupovezanosti i mogućnosti angažiranja širokog spektra posrednih aktera. Umjesto monolitnih operacija koje je nekada provodio KGB, današnje aktivne mjere uključuju simultano korištenje propagande, koordiniranih digitalnih kampanja, pravnog pritiska, manipulacije društvenim podjelama, ekonomskih instrumenata i paradržavnih mreža koje djeluju izvan formalne državne strukture. Ovaj razvoj stvorio je operativno okruženje u kojem je sve teže razgraničiti granicu između legitimne političke komunikacije i prikrivenog pokušaja utjecaja. Prema Riddu (2020), savremene aktivne mjere zadržale su stratešku logiku klasičnih sovjetskih operacija, ali su postale vidljivije, brže i adaptabilnije zahvaljujući novim tehnološkim mogućnostima. Digitalne platforme omogućavaju precizno ciljanje publike, automatizaciju poruka i smanjenje rizika od atribucije, što državnim i nedržavnim akterima omogućava provođenje niza operacija koje formalno ostaju u „sivoj zoni“ između rata i mira.

Države sa dugom tradicijom specijalnih informacijsko-političkih operacija poput Rusije prilagodile su historijski model aktivnih mjera digitalnom dobu. Radovi Thomasa (2014) i Galeottija (2022) ukazuju da ruski pristupi danas uključuju integraciju državnih institucija, privatnih kompanija, medijskih mreža, plaćenih političkih operativaca i kriminalnih struktura koje djeluju kao produžena ruka strategije političkog utjecaja. Kina je prema istraživanjima Brady (2015) i Hamilton & Ohlberg (2020), razvila sofisticiran sistem „političkog oblikovanja okruženja“ kroz mreže partijskih organa, tehnoloških kompanija i dijasporskih organizacija, dok Iran i Turska razvijaju vlastite hibridne modele u kojima se aktivne mjere isprepliću s kulturnim, religijskim i regionalnim ambicijama (Axworthy, 2016; Coşkun, 2023)

U takvom okruženju savremene aktivne mjere više nisu izolirani incident političkog subverzionizma, nego kontinuirani proces u kojem države ulažu napore u oblikovanje narativa, manipulaciju percepcije prijetnje, stvaranje društvenih pukotina i jačanje svojih satelitskih struktura u inostranstvu. Ključna karakteristika ovog procesa jeste činjenica da se operacije izvode kroz višeslojne, decentralizirane i teško atribuirane kanale, što ih čini posebno pogodnim za geopolitička okruženja obilježena krizama, polarizacijom i informacijskim preopterećenjem.

7.2. Digitalno informacijsko okruženje kao poligon za aktivne mjere

Digitalno informacijsko okruženje postalo je ključni prostor za provođenje savremenih aktivnih mjera, jer omogućava simultano kreiranje, distribuciju i amplifikaciju političkih narativa uz minimalne troškove i uz znatno smanjen rizik od atribucije. Za razliku od tradicionalnih propagandnih tehnika, digitalne operacije koriste algoritamsku logiku društvenih mreža kako bi ciljale specifične grupe s visokom emocionalnom osjetljivošću, generirajući reakcije koje proizvode polarizaciju i mobilizaciju. Fenomen „emocionalnog angažmana“, koji neurorazumijevanje i kognitivna ograničenja publike pretvara u operativnu prednost, omogućava akterima da u kratkom vremenu kreiraju viralne narative koji se šire brže nego što ih institucije mogu detektovati i neutralisati. Također, u navedenom su ključne tri komunikološke teorije bez kojih uspješna operacija utjecaja ne može funkcionisati: McCombsova i Shawova (1972) agenda setting teorija, koja pokazuje kako mediji određuju o čemu publika misli; Entmanova (1993) teorija uokviravanja, koja naglašava moć oblikovanja interpretativnih okvira događaja; te Katzov i Lazarsfeldov (1955) model dvosmjernog toka komunikacije, koji pojašnjava ulogu opinion leadera, odnosno u savremenom kontekstu verificiranih naloga i političkih influensera koji amplificiraju i normaliziraju narativ. Upravo ova teorijska podloga omogućava razumijevanje zašto digitalne operacije utjecaja ne djeluju linearno niti isključivo putem jedne poruke, nego kroz mrežu mikro-interakcija koje kumulativno proizvode politički efekt. Operativni akteri ciljaju emocionalne predispozicije publike, koriste opinion leadere za legitimizaciju narativa i oslanjaju se na algoritamske preporuke koje pojačavaju sadržaje s visokim angažmanom, čime se stvaraju tzv. „informacijski baloni“ u kojima narativi aktivnih mjera postaju dominantni. Ovakva dinamika omogućava da operacija traje kontinuirano, bez potrebe za centraliziranom komandom, jer se jednom plasirani narativ održava kroz spontano sudjelovanje korisnika, automatizirane mreže i političke aktere koji ga preuzimaju u sopstvenom interesu. Time digitalno okruženje postaje ne samo kanal distribucije, nego i aktivni akcelerator političkog utjecaja, u kojem se granica između manipulisane i organske komunikacije sve teže razaznaje.

Savremene digitalne aktivne mjere obično se sastoje od tri međusobno povezana sloja (Tabela 2). Prvi sloj podrazumijeva proizvodnju sadržaja koja se kreće od sofisticiranih propagandnih videa i manipulisanih fotografija do memova dizajniranih za emotivnu reakciju. Drugi sloj čini automatizirana distribucija kroz botovske mreže, lažne profile i koordinirane online zajednice koje služe kao mehanizam amplifikacije. Treći sloj predstavlja pojačavanje dosega putem influensera, alternativnih medija i političkih aktera koji svjesno ili nesvjesno preuzimaju i šire narativ, što digitalnu operaciju čini društveno „normalizovanom“.

Tabela 2 Slojevi savremenih digitalnih aktivnih mjera

Sloj	Opis	Prošireni primjeri aktivnosti
1. Proizvodnja sadržaja	Kreiranje izvornog materijala dizajniranog da pokrene emocionalnu reakciju, oblikuje narativ ili generira pažnju.	Produkcija propagandnih videa visokog emocionalnog naboja; manipulirane ili „deepfake“ fotografije i snimci; memovi koji pojednostavljuju kompleksne političke teme; fabricirani članci i „istraživačke priče“ bez izvora; kreiranje lažnih ekspertskih analiza; selektivna prezentacija procurenih dokumenata
2. Automatizirana distribucija	Širenje i amplifikacija sadržaja putem tehničkih i organiziranih mehanizama koji povećavaju vidljivost i privid „organskog“ dosega.	Upotreba botovskih mreža za masovno dijeljenje sadržaja; koordinirane kampanje kroz stotine lažnih profila; automatizirani komentari koji stvaraju privid konsenzusa ili kontroverze; orkestrirane aktivnosti unutar zatvorenih grupa na Telegramu, WhatsAppu i Discordu; kreiranje lažnih trending tema; manipulacija algoritmima preporuka na platformama kao što su YouTube i TikTok.
3. Pojačavanje dosega (amplifikacija)	Legitimacija i normalizacija narativa kroz utjecajne aktere koji ga prenose široj publici, često nesvjesno, čime se operacija učvršćuje u javnom prostoru.	Distribucija narativa preko influensera, političkih komentatora i provladinih novinara; preuzimanje sadržaja od strane alternativnih medija i portala koji objavljuju senzacionalističke verzije; širenje kroz političke organizacije i interesne grupe; „organically looking“ preuzimanje narativa od javnih ličnosti, ekstremističkih grupa ili dijasporskih mreža.

Brojna istraživanja, uključujući radove Bolover & Howarda (2017) i Haile (2024), pokazuju da su uspješnost i trajanje digitalne operacije manje određeni tehničkim kapacitetima, a daleko više sposobnošću narativa da se uklopi u postojeće društvene polarizacije.

Specifičnost digitalnih aktivnih mjera jeste njihova sposobnost da funkcionišu kao „simultane kampanje“, u kojima stotine malih poruka proizvode kumulativni efekat. Državni akteri poput Rusije, Kine, Irana, Izraela ili Sjednjenih Amerčkih Država intenzivno koriste ovu dinamiku, ali i nedržavni akteri kao što su razne ekstremističke grupe, političke partije i komercijalni subjekti. Digitalni prostor omogućava kreiranje tzv. „informacijskog šuma“, gdje je cilj ne samo plasirati dezinformaciju nego i potopiti javni prostor tolikim brojem kontradiktornih narativa da publika više ne može razlikovati relevantne informacije od konstrukcija. Kao što ukazuju Wardle i Derakhshan (2017), cilj savremenih informacijskih operacija nije samo uvjeravanje, nego prvenstveno erozija

povjerenja, zbunjivanje i stvaranje osjećaja da su svi izvori jednako nepouzdani. Digitalna infrastruktura omogućava i drugačije forme aktivnih mjera, uključujući hakovanje informacija i njihovo selektivno objavljivanje, manipulaciju algoritmima preporuka, eksternu kontrolu digitalnih platformi kroz investicije i regulaciju, te upotrebu vještačke inteligencije za kreiranje uvjerljivog lažnog sadržaja (deepfake, voice-cloning, synthetic actors). Studije NATO StratCom COE (NATO StratCom COE, 2020) ukazuju da su tehnike manipulacije digitalnog prostora postale toliko sofisticirane da više ne zahtijevaju masovne bot mreže, nego precizno dizajnirane mikro kampanje koje ciljaju emocionalno najosjetljivije segmente populacije. Savremeni trendovi pokazuju da digitalne aktivne mjere imaju dvije ključne prednosti, a to su skalabilnost i replikabilnost. Jednom proizveden narativ može se ponovo aktivirati u različitim političkim kontekstima, dok se tehničke infrastrukture (bot mreže, lažni portali, koordinirane grupe) mogu koristiti za više operacija istovremeno. Time digitalni prostor postaje produžetak političkog i geopolitičkog nadmetanja, u kojem se informacija tretira kao oružje, a percepcija kao najvažniji strateški resurs.

7.3. Ruske aktivne mjere nakon 2014. godine

Ruske aktivne mjere nakon 2014. godine predstavljaju najvidljiviji savremeni primjer integrisanog modela političko-informacijskog djelovanja, u kojem se klasične metode sovjetske subverzije prepliću sa digitalnim instrumentima, ekonomskim pritiscima i obavještajnim aktivnostima. Aneksija Krima i početak rata na istoku Ukrajine označili su trenutak u kojem Rusija prelazi sa tradicionalne politike utjecaja na strategiju sistemskog oblikovanja međunarodnog okruženja. Brojni autori, uključujući Galeottija (2022), Kilcullena (2020) i Rida (2020), ističu da ovaj period obilježava formalizacija „nelinearnog ratovanja“ kao centralnog ruskog pristupa, u kojem se informacijske operacije, cyber aktivnosti i diplomatski potezi provode istovremeno i komplementarno.

Digitalna dimenzija ruskih aktivnih mjera pokazala se posebno izraženom u nizu operacija koje su ciljale političke procese u Sjedinjenim Američkim Državama, Evropskoj uniji i postsovjetskom prostoru. Najpoznatiji primjer je američka predizborna kampanja 2016. godine, koju su istraživali američki Kongres, FBI i specijalni tužilac Robert Mueller. Aktivnosti Internet Research Agency (IRA) iz Sankt Peterburga, opisane u izvještajima Muellerove istrage (2019), uključivale su kreiranje hiljada lažnih profila, koordinirane kampanje za polarizaciju biračkog tijela, ciljane poruke za Afroameričke zajednice i infiltraciju u online forume s ciljem kreiranja umjetnog osjećaja političke fragmentacije. Slične operacije dokumentirane su tokom referenduma o Brexitu, izbora u Francuskoj, Njemačkoj, Italiji i nizu balkanskih država. Pored digitalnih operacija, ruske aktivne mjere nakon 2014. uključuju sofisticiranu kombinaciju energetskog pritiska, podrške političkim i ekstremističkim grupama, upotrebe diplomatije i paradržavnih mreža. Energetska ovisnost pojedinih evropskih država koristila se kao poluga za oblikovanje njihovih političkih odluka, dok su obavještajne službe, prema

procjenama EUROPOL-a i NATO-a, intenzivirale aktivnosti usmjerene na infiltraciju u nacionalne institucije, partije i medijske organizacije. Uloga ruskih medijskih kuća, poput RT-a i Sputnika, analizirana u radovima Yablokova i Chatterjeea (2022), pokazuje kako se propagandni i polu-propagandni sadržaji plasiraju kroz multimedijalne platforme, često kombinovane s lokalnim desničarskim, populističkim ili euroskeptičnim narativima. U postsovjetskom prostoru, posebno u Ukrajini, Gruziji i Moldaviji, ruske aktivne mjere funkcionišu kao dio šireg modela specijalnih operacija u kojima se informacijska, vojna i politička komponenta prepliću. Prema istraživanjima Lange-Ionatamišvili (2015), Kostyrev (2023) i drugih, Rusija je koristila digitalne kampanje za delegitimizaciju ukrajinskih institucija, selektivno objavljivanje hakovanih materijala, psihološke operacije usmjerene na vojnike i civile, te kreiranje lažnih izvještaja o ratnim zločinima nad ruskim stanovništvom kako bi se stvorila moralna konfuzija i narušila međunarodna podrška. Ove operacije nisu bile *ad hoc*, već dio dugoročne strategije čiji je cilj oblikovanje percepcije o Ukrajini kao disfunkcionalnoj državi ovisnoj o stranim akterima. Na Balkanu se ruski utjecaj manifestuje kroz kombinaciju političkog patronata, obavještajnog djelovanja i podrške medijima i organizacijama koje promovišu anti-NATO i anti-EU narative. Operacije u Crnoj Gori 2016. godine, uključujući pokušaj destabilizacije vlasti i sprječavanja pristupanja NATO-u, imaju sve elemente klasičnih aktivnih mjera od infiltraciju u političke strukture, podršku radikalnim grupama, kampanje dezinformacija pa sve do uske koordinacije sa lokalnim akterima. U Bosni i Hercegovini, Crnoj Gori, kao i Srbiji, ruski narativi se šire kroz medijske kanale, vjerske institucije i političke aktere koji zagovaraju neutralnost, oslanjajući se na emocionalno snažne teme iz historije i kolektivnog identiteta.

7.4. Izraelske aktivne mjere u savremenom političkom i geopolitičkom okruženju

Izraelske aktivne mjere karakterizira jedinstvena kombinacija sofisticirane obavještajne arhitekture, tehnološke nadmoći i globalnih političkih mreža, što ih čini specifičnim oblikom operativnog djelovanja u savremenom međunarodnom okruženju. Za razliku od ruske ili kineske doktrine, izraelski pristup ne počiva prvenstveno na masovnim informacijskim operacijama, već na visoko ciljanim, precizno usmjerenim aktivnostima koje spajaju obavještajni rad, diplomatski pritisak, cyber operacije i globalno utjecajne narative o sigurnosnim prijetnjama, antiterorizmu i legitimnosti odbrambenih akcija. Ove operacije naglašavaju proaktivnu kontrolu informacija i oblikovanje percepcije o izraelskim sigurnosnim potrebama, što ih smješta u okvir specijalnih mjera namijenjenih upravljanju krizama i stvaranju političkog prostora za djelovanje. Jedna od ključnih karakteristika izraelskih aktivnih mjera jeste upotreba tehnoloških instrumenata i cyber kapaciteta kroz aktivnosti službi kao što su Mossad, Aman i Shin Bet. Izrael se u relevantnoj literaturi (Clarke & Knake, 2019; Bergman, 2018) opisuje kao jedna od najnaprednijih država u pogledu cyber operacija,

uključujući ofanzivne i defanzivne aktivnosti, te upotrebu digitalnih alata za nadzor protivničkih i savezničkih struktura. U tom kontekstu, udružena cyber operacija koja je ciljala iranska nuklearna postrojenja u Natanzu pomoću „Stuxnet" kompjuterskog virusa se često navodi kao najpoznatiji primjer sofisticirane aktivne mjere koja kombinuje cyber napad, političku poruku i strateško odvraćanje. Ovakav model pokazuje da Izrael ne koristi digitalni prostor primarno za masovne operacije utjecaja, nego za precizne, visokorizične operacije s jasnim geopolitičkim ciljem.

Informacijske operacije Izraela fokusirane su na oblikovanje međunarodne percepcije konflikta izraelsko-palestinskih odnosa, sigurnosnih prijetnji i legitimiteta izraelskih vojnih operacija. U digitalnom prostoru, Izrael koristi dvoslojni pristup. Prvi sloj uključuje institucionalne komunikacijske kampanje Ministarstva vanjskih poslova, IDF-a i vladinih glasnogovornika koji brzo distribuiraju (dez)informacije, vizualne materijale, infografike i video zapise predstavljene kao faktografski i transparentni prikazi događaja. Drugi sloj obuhvata mrežu domaćih i stranih (pretežno američkih) procionističkih nevladinih organizacija, lobističkih grupa, dijasporskih zajednica i think tankova koji preuzimaju ulogu „amplifikatora" poruka, često s fokusom na delegitimizaciju kritika Izraela kroz narative o antisemitizmu, ekstremizmu i dezinformacijama. Prema analizi Yaquba i Tabassuma (2025), ovaj model funkcioniše kao sofisticirana verzija „strategijskog narativnog okvira" koji nastoji zadržati međunarodnu podršku kroz redefiniranje interpretativnih kategorija konflikta. U tom sistemu posebno se ističe izraelska hasbara, institucionalno utemeljen mehanizam strateške komunikacije koji kombinuje diplomatske resurse, digitalne platforme i široku mrežu aktera iz civilnog sektora. Hasbara se ne svodi samo na objašnjavanje politike, već djeluje kao koordinirani aparat za oblikovanje percepcije, u kojem se koriste profesionalni komunikatori, PR agencije i ciljane kampanje namijenjene stranim javnostima.

Brojne istrage međunarodnih medijskih konzorcija ukazuju da Izrael i povezane organizacije angažuju i finansiraju različite influensere, youtubere i online kreatore sadržaja čija je uloga amplifikacija službenih narativa, neutralizacija kritika i stvaranje privida široke međunarodne podrške izraelskim operacijama, te iste plaća po nekoliko hiljada američkih dolara (Middle East Monitor, 2025). Ovaj model uključuje i praksu sistematskog negiranja ili reinterpretacije zločina, što se posebno manifestuje na društvenim mrežama. Bez obzira na objavljene satelitske snimke, geolocirane dokaze, izvještaje međunarodnih organizacija ili forenzički potvrđene materijale o ubijenim civilima, izraelski komunikacijski aparat često primjenjuje strategije osporavanja kroz tvrdnje da su dokazi „fabricirani", „montirani" ili „proizvedeni u propagandne svrhe".[70] Ovakav pristup ima za cilj

[70] Za više vidjeti objave zvaničnih naloga IDF-a, Ministarstva vanjskih poslova i raznih zvaničnih izraelskih političkih aktera na društvenoj mreži X. U navedenom je primjetan diskurs

da naruši pouzdanost nezavisnih izvora i proizvede stanje epistemološke konfuzije u kojem publika više ne može razlikovati vjerodostojne informacije od propagandno rekonstruiranih narativa.

7.5. Aktivne mjere Sjedinjenih Američkih Država u savremenom geopolitičkom okruženju

Američke aktivne mjere predstavljaju specifičan model operacija utjecaja koji kombinira obavještajne kapacitete, diplomatsku moć, tehnološku dominaciju i globalnu infrastrukturnu prisutnost. Za razliku od tradicionalnih sovjetskih ili savremenih ruskih aktivnih mjera, koje često funkcionišu kao prikrivene subverzione aktivnosti, američki model u velikoj mjeri počiva na formaliziranim instrumentima "soft power", strateškoj komunikaciji, digitalnim kampanjama, partnerstvima s tehnološkim kompanijama i institucionalnim mehanizmima koji omogućavaju utjecaj bez formalnog narušavanja međunarodnih normi. Ipak, deklasifikovani dokumenti CIA-e, izvještaji Senata i brojni akademski radovi ukazuju da su Sjedinjene Države decenijama provodile širok spektar aktivnih mjera od psiholoških operacija do političke inženjeringa s ciljem oblikovanja globalnog poretka u skladu s američkim strateškim interesima (Bloom, 2003; Prados, 2006).

Historijski posmatrano, američke aktivne mjere obuhvataju operacije usmjerene na utjecanje na izbore, destabilizaciju režima, podršku opozicijama i širenje proameričkih narativa. Najpoznatiji primjeri su operacije CIA-e tokom Hladnog rata, uključujući Iran 1953. godine, Gvatemalu 1954., Čile 1973. godine, pa sve do podrške antikomunističkim pokretima i medijskim kampanjama širom Istočne Evrope. Deklasifikovani dokumenti ukazuju da su ove operacije kombinovale psihološke operacije (PSYOP), finansiranje političkih aktera, kontrolu medijskih narativa i oblikovanje percepcije o američkoj ulozi u svijetu. U tom smislu, američki pristup karakteriše visoka institucionalna koordinacija i sposobnost integracije obavještajnih, ekonomskih i diplomatskih instrumenata u jedinstvenu operativnu cjelinu. Savremene američke aktivne mjere sve više se oslanjaju na digitalne platforme, tehnološki sektor i institucionalizirane kapacitete strateške komunikacije. Programi kao što su Global Engagement Center (GEC) pri State Departmentu, USAID-ove demokratske inicijative sve do njihovog ukidanja 2025. godine, NATO-ovi strateški komunikacijski centri i različiti javno-privatni partneri imaju ključnu ulogu u oblikovanju globalnih narativa, posebno u zemljama koje se suočavaju s autoritarnim utjecajima. Prema Brooks & Wohlforth (2016), američki narativni okvir temelji se na promociji demokratskih vrijednosti, ljudskih prava, ekonomske otvorenosti i sigurnosne saradnje. Iako ove inicijative formalno pripadaju domenu javne diplomatije, u praksi

koji se kreće od negiranja genocida pa sve do potvrđivanja istog, te obećanja da će se genocid nastaviti u budućnosti.

funkcionišu kao koordinirane operacije utjecaja koje oblikuju percepciju saveznika, partnera i javnosti širom svijeta.

Značajan element modernih američkih aktivnih mjera odnosi se na upotrebu tehnoloških kompanija kao nenametljivih, ali izuzetno moćnih amplifikatora. Američke firme poput Meta, Googlea i X Corp posjeduju infrastrukturu koja posredno utiče na političku dinamiku mnogih država, kroz algoritamsko rangiranje sadržaja, uklanjanje (dez)informacija i kontrolu online narativa. Razne istrage[71] pokazale su da postoji kontinuirana komunikacija između američkih sigurnosnih agencija i velikih tehnoloških platformi, posebno u kontekstu borbe protiv terorizma, stranog utjecaja i malignih kampanja. Ovaj odnos je temelj za operacije koje omogućavaju filtriranje, prioritetno isticanje ili suzbijanje određenih političkih sadržaja, što mnogi autori smatraju „strukturnom aktivnom mjerom" 21. stoljeća (Tufekci, 2015; Greenwald, 2020).

Američke aktivne mjere uključuju i sofisticirane oblike *lawfare*-a, posebno kroz sankcionisanje pojedinaca, institucija i država, kao i upotrebu međunarodnih normativnih mehanizama kao instrumenta pritiska[72]. Iako se sankcije često predstavljaju kao alat vanjske politike, one djeluju kao aktivne mjere jer ciljaju promjenu političkog ponašanja, izazivanje pritiska javnosti ili fragmentaciju elita. Paralelno s tim, američke obavještajne službe nastavljaju koristiti ciljane psihološke operacije i informacijske kampanje, naročito u kontekstu borbe protiv terorizma i ekstremističkih grupa, gdje narativni prostor postaje jednako važan kao i operativna djelovanja na terenu.

7.6. Komparativni prikaz aktivnih mjera i obavještajnih aktivnosti SAD-a, Rusije i Izraela

Komparativna analiza aktivnih mjera u savremenom međunarodnom okruženju omogućava razumijevanje različitih strategijskih pristupa koje države koriste kako bi ostvarile političku i sigurnosnu prednost bez oslanjanja na otvorenu primjenu vojne sile. Rusija, Izrael i Sjedinjene Američke Države predstavljaju tri paradigmalno različita modela u primjeni aktivnih mjera, pri čemu svaki od njih odražava specifičnu kombinaciju historijskih iskustava, institucionalnih

[71] U prošlosti dok je X bio pod vlasništvom Jack Dorsya i zvao se Twitter, operacije utjecaja su bile primjente i služile su kao amplifikator moći Sjedinjenih Američkih Država. Istraživači su otkrili da američka Centralna komanda (CENTCOM) provodila je koordinirane informacione operacije koristeći društvenu mrežu Twitter, uz direktnu tehničku podršku same platforme. Na zahtjev zvaničnika Pentagona, Twitter je tzv. "whitelistovao" više desetina arapskih naloga povezanih s američkom vojskom, čime im je omogućeno da izbjegnu algoritamsku detekciju i zabrane (Fang, 2022).

[72] Primjer upotrebe pravnih instrumenata u svrhu ograničavanja širenja određenih narativa vidljiv je u slučaju američkog influensera Evana Kilgorea. Protiv njega i nekolicine drugih influensera su direktor FBI-a i njegova partnerka pokrenuli niz tužbi nakon što su na društvenim mrežama iznesene tvrdnje da je partnerka direktora navodno povezana s izraelskim Mossadom te je insinuirano da je njihova veza rezultat takozvane „honeypot" operacije.

kapaciteta i geopolitičkih ciljeva (Tabela 3). Razlike među njima nisu samo metodološke, već i doktrinarne, jer svaki akter drugačije pristupa kreiranju narativa, upravljanju informacijama, subverziji političkih procesa i oblikovanju kognitivnog okruženja u ciljanom društvu.

Tabela 3 Komparacija ruskih, izraelskih i američkih pristupa aktivnim mjerama i političkom nasilju

Dimenzija	**Rusija**	**Izrael**	**Sjedinjene Američke Države**
1. Doktrinarni okvir	Tradicija „aktivnih mjera" KGB-a i modernog „hibridnog rata"; strateški fokus na destabilizaciju protivnika kroz dugotrajne, prikrivene operacije.	Model *hasbare*, strateške komunikacije i preventivne operacije Mossada; spajanje klasičnih PSYOP-a s digitalnim operacijama i globalnim narativnim kampanjama.	Doktrina „demokratske ekspanzije", meke moći i digitalnih PSYOP operacija; operacije u funkciji širenja američkog međunarodnog poretka.
2. Primarni strateški cilj	Erozija unutrašnje stabilnosti protivnika i slabljenje NATO/EU okvira; stvaranje „sigurnosnih praznina" koje Rusija može iskoristiti.	Zaštita državnog imidža, delegitimizacija kritičara, neutralizacija političkih prijetnji i globalno oblikovanje percepcije sukoba.	Jačanje globalne hegemonije, upravljanje političkim tokovima u drugim državama i podrška povoljnim režimima ili pokretima.
3. Glavni instrumenti	Dezinformacijske kampanje; infiltracija partija i pokreta; finansiranje ekstremističkih grupa; politička subverzija; cyber napadi; atentati.	Plaćeni influenseri; digitalne hasbara mreže; ciljane PR kampanje; globalne „image management" operacije; specijalne operacije Mossada.	Obavještajna podrška savezničkim pokretima; PSYOP jedinice vojske; USAID meka moć; kontrola globalnih medija; digitalni nadzor.
4. Operativni pristup	„Dugotrajno podgrijavanje" konflikta; latentne operacije niskog intenziteta; stvaranje unutrašnjih pukotina i društvene atomizacije.	Visokointenzitetno digitalno djelovanje; brza amplifikacija narativa; kombinacija javne i tajne diplomatije; diskreditacijske kampanje.	Upravljački pristup zasnovan na višefaznim operacijama; kombinovanje javnih politika, obavještajnog djelovanja i legalnih struktura.

5. Ciljani akteri	Susjedne države, NATO članice, slabije demokracije, manjinske grupe, opozicija, mediji.	Globalna javnost, međunarodne organizacije, influenseri, analitičari, akademske zajednice, politički akteri koji kritikuju izraelsku politiku.	Države u tranziciji, saveznici pod pritiskom, autoritarni režimi u regionima od strateške važnosti, rivalske sile.
6. Tipične operacije	Kampanje protiv ukrajinske Vlade, trovanje i ubistva bivših FSB službenika, organiziranje separatističkih pokreta.	Digitalne PR kampanje o sukobu u Gazi; agresivno negiranje ratnih zločina; targetiranje novinara i NVO; specijalne „preventivne likvidacije“.	Podrška pokretima tokom Hladnog rata; „color revolutions“ model; anti-ISIS digitalne kampanje; specijalne operacije CIA-e.
7. Intenzitet i obim djelovanja	Srednji do visok; visok volumen dugoročnih operacija usmjerenih na stratešku eroziju političkih sistema.	Visok; intenzivna, brza i globalno usmjerena digitalna i informacijska dominacija uz nisku toleranciju na reputacijski rizik.	Varira; često srednji intenzitet uz širok obim operacija koje se provode kroz institucionalne mehanizme.
8. Političke posljedice za ciljana društva	Podjele, secesionistički pokreti, slabljenje demokratije, pad povjerenja u institucije, destabilizacija.	Zasićenje informativnog prostora, normalizacija narativa, prikrivanje ratnih zločina, pritisak na medije i akademiju.	Promjena režima, prilagođavanje vanjske politike, zavisnost od američkih struktura moći, narativna transformacija.
9. Stupanj prikrivenosti	Visok; operacije se često kreiraju tako da izgledaju kao spontani unutrašnji procesi.	Srednji; kombinacija prikrivenih aktivnosti i javno orkestriranih PR kampanja.	Varijabilan; od potpuno tajnih operacija CIA-e do javno deklarisanih „demokratskih projekata“.
10. Dominantna sfera djelovanja	Informacijski, politički, vojno-obavještajni i cyber prostor.	Digitalni prostor, diplomatska arena, globalni mediji i mreže influensera.	Diplomatska i ekonomska sfera, podrška pokretima, digitalni PSYOP, globalni mediji.

Ruski model aktivnih mjera karakterizira historijska kontinuitet sovjetske „subverzivne škole“ i savremene doktrine hibridnog rata. Njegova osnovna pretpostavka je da se politička destabilizacija protivnika može postići dugotrajnim, slojevitim i višefaznim operacijama usmjerenim na eroziju povjerenja u institucije, poticanje društvenih podjela i stvaranje političke dezorijentisanosti. Obavještajne službe Rusije koriste instrumente širokog spektra

koji obuhvataju informacijske kampanje, infiltriranje političkih aktera, finansiranje ekstremističkih skupina, podršku separatističkim pokretima i izvođenje atentata. Intenzitet ovih mjera je srednji do visok, obim uključuje istovremeno djelovanje u političkom, informativnom i vojno-obavještajnom sektoru, dok volumen operacija podrazumijeva dugotrajno održavanje destabilizirajućih procesa na više geografskih i institucionalnih frontova.

Izraelski pristup aktivnim mjerama posjeduje distinktivan karakter zasnovan na doktrinarnom spoju strateških komunikacija, digitalnih operacija i preventivnog djelovanja Mossada. Savremeni koncept hasbare pretvorio se u globalni sistem orkestriranog upravljanja percepcijom koji uključuje intenzivnu upotrebu društvenih mreža, amplifikaciju narativa kroz utjecajne pojedince, profesionalne PR kampanje i agresivne komunikacijske modele usmjerene na neutralizaciju kritičkih glasova. Izraelske aktivne mjere imaju visok intenzitet i mali vremenski prag djelovanja, obimno pokrivaju međunarodni informacijski prostor, a volumen operacija je fleksibilan i skalabilan u zavisnosti od reputacijskog rizika ili trenutnih političkih potreba. Ovakav pristup omogućava brzo stvaranje narativne dominacije i uspostavljanje kognitivne kontrole u globalnom diskursu.

Američki model aktivnih mjera najvećim dijelom se oslanja na spoj meke moći, institucionalne moći i digitalnih psiholoških operacija. U svojoj suštini, američke operacije su projektovane da podrže i reprodukuju postojeći međunarodni poredak u kojem SAD imaju dominantnu ulogu. To podrazumijeva višefazne operacije koje uključuju obavještajnu podršku partnerskim režimima, upotrebu PSYOP jedinica, aktiviranje mreža poput USAID-a, Naionalne zaklade za demokratiju (NED), Međunarodnog republikanskog instituta (IRI) i Nacionalnog demokratskog instituta (NDI), te digitalno djelovanje usmjereno na upravljanje politčkim narativima u državama od strateškog značaja. Intenzitet američkih aktivnih mjera je varijabilan, obim je širok jer obuhvata istovremeno djelovanje na diplomatskom, medijskom, tehnološkom i političkom nivou, dok volumen zavisi od procjene rizika, prioriteta i dugoročnih geopolitičkih interesa.

Uporedni prikaz tri modela pokazuje da svaki akter koristi aktivne mjere kao instrument političkog nasilja u specifičnom operativnom okruženju, pri čemu razlike u doktrini i institucionalnoj kulturi određuju način primjene i efikasnost ovih mjera. Rusija nastoji destabilizirati protivnika stvaranjem dugotrajnih strukturalnih slabosti; Izrael teži uspostaviti narativnu dominaciju i reputacijsku kontrolu; dok SAD primjenjuju širok spektar instrumenata sa ciljem održavanja globalnog poretka koji im je povoljan. Upravo zbog te diverzifikacije pristupa, savremene aktivne mjere nisu uniformna kategorija, već spektrum političko-obavještajnih aktivnosti čija se primjena stalno prilagođava dinamici međunarodne politike, tehnološkim promjenama i potrebama strateškog djelovanja na globalnoj sceni.

8. Zaključak

Moderni svijet obilježen je paralelnim postojanjem vidljivih i nevidljivih ratova, pri čemu ovi drugi često proizvode dalekosežnije posljedice jer djeluju izvan fizičkog prostora i agresiju preusmjeravaju u sferu uma, percepcije i kolektivne svijesti. Aktivne mjere predstavljaju ključno oružje takvog latentnog rata, budući da omogućavaju manipulaciju stvarnošću, preoblikovanje društvene zbilje i usmjeravanje političkog ponašanja ciljane populacije. Maliciozne političke aktivnosti poput propagande, indoktrinacije i subverzije nisu puki prateći elementi političkih konflikata, već mehanizmi sistematskog porobljavanja neprijateljskog društva koje se posmatra kao resurs koji treba preuzeti, asimilirati i kroz vrijeme potpuno integrisati u interese agresivnog aktera. Upravo zbog toga se aktivne mjere nakon Hladnog rata vraćaju na centralnu poziciju obavještajno-operativnog djelovanja i postaju primarni instrument savremenog specijalnog rata.

Ključna prednost aktivnih mjera ogleda se u njihovoj sposobnosti da djeluju nevidljivo i nenametljivo, bez upotrebe fizičkog nasilja koje bi generisalo reakciju, otpor i nacionalno ujedinjenje. Za razliku od konvencionalnog rata koji izaziva koheziju napadnutih, nekonvencionalno djelovanje proizvodi suprotan učinak. Ono atomizira društvo, produbljuje postojeće tenzije i amplificira razlike zasnovane na rasi, klasi, političkoj orijentaciji, identitetu ili obrazovanju, čime se stvaraju uslovi za unutrašnje fragmentacije koje postaju funkcionalne agresoru. Napadnuto društvo se pritom ne urušava kao posljedica spoljne sile, već kao rezultat vlastitih unutrašnjih lomova, induciranih i koordiniranih spolja. Upravo u tome leži sofisticiranost političkog nasilja provedenog aktivnim mjerama: umjesto da razara tijelo, ono razara sposobnost zajednice da kritički misli, racionalno odlučuje i održava političku koheziju. Savremeno digitalno okruženje dodatno je multiplikovalo moć aktivnih mjera, omogućivši da identiteti, percepcije i narativi cirkulišu mnogo brže i agresivnije nego u prošlim epohama. Društvene mreže postale su novo bojno polje na kojem se konstruiraju lažni konflikti, radikaliziraju marginalne grupe i stvaraju pseudo-pokreti bez stvarnog idejnog uporišta, što agresivnim akterima otvara prostor za orkestrirano djelovanje. Ovaj fenomen nije nov. Već tokom Hladnog rata Sovjetski Savez je infiltrirao i podržavao različite društvene pokrete u Sjedinjenim Američkim Državama kako bi potkopao društvenu koheziju i narušio legitimnost političkog sistema. Danas se isti obrasci repliciraju, ali kroz sofisticiranije digitalne i kognitivne platforme koje omogućavaju dublju i bržu penetraciju u društvenu strukturu napadnutih zajednica.

Iako se aktivne mjere sastoje od širokog spektra aktivnosti, njihova centralna osovina ostaje u dezinformaciji koja omogućava formiranje novog društveno-političkog narativa kroz plasiranje lažnih, fabriciranih i manipulativnih

informacija. Sovjetske operacije poput „Denver“ i „Pandora“ ostale su trajno zabilježene kao primjeri uspješnog subverzivnog djelovanja, dok savremeni digitalni prostor svakodnevno generira nove dezinformacijske kampanje koje nalaze svoju publiku i iznova proizvode politički poremećaj. U tom smislu, dezinformacija nije samo tehnika, nego temeljni alat za postizanje strateških promjena unutar ciljane zajednice.

Dakle, aktivne mjere predstavljaju moćno oružje specijalnog rata kojim se induciraju unutrašnji konflikti, proizvodi društvena konfuzija i potkopava sposobnost političke zajednice da racionalno djeluje. Njihov krajnji cilj nije samo oslabiti stanovništvo, već ga transformisati u docilnu, pasivnu i međusobno sukobljenu masu koja nesvjesno ostvaruje interese agresora. Takvo stanje pruža dovoljno prostora za nesmetanu realizaciju drugih političkih, ekonomskih i obavještajnih aktivnosti koje dugoročno mijenjaju strukturu moći, suverenitet i političku arhitekturu napadnutog društva. Aktivne mjere stoga nisu samo prateći element savremenog sukobljavanja, nego centralni instrument političkog nasilja i temeljni mehanizam savremenih obavještajno-operativnih strategija.

LITERATURA

Andrew, C., & Mitrokhin, V. (2000). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of KGB.* Basic Books.

Axworthy, M. (2016). *Revolutionary Iran: A History of the Islamic Republic.* Oxford: Oxford University Press.

Bergman, R. (2018). *Rise and Kill First: The Secret History of Israel's Targeted Assassinations.* New York: Penguin Random House LCC.

Bezmenov, Y. A. (1985). Soviet Subversion of The Free World. (G. E. Griffin, Voditelj intervjua) Preuzeto od https://youtu.be/sQN4c3uN_tA

Bloom, W. (2003). *Killing Hope.* London: Zed Books.

Bolsover, G., & Howard, P. (2017). Computational Propaganda and Political Big Data: Moving Toward a More Critical Research Agenda. *Big Data*.

Brady, A.-M. (2015). China's Foreign Propaganda Machine. *Journal of Democracy*, 51-59.

Brooks, S. G., & Wohlforth, W. C. (2016). *America Abroad: The United States' Global Role in the 21st Century.* Oxford : Oxford University Press.

Buzan, B. (1983). *People, States and Fear: National Security Problem in International Relations.* Brighton, Sussex: Wheatsheaf Books.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain - Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* New Yokr: Penguin Press.

CNN. (10. 05 2000). *Inside the KGB - An interview with retired KGB Maj. Gen. Oleg Kalugin*. Preuzeto od CNN Interactive: http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/

Coşkun, A. (22. 06 2023). *Continuity and change in Turkish foreign policy*. Preuzeto od Atlantic Council: https://www.atlanticcouncil.org/content-series/ac-turkey-defense-journal/continuity-and-change-in-turkish-foreign-policy

Donnelly, J. (2006). Sovereign Inequalities and Hierarchy in Anarchy: American Power and International Society. *European Journal of International Relations*, 139-170.

Entman, R. M. (1993). Framing: Toward Clarification of a Fractured Paradigm . *Journal of Communication*, 51–58.

Fang, L. (20. 12 2022). *Twitter Aided the Pentagon in Its Covert Online Propaganda Campaign*. Preuzeto od The Intercept: https://theintercept.com/2022/12/20/twitter-dod-us-military-accounts

Fridman, O. (2017). Hybrid Warfare or Gibridnaya Yoyna? *RUSI Journal 162, no. 1*, 42-49.

Galeotti, M. (2019). Active Measures: Russia's Covert Geopolitical Operations. *Marshall Center Security Insight, no. 31*.

Galeotti, M. (2021). Active Measures: Russia's Covert Global Reach. U G. P. Herd, *Russia's Global Reach: A Security and Statecraft Assessment* (str. 118-126). The George C. Marshall European Center for Security Studies .

Galeotti, M. (2022). *The Weaponisation of Everything - A Field Guide to The New Way of War*. New Heaven and London: Yale University Press.

Haile, Y. A. (2024). The theoretical wedding of computational propaganda and information operations: Unraveling digital manipulation in conflict zones. *New Media & Society*.

Hamilton, C., & Ohlberg, M. (2020). *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World.* New York: Oneworld Publications.

Jasper, S. (2020). *Russian Cyber Operations.* Washington DC: Georgetown University Press.

Katz, E., & Lazarsfeld, P. (1955). *Personal Influence: The Part Played by People in the Flow of Mass Communications.* New York: Free Press.

Kilcullen, D. (2020). *The Dragons and The Snakes: How the Rest Learned to Fight the West.* Oxford: Oxford University Press.

Kostyrev, A. (2023). NATO-Ukraine Strategic Communications: Theory and Practice. *Hileya Scientific Bulletin*, 82-95.

Kramer, M. (2019). Operation "Denver": The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 1). *Journal of Cold War Studies* , 71–123. Preuzeto od The MITPress Reader.

Kux, D. (1985). SOVIET ACTIVE MEASURES AND DISINFORMATION: OVERVIEW AND ASSESSMENT. *The US Army War College Quarterly*, 19-28.

Lange-Ionatamišvili, E. (2015). *Analysis of Russia's information campaign against Ukraine*. Riga: NATO StratCom COE.

McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly*, 176-187.

Middle East Eye. (03. 10 2025). *Israel paying US influencers to reverse negative public opinion: Report*. Preuzeto od Middle East Eye: https://www.middleeasteye.net/news/israel-paying-us-influencers-reverse-negative-public-opinion-report

Middle East Monitor. (02. 10 2025). *Israel pays influencers up to $7,000 per post to occupy information space*. Preuzeto od Middle East Monitor: https://www.middleeastmonitor.com/20251002-israel-pays-influencers-up-to-7000-per-post-to-occupy-information-space

Military Balance. (2015). Complex Crises Call for Adaptable and Durable Capabilities. *Military Balance*, 1-5.

Mueller, R. S. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Washington, D.C. : U.S. Department of Justice .

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, 4*(2), 314-338.

Muhić, E. (2025). Psihološke operacije na društvenim mrežama - primjeri, tehnike, taktike i procedure. *Zaštita i sigurnost, 5*(1). doi:https://doi.org/10.70329/2744-2403.2025.5.9.7

Muhić, E. (2025). *Teoretsko-metodološki aspekti specijalnog rata* . Sarajevo: FKN - Doktorska disertacija.

NATO StratCom COE. (2020). *Social Media Manipulation.* Riga: NATO StratCom COE.

Prados, J. (2006). *Safe for Democracy: The Secret Wars of the CIA.* Chicago : Ivan R. Dee.

Radin, A., Demus, A., & Marcinek, K. (2020). *Understanding Russian Subversion: Patterns, Threats, and Responses.* RAND .

Rid, T. (2019). *Active Measures: The Secret History of Dissinformation and Political Warfare.* New York: Farar, Strauss and Birdux.

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *Journal of Slavic Military Studies*, 101–130.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making.* Council of Europe.

Yablokov, I., & Chatterje-Doody, P. (2022). *Russia Today and Conspiracy Theories.* London: Routledge.

Yaqub, Z., & Tabassum, S. (2025). Israel's Soft Power Application through Digital Diplomacy against Hamas to Iran Wars (2023-2025). *Advance Social Science Archive Journal* .

Popis tabela

THE ROLE OF INTELLIGENCE SERVICES IN IMPLEMENTING ACTIVE MEASURES AS A FORM OF POLITICAL VIOLENCE

DOI: *10.70329/2744-2403.2025.5.10.10*

Original scientific paper

Dr. Emir Muhić[73]

Abstract

This paper examines the role of intelligence services in conducting active measures as a specific form of political violence that operates within the spheres of perception, information, and cognitive manipulation rather than through physical force. Active measures are presented as a sophisticated political weapon through which states, via their intelligence and propaganda apparatus, influence the socio-political architecture of an adversary by means of covert, deniable, and long-term operations. Methods such as disinformation campaigns, infiltration of political structures, compromising of key leaders, the induction of social tensions, and the fragmentation of collective identities create an alternative political reality that serves the strategic interests of the aggressor. The study underscores that active measures are latent, difficult to detect, and deeply embedded within the contemporary forms of special warfare, which contributes to their effectiveness and to the persistent lack of understanding within academic, institutional, and political environments. Special attention is devoted to the necessity of building resilient institutional mechanisms, strengthening media literacy, and developing strategic communication as essential components of defence against this concealed form of political violence that undermines sovereignty, social cohesion, and the stability of modern states.

Keywords: *intelligence services, active measures, political violence, special warfare, disinformation, hybrid operations.*

[73] emirmuhic@fkn.unsa.ba

1. Introduction

Unconventional wars that reject open armed conflict and the use of legal and legitimate state militaries require tools that undermine the sovereignty and integrity of an opponent, whether a state or non-state actor, at a liminal level. Conventional, armed wars are economically and resource-wise unsustainable and politically unsuitable, which implies the need to employ other methods for endangering, controlling, or destroying an adversary. One of the successful methods of special warfare, conducted by intelligence services under the direction of state leadership and producing significant consequences for national and international security, is the use of active measures. Active measures essentially represent a political weapon, a tool through which the goals defined by state decision-makers are achieved.

As such, they belong to the system of special warfare and serve as a highly effective instrument for shaping a specific political environment and a particular socio-political and cultural narrative. Through active measures, a "new reality" is created, one that is necessary for further advancement of strategic goals. Active measures have proven to be a political weapon that has continuously shaped socio-political relations favourable to state leadership since the 1920s. A significant challenge related to active measures lies in the limited understanding of this concept within academic circles, where it is often narrowly reduced to disinformation and fake news. Active measures should instead be viewed as a broad spectrum of methods and actions undertaken by intelligence services to influence political decision-makers and the policy of the targeted state.

The central focus of this research is the operational role of intelligence services in conducting active measures aimed at destabilising a target state. It is necessary to better understand the modus operandi of intelligence services that carry out active measures as a form of political violence. A major problem stems from the very nature of active measures, which are latent, invisible, difficult to prove, and highly sophisticated, while the conspiratorial character of intelligence activities further complicates their study. Questions concerning the measures, methods of implementation, objectives, techniques, and other elements of the operational work of intelligence services remain largely unknown and must be demystified in order to develop effective resilience programmes and systems.

2. Defining Active Measures and Political Violence

Active measures represent a highly efficient and effective weapon used by aggressive political actors in their struggle for political power or resources at the regional or global level. Their origins are linked to the Bolshevik counterintelligence operation "Trust" from 1921, directed against exiled monarchists (Rid, 2019). They continued to be used throughout the Cold War period (Galeotti, 2019), a time marked by unconventional political, diplomatic, and military confrontations[74] between the Soviet Union and the West. The phrase "active measures" has its roots in the Soviet KGB and encompasses disinformation campaigns, attempts at political influence, and the operation of proxy groups and parties connected to the Soviet Union (Kux, 1985). Rid (2019) defines active measures as strategic activities employed by intelligence services to manipulate, deceive, and undermine political processes in order to achieve geopolitical goals. They are a key instrument of political warfare that goes beyond traditional espionage and includes offensive operations aimed at shaping political, social, and economic decisions within targeted states.

Because of their offensive nature, active measures aim to achieve the disorganization, destabilization, and demoralization of the opponent, whether a political community, an organization, a corporation, or an individual. They are closely linked to the concept of ideological subversion described by the KGB defector Yuri Bezmenov. Galeotti (2019) notes that the term "active measures" was used by the Soviet Union from the 1950s to describe a wide range of covert and deniable political influence and subversive operations. These activities included establishing front or proxy organizations, supporting friendly political systems, organizing local unrest, and spreading disinformation. Radin, Demus, and Marcinek (2020) view active measures as covert and deniable political influence and subversive operations that can range from corruption and disinformation to open assassinations and even support for coups. Active measures are also strongly connected to the concept of special warfare, which is defined as a coordinated political, economic, psychological-propaganda, intelligence-subversive, and military activity carried out to influence and intervene in the territory of another state, where

[74] In this confrontation between the Soviets and the West, the primary objective was to defeat the enemy without the direct use of military force. Instead, the focus was on non-kinetic, unconventional, and asymmetric measures aimed at influencing and targeting the minds of selected groups. When military force was used, it took the form of proxy wars (Korea, Vietnam, Afghanistan), in which major actors provided advisory support or direct military assistance to the side fighting against their ideological opponent.

the use of conventional military force is considered a last resort (Muhić, 2025). Within this framework, special warfare employs active measures as a tool for reaching strategic and operational objectives through a series of campaigns and operations implemented over a longer period. Since the nature of special warfare is long-term and cyclical (Muhić, 2025), its operations are prolonged, continuous, and interconnected, aligning with other measures, activities, and actors involved in their execution.

Essentially, active measures are conducted through the media and information systems, political engagement, education, physical violence, and other suitable methods that can directly influence the targeted society, nation, or community in order to affect political decision-makers. Currently, the academic community in the region does not properly recognize the term "active measures," and instead often inadequately applies the concept of "disinformation" to activities aimed at influencing decision-making. Furthermore, there is no clear understanding or differentiation of how dominance in the information space is achieved through influence operations, psychological operations, and information operations, with different modalities frequently being labelled simply as disinformation. As Rid (2019) emphasizes, active measures always include the use of disinformation, but this is not their only element. Some projects are designed to facilitate particular political decisions by creating a "favourable" environment that leads a community, group, or government toward a specific outcome. This is also achieved by actively promoting facts that benefit the targeted group while causing reputational or other types of harm to the adversary. The almost invisible guiding of events toward a specific goal represents the modus operandi through which victory is achieved without entering an open, conventional conflict.

Active measures are also not spontaneous lies told by politicians, but rather the deliberate and methodical output of large bureaucracies. The statements of political actors, even when they appear simple or insignificant, often carry a message aimed at a particular audience or serve as the foundation for creating future narratives. These statements are not limited to political figures only, but also include revisionist narratives spread by non-political or pseudo-political actors seeking to alter historical facts. By placing specific information into the public space, an anchoring point is created for building false narratives that will later support a strategic goal. Achieving such an outcome requires a critical mass of citizens who will consciously or unconsciously accept the falsehood.

Active measures are, at their core, a political weapon based on written or spoken actions conducted by political and other state-relevant actors, with the

aim of altering the existing socio-political environment. They represent a sophisticated form of political violence because they operate without the use of physical force, yet they shape political decisions, attitudes, and the behaviour of targeted groups, communities, and societies through coercive influence. These methods and activities function in symbiosis with the work of intelligence services, which support political or other actors either by gathering information or by disseminating it. In the modern cyber environment, the spread of information, disinformation, misinformation, and malinformation has become the main tool for creating violent political dominance that does not rely on physical destruction, but on eroding trust, delegitimizing institutions, and restricting free political choice. Such activity creates systemic asymmetry of power and prevents the proper functioning of democratic and liberal governance principles. Active measures therefore constitute a specific form of political violence which, although non-violent in the physical sense, operates through coercion in the realm of decision-making, perception-shaping, and the construction of an operational environment in which the targeted community begins to make decisions against its own interests.

Political violence in this context does not refer only to the use of force, but to any action intended to undermine the ability of a state or society to independently manage its political processes, thereby directly influencing the distribution of power. In that sense, active measures function as a "silent coercive apparatus" through which the aggressive actor imposes its own narratives and interpretations of reality while simultaneously narrowing the manoeuvring space of legitimate political actors within the targeted society. The political violence produced through the application of active measures creates three key effects. First, it disrupts the vertical legitimacy of government by eroding trust in institutions, where every invented crisis or fabricated narrative becomes a catalyst for political instability. Second, it destroys the horizontal cohesion of society by generating deep symbolic divisions, identity-based conflicts, and permanent suspicion among social groups that no longer share a common framework of truth. Third, it establishes cognitive occupation, as the targeted society begins to internalize narratives crafted outside its own borders. Such occupation represents the most advanced and dangerous form of political violence, since it is achieved without physical coercion, without military force, and without visible conflict, yet it produces far more severe long-term consequences for political sovereignty.

3. Active Measures and Intelligence Services

Active measures, as a political weapon, are primarily based on non-violent action that can nevertheless produce physical violence as a consequence. Russian Major General Vladimirov wrote that "modern wars are fought at the level of consciousness and ideas" and that "modern humanity exists in a state of permanent war," in which it "constantly oscillates between phases of real armed conflict and constant preparation for it" (Galeotti, 2021). The Soviet KGB, particularly Department D, sought to weaken and ultimately destroy the United States through sophisticated intelligence operations that were primarily non-violent and grounded in disinformation. Former KGB officer, Lieutenant General Oleg Kalugin, described subversion and active measures as "the heart and soul of Soviet intelligence," noting that "subversion, not intelligence collection," was the core activity (CNN, 2000). These operations were conducted through specific foreign-policy activities of the Soviet Union, characterized as "white," "grey," or "black" operations (Kux, 1985). According to Kux (1985), "white" operations consisted of regular diplomatic, trade, or humanitarian activities, "grey" operations involved the work of illegal communist groups in the West, and "black" operations included covert actions conducted by agents who spread disinformation, lies, forgeries, plagiarized material, and similar content. In modern times, the distinction between "white," "grey," and "black" operations has largely disappeared, and it has become almost impossible to identify the actors conducting them due to the saturation of the information space and the intensity of propaganda that conceals these activities. Anarchy in the international system has produced a constant struggle among states for the hegemonic position currently held by the United States (Donnelly, 2006). However, ongoing geopolitical developments increasingly challenge this order, leading once again to widespread use of "white," "grey," and "black" operations instead of conventional military actions. These operations enable the continuous application of political violence against various actors and allow the achievement of strategic goals without open confrontation or conventional warfare, which could otherwise result in catastrophic outcomes such as nuclear exchange, the collapse of the modern system, or massive cyberattacks on critical infrastructure. Intelligence services are key actors that employ active measures to enable what Kilcullen (2020) terms the liminal dimension of war. The liminal dimension represents a state in which no open armed conflict is present, yet intelligence activities are clearly visible. The scope and political-social impact of active measures were particularly significant during the Cold War, when the Soviet KGB conducted numerous disinformation operations, such as Operation "Denver," which aimed to blame the U.S. military for creating the HIV/AIDS virus (Kramer, 2019), and subversive

operations such as "Pandora," designed to provoke racial unrest in the United States (Andrew & Mitrokhin, 2000). The post-Soviet era created a different climate in socio-political relations. The rise of religious radicalism, extremism, and terrorism led to greater reliance on kinetic rather than non-kinetic operations. After the terrorist attacks of 11 September 2001, the focus shifted to kinetic action (the invasions of Iraq and Afghanistan), where active measures alone were inadequate and inappropriate, thus requiring military force. The period of the so-called Arab Spring as a chain of insurgencies in the Middle East, the emergence of ISIL, and the Russian occupation of Crimea all highlighted the continued relevance of active measures and the renewed use of political violence against opponents. The operational work of intelligence services on behalf of aggressive political actors has enabled the initiation of socio-political processes such as uprisings, insurgencies, and civil wars. The importance of active measures depends on the position and strength of the actors who use them and the actors they target. The reason active measures were not widely applied during the "Global War on Terror" lies in the vulnerability of the opposing actors, terrorist organizations, insurgents, and rebel groups[75] in the Middle East who were suitable for military action and significantly inferior in technological, economic, socio-political, and cultural terms. Under such circumstances, there was no need to apply active measures against these targets. Additionally, specific counter-insurgency (COIN)[76] strategies proved unsuccessful in Iraq and Afghanistan. Civilian casualties, often described as collateral damage, served as a radicalizing and recruitment factor for insurgent groups such as the Taliban, Shia and Sunni militias in Iraq, and terrorist organizations like Al-Qaeda, which capitalized on these incidents to justify retaliation and mobilize new members.

[75] The complexity of the conflict with various groups that shared a common denominator, a resistance against coalition forces lies in the fact that not all of them were loyal to Al-Qaeda and its affiliates. Certain factions were loyal to Saddam Hussein, while others followed mujahideen or Taliban leaders, and their primary goal was to fight against a foreign force that had entered their territory. Within the context of the Global War on Terror (GWOT), it is essential to distinguish between local actors in Iraq and Afghanistan, their goals and reasons for fighting, and the foreign fighters gathered around Osama bin Laden within Al-Qaeda.

The notion that everyone resisting U.S. and coalition forces was simply a terrorist is an obvious example of misunderstanding geopolitical and internal dynamics. Such misinterpretation strengthens neo-colonial ideas and legitimizes crimes committed against Arab-Muslims in order to preserve the narrative of a "clash of civilizations," while the conflict itself did not take place on U.S. or European soil, but on the territory of the "cultural" enemy.

[76] Counter-insurgency - a set of political-social, military, and economic measures used to suppress insurgent, guerrilla, partisan, or rebellion movements, as well as their objectives and the support they receive from the local population.

On the other hand, when it comes to major global and regional powers such as Russia, China, Iran, and North Korea referred to by Kilcullen (2020) as "dragons" and organized crime groups, terrorist organizations, and cartels described by the same author as "snakes", active measures represent a suitable weapon for threatening, disrupting, destabilizing, controlling, defeating, or destroying them. The use of active measures moves the conflict into the domain of special warfare, which is based on the actions of intelligence services through secret, conspiratorial, and malicious activities aimed at attacking a society or nation without the use of conventional armed force. Special warfare, as a method and instrument for achieving strategic goals formulated by state policy and carried out by intelligence agencies, enables influence on specific groups that pose a threat to national security at the global level. It can also serve as a tool for achieving local or regional dominance over technologically and socio-politically weaker actors. Modern strategies and doctrines are increasingly oriented toward invisible occupation and control of an adversary's population through the use of various influence activities and measures at the political, economic, educational, cultural, and other levels. Scholars of the Copenhagen School, such as Barry Buzan, emphasized five security sectors (Buzan, 1983), and each of these sectors came to be associated with specific types of threats. However, in the contemporary era, these sectors have diversified and expanded, requiring particular attention to the cyber and educational sectors, which can be viewed as new additions within security studies. These two sectors are particularly suitable for active measures. The first, the cyber sector, is used for disseminating misinformation, disinformation, and malinformation, as well as for info-kinetic attacks, while the educational sector is used for societal indoctrination through a compromised school and academic system. In this context, there is a blend of the previously mentioned "white," "grey," and "black" operations, and all state, political, and intelligence-security levels are involved in their implementation.

4. Subversive Activities and the Political Violence of Intelligence Services

Intelligence services, as state-controlled institutions with the capability to conduct both kinetic and non-kinetic special operations, represent suitable actors for carrying out active measures. Just as the Soviet KGB conducted operations during the bipolar division of the twentieth century to reshape the ideological orientation of the U.S. population and weaken American influence globally, many intelligence services continue to engage in similar activities today.

Achieving the strategic goals of an aggressive actor striving for hegemony requires continuous intelligence engagement with both opponents and neutral actors. Through such intelligence treatment, favourable conditions are created for political, diplomatic, and economic gains that arise from disrupting, weakening, or damaging the adversary, as well as indoctrinating neutral parties. Intelligence services effectively conduct sabotage against the political and social order through the following activities:

- The spread of disinformation, misinformation, and malinformation
- Active offensive propaganda efforts
- Providing support to political opposition groups
- Sabotaging the electoral process
- Creating an atmosphere of fear and insecurity within the targeted society
- Legal, economic, and diplomatic undermining of independence, sovereignty, and territorial integrity
- Establishing subversive ideologically loyal organizations
- Financing criminal and terrorist organizations
- Organizing, encouraging, and conducting assassinations and political killings
- Inciting civil unrest, disobedience, and violence.

To clearly systematize the activities listed above and better understand them within the context of contemporary political violence, the following section presents a typology of subversive measures (Table 1), along with their instruments, objectives, and expected consequences.

Table 3 Typology of Subversive Activities of Intelligence Services

Category of Subversive Activity	**Operational Instruments**	**Primary Objective**	**Consequences for the Targeted State**
1. Information Operations	Disinformation, misinformation, malinformation, bot networks, deepfake content, media control, psychological operations	Cognitive destabilisation of the population	Polarisation, decline of institutional trust, mass confusion, delegitimisation of government
2. Propaganda Activities	Systematic campaigns, amplification of narratives through influencers, networks	Establishing an alternative reality	Normalisation of extreme views, shrinking of public

	of "useful idiots," academic or cultural support	and ideological dominance	space, change in political preferences
3. Political Infiltration	Support to opposition groups, financing of parties, support to protest movements, insertion of agents into political structures	Weakening of ruling structures and creation of internal chaos	Collapse of political stability, mobilisation of discontent, erosion of institutional legitimacy
4. Electoral Sabotage	Manipulation of voter registries, leaking compromised data, financing campaigns, cyberattacks	Creating the narrative that elections are illegitimate or manipulated	Delegitimisation of the electoral process, mass protests, institutional breakdown
5. Weakening the State through Legal and Economic Pressure ("lawfare")	Lawsuits, sanctions, blockades, special trade regimes, manipulation of international institutions	Forcing the state to alter its political decisions	Economic damage, loss of sovereignty, legal disorder, political vulnerability
6. Establishment of Subversive Organisations	Creation of NGOs, think tanks, movements, religious or cultural groups loyal to a foreign power	Long-term indoctrination and societal control	Transformation of political culture, "soft" takeover of institutions
7. Supporting Criminal and Terrorist Networks	Financing, training, logistics, arms trafficking	Weakening the state from within by creating parallel power structures	Erosion of the monopoly of force, increased violence, delegitimisation of law enforcement
8. Organisation of Assassinations and Political Killings	Contracted assassins, covert operations, use of criminal structures	Eliminating key individuals who obstruct the foreign actor's interests	Political shock, power vacuum, intimidation of opposition and society
9. Social Destabilisation	Incitement of unrest, radicalisation, identity-based conflicts, calls for secession	Creating conditions for political violence and system breakdown	Civil conflict, deep societal divisions, preconditions for intervention by a "protective power"

These activities enable an aggressive intelligence service to create an operational environment suitable for major strategic actions such as taking over the modern political system, exploiting or destroying critical infrastructure, conducting diplomatic overshadowing and isolating the target state from international channels, appropriating or exploiting resources, controlling air, maritime, or land borders, and exercising control or oversight over telecommunications. Above all, active measures as a form of political violence move beyond the physical dimension of coercion and enter the cognitive sphere, influencing targeted nations, societies, and groups. Intelligence services, using their personnel, technical, and technological capabilities, actively seek to place the target population in a state of fear, anxiety, and panic. The absence of active countermeasures by the victim state and its institutions (intelligence services, educational systems, etc.), or even the lack of recognition of active measures conducted by an aggressive intelligence service, amounts to political-ideological occupation.

This is not a traditional occupation carried out through armed forces, military-police presence, or counter-insurgency operations. Instead, the occupation is implemented through control of narratives, attitudes, opinions, behaviours, and the creation of events that shape them. Implementing countermeasures in such a scenario is extremely sophisticated, with additional difficulties arising from enemy infiltration, the use of useful idiots[77], the financing of opposition groups, and related activities.

In carrying out political violence, actions such as spreading disinformation and influencing or obstructing electoral and political processes play a key role in maintaining the required level of repression that generates significant socio-political disturbances. The escalation of these disturbances leads to divisions, segmentation, and atomization of society and the nation, creating an operational environment suitable for advancing to activities such as calls for secession and attempts to realize it, or provoking internal conflicts that may escalate into open armed warfare. Aggressive intelligence services, through active, covert, and clandestine operations within the political, economic, and social system, achieve far greater success than would be possible through conventional warfare or direct military force. By using disinformation, propaganda, controlled and targeted physical violence, legal and procedural obstruction of political processes, and by exploiting identity politics that generate divisions and deepen conflict, these services exert strategic pressure that reshapes the internal landscape of the targeted state.

[77] A Cold War era term used to describe ideological and genuine supporters of communism and socialism in the United States who were exploited by the Soviet KGB for various activities such as protests, speeches, attacks, and similar actions.

5. Active Measures and Ideological Subversion

State-driven operations cannot succeed without the systematic weakening of the adversary, which is carried out through ideological subversion. Former KGB operative Yuri Bezmenov frequently discussed this process in his interviews, emphasising four stages through which a society must pass in order to become vulnerable to foreign influence. He described these stages: demoralisation, destabilisation, crisis, and normalisation as phases designed to gradually weaken social bonds and provoke fear, intolerance, distrust, and hatred (Bezmenov, 1985). Bezmenov (1985) explained these stages as follows: a) Demoralisation: This phase takes 15 to 20 years, the time required to educate and form one generation. The process is assisted by media actors and teachers who have become sympathetic, consciously or unconsciously, to the ideological aims of the subverting power. b) Destabilisation: Following demoralisation, this stage lasts two to five years and focuses on disrupting foreign relations, defence structures, and the economy of the targeted state. c) Crisis: Around six weeks of intense chaos serve as a crucial socio-political turning point. d) Normalisation: This phase reshapes public understanding of what constitutes the status quo. Bezmenov's description also includes the possibility of military takeover and the public's broad acceptance of the enemy's forces as liberators.

According to Bezmenov, active measures were used to weaken American society by spreading anti-Western ideas such as anarchism, communism, socialism, Marxism, and other left-oriented ideologies. The aim was to spark conflicts within American society based on race, ethnicity, class, and sexual identity. In this form of ideological subversion, one can also see the symbiotic use of other methods of special warfare, such as propaganda, sabotage, diversion, assassinations, and political killings. Although the central objective of ideological subversion is the weakening of the state and nation, this cannot be achieved without a combination of additional measures and methods that together form a coherent system of special warfare.

In the implementation of active measures, which aim to weaken the targeted state and nation, disinformation forms the core of the attack. It is a built-in component of all other activities, whether as a primary or supporting element. In the case of ideological subversion, however, disinformation takes centre stage. Its power lies in its ability to reshape reality and alter objective truth through manipulation of information. Bezmenov noted that only 15 percent of the Soviet effort was dedicated to espionage, while the remaining 85 percent was allocated to active measures, specifically ideological subversion. The goal

was to alter the American perception of reality to such an extent that even with first-hand knowledge of events, citizens would take no action to defend their state, nation, society, community, or family (Bezmenov, 1985). Today, when observing the intelligence practices of global and regional powers, the importance of controlling the media environment especially social networks and the spreading of narratives is evident. For example, Israel, during its genocidal operations in Gaza, has used influencers and social media to spread propaganda and conduct psychological operations, with some influencers reportedly paid up to 7,000 USD (Middle East Eye, 2025). Social networks play a crucial role in contemporary psychological operations, enabling rapid dissemination of disinformation and manipulation of public perception (Muhić, 2025). *Hasbara*, Israel's public diplomacy strategy, is designed to shape the views and opinions of broad audiences toward justifying the killing of Semitic, specifically Arab and Muslim populations. The aim is to present Arabs and Muslims as a threat to Europe, while portraying Israel as the protective barrier safeguarding Christianity. These narratives are strongly influenced by Huntington's ideas on the "clash of civilizations" and the supposed incompatibility of Islam with European values[78]. Amplification of dehumanising messages occurs through paid influencers, useful idiots, and official state channels. Currently, however, these operations have limited success due to the absence of censorship on platforms such as X, which remains dominant for the spread of political content. On this platform, users can witness genocide, atrocities, and crimes against humanity committed by the Israeli state and military in real time. As a result, *hasbara* often produces

[78] In this context, Huntington's arguments about the clash between East and West and the prospect of new crusades are essential. These ideas first manifested in the aggression against the Republic of Bosnia and Herzegovina carried out by the Yugoslav People's Army, and later by the so-called Army of Republika Srpska. Confirmation of this narrative appeared in two works, Rebecca West's *Black Lamb and Grey Falcon* and Robert Kaplan's *Balkan Ghosts* both of which portrayed the region as filled with "ancient hatreds" and in need of a cathartic ethnic conflict in which oppressed Orthodox communities would allegedly seek revenge for the period of Ottoman rule. These books became required reading for American policymakers, who, influenced by such interpretations, allowed the Serbian aggressor to commit war crimes and genocide. Furthermore, the conflicts in the Middle East following the terrorist attacks of 11 September 2001 strengthened the idea of incompatibility betwe en East and West, with Huntington's theses appearing almost prophetic. A new crusade began thousands of kilometres away from the Judeo-Christian world, justified by the claim that terrorism carried out by Arabs who had only recently freed themselves from British and French colonial domination posed a threat to the entire globe. The millions of Muslims killed in the Middle East, as well as the hundreds of thousands of Palestinians who lost their lives, demonstrate how state-sponsored propaganda and active measures can reshape a narrative and portray the victim as the perpetrator.

the opposite effect, and influencers spreading its narratives are increasingly labelled as paid agents of Israel.

In situations where information dominance must be achieved and maintained, it is necessary to inject a sufficient volume of disinformation and malinformation into society, ensuring that their dissemination is continuous and widespread. Disinformation alters the informational environment because provocateur agents release specific narratives into the political-social sphere, falsify sources, and reinforce ongoing offensive operations against protected elements of the state. In the case of active measures, the spread of disinformation such as that used in the KGB's "Pandora" and "Denver" operations weakens the targeted society and destroys its internal cohesion. The same approach can be applied globally when the objective is to label a particular nation or state as an international threat. A clear example of this is the false claim that Iraq possessed weapons of mass destruction, which originated from an unreliable source. However, truthful information can also be used as an instrument of influence. During the 1960s, the Soviets printed leaflets in English and French describing racial discrimination against African Americans and disseminated them across African states that maintained close ties with their former colonisers, the British and the French (Andrew & Mitrokhin, 2000; Rid, 2019). By using truth and factual evidence, the Soviet KGB sought to create new ideological frameworks that would discourage cooperation with Europeans and former colonial powers, encouraging instead a turn toward socialism, which was presented as blind to race, ethnicity, and other biological or cultural differences. Today, when disinformation can be debunked more easily, aggressive actors conducting active measures can achieve significant success simply by amplifying truth and facts. This makes it difficult to produce a counter-narrative or justify the underlying causes of certain events. The release of truthful information is planned and coordinated with other measures such as propaganda, disinformation, deception, plagiarism, and similar methods which serve to present the truth in a completely different light.

6. Modern Technologies and Active Measures

The development of the internet and social media has enabled the rapid spread of information. However, when information becomes compromised, malicious, or fabricated, it transforms into a political weapon. News about wars, terrorist attacks, political campaigns, and political repression often serves a dual purpose: first, to inform the public, and second, to provoke specific emotional responses within society or among targeted groups that must be demoralised or radicalised in line with strategic objectives.

Technologies such as the internet and social media have shifted the battlefield into the cognitive domain - the human mind which has become the new frontline. Platforms like X, Facebook, Instagram, TikTok, Reddit, 4Chan, and others have become arenas where political actors compete to achieve goals such as radicalisation or demoralisation. The concept of hybrid warfare, popularised around 2010, describes a system in which unconventional methods and tools are used to subordinate an opponent, with conventional armed force largely absent. The *Military Balance* report of the International Institute for Strategic Studies (2015) described Russian hybrid warfare as "the use of military and non-military tools in an integrated campaign designed to achieve surprise, seize initiative, and gain psychological as well as physical advantage, employing diplomatic means; sophisticated and rapid information, electronic, and cyber operations; covert and occasionally overt military and intelligence actions; and economic pressure." The novelty in modern warfare is precisely the use of non-military effectors that dominate the cyber and information environments. With the expansion of cyberspace as a new domain of human life, intelligence collection and operational activity have become significantly easier and more effective (Muhić, 2024). Some Western observers attempted to interpret Russian actions in annexed Crimea in 2014 through the so-called Gerasimov Doctrine, although in practice Russia does not formally recognise the Western concept of hybrid warfare, despite limited academic writings on *gibridnaya voyna* (Fridman, 2017). While the Western concept largely focuses on military activity to achieve synergistic effects, the Russian equivalent encompasses all spheres of public life (Jasper, 2020). Accordingly, Russia was not conducting hybrid warfare in Crimea, but rather intelligence operations that fall under active measures and political violence. The deployment of "little green men"[79], as labelled by Western media, was a classical intelligence action involving special forces without insignia to ensure plausible deniability. Through coordination between intelligence, security, military, and political elements, a specific environment is created in which the adversary and its allies cannot react swiftly or effectively, allowing strategic objectives to be achieved with minimal losses, whether human or political. Such operations have also been observed historically. The U.S. CIA used its own unmarked special units in various conflict zones from Vietnam and Panama to Afghanistan, Iraq, Libya, and Syria.

[79] "Little green men" were masked Russian soldiers and members of Spetsnaz who operated in Crimea in 2014 without any identifying insignia, both before and during the annexation. This provided Moscow with international "plausible deniability" regarding their involvement. It also enabled Russian diplomacy to negotiate, pressure, deceive, and ultimately execute all strategically important objectives in Crimea, while the West attempted to formulate an adequate political response one that ultimately never materialised.

Today, as the Russian invasion of Ukraine continues on a large scale, active measures that is, certain non-kinetic and unconventional aspects of warfare are still being applied, particularly through troll and bot activity on social media platforms. Trolls and bots, acting as the "soldiers" of hybrid warfare, aim to spread and entrench narratives such as supposed Ukrainian Nazism in the minds of audiences worldwide. This enables the continued prosecution of the war and the justification of various crimes through the dehumanisation of Ukrainians, who are assigned the label of "Nazis." Revisionism and the fabrication of reality represent key tasks of trolls and bots, whose strength lies in their numbers. Their sheer volume makes it possible for a specific narrative to appear as the dominant view of society, as it becomes widely disseminated and receives large amounts of affirmation in the form of likes, retweets, upvotes, or positive reactions on local portals. In this context, war becomes hybrid and expands into the domain of cyberspace, which is suitable for other forms of action such as hacking operations. Striking an enemy headquarters with precision-guided missiles or rockets brings significant advantages, yet such operations are costly and require extensive intelligence work and preparation. By contrast, cyberattacks can be launched at any time, from anywhere, and can, besides destroying infrastructure, also extract protected information held by the adversary. The evolution of warfare has made it ubiquitous, wide-ranging, and extensive. Active measures, as a political instrument, operate synergistically with pseudo-kinetic strikes carried out within the cyber domain.

7. Examples of Active Measures in Contemporary Political and Geopolitical Dynamics

7.1. Modern Reinterpretation of Active Measures

Modern active measures no longer appear as strictly secret operations under the direct control of a single intelligence service, but rather as a complex set of political, informational, and institutional activities aimed at destabilising an opponent or shaping a favourable political outcome. Although the term originates from the Soviet doctrinal corpus, its contemporary variants have undergone significant transformation due to digital technologies, global interconnectedness, and the ability to mobilise a wide range of intermediary actors. Instead of the monolithic operations once conducted by the KGB, today's active measures involve the simultaneous use of propaganda, coordinated digital campaigns, legal pressure, manipulation of social divisions, economic instruments, and para-state networks that operate outside formal state structures. This evolution has created an operational environment in which the boundary between legitimate political communication and covert attempts at influence is increasingly difficult to distinguish. According to Rid

(2020), modern active measures retain the strategic logic of classic Soviet operations, but have become more visible, faster, and more adaptive thanks to new technological capabilities. Digital platforms enable precise audience targeting, automated messaging, and reduced attribution risk, allowing state and non-state actors to carry out a wide array of operations that formally remain in the "grey zone" between war and peace.

States with a long tradition of special information–political operations, such as Russia, have adapted their historical model of active measures to the digital age. Research by Thomas (2014) and Galeotti (2022) shows that modern Russian approaches integrate state institutions, private companies, media networks, paid political operatives, and criminal structures that function as extensions of the state's political-influence strategy. China, according to studies by Brady (2015) and Hamilton & Ohlberg (2020), has developed a sophisticated system of "political environment shaping" through networks of Party organs, technology companies, and diaspora organisations, while Iran and Turkey have created their own hybrid models in which active measures intertwine with cultural, religious, and regional ambitions (Axworthy, 2016; Coşkun, 2023).

In such an environment, modern active measures are no longer isolated incidents of political subversion, but an ongoing process in which states invest sustained effort into shaping narratives, manipulating threat perceptions, creating social fractures, and strengthening their satellite structures abroad. A defining characteristic of this process is that operations are carried out through multilayered, decentralised, and difficult-to-attribute channels, which makes them particularly effective in geopolitical environments marked by crises, polarisation, and information overload.

7.2. The Digital Information Environment as a Platform for Active Measures

The digital information environment has become a central arena for conducting modern active measures, as it enables the simultaneous creation, distribution, and amplification of political narratives at minimal cost and with a significantly reduced risk of attribution. Unlike traditional propaganda techniques, digital operations exploit the algorithmic logic of social networks to target specific groups with high emotional sensitivity, generating reactions that produce polarisation and mobilisation. The phenomenon of emotional engagement, which turns the audience's cognitive limitations and neuropsychological biases into operational advantages, allows actors to rapidly create viral narratives that spread faster than institutions can detect and neutralise them. Three communication theories are essential for the success of any influence operation. McCombs and Shaw's (1972) agenda-setting theory

explains how media determine what the public thinks about. Entman's (1993) framing theory highlights the power of shaping interpretive frameworks through which events are understood. Katz and Lazarsfeld's (1955) two-step flow model clarifies the role of opinion leaders in the modern environment, verified accounts and political influencers who amplify and normalise narratives. This theoretical foundation explains why digital influence operations do not function linearly or through a single message; instead, they operate through a network of micro-interactions that cumulatively produce a political effect. Operational actors target the emotional predispositions of the audience, use opinion leaders to legitimise the narrative, and rely on algorithmic recommendation systems that boost content with high engagement. This creates so-called information bubbles in which the narratives of active measures become dominant. Such dynamics allow operations to persist continuously without the need for centralised command, as once a narrative is introduced, it can be maintained through spontaneous user participation, automated networks, and political actors who adopt it for their own purposes. Consequently, the digital environment becomes not only a channel of distribution but also an active accelerator of political influence, where the boundary between manipulated and organic communication becomes increasingly difficult to discern.

Modern digital active measures commonly consist of three interconnected layers (Table 2). The first layer involves content production, ranging from sophisticated propaganda videos and manipulated images to emotionally charged memes. The second layer is automated distribution through bot networks, fake profiles, and coordinated online communities that serve as amplification mechanisms. The third layer consists of reach expansion via influencers, alternative media, and political actors who knowingly or unknowingly adopt and promote the narrative, thereby making the digital operation socially "normalised."

Table 4 Layers of Contemporary Digital Active Measures

Layer	**Description**	**Expanded Examples of Activities**
1. Content Production	Creation of original material designed to trigger an emotional reaction, shape a narrative, or attract attention.	Production of high-emotion propaganda videos; manipulated or deepfake photos and recordings; memes that oversimplify complex political issues; fabricated articles and "investigative stories" without sources; creation of fake expert analyses; selective presentation of leaked documents.

2. Automated Distribution	Dissemination and amplification of content through technical and organised mechanisms that increase visibility and the appearance of "organic" reach.	Use of bot networks for mass sharing; coordinated campaigns across hundreds of fake profiles; automated comments that create the illusion of consensus or controversy; orchestrated activity within closed groups on Telegram, WhatsApp, and Discord; creation of fake trending topics; manipulation of recommendation algorithms on platforms such as YouTube and TikTok.
3. Reach Amplification	Legitimation and normalisation of narratives through influential actors who transmit them to wider audiences often unknowingl thus embedding the operation into public space.	Spreading narratives through influencers, political commentators, and pro-government journalists; adoption of content by alternative media and portals that publish sensationalised versions; dissemination through political organisations and interest groups; "organic-looking" uptake by public figures, extremist groups, or diaspora networks.

Numerous studies, including those by Bolover & Howard (2017) and Haile (2024), show that the success and longevity of a digital operation are determined less by technical capacities and far more by the ability of a narrative to fit into existing social polarisation.

A defining feature of digital active measures is their ability to function as "simultaneous campaigns," where hundreds of small messages produce a cumulative effect. State actors such as Russia, China, Iran, Israel, and the United States intensively use this dynamic, but so do non-state actors including extremist groups, political parties, and commercial entities. The digital environment enables the creation of an "information noise" effect, where the objective is not only to disseminate disinformation but also to flood the public space with so many contradictory narratives that the audience becomes unable to distinguish relevant information from deliberate fabrication. As Wardle and Derakhshan (2017) note, the primary goal of contemporary information operations is not persuasion in the traditional sense, but the erosion of trust, the creation of confusion, and the feeling that all sources are equally unreliable. Digital infrastructure also enables other forms of active measures, including hacking and selective disclosure of stolen information, manipulation of recommendation algorithms, external control of digital platforms through investment and regulation, and the use of artificial intelligence to generate convincing fabricated content (deepfakes, voice-cloning, synthetic actors). Research by the NATO StratCom COE (2020)

shows that techniques used to manipulate the digital space have become so sophisticated that they no longer require massive bot networks, but instead rely on precisely designed micro-campaigns targeting the most emotionally sensitive segments of the population. Current trends indicate that digital active measures have two key advantages: scalability and replicability. Once created, a narrative can be reactivated in different political contexts, while technical infrastructures (bot networks, fake portals, coordinated groups) can be reused across multiple operations simultaneously. As a result, the digital space becomes an extension of political and geopolitical competition, where information is treated as a weapon and perception as the most important strategic resource.

7.3. Russian Active Measures After 2014

Russian active measures after 2014 represent the most visible contemporary example of an integrated model of political-informational operations in which classical Soviet subversion methods intertwine with digital instruments, economic pressure, and intelligence activity. The annexation of Crimea and the outbreak of war in eastern Ukraine marked the moment when Russia shifted from traditional influence operations to a strategy of systematically shaping the international environment. Numerous authors, including Galeotti (2022), Kilcullen (2020), and Rid (2020), note that this period formalised *non-linear warfare* as Russia's central approach, characterised by the simultaneous and complementary use of information operations, cyber activities, and diplomatic manoeuvres.

The digital dimension of Russian active measures became particularly visible in a series of operations targeting political processes in the United States, the European Union, and the post-Soviet region. The most notable example is the 2016 U.S. presidential election, investigated by the U.S. Congress, the FBI, and Special Counsel Robert Mueller. The activities of the Internet Research Agency (IRA) from St. Petersburg, as detailed in Mueller's 2019 report, included the creation of thousands of fake profiles, coordinated campaigns aimed at polarising the electorate, targeted messaging to African-American communities, and infiltration of online forums to create an artificial sense of political fragmentation. Similar operations were documented during the Brexit referendum, elections in France, Germany, and Italy, as well as in several Balkan states. Beyond digital operations, Russian active measures after 2014 include a sophisticated combination of energy pressure, support to political and extremist groups, diplomatic engagement, and para-state networks. Energy dependence of certain European states was used as leverage to influence political decision-making, while intelligence services, according to assessments by EUROPOL and NATO, intensified infiltration attempts targeting national institutions, political parties, and media organisations. The

role of Russian media outlets such as RT and Sputnik, analysed in the works of Yablokov and Chatterjee (2022), demonstrates how propagandistic and semi-propagandistic content is disseminated through multimedia platforms, often blended with local right-wing, populist, or Eurosceptic narratives. In the post-Soviet space especially in Ukraine, Georgia, and Moldova Russian active measures function as part of a broader model of special operations in which informational, military, and political components overlap. According to research by Lange-Ionatamishvili (2015), Kostyrev (2023), and others, Russia has used digital campaigns to delegitimise Ukrainian institutions, selectively publish hacked materials, conduct psychological operations targeting soldiers and civilians, and fabricate reports of war crimes against Russian populations in order to create moral confusion and weaken international support. These operations were not ad hoc, but part of a long-term strategy aimed at shaping perceptions of Ukraine as a dysfunctional state dependent on foreign actors. In the Balkans, Russian influence manifests through a combination of political patronage, intelligence operations, and support for media outlets and organisations promoting anti-NATO and anti-EU narratives. The 2016 operations in Montenegro including attempts to destabilise the government and prevent NATO accession contain all the elements of classical active measures, from infiltration into political structures and support for radical groups to disinformation campaigns and close coordination with local actors. In Bosnia and Herzegovina, Montenegro, and Serbia, Russian narratives spread through media channels, religious institutions, and political actors who advocate neutrality, relying on emotionally charged themes rooted in history and collective identity.

7.4. Israeli Active Measures in the Contemporary Political and Geopolitical Environment

Israeli active measures are characterised by a unique combination of sophisticated intelligence architecture, technological superiority, and global political networks, which makes them a distinct operational model within the modern international environment. Unlike Russian or Chinese doctrine, Israel's approach does not rely primarily on large-scale information operations, but rather on highly targeted, precisely directed activities that fuse intelligence work, diplomatic pressure, cyber operations, and globally influential narratives about security threats, counterterrorism, and the legitimacy of defensive action. These operations emphasise proactive information control and the shaping of international perceptions of Israel's security needs, placing them within a broader framework of special measures designed to manage crises and secure political freedom of manoeuvre. One of the defining features of Israeli active measures is the use of advanced

technological tools and cyber capabilities through agencies such as Mossad, Aman, and Shin Bet. In relevant literature (Clarke & Knake, 2019; Bergman, 2018), Israel is often described as one of the most advanced states in terms of cyber operations, encompassing offensive and defensive activity and the use of digital tools for the surveillance of adversarial and allied structures. In this context, the joint U.S. - Israeli cyber operation targeting Iran's nuclear facilities at Natanz through the "Stuxnet" computer virus is frequently cited as a prominent example of a sophisticated active measure that combines a cyberattack, a political message, and strategic deterrence. This model demonstrates that Israel does not use the digital domain primarily for mass influence operations, but for precise, high-risk actions with clear geopolitical objectives.

Israel's information operations focus on shaping international perception of the Israeli–Palestinian conflict, security threats, and the legitimacy of Israeli military actions. In the digital domain, Israel employs a two-layered communication strategy. The first layer consists of institutional communication campaigns by the Ministry of Foreign Affairs, the IDF, and government spokespersons who rapidly disseminate (dis)information, visual material, infographics, and video content framed as factual and transparent representations of events. The second layer includes a network of domestic and foreign (primarily American) pro-Zionist NGOs, lobbying groups, diaspora organisations, and think tanks that serve as amplifiers of key messages, often focusing on delegitimising criticism of Israel through narratives of antisemitism, extremism, and disinformation. According to Yaqub and Tabassum (2025), this model functions as a sophisticated form of a "strategic narrative framework" aimed at preserving international support by reshaping the interpretative categories of the conflict. Within this system, *hasbara* stands out as an institutionalised mechanism of strategic communication that combines diplomatic resources, digital platforms, and a wide network of civil-society actors. Hasbara is not merely an explanation of state policy; it functions as a coordinated apparatus for perception management, involving professional communicators, PR agencies, and targeted campaigns directed at foreign audiences.

Multiple investigations conducted by international media consortia indicate that Israel and affiliated organisations hire and fund various influencers, YouTubers, and online content creators whose role is to amplify official narratives, neutralise criticism, and create the appearance of broad international support for Israeli operations, often paying them several thousand U.S. dollars per campaign (Middle East Monitor, 2025). This model also includes systematic denial or reinterpretation of atrocities, a practice especially visible on social media platforms. Despite satellite imagery,

geolocated evidence, reports by international organisations, or forensically verified material documenting civilian casualties, the Israeli communication apparatus often employs strategies of contestation claiming that evidence is "fabricated," "manipulated," or "produced for propaganda purposes"[80]. This approach aims to undermine the credibility of independent sources and produce a state of epistemological confusion in which the public can no longer distinguish reliable information from propagandistically reconstructed narratives.

7.5. Active Measures of the United States in the Contemporary Geopolitical Environment

American active measures represent a distinct model of influence operations combining intelligence capabilities, diplomatic leverage, technological dominance, and global infrastructural presence. Unlike traditional Soviet or contemporary Russian active measures which often function as covert subversive actions the U.S. model relies heavily on formalised "soft power" instruments, strategic communication, digital campaigns, partnerships with technology companies, and institutional mechanisms that enable influence without overtly violating international norms. Nevertheless, declassified CIA documents, U.S. Senate reports, and a wide body of academic research demonstrate that the United States has for decades engaged in a broad spectrum of active measures ranging from psychological operations to political engineering aimed at shaping the global order in line with American strategic interests (Bloom, 2003; Prados, 2006).

Historically, U.S. active measures have included operations targeting elections, destabilising regimes, supporting opposition groups, and spreading pro-American narratives. The best-known examples include CIA operations during the Cold War: Iran in 1953, Guatemala in 1954, Chile in 1973, and various support programmes for anti-communist movements and media campaigns across Eastern Europe. Declassified archives show that these operations combined psychological operations (PSYOP), financial support to political actors, media-narrative shaping, and carefully constructed perceptions of America's role in global affairs. In this sense, the U.S. approach is characterised by high institutional coordination and a strong capacity to integrate intelligence, economic, and diplomatic instruments into a unified operational framework. Contemporary American active measures rely increasingly on digital platforms, the technological sector, and

[80] For further reference, see the posts of official IDF accounts, the Ministry of Foreign Affairs, and various Israeli political officials on the social network X. These posts display a discourse that ranges from denying the genocide to openly acknowledging it, including statements suggesting that such actions will continue in the future.

institutionalised strategic-communication capacities. Programmes such as the State Department's Global Engagement Center (GEC), USAID's democracy-promotion initiatives (prior to their dissolution in 2025), NATO strategic-communications centres, and a range of public-private partnerships play a key role in shaping global narratives, particularly in states exposed to authoritarian influence. According to Brooks & Wohlforth (2016), the American narrative framework is built on promoting democratic values, human rights, economic openness, and security cooperation. Although these initiatives formally fall under the umbrella of public diplomacy, in practice they function as coordinated influence operations shaping the perceptions of allies, partners, and foreign publics.A significant element of modern American active measures is the use of technology companies as unobtrusive yet extremely powerful amplifiers. U.S. firms such as Meta, Google, and X Corp possess digital infrastructures that indirectly shape the political dynamics of many states through algorithmic ranking, content moderation, the removal of (mis/dis)information, and the control of online narratives. Various investigations[81] have shown continuous communication between U.S. security agencies and major technology platforms, particularly in the context of counterterrorism, foreign influence, and malign information campaigns. This relationship forms the foundation for operations that allow filtering, prioritising, or suppressing specific political content, what many authors describe as a "structural active measure" of the 21st century (Tufekci, 2015; Greenwald, 2020). U.S. active measures also include sophisticated forms of lawfare, especially through sanctions targeting individuals, institutions, and states, as well as the use of international normative mechanisms as instruments of political pressure[82]. Although sanctions are often presented as tools of foreign policy, they function as active measures because they aim to change political behaviour, generate public pressure, or fragment elite decision-making. Parallel to these efforts, U.S. intelligence agencies continue to employ targeted psychological operations and information campaigns, particularly in

[81] In the past, when X was owned by Jack Dorsey and was still called Twitter, influence operations were already present and served as an amplifier of the power of the United States. Researchers discovered that the U.S. Central Command (CENTCOM) conducted coordinated information operations using the Twitter platform, with direct technical support from the company itself. At the request of Pentagon officials, Twitter "whitelisted" dozens of Arabic-language accounts connected to the U.S. military, allowing them to bypass algorithmic detection and platform restrictions (Fang, 2022).

[82] A clear example of using legal instruments to restrict the spread of certain narratives can be seen in the case of the American influencer Evan Kilgore. The FBI Director and his partner filed a series of lawsuits against him and several other influencers after claims circulated on social media suggesting that the Director's partner was allegedly connected to the Israeli Mossad, and implying that their relationship was the result of a so-called "honeypot" operation.

counterterrorism and counter-extremism contexts where the narrative space has become as important as operational activities on the ground.

7.6. Comparative Overview of Active Measures and Intelligence Activities of the U.S., Russia, and Israel

A comparative analysis of active measures in the contemporary international environment makes it possible to understand the different strategic approaches that states use to gain political and security advantages without relying on open military force. Russia, Israel, and the United States represent three paradigmatically different models in the application of active measures, each reflecting a specific combination of historical experience, institutional capacity, and geopolitical objectives (Table 4). The differences between them are not only methodological but also doctrinal, since each actor approaches narrative creation, information management, subversion of political processes, and the shaping of the cognitive environment in the targeted society in a distinct way.

Table 5 Comparative Overview of Active Measures and Intelligence Activities of Russia, Israel, and the United States

Dimension	**Russia**	**Israel**	**United States**
1. Doctrinal framework	Tradition of KGB "active measures" and modern hybrid warfare; strategic focus on destabilising opponents through long-term, covert operations.	Hasbara model, strategic communication, and Mossad's preventive operations; combination of classical PSYOP with digital influence and global narrative campaigns.	Doctrine of democratic expansion, soft power, and digital PSYOP; operations aimed at maintaining the U.S.-led international order.
2. Primary strategic objective	Erosion of internal stability in target states; weakening NATO/EU structures; creating "security vacuums" Russia can exploit.	Protecting state image, delegitimising critics, neutralising threats, and shaping global perceptions of conflict.	Strengthening global hegemony, influencing political processes abroad, and supporting favourable regimes or movements.
3. Main instruments	Disinformation campaigns; infiltration of parties and groups; funding extremists; political subversion; cyber	Paid influencers; digital hasbara networks; targeted PR campaigns; global image-management	Intelligence support to allied groups; military PSYOP; USAID-based soft power; control of

	attacks; assassinations.	operations; Mossad special operations.	global media flows; digital surveillance.
4. Operational approach	Slow, long-term destabilisation; low-intensity covert operations; creation of internal fractures and social atomisation.	High-intensity digital activity; rapid narrative amplification; mix of public diplomacy and covert pressure.	Multi-phase governance approach; combination of public policy, intelligence actions, and legal tools.
5. Targeted actors	Neighbouring states, NATO members, fragile democracies, minority groups, opposition parties, media.	Global audiences, international organisations, influencers, analysts, academics, political critics.	Transitional states, pressured allies, authoritarian regimes in strategic regions, rival powers.
6. Typical operations	Campaigns against Ukraine; poisoning of defectors; support for separatist movements.	Digital PR on Gaza conflict; denial of war crimes; pressure on journalists and NGOs; "preventive eliminations."	Cold War regime-change operations; support for colour-revolution models; anti-ISIS digital campaigns; CIA special operations.
7. Intensity and scale	Medium to high; large volume of long-term operations aimed at political erosion.	High; fast, global digital dominance; low tolerance for reputational risk.	Variable; usually medium intensity with wide operational reach through institutions.
8. Political consequences for targets	Social division, secessionism, democratic decline, loss of trust in institutions, destabilisation.	Oversaturation of the information space; normalisation of narratives; concealment of war crimes; pressure on media and academia.	Regime change; foreign-policy shifts; dependence on U.S. influence; narrative transformation.
9. Level of covertness	High; operations designed to appear as internal developments.	Medium; combination of covert actions and public PR campaigns.	Variable; from secret CIA actions to openly declared "democracy-promotion" projects.
10. Dominant sphere of activity	Information, political, military-intelligence, cyber.	Digital, diplomatic, global media, influencer networks.	Diplomatic, economic, digital PSYOP, global media.

The Russian model of active measures is characterised by the historical continuity of the Soviet "subversive school" and the modern doctrine of hybrid warfare. Its core assumption is that the political destabilisation of an opponent can be achieved through long-term, layered, and multi-phase operations aimed at eroding trust in institutions, encouraging social divisions, and creating political disorientation. Russian intelligence services use a wide range of instruments, including information campaigns, infiltration of political actors, financing extremist groups, supporting separatist movements, and carrying out assassinations. The intensity of these measures ranges from medium to high, their scope includes simultaneous action in the political, informational, and military-intelligence sectors, while the volume of operations implies the long-term maintenance of destabilising processes across multiple geographical and institutional fronts.

The Israeli approach to active measures has a distinct character based on a doctrinal combination of strategic communication, digital operations, and preventive actions carried out by Mossad. The modern concept of hasbara has transformed into a global system of orchestrated perception management that includes intensive use of social media, amplification of narratives through influential individuals, professional PR campaigns, and aggressive communication models aimed at neutralising critical voices. Israeli active measures are high in intensity and operate within a short reaction window. They cover the international information space extensively, while the volume of operations is flexible and scalable depending on reputational risk or current political needs. This approach enables rapid creation of narrative dominance and the establishment of cognitive control within global discourse.

The American model of active measures relies largely on a combination of soft power, institutional influence, and digital psychological operations. At its core, U.S. operations are designed to support and reproduce the existing international order in which the United States holds a dominant role. This includes multi-phase operations involving intelligence support to partner regimes, the use of military PSYOP units, the activation of networks such as USAID, the National Endowment for Democracy (NED), the International Republican Institute (IRI), and the National Democratic Institute (NDI), as well as digital activities aimed at shaping political narratives in strategically important states. The intensity of American active measures is variable, their scope is wide because they involve simultaneous action at the diplomatic, media, technological, and political levels, while the volume depends on risk assessments, priorities, and long-term geopolitical interests.

A comparative overview of the three models shows that each actor uses active measures as an instrument of political violence within a specific operational environment, with differences in doctrine and institutional culture determining the method and effectiveness of these measures. Russia seeks to destabilise its opponent by creating long-term structural weaknesses; Israel aims to establish narrative dominance and reputational control; while the United States employs a broad spectrum of instruments to maintain an international order favourable to its interests. Because of this diversification of approaches, contemporary active measures are not a uniform category but a spectrum of political-intelligence activities whose application is constantly adapted to the dynamics of international politics, technological change, and the needs of strategic action on the global stage.

CONCLUSION

The modern world is marked by the parallel existence of visible and invisible wars, with the latter often producing far-reaching consequences because they operate outside the physical domain and redirect aggression into the sphere of the mind, perception, and collective consciousness. Active measures represent a key weapon of this latent type of warfare, since they enable the manipulation of reality, the reshaping of social conditions, and the steering of political behaviour within the targeted population. Malicious political activities such as propaganda, indoctrination, and subversion are not merely accompanying elements of political conflict, but mechanisms of systematic subjugation of the enemy society, which is viewed as a resource that must be seized, assimilated, and gradually integrated into the interests of the aggressive actor. For this reason, active measures have returned to the centre of intelligence and operational activity after the Cold War and have become a primary instrument of contemporary special warfare.

The main advantage of active measures lies in their ability to operate invisibly and unobtrusively, without the use of physical violence that would provoke a reaction, resistance, and national unity. Unlike conventional war, which typically strengthens cohesion among the attacked population, unconventional action produces the opposite effect. It atomises society, deepens existing tensions, and amplifies differences based on race, class, political orientation, identity, or education, thereby creating conditions for internal fragmentation that becomes useful to the aggressor. The targeted society does not collapse as a result of external force, but as the consequence of its own internal fractures, induced and coordinated from the outside. Here lies the sophistication of political violence carried out through active measures: instead of destroying the body, it undermines the community's ability to think critically, make

rational decisions, and maintain political cohesion. The modern digital environment has further multiplied the power of active measures, allowing identities, perceptions, and narratives to circulate far more rapidly and aggressively than in previous eras. Social networks have become a new battlefield where artificial conflicts are constructed, marginal groups are radicalised, and pseudo-movements emerge without real ideological foundations, giving aggressive actors space for orchestrated intervention. This phenomenon is not new. During the Cold War, the Soviet Union infiltrated and supported various social movements in the United States in order to undermine social cohesion and damage the legitimacy of the political system. Today, the same patterns are repeated, but through more sophisticated digital and cognitive platforms that allow deeper and faster penetration into the social structure of targeted communities.

Although active measures consist of a wide spectrum of activities, their central axis remains disinformation, which enables the creation of a new socio-political narrative through the distribution of false, fabricated, and manipulative information. Soviet operations such as "Denver" and "Pandora" remain lasting examples of successful subversive action, while the modern digital environment generates new disinformation campaigns daily, each finding its audience and repeatedly producing political disruption. In this sense, disinformation is not simply a technique but a fundamental tool for achieving strategic changes within a targeted community.

Therefore, active measures represent a powerful weapon of special warfare through which internal conflicts are induced, social confusion is produced, and the ability of a political community to act rationally is undermined. Their ultimate goal is not only to weaken the population, but to transform it into a docile, passive, and mutually divided mass that unknowingly fulfils the interests of the aggressor. Such a condition creates sufficient space for the unimpeded execution of other political, economic, and intelligence activities that gradually reshape the power structure, sovereignty, and political architecture of the targeted society. Active measures are therefore not merely an auxiliary element of modern confrontation, but the central instrument of political violence and the fundamental mechanism of contemporary intelligence-operational strategies.

Bibliography

Andrew, C., & Mitrokhin, V. (2000). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of KGB.* Basic Books.

Axworthy, M. (2016). *Revolutionary Iran: A History of the Islamic Republic.* Oxford: Oxford University Press.

Bergman, R. (2018). *Rise and Kill First: The Secret History of Israel's Targeted Assassinations.* New York: Penguin Random House LCC.

Bezmenov, Y. A. (1985). Soviet Subversion of The Free World. (G. E. Griffin, Voditelj intervjua) Preuzeto od https://youtu.be/sQN4c3uN_tA

Bloom, W. (2003). *Killing Hope.* London: Zed Books.

Bolsover, G., & Howard, P. (2017). Computational Propaganda and Political Big Data: Moving Toward a More Critical Research Agenda. *Big Data*.

Brady, A.-M. (2015). China's Foreign Propaganda Machine. *Journal of Democracy*, 51-59.

Brooks, S. G., & Wohlforth, W. C. (2016). *America Abroad: The United States' Global Role in the 21st Century.* Oxford : Oxford University Press.

Buzan, B. (1983). *People, States and Fear: National Security Problem in International Relations.* Brighton, Sussex: Wheatsheaf Books.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain - Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* New Yokr: Penguin Press.

CNN. (10. 05 2000). *Inside the KGB - An interview with retired KGB Maj. Gen. Oleg Kalugin*. Preuzeto od CNN Interactive: http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/

Coşkun, A. (22. 06 2023). *Continuity and change in Turkish foreign policy*. Preuzeto od Atlantic Council: https://www.atlanticcouncil.org/content-series/ac-turkey-defense-journal/continuity-and-change-in-turkish-foreign-policy

Donnelly, J. (2006). Sovereign Inequalities and Hierarchy in Anarchy: American Power and International Society. *European Journal of International Relations*, 139-170.

Entman, R. M. (1993). Framing: Toward Clarification of a Fractured Paradigm . *Journal of Communication*, 51–58.

Fang, L. (20. 12 2022). *Twitter Aided the Pentagon in Its Covert Online Propaganda Campaign*. Preuzeto od The Intercept: https://theintercept.com/2022/12/20/twitter-dod-us-military-accounts

Fridman, O. (2017). Hybrid Warfare or Gibridnaya Yoyna? *RUSI Journal 162, no. 1*, 42-49.

Galeotti, M. (2019). Active Measures: Russia's Covert Geopolitical Operations. *Marshall Center Security Insight, no. 31*.

Galeotti, M. (2021). Active Measures: Russia's Covert Global Reach. U G. P. Herd, *Russia's Global Reach: A Security and Statecraft Assessment* (str. 118-126). The George C. Marshall European Center for Security Studies .

Galeotti, M. (2022). *The Weaponisation of Everything - A Field Guide to The New Way of War.* New Heaven and London: Yale University Press.

Haile, Y. A. (2024). The theoretical wedding of computational propaganda and information operations: Unraveling digital manipulation in conflict zones. *New Media & Society*.

Hamilton, C., & Ohlberg, M. (2020). *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World.* New York: Oneworld Publications.

Jasper, S. (2020). *Russian Cyber Operations.* Washington DC: Georgetown University Press.

Katz, E., & Lazarsfeld, P. (1955). *Personal Influence: The Part Played by People in the Flow of Mass Communications.* New York: Free Press.

Kilcullen, D. (2020). *The Dragons and The Snakes: How the Rest Learned to Fight the West.* Oxford: Oxford University Press.

Kostyrev, A. (2023). NATO-Ukraine Strategic Communications: Theory and Practice. *Hileya Scientific Bulletin*, 82-95.

Kramer, M. (2019). Operation "Denver": The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 1). *Journal of Cold War Studies* , 71–123. Preuzeto od The MITPress Reader.

Kux, D. (1985). SOVIET ACTIVE MEASURES AND DISINFORMATION: OVERVIEW AND ASSESSMENT. *The US Army War College Quarterly*, 19-28.

Lange-Ionatamišvili, E. (2015). *Analysis of Russia's information campaign against Ukraine.* Riga: NATO StratCom COE.

McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly*, 176-187.

Middle East Eye. (03. 10 2025). *Israel paying US influencers to reverse negative public opinion: Report*. Preuzeto od Middle East Eye: https://www.middleeasteye.net/news/israel-paying-us-influencers-reverse-negative-public-opinion-report

Middle East Monitor. (02. 10 2025). *Israel pays influencers up to $7,000 per post to occupy information space*. Preuzeto od Middle East Monitor: https://www.middleeastmonitor.com/20251002-israel-pays-influencers-up-to-7000-per-post-to-occupy-information-space

Military Balance. (2015). Complex Crises Call for Adaptable and Durable Capabilities. *Military Balance*, 1-5.

Mueller, R. S. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Washington, D.C. : U.S. Department of Justice .

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, 4*(2), 314-338.

Muhić, E. (2025). Psihološke operacije na društvenim mrežama - primjeri, tehnike, taktike i procedure. *Zaštita i sigurnost, 5*(1). doi:https://doi.org/10.70329/2744-2403.2025.5.9.7

Muhić, E. (2025). *Teoretsko-metodološki aspekti specijalnog rata* . Sarajevo: FKN - Doktorska disertacija.

NATO StratCom COE. (2020). *Social Media Manipulation.* Riga: NATO StratCom COE.

Prados, J. (2006). *Safe for Democracy: The Secret Wars of the CIA.* Chicago : Ivan R. Dee.

Radin, A., Demus, A., & Marcinek, K. (2020). *Understanding Russian Subversion: Patterns, Threats, and Responses.* RAND .

Rid, T. (2019). *Active Measures: The Secret History of Dissinformation and Political Warfare.* New York: Farar, Strauss and Birdux.

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *Journal of Slavic Military Studies*, 101–130.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making.* Council of Europe.

Yablokov, I., & Chatterje-Doody, P. (2022). *Russia Today and Conspiracy Theories.* London: Routledge.

Yaqub, Z., & Tabassum, S. (2025). Israel's Soft Power Application through Digital Diplomacy against Hamas to Iran Wars (2023-2025). *Advance Social Science Archive Journal* .

ODNOSI BOSNE I HERCEGOVINE I SJEVERNOATLANTSKOG SAVEZA

***DOI**: 10.70329/2744-2403.2025.5.10.11*

Pregledni naučni rad

Dr. sc. Amina Smailhodžić[83]

Sažetak

Odnos Bosne i Hercegovine i Sjevernoatlantskog saveza (NATO-a) mijenjao se vremenom. Sjevernoatlantski savez pruža podršku stabilnosti, funkcionalnosti i demokratičnosti Bosne i Hercegovine. S institucijama Bosne i Hercegovine, Sjevernoatlantski savez radi na unapređenju uzajamno korisnog odnosa. Bosna i Hercegovina i Sjevernoatlantski savez zajedno rade na reformi sektora odbrane i sigurnosti u Bosni i Hercegovini, razvijajući odgovornost i transparentnost odbrambenih institucija Bosne i Hercegovine i osiguravajući demokratsku kontrolu nad Oružanim snagama Bosne i Hercegovine. U Bosni i Hercegovini djeluje NATO Štab Sarajevo, čija je osnovna misija zasnovana na partnerstvu. Nato Štab Sarajevo ima dobru saradnju s Oružanim snagama Bosne i Hercegovine kako u oblastima razvoja snaga, obuke i propisa, tako i u planiranju i izvođenju aktivnosti obuke.

***Ključne riječi:** NATO, stabilnost, funkcionalnost, demokratičnost, NATO Štab Sarajevo, partnertsvo*

[83]Univerzitet u Sarajevu - Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, e-mail: asmailhodzic@fkn.unsa.ba

1. Uvod

Početni odnosi između Bosne i Hercegovine i Sjevernoatlantskog saveza datiraju iz kasnih 1990- ih i ranih 2000-ih godina. Organizacija Sjevernoatlantskog ugovora, pod nazivom i Sjevernoatlantski savez, poznat je po skraćenici NATO (eng. North Atlantic Treaty Organisation), predstavlja međunarodnu organizaciju vojno-političke prirode. Potpisivanjem Sjevernoatlantskog ugovora (Washingtonskog ugovora) 1949. godine između država nekadašnjeg zapadnog bloka osnovan je Sjevernoatlantski savez (u daljnjem tekstu NATO). Sjevernoatlantsko vijeće (eng. North Atlantic Council) predstavlja jedino tijelo NATO-a formalno uspostavljeno Sjevernoatlantskim ugovorom, na osnovu kojeg crpi svoje ovlasti. Politički centar NATO-a i sjedište Sjevernoatlantskog vijeća je u Briselu, u Belgiji. U sastavu NATO-a su 32 države. Bosna i Hercegovina ima svojstvo kandidata za članstvo.

Bosna i Hercegovina se kroz svoju sigurnosnu politiku opredijelila za aktivnu međunarodnu saradnju kako na političkom tako i na sigurnosnom i ekonomskom planu. Vanjska politika Bosne i Hercegovine usmjerena je ka očuvanju i unapređenju trajnog mira, sigurnosti i stabilnog demokratskog i sveukupnog državnog razvoja i doprinosa međunarodnom miru i sigurnosti.[84] Iako je pristupanje NATO-u deklarirani ključni strateški cilj vanjske politike BiH, potvrđen Zakonom o odbrani BiH, brojnim parlamentarnim deklaracijama, odlukama i strateškim dokumentima vanjske politike Predsjedništva BiH, postoji snažan nesporazum među domaćim političkim elitama, konkretnije između lidera RS-a i FBiH-a, u vezi sa vanjskopolitičkim odnosom BiH prema NATO-u (Hasić & Džananović, 2023).

Primarni ciljevi Bosne i Hercegovine s NATO-om vezani su za vladavinu zakona, razvijanje saradnje sa euroatlantskim i europskim strukturama, demokratsku kontrolu Oružanih snaga, kao i obavještajno – sigurnosnog sistema, vojnu interoperabilnost, planiranje i budžetiranje odbrane, upravljanje ljudskim resursima i kriznim situacijama, javnu diplomatiju i reformu sektora odbrane. Uspostava mira i transparentnosti institucija predstavljaju misiju NATO-a.

Savez se, u ispunjavanju svojih zadataka, temelji na visokom stepenu koordiniranja i planiranja na političkom nivou, kao i na vojnom odbrambenom polju (Najetović, 2001). Države koje su pristupile NATO savezu postigle su pomak u skoro svim segmentima. Značajno su unaprijedile sigurnosne i

[84]Više pogledati: Prezentacijski dokument. Partnerstvo za mir. Decembar. 2006. , https://mod.gov.ba/files/file/nato/prez_dokum_hr.pdf, 16.10.2025.

institucionalne kapacitete. NATO je međudržavna organizacija koja nema vlastite oružane snage. Većina snaga koja je na raspolaganju NATO-u u potpunosti ostaje pod nacionalnim zapovjedništvom i kontrolom, sve dok države članice ne pozovu na izvršenje zadatka (Turković, 2006).

Bosna i Hercegovina proces pridruživanja najvećem vojno-političkom savezu obavlja još od 2006. godine potpisivanjem programa Partnerstvo za mir (eng. Partnership for Peace –PfP), koji predstavlja glavni indikator razvoja sigurnosnih odnosa države partnera i NATO-a. Na osnovu programa PfP razvija se i intenzivira vojna i politička saradnja u Europi, smanjuje se prijetnja miru i dodatno se jača stabilnost.

2. Razvoj odnosa Bosne i Hercegovine sa NATO-om

Bosna i Hercegovina godinama razvija bliske odnose s NATO savezom. Saradnja je nastala iz nastojanja da se zaustavi rat 1990-ih godina i intenzivirala je kroz različite partnerske programe. NATO je podržao nastojanja Ujedinjenih nacija (u daljnjem tekstu UN-a) da se prekine rat u Bosni i Hercegovini u periodu 1992. - 1995. godine. U Bosnu i Hercegovinu je poslije šest dana od potpisivanja Općeg okvirnog sporazuma za mir, 14. decembra 1995. godine poslao Multinacionalne snage za implementaciju sa mandatom UN-a (u daljnjem tekstu IFOR). Osnovna zadaća IFOR-a je bila dosljedna provedba vojnih elemenata Općeg okvirnog sporazuma za mir. IFOR-ova misija podrazumijevala je da se osigura prestanak neprijateljstava, kao i da se izvši razdvajanje vojski i premosti teritorij između dva entiteta. U roku od godinu dana, IFOR je završio svoj zadatak, a u decembru 1996. godine zamijenile su ga manje Stabilizacijske snage (u daljnjem tekstu SFOR). Misija SFOR-a je unaprijeđena i obuhvatala je osim podrške napredovanja mirovnog mehanizma i podršku civilnim agencijama, koje su bile usmjerene na uspostavljanje trajnog mira.

Deklarirani cilj Bosne i Hercegovine je postizanje punog članstva u vojno-političkom savezu. Savez svojim članicama pruža sigurnost i nastoji postići stabilnost i sigurnost na cjelokupnom euroatlantskom području. Pomoću komplementarnih mehanizama odvija se saradnja Bosne i Hercegovine i NATO-a. Svrha tih mehanizama je povećanje interoperabilnosti bezbjednosno-odbrambenih kapaciteta države koja teži priključenju Savezu, kroz veoma zahtjevan proces izgradnje standarda i sistema vrijednosti koji je kompatibilan sa NATO članicama. [85]Način priključenja NATO-u ima specifičnu, jasno definisanu proceduru. Integracija u NATO se u tehničkom smislu odvija kroz učešće u

[85] Više pogledati: Partner. Mjesečnik o evroatlantskim integracijama, odbrani i vojsci. Broj 2, mart 2008., http://www.mod.gov.me/files/1206620684.pdf, 10.11.2025.

političko-vojnom programu Partnerstvu za mir (u daljnjem tekstu PfP) i u Akcionom planu za članstvo (Membership Action Plan - MAP). Bosna i Hercegovina je obznanila svoju namjeru da obavi promjene koje su potrebne da bi do sredine 2004. godine postala kredibilan kandidat za ulazak u PfP, program koji bi predstavljao korak naprijed za integraciju u NATO, kao i u Europsku uniju (EU). Promjene koje je Bosna i Hercegovina trebala izvršiti podrazumijevale su transformaciju Oružanih snaga u savremene, sposobne snage, koje su bogato opremljene. Osim toga, Bosna i Hercegovina trebala je na državnom nivou uspostaviti efikasnu komandu i kontrolu uz parlamentarni nadzor nad svim pitanjima koja se tiču odbrane.

Donošenje novih zakona u području odbrane 2003. i 2004. godine, kao i promjene koje su se dogodile u entitetskim ustavima svakako su osigurale jedinstven razvoj odbrambene strukture, s određenom podjelom odgovornosti između entiteta i države. U Bijeloj knjizi odbrane iz 2005. godine navedeno je da je proces reformi odbrambenog sistema Bosne i Hercegovine započeo 2003. godine osnivanjem Komisije za reformu u oblasti odbrane Bosne i Hercegovine. Proces reformi odbrambenog sistema Bosne i Hercegovine podstaknut je sa mnogim barijerama i odlukama za otklanjanjem takvih barijera koje su postojale među Vojskom Federacije Bosne i Hercegovine i Vojskom Republike Srpske. Barijere su se ogledale u nadležnostima države i entiteta Federacije Bosne i Hercegovine i Republike Srpske kada je u pitanju oblast odbrane, sastav i veličina koji su zagušili standarde, nepotpunost kontrole i komande na državnom nivou, nepotpunost transparentnosti, kao i ogromni finansijski troškovi koji su vezani za odbranu i neadekvatnost opreme (Smailhodžić, 2019). Radni okvir Komisije za reformu u oblasti odbrane Bosne i Hercegovine činili su principi koji se mogu rezimirati na način da je Bosna i Hercegovina iskazala želju da uđe u NATO, dok je NATO postavio uvjet da Bosna i Hercegovina treba imati jednu profesionalnu vojnu silu, jer struktura odbambenog sistema nije bila prihvatljiva. Bosna i Hercegovina je trebala ukinuti i služenje obaveznog vojnog roka. Sve bi to zadovoljilo uvjete koje je postavio NATO, a istovremeno i potrebe Bosne i Hercegovine.

Odnosi između Bosne i Hercegovine i NATO-a ostvaruje se partnerstvom, koje obuhvata ne samo savjetovanje već i podršku Bosni i Hercegovini u promovisanju mira, stabilnosti, provođenju procesa reformi i jačanju odbrambenih institucija. Odnos Bosne i Hercegovine i NATO-a je krajem 2004. godine doživio promjenu kada je NATO sve zadatke, koje se odnose na provođenje mira predao Snagama Europske unije i na taj način znatno smanjio svoje prisustvo na NATO Štab. Nakon što su mirovne Snage Europske unije (u daljnjem tekstu EUFOR) preuzele odgovornost za održavanje bezbjednosti u Bosni i Hercegovini 2004. godine, NATO je nastavio da pruža podršku transformaciji bosanskohercegovačkog društva kroz aranžmane Berlin plus. Osnovan je NATO vojni Štab u Sarajevu

kako bi direktno pomogao lokalnim vlastima u reformama odbrane. Pomoću NATO Štaba Sarajevo, NATO na zahtjev vlasti pruža Bosni i Hercegovini pomoć i savjete. Aktivnosti NATO Štaba su nadopunjene kako bi objedinile cilj Bosne i Hercegovine da pristupi NATO- u.

Ključni element za ulazak u PfP predstavlja Okvirni dokument, izdat od NATO-a 1994. godine. Bosna i Hercegovina je prihvatila poziv u program PfP i na osnovu toga potvrdila posvećenost ciljevima i načelima, koji su naznačeni u Okvirnom dokumentu PfP-a. Okvirni dokument, Bosna i Hercegovina je potpisala 14. decembra 2006. godine na svečanosti koja se održala u Briselu, u Štabu NATO-a, tačno poslije 11. godina od potpisivanja Općeg okvirnog sporazuma za mir. U novembru 2006. godine na NATO Samitu održanom u Rigi, Bosna i Hercegovina je pozvana,a u decembru iste godine formalno je pristupila NATO programu Partnerstvo za mir (Hasić & Džananović, 2023). Za Bosnu i Hercegovinu ulazak u PfP je značio bitan korak u jačanju saradnje, a uključivao je modernizaciju Oružanih snaga Bosne i Hercegovine, jačanje demokratske kontrole i izvođenje zajedničkih vježbi. NATO, svjestan toga da je Općim okvirnim sporazumom za mir uveden posebni ustavni poredak, bio je spreman da prihvati odvojene entitetske oružane snage, pod uvjetom da se prevaziđu unutrašnje podjele, da se ojača podrška državnih institucija, da se uhapse ratni zločinci i da se ispune odgovarajući kriteriji, koji podrazumijevaju sigurnosnu politiku Bosne i Hercegovine i demokratski parlamentarni nadzor na nivou države, zajedničku doktrinu, standarde opreme i obuke za Vojsku Federacije i Vojsku Republike Srpske, zajedničke pokazne vježbe, transparentnost odbrambenih planova i transparentnost finansiranja. Osim toga, NATO je zahtijevao i promovisanje pomirenja, regionalne saradnje i stabilnosti.

Bosna i Hercegovina podržava temeljni koncept PfP i želi doprinijeti sigurnosti i stabilnosti u Euroatlantskom prostoru, smanjenju prijetnji miru i jačanju veza kroz aktivnu saradnju, te posvećenost općim demokratskim principima.[86] Proces reforme odbrane Bosne i Hercegovine zasnovan je na principu kolektivne sigurnosti i zahtijeva stvaranje profesionalnih Oružanih snaga, koje su interoperabilne sa snagama NATO-a. Kao partner, Bosna i Hercegovina nastoji sudjelovati u stvaranju savremene sigurnosne politike na prostoru Europe. NATO je u vezi ambicije BiH zauzeo pozitivan stav i ne samo definirao šta zemlja treba uraditi da postane kredibilan kandidat za članstvo u PfP-u nego i pomagao napore BiH da to ostvari (Maxwell &Olsen, 2013).

U tu svrhu, Bosna i Hercegovina učestvuje od maja 2007. godine u Procesu planiranja i preispitivanja (u daljnjem tekstu PARP). Poslije PARP-a predstoji

[86] Više pogledati: https://www.mvp.gov.ba/vanjska_politika_bih/multilateralni_odnosi/sjevernoatlantski_savez_nato/bih_i_nato/?id=112, 21.10.2025.

Individualni partnerski program (IPP), koji predstavlja radni program između države članice PfP-a i NATO-a. Poslije toga slijedi Individualni partnerski akcijski plan (IPAP), koji predstavlja mehanizam saradnje države partnera i NATO-a. Viši komplementarni nivo u kojem Bosna i Hercegovina učestvuje od aprila 2008. godine, od Samita NATO- a u Bukureštu je Intenzivirani dijalog (ID). Na osnovu Akcionog plana za članstvo (u daljnjem tekstu MAP-a) od Bosne i Hercegovine se traži da ostvari odgovarajuće ciljeve koji se odnose ne samo na vojna, odbrambena i sigurnosnu pitanja već i na politička, ekonomska i pravna pitanja u području resursa. Pravna pitanja zahtijevaju da Bosna i Hercegovina ima uređen zakonodavni sklop tako da saradnja s NATO-om bude kompatibilna u skladu s nacionalnim pravnim mehanizmom. Predsjedništvo BiH je u junu 2009. godine donijelo odluku da aplicira za MAP. Bh. delegacija, predvođena predsjedavajućim Predsjedništva BiH Željkom Komšićem, je 2. oktobra 2009. godine zvanično uručila aplikaciju za ulazak BiH u Akcijski plan za članstvo. Bosna i Hercegovina je očekivala da će biti pozvana u MAP u decembru 2009. godine, za vrijeme sastanka Sjevernoatlantskog vijeća NATO-a na ministarskom nivou, međutim, to se nije desilo, prvenstveno zbog zastoja u reformskim procesima u BiH. Međutim, u zvaničnoj izjavi generalnog sekretara NATO-a nakon ovog sastanka kaže se da nije pitanje da li će BiH ući u MAP i NATO, nego je pitanje kada će se to desiti. On je pozvao političke lidere u BiH da nastave sa reformskim procesima, jer će od pozitivnih rezultata zavisiti i datum kada će BiH ući u MAP.[87] Rezultat toga bio je uslovno članstvo. Bosna i Hercegovina je 2010. godine dobila mogućnost aktiviranja MAP-a. MAP predstavlja neophodan korak za integraciju Bosne i Hercegovine u NATO. Međutim, proces je usporen zbog unutrašnjih političkih neslaganja.

Geneza odnosa i pravaca djelovanja Bosne i Hercegovine u geopolitičkom sistemu međunarodnih odnosa, posebno u kontekstu saradnje ili potencijalnog članstva u NATO-u, primarno su obilježile unutrašnje složenosti i vanjski pritisci. Historijski kontekst zamršenih odnosa između postjugoslovenskih i balkanskih država s jedne strane i NATO-a i moćnih igrača poput Rusije s druge strane, pružaju duboko ukorijenjenu strukturu za razumijevanje izazova sa kojima se BiH danas suočava. Sistem kolektivne odbrane NATO-a nudi privlačno obećanje vojne sigurnosti i zaštite od potencijalnih prijetnji, garancija od koje bi Bosna i Hercegovina mogla imati velike koristi. Međutim, etnopolitičke podjele države, kombinovane sa vanjskim, pogotovo malignim uticajima, iz Srbije, čiju vanjsku politiku političke vođe Republike Srpske replikuju, te Rusije, učinile su putanju BiH ka članstvu NATO zamršenom i ispresijecanom (Hasić & Džananović, 2023).

NATO je danas finansijski najbogatija organizacija Svijeta. Postavio je sebi za cilj osiguranje zajedničke odbrane da bi na temelju toga garantirao buduću

[87] Više pogledati: Atlantska inicijativa. Bosna i Hercegovina i NATO. Februar 2010.

sigurnost i očuvao mir. Temelji se na visokom stepenu planiranja i koordiniranja na vojnom, odbrambenom i političkom nivou. Države koje su pristupile NATO savezu postigle su pomak u skoro svim segmentima. Značajno su unaprijedile sigurnosne i institucionalne kapacitete. NATO nastoji adekvatno odgovoriti na skoro sve izazove nestabilnosti savremenog svijeta. Kolektivnom odbranom, članom 5 Sjevernoatlantskog ugovora izašao je iz svojih granica postavši globalni učesnik. NATO je ugradio pravne okvire svojih cjelovitih reformi na unutrašnjem planu, koje se tiču kako strukture i komandovanja tako i konkretnih snaga. Osim toga, NATO je odredio razvijanje odnosa sa mnogo različitim državama i regijama svijeta, što je naročito značajno za dugačku paletu ciljeva koje će samostalno ili zajedno s drugim odgovarajućim organizacijama u međunarodnoj zajednica ostvarivati. NATO garantuje sigurnost. Svoje vojne i političke strukture je transformirao i prilagodio kako bi ispunio zadatke osiguravanja mira i upravljanja u kriznim situacijama. Pripadanje NATO-u zahtijeva i intenzivno djelovanje kako bi sigurnost bila uvećana. Svaka država članica ima posebne obaveze koje se tiču odbrane i sigurnosti.

Shvaćanje prirode sigurnosti uključuje i domene koje podrazumijevaju aktivno uključivanje institucija u oblasti ekonomije. S tim u vezi, svaka država koja želi da postane članica NATO-a, prolazi i kroz niz ekonomskih reformi u okviru procesa transformacije društva, čime se otvaraju nove razvojne mogućnosti. Članstvo pruža pouzdanu garanciju da će članice priskočiti jedna drugoj u pomoć, pojedinačno ili kolektivno, u slučaju oružanog napada na bilo koju od njih. Nijedna zemlja nije primorana da računa samo na sebe i vlastite ekonomske resurse u suočavanju sa temeljnim sigurnosnim izazovima. Istovremeno, nijedna zemlja se ne odriče ni prava da ispunjava obaveze prema svom narodu, te je i dalje odgovorna za svoju odbranu. NATO to ne radi umjesto njih; on im samo daje sredstva da djeluju kao cjelina. Savez omogućava zemljama članicama da zajedničkim naporima ostvare ključne ciljeve nacionalne sigurnosti. Sveobuhvatnoj stabilnosti doprinosi osjećaj da zemlje uživaju u jednakoj sigurnosti u svojstvu članica Saveza, nezavisno od svog položaja ili vojne snage.[88] Bosna i Hercegovina je država, koja unutar Općeg okvirnog sporazuma za mir u Bosni i Hercegovini izgrađuje mir, uz ovlaštenja Ureda visokog predstavnika - Aneksa 10 i uz prisustvo europskih vojnih snaga EUFOR Althea. Sigurnosni izazovi sa kojima se suočava trebaju se posmatrati u okviru odnosa globalnog okruženja. U institucijama odbrane sistem odbrambenog planiranja je usaglašen je sa NATO normama. Opća sigurnost, mir i stabilnost su preduvjet i nužan ambijent za dobrobit i funkcioniranje svakog društva.[89] Sigurnost je cilj kojem teži svake društvena zajednica i država, istodobno ona je nasušna potreba i želja

[88]Više pogledati: Atlantska inicijativa. Bosna i Hercegovina i NATO. Februar 2010.
[89]Više pogledati: Bijela knjiga odbrane Bosne i Hercegovine. Juni 2005. godine. http://www.mod.gov.ba/files/file/dokumenti/Bijela-knjiga-bs.pdf, 7.10.2025.

svih pripadnika društvene zajednice, nužan i bitan uvjet reda i mira što omogućava stabilan društveni razvitak i preduvjet razvitka društva i države uopće (Vencl, Jamnić, & Pušeljić, 2021).

Ključni element za ostvarivanje vojne sigurnosti Bosne i Hercegovine je postati članicom NATO-a, jer joj u tom slučaju njen nacionalni suverenitet i teritorijalni integritet garantira cijeli Savez.[90] U Briselu, u sjedištu NATO-a, na sastanku Komiteta za partnerstvo i kooperativnu sigurnost usvojen je Prvi individualno prilagođeni partnerski program (ITPP – Individual Tailored Partnership Programme) između Bosne i Hercegovine i NATO-a. Time je učinjen važan korak u okviru implementacije MAP-a. Glavni ciljevi Bosne i Hercegovine u provođenju saradnje s NATO-om zahtijevaju jačanje vladavine zakona, demokratsku kontrolu oružanih snaga, veću saradnju s europskim i euroatlantskim strukturama i rješavanje sigurnosnih problema. Ostvarenim kvalitetom suradnje Bosne i Hercegovine sa NATO savezom treba da se potvrdi da je ona pouzdan partner i da posjeduje respektivne kapacitete, koji mogu značajno da doprinesu jačanju mira i stabilnosti u regiji jugoistočne Europe. Za Bosnu i Hercegovinu regionalna obrambena suradnja i odnosi sa susjedima važan su aspekt njihove euroatlantske politike. Takvom suradnjom će stvoriti uvjete za unutarnju i vanjsku interoperabilnost, a time i veću operativnu sposobnost za izvršavanje misija Oružanih snaga Bosne i Hercegovine, a posebno misija očuvanja mira i humanitarnih misija (Petrović, 2022)

Bosna i Hercegovina ima prioritet da zaštiti neovisnost, suverenitet i teritorijalni integritet, da zaštiti ustavni poredak i njime zajamčena ljudska prava i slobode, da razvija ekonomiju kao preduvjet stvaranja realnih uslova za poboljšanje životnog standarda građana, priključenje Europskoj Uniji, kao najpovoljnijem načinu realizacije ovog prioriteta i da se priključi i pristupi kolektivnim sistemima sigurnosti. Bez ikakvih ograničenja Bosna i Hercegovina prihvata koncept kolektivne sigurnosti, kao najznačajniji stup vlastite vojne strategije, te zbog toga teži ka što bržem ulasku u NATO. Bosna i Hercegovina, bez ikakve sumnje, bezbjedonosno je najugroženija država, ne samo zapadnog nego i čitavog Balkana, a možda i Evrope u cjelini. Bez obzira što trenutno nije suočena s neposrednom vanjskom prijetnjom, zbog nerazriješenih odnosa vezanih za blisku ratnu prošlost nalazi se u latentno neprijateljskom okruženju. Osim toga, u Bosni i Hercegovini prisutan je permanentni rizik od unutrašnjeg cijepanja izazvanog djelovanjem nemirujućih etničkih podjela. Utoliko više članstvo u najmoćnijem vojnom savezu na svijetu za Bosnu i Hercegovinu trebalo bi predstavljati ne samo

[90] https://www.mvp.gov.ba/vanjska_politika_bih/multilateralni_odnosi/sjevernoatlantski_savez_nato/bih_i_nato/?id=112, 21.10.2025.

poželjan, već i najlogičniji mogući izbor.[91]Bosna i Hercegovina je prvi Program reformi predala NATO-u 2019. godine, što predstavlja korak naprijed dosadašnjoj saradnji.

3. Zaključak

NATO, kao vojno-politička organizacija osigurava kako pomoć tako i usluge državama. Kroz kolektivne odnose nastoji riješiti sigurnosne problem kroz prizmu međukolektivnih odnosa i saradnju. Ima za cilj unaprijediti odbrambene kapacitete država kako bi se povećala njihova sigurnost. Odnos Bosne i Hercegovine i NATO-a obilježen je dugoročnom saradnjom zasnovanom na Partnerstvu, sigurnosnim reformama i podršci stabilnosti države. NATO je odigrao glavnu ulogu u poslijeratnoj obnovi Bosne i Hercegovine. Odnosi Bosne i Hercegovine i NATO-a su se nastavili širiti izvan okvira Općeg okvirnog sporazuma za mir. Bosna i Hercegovina je država partner NATO-a, ali još uvijek ne i članica. Saradnja se nastavlja kroz Program reformi, zajedničke vježbe, podršku reformi odbrane i sigurnosti i pomoć u kriznim situacijama. Pristupanje NATO-u ovisi od postizanja političkog konsenzusa unutar Bosne i Hercegovine i nastavka reformi. Dok se tehnički kapaciteti i saradnja kontinuirano poboljšavaju, različiti politički stavovi ostaju glavna prepreka daljnjem napretku. Iz tog razloga, odnos Bosne i Hercegovine može se opisati kao trenutno stabilno partnerstvo, koje za posljedicu ima otvoreno pitanje konačnog strateškog opredjeljenja. Svakako važno je napomenuti da pristupanje Bosne i Hercegovine NATO-u značajno doprinosi poboljšanju trenutne sigurnosne situacije. NATO garantuje zaštitu suvereniteta i teritorijalnog integriteta Bosne i Hercegovine. Pristupanje Bosne i Hercegovine NATO – u značajno je i iz segmenta politike. Ulaskom u NATO savez Bosna i Hercegovina ne samo da bi dodatno unaprijedila vladavinu prava i demokratiju već bi i dodatno učvrstila regionalnu saradnju. Najznačajnije pogodnosti ulaska u NATO su stabilnost i osnažena sigurnost. Oružane snage Bosne i Hercegovine ostvarile su veliki napredak u prilagođavanju NATO standardima.

[91] Više pogledati: Zaključci o potrebi članstva Bosne i Hercegovine u NATO detaljno opisani u: Marinković, Milan, *Zašto prijem u NATO mora biti prioritet BiH*. (2013)., https://www.tacno.net/polemika/zasto-je-opasno-forsirati-clanstvo-u-nato-paktu-bez-unutrasnjeg-koncenzusa-u-bih/, 15.10.2025.

LITERATURA

1. Hasić, J., & Džananović, N., 2023. Perspektive sa margina. Dekonstrukcija preovladavajućih političkih narativa o odnosima Bosne i Hercegovine sa NATO-om. Sarajevo: Fakultet političkih nauka Univerziteta u Sarajevu.
2. Maxwel, R. &Olsen A., J.,2013. Destinacija NATO: Reforma odbrane u Bosni i Hercegovini 2003-2013. London: Royal United Services Institute for Defence and Security Studies. Whitehall
3. Najetović, D., 2001. Širenje sigurnosti u Evro-Atlantskom području-uloga NATO-a i partnerskih zemalja. Sarajevo: Vijeće Kongresa bošnjačkih intelektualaca.
4. Petrović, Ž., 2022. Ujedinjeni narodi i NATO u ratnoj i postratnoj Bosni i Hercegovini. Sarajevo: Zaštita i sigurnost. Godina 2. Broj 1, 90-109.
5. Smailhodžić, A., 2019. Saradnja Sjevernoatlantskog saveza i Bosne i Hercegovine. Sarajevo: Kriminalističke teme, 17-36.
6. Turković, B., 2006. NATO od sigurnosnog saveza do savremenih izazova. Sarajevo: Centar za sigurnosne studije.
7. Vencl, K., Jamnić, S., & Pušeljić, M., 2021. Policija kao temelj sigurnosti u državi. Sarajevo: Zaštita i sigurnost. Godina 1. Broj 1, 19-34.

a. Ostalo

8. Atlantska inicijativa., 2010. Bosna i Hercegovina i NATO. Sarajevo.
9. Bijela knjiga odbrane Bosne i Hercegovine. 2005., dostupno na: https://www.mod.gov.ba/files/file/dokumenti/Bijela-knjiga-bs.pdf . (Pristupljeno: 7.10.2025.)
10. Partner. 2008. Mjesečnik o evroatlantskim integracijama, odbrani i vojsci. Broj 2., dostupno na: http://www.mod.gov.me/files/1206620684.pdf . (Pristupljeno: 10.11.2025.)

11. Prezentacijski dokument. 2006. Partnerstvo za mir, dostupno na: https://mod.gov.ba/files/file/nato/prez_dokum_hr.pdf . (Pristupljeno: 16.10.2025.)

12. https://www.mvp.gov.ba/vanjska_politika_bih/multilateralni_odnosi/sjevernoatlantski_savez_nato/bih_i_nato/?id=112 , (Pristupljeno: 21.10.2025.)

13. https://www.tacno.net/polemika/zasto-je-opasno-forsirati-clanstvo-u-nato-paktu-bez-unutrasnjeg-koncenzusa-u-bih/ . (Pristupljeno: 15.10.2025.)

THE RELATIONS BETWEEN BOSNIA AND HERZEGOVINA AND THE NORTH ATLANTIC TREATY ORGANIZATION

DOI: *10.70329/2744-2403.2025.5.10.11*

Overview Scientific Paper

Dr. sc. Amina Smailhodžić

Abstract

The relationship between Bosnia and Herzegovina and the North Atlantic Treaty Organization (NATO) has evolved over time. NATO provides support for the stability, functionality, and democracy of Bosnia and Herzegovina. Together with the institutions of Bosnia and Herzegovina, NATO works to improve a mutually beneficial relationship. Bosnia and Herzegovina and NATO collaborate on the reform of the defense and security sector in Bosnia and Herzegovina, enhancing the responsibility and transparency of Bosnia and Herzegovina's defense institutions, and ensuring democratic control over the Armed Forces of Bosnia and Herzegovina. NATO Headquarters Sarajevo operates in Bosnia and Herzegovina, with its main mission focused on partnership. NATO Headquarters Sarajevo maintains a strong cooperation with the Armed Forces of Bosnia and Herzegovina in areas such as force development, training and regulations, as well as in planning and executing training activities.

Keywords: *NATO, stability, functionality, democracy, NATO Headquarters Sarajevo, partnership*

1. Introduction

The initial relations between Bosnia and Herzegovina and the North Atlantic Treaty Organization date back to the late 1990s and early 2000s. The North Atlantic Treaty Organization, commonly known by its abbreviation NATO (English: North Atlantic Treaty Organization), is an international military-political organization. The North Atlantic Treaty Organization (hereinafter NATO) was established by the signing of the North Atlantic Treaty (Washington Treaty) in 1949, between the countries of the former Western Bloc. The North Atlantic Council is the only body of NATO formally established by the North Atlantic Treaty, and it derives its authority from it. The political center of NATO and the headquarters of the North Atlantic Council are located in Brussels, Belgium. NATO currently consists of 32 member states, with Bosnia and Herzegovina holding the status of a membership candidate.

Through its security policy, Bosnia and Herzegovina has committed to active international cooperation in political, security, and economic matters. Bosnia and Herzegovina's foreign policy is focused on maintaining and enhancing lasting peace, security, democratic stability, and overall state development, as well as contributing to international peace and security.[92] Although NATO membership is declared as a key strategic goal of Bosnia and Herzegovina's foreign policy, confirmed by the Law on Defense of Bosnia and Herzegovina, numerous parliamentary declarations, decisions, and strategic foreign policy documents of the Presidency of Bosnia and Herzegovina, there remains a strong disagreement among domestic political elites, particularly between the leaders of the Republika Srpska (RS) and the Federation of Bosnia and Herzegovina (FBiH), regarding Bosnia and Herzegovina's foreign policy orientation toward NATO (Hasić & Džananović, 2023).

Bosnia and Herzegovina's primary objectives with NATO are related to the rule of law, developing cooperation with Euro-Atlantic and European structures, democratic control of the Armed Forces, intelligence and security systems, military interoperability, defense planning and budgeting, human resources and crisis management, public diplomacy, and defense sector reforms. The establishment of peace and transparency in institutions is a key mission of NATO.

In fulfilling its tasks, NATO relies on a high degree of coordination and planning at the political level, as well as in the military defense sector (Najetović, 2001). Countries that have joined NATO have made significant progress in almost all

[92] For more details, see The Presentation Document Partnership for Peace. December 2006, https://mod.gov.ba/files/file/nato/prez_dokum_hr.pdf, 16.10.2025.

areas, particularly in enhancing their security and institutional capacities. NATO is an intergovernmental organization that does not have its own armed forces. Most of the forces available to NATO remain entirely under national command and control, unless member states call upon them to execute a task (Turković, 2006).

Bosnia and Herzegovina has been undergoing the process of joining the largest military-political alliance since 2006, when it signed the Partnership for Peace (PfP) program, which is the primary indicator of the development of security relations between the partner country and NATO. Based on the PfP program, military and political cooperation in Europe is developed and intensified, the threat to peace is reduced, and stability is further strengthened.

2. Development of relations between Bosnia and Herzegovina and NATO

Bosnia and Herzegovina has been developing close relations with NATO over the years. The cooperation originated from efforts to halt the war of the 1990s and intensified through various partnership programs. NATO supported the efforts of the United Nations (hereinafter UN) to end the war in Bosnia and Herzegovina between 1992 and 1995. After the signing of the General Framework Agreement for Peace (Dayton Agreement) on December 14, 1995, NATO sent the Multinational Implementation Force (hereinafter IFOR) to Bosnia and Herzegovina six days later, under a UN mandate. The primary task of IFOR was to ensure the implementation of the military provisions of the General Framework Agreement for Peace. IFOR's mission included ensuring the cessation of hostilities, separating the warring factions, and bridging the territory between the two entities. Within a year, IFOR completed its mission, and in December 1996, it was replaced by the smaller Stabilization Force (hereinafter SFOR). The mission of SFOR was enhanced and expanded to include support for the progress of the peace mechanism and assistance to civil agencies focused on establishing lasting peace.

The declared goal of Bosnia and Herzegovina is to achieve full membership in the military-political alliance. NATO provides security to its members and aims to achieve stability and security across the entire Euro-Atlantic region. Through complementary mechanisms, cooperation between Bosnia and Herzegovina and NATO takes place. The purpose of these mechanisms is to increase the interoperability of the country's defense and security capacities, which seeks to join the Alliance, through a highly demanding process of building standards and

systems of values compatible with NATO members.[93] The process of NATO accession follows a specific, clearly defined procedure. Technically, integration into NATO occurs through participation in the political-military Partnership for Peace (hereinafter PfP) program and the Membership Action Plan (hereinafter MAP). Bosnia and Herzegovina announced its intention to make the necessary changes to become a credible candidate for joining the PfP program by mid-2004. This would represent a step forward for integration into NATO and the European Union (EU). The changes Bosnia and Herzegovina needed to implement involved transforming the Armed Forces into modern, capable forces that are well-equipped. Additionally, Bosnia and Herzegovina needed to establish efficient command and control at the state level, along with parliamentary oversight over all defense-related issues.

The adoption of new defense laws in 2003 and 2004, as well as changes in the entity constitutions, ensured the unified development of the defense structure, with a certain division of responsibilities between the entities and the state. The 2005 White Paper on Defense stated that the process of reforming Bosnia and Herzegovina's defense system began in 2003 with the establishment of the Commission for the Reform of Bosnia and Herzegovina's Defense. The process of reforming the defense system of Bosnia and Herzegovina was driven by many barriers and decisions aimed at removing these barriers, which existed between the Armed Forces of the Federation of Bosnia and Herzegovina and the Armed Forces of the Republic of Srpska. The barriers were reflected in the competences of the state and the entities of the Federation of Bosnia and Herzegovina and the Republic of Srpska in the defense sector, the composition and size of which hindered meeting standards, the incompleteness of control and command at the state level, lack of transparency, as well as the enormous financial costs associated with defense and inadequate equipment (Smailhodžić, 2019). The working framework of the Commission for Defense Reform in Bosnia and Herzegovina was built upon principles that can be summarized by the fact that Bosnia and Herzegovina expressed its desire to join NATO, while NATO set the condition that Bosnia and Herzegovina must have one professional military force, as the defense system structure was deemed unacceptable. Bosnia and Herzegovina also needed to abolish mandatory military service. Meeting these conditions would fulfill NATO's requirements and at the same time address Bosnia and Herzegovina's defense needs.

The relationship between Bosnia and Herzegovina and NATO is based on partnership, which encompasses not only advisory support but also assistance in

[93] For more details, see: Partner: Monthly Magazine on Euro-Atlantic Integration, Defense and the Armed Forces, Issue No. 2, March 2008, http://www.mod.gov.me/files/1206620684.pdf, 10.11.2025.

promoting peace, stability, implementing reform processes, and strengthening defense institutions. Relations between Bosnia and Herzegovina and NATO underwent a significant change at the end of 2004, when NATO transferred all tasks related to peace implementation to the European Union Force (hereinafter EUFOR), significantly reducing its presence, with only NATO Headquarters remaining in Sarajevo. After EUFOR took responsibility for maintaining security in Bosnia and Herzegovina in 2004, NATO continued to support the transformation of Bosnian society through the Berlin Plus arrangements. NATO established a military Headquarters in Sarajevo to directly assist local authorities in defense reforms. Through NATO Headquarters Sarajevo, NATO, at the request of the Bosnian authorities, provides assistance and advice. NATO's activities are complemented to consolidate Bosnia and Herzegovina's goal of joining NATO.

A key document for joining the PfP program is the Framework Document, issued by NATO in 1994. Bosnia and Herzegovina accepted the invitation to join the PfP program and confirmed its commitment to the objectives and principles outlined in the PfP Framework Document. Bosnia and Herzegovina signed the Framework Document on December 14, 2006, during a ceremony held at NATO Headquarters in Brussels, exactly 11 years after the signing of the General Framework Agreement for Peace. In November 2006, at the NATO Summit in Riga, Bosnia and Herzegovina was invited, and in December of the same year, it formally joined the NATO Partnership for Peace program (Hasić & Džananović, 2023).

For Bosnia and Herzegovina, joining the PfP represented an important step in strengthening cooperation, involving the modernization of Bosnia and Herzegovina's Armed Forces, strengthening democratic control, and conducting joint exercises. NATO, recognizing that the General Framework Agreement for Peace had introduced a special constitutional order, was willing to accept separate entity armed forces, provided that internal divisions were overcome, support for state institutions was strengthened, war criminals were arrested, and relevant criteria were met. These criteria included Bosnia and Herzegovina's security policy, democratic parliamentary oversight at the state level, a common doctrine, equipment standards, and training for both the Army of the Federation and the Army of the Republic of Srpska, joint demonstration exercises, transparency of defense plans, and transparency of funding. Furthermore, NATO demanded the promotion of reconciliation, regional cooperation, and stability.

Bosnia and Herzegovina supports the fundamental concept of the PfP and aims to contribute to the security and stability of the Euro-Atlantic area, reduce threats to peace, and strengthen ties through active cooperation, as well as a commitment to general democratic principles.[94] The defense reform process in Bosnia and

[94] For more details, see:

Herzegovina is based on the principle of collective security and requires the creation of professional Armed Forces that are interoperable with NATO forces. As a partner, Bosnia and Herzegovina seeks to participate in the creation of a modern security policy in Europe. NATO has adopted a positive stance toward Bosnia and Herzegovina's ambitions, not only defining what the country needs to do to become a credible candidate for PfP membership but also assisting Bosnia and Herzegovina in achieving this goal (Maxwell & Olsen, 2013).

To this end, Bosnia and Herzegovina has been participating in the Planning and Review Process (hereinafter PARP) since May 2007. After PARP, the next step is the Individual Partnership Program (IPP), which is a working program between a PfP member state and NATO. Following that, the Individual Partnership Action Plan (IPAP) follows, representing a cooperation mechanism between the partner state and NATO. At a higher complementary level, Bosnia and Herzegovina has been participating in the Intensified Dialogue (ID) since April 2008, following the NATO Summit in Bucharest. Under the Membership Action Plan (hereinafter MAP), Bosnia and Herzegovina is required to achieve relevant goals that pertain not only to military, defense, and security issues but also to political, economic, and legal matters related to resources.

Legal matters require that Bosnia and Herzegovina has an organized legislative framework to ensure that cooperation with NATO is compatible with the national legal mechanisms. In June 2009, the Presidency of Bosnia and Herzegovina made the decision to apply for the MAP. The Bosnian delegation, led by the Chairman of the Presidency of Bosnia and Herzegovina, Željko Komšić, officially submitted the application for Bosnia and Herzegovina's membership in the Membership Action Plan on October 2, 2009.

Bosnia and Herzegovina expected to be invited to the MAP in December 2009, during the NATO North Atlantic Council ministerial meeting, however, this did not occur, primarily due to delays in reform processes in Bosnia and Herzegovina. Nonetheless, in an official statement following this meeting, NATO's Secretary-General stated that it is not a matter of if Bosnia and Herzegovina will join MAP and NATO, but when this will happen. He urged the political leaders in Bosnia and Herzegovina to continue with the reform processes, as the timing of Bosnia and Herzegovina's entry into MAP would depend on the positive results of these reforms.[95] The result of this was conditional membership. In 2010, Bosnia and Herzegovina was given the opportunity to activate the Membership Action Plan

https://www.mvp.gov.ba/vanjska_politika_bih/multilateralni_odnosi/sjevernoatlantski_savez_nato/bih_i_nato/?id=112, 21.10.2025.

[95] For more details, see: Atlantic Initiative. Bosnia and Herzegovina and NATO. February 2010

(MAP). MAP represents a necessary step for Bosnia and Herzegovina's integration into NATO. However, the process was slowed down due to internal political disagreements.

The genesis of Bosnia and Herzegovina's relations and its course of action within the geopolitical system of international relations, particularly in the context of cooperation or potential NATO membership, has primarily been marked by internal complexities and external pressures. The historical context of the complex relationships between post-Yugoslav and Balkan states on one side, and NATO and powerful players like Russia on the other, provides a deeply rooted structure for understanding the challenges Bosnia and Herzegovina faces today. NATO's collective defense system offers an attractive promise of military security and protection from potential threats—guarantees from which Bosnia and Herzegovina could greatly benefit. However, the ethnopolitical divisions within the country, combined with external, particularly malign influences from Serbia (whose foreign policy is mirrored by the political leaders of Republika Srpska) and Russia, have made Bosnia and Herzegovina's path to NATO membership complicated and fractured (Hasić & Džananović, 2023).

NATO is today the financially wealthiest organization in the world. Its goal is to ensure collective defense in order to guarantee future security and maintain peace. It is based on a high level of planning and coordination at military, defense, and political levels. Countries that have joined NATO have made significant progress in nearly all areas, greatly improving their security and institutional capacities. NATO strives to adequately respond to almost all challenges of instability in the modern world. Through collective defense, as outlined in Article 5 of the North Atlantic Treaty, it has extended its reach beyond its borders, becoming a global participant. NATO has established legal frameworks for its comprehensive internal reforms, concerning both structure and command as well as specific forces.

Additionally, NATO has focused on developing relationships with many different countries and regions around the world, which is particularly important for the broad range of goals it will pursue either independently or in collaboration with other appropriate organizations in the international community. NATO guarantees security. It has transformed and adapted its military and political structures to fulfill the tasks of ensuring peace and managing crises. Membership in NATO also requires active engagement to increase security. Each member state has specific defense and security obligations.

Understanding the nature of security includes domains that require active involvement of institutions in the economic sphere. In this regard, every country seeking NATO membership undergoes a series of economic reforms within the process of societal transformation, thereby opening new development

opportunities. Membership provides a reliable guarantee that member states will come to each other's aid, individually or collectively, in the event of an armed attack on any of them. No country is forced to rely solely on itself and its own economic resources when facing fundamental security challenges. At the same time, no country renounces its right to fulfill obligations to its people, and remains responsible for its own defense. NATO does not do this for them; it simply provides the means for them to act as a whole. The alliance enables member countries to achieve key national security goals through joint efforts. Comprehensive stability is further supported by the sense that countries enjoy equal security as members of the Alliance, regardless of their position or military strength.[96]

Bosnia and Herzegovina is a country that, within the framework of the General Framework Agreement for Peace in Bosnia and Herzegovina, is building peace, with the authority of the Office of of the High Representative (Annex 10) and the presence of European military forces, EUFOR Althea. The security challenges it faces should be viewed within the context of global relations. In the defense institutions, the defense planning system is aligned with NATO standards. General security, peace, and stability are prerequisites and essential conditions for the well-being and functioning of any society. Security is the goal of every social community and state, and at the same time, it is a vital need and desire of all members of the community. It is a necessary and important condition for order and peace, enabling stable social development and serving as a prerequisite for the overall development of society and the state (Vencl, Jamnić, & Pušeljić, 2021).

A key element for achieving military security in Bosnia and Herzegovina is to become a member of NATO, as in that case, its national sovereignty and territorial integrity would be guaranteed by the entire Alliance.[97] In Brussels, at NATO's Headquarters, the first Individual Tailored Partnership Programme (ITPP) was adopted between Bosnia and Herzegovina and NATO during a meeting of the Partnership and Cooperative Security Committee. This marked an important step in the implementation of the Membership Action Plan (MAP). Bosnia and Herzegovina's main objectives in cooperating with NATO include strengthening the rule of law, ensuring democratic control over the armed forces, increasing cooperation with European and Euro-Atlantic structures, and addressing security issues. The quality of the cooperation achieved between Bosnia and Herzegovina and NATO should confirm that it is a reliable partner, possessing the relevant capacities that can significantly contribute to strengthening peace and stability in

[96] For more details, see: Atlantic Initiative. Bosnia and Herzegovina and NATO. February 2010.

[97] https://www.mvp.gov.ba/vanjska_politika_bih/multilateralni_odnosi/sjevernoatlantski_savez_nato/bih_i_nato/?id=112, 21.10.2025.

the Southeast European region. For Bosnia and Herzegovina, regional defense cooperation and relations with neighboring countries are important aspects of their Euro-Atlantic policy. Such cooperation will create conditions for both internal and external interoperability, thereby enhancing the operational capabilities of the Armed Forces of Bosnia and Herzegovina, particularly for peacekeeping and humanitarian missions (Petrović, 2022).

Bosnia and Herzegovina prioritizes the protection of its independence, sovereignty, and territorial integrity, safeguarding the constitutional order and the human rights and freedoms guaranteed by it, developing the economy as a prerequisite for creating real conditions to improve the citizens' standard of living, joining the European Union as the most favorable way to achieve this priority, and joining collective security systems. Bosnia and Herzegovina fully embraces the concept of collective security as the most important pillar of its military strategy, which is why it strives for NATO membership as quickly as possible. Bosnia and Herzegovina is undoubtedly the most security-vulnerable country, not only in the West but throughout the entire Balkans and perhaps even Europe.

Despite not currently facing an immediate external threat, due to unresolved issues related to its recent war history, it exists in a latent adversarial environment. Additionally, Bosnia and Herzegovina faces the permanent risk of internal fragmentation, caused by persistent ethnic divisions. For these reasons, membership in the world's most powerful military alliance should not only be a desirable but also the most logical choice for Bosnia and Herzegovina.[98] Bosnia and Herzegovina submitted its first Reform Program to NATO in 2019, which represents a step forward in the existing cooperation.

[98] For more details, see: Marinković, Milan, Why Bosnia and Herzegovina's NATO Membership Must Be a Priority. (2013).)., https://www.tacno.net/polemika/zasto-je-opasno-forsirati-clanstvo-u-nato-paktu-bez-unutrasnjeg-koncenzusa-u-bih/, 15.10.2025.

3. Conclusion

NATO, as a military-political organization, provides both assistance and services to states. Through collective relations, it seeks to resolve security issues through inter-collective relations and cooperation. Its goal is to improve the defense capabilities of states in order to increase their security. The relationship between Bosnia and Herzegovina and NATO has been characterized by long-term cooperation based on Partnership, security reforms, and support for the stability of the state. NATO played a key role in Bosnia and Herzegovina's post-war reconstruction. The relations between Bosnia and Herzegovina and NATO have continued to expand beyond the framework of the General Framework Agreement for Peace. Bosnia and Herzegovina is a NATO partner country, but still not a member.

Cooperation continues through the Reform Program, joint exercises, support for defense and security reforms, and assistance in crisis situations. NATO membership depends on achieving political consensus within Bosnia and Herzegovina and continuing reforms. While technical capacities and cooperation continue to improve, differing political views remain the main obstacle to further progress. For this reason, the relationship between Bosnia and Herzegovina and NATO can be described as a currently stable partnership, which results in the open question of the country's final strategic orientation.

It is important to note that Bosnia and Herzegovina's accession to NATO would significantly contribute to improving the current security situation. NATO guarantees the protection of Bosnia and Herzegovina's sovereignty and territorial integrity. Bosnia and Herzegovina's NATO membership is also significant from a political perspective. By joining the NATO alliance, Bosnia and Herzegovina would not only further improve the rule of law and democracy, but also strengthen regional cooperation. The most important benefits of NATO membership are stability and enhanced security. The Armed Forces of Bosnia and Herzegovina have made significant progress in aligning with NATO standards.

REFERENCES

1. Hasić, J., & Džananović, N., 2023. Perspectives from the Margins. Deconstructing Prevailing Political Narratives on Bosnia and Herzegovina's Relations with NATO. Sarajevo: Faculty of Political Science, University of Sarajevo.

2. Maxwell, R. & Olsen A., J.,2013. Destination NATO: Defence Reform in Bosnia and Herzegovina 2003-2013. London: Royal United Services Institute for Defence and Security Studies. Whitehall

3. Najetović, D., 2001. Expanding Security in the Euro-Atlantic Area - the Role of NATO and Partner Countries. Sarajevo: Council of the Congress of Bosnian Intellectuals.

4. Petrović, Ž., 2022. The United Nations and NATO in War and Post-War Bosnia and Herzegovina. Sarajevo: Protection and Security. Year 2. Number 1, 90-109.

5. Smailhodžić, A., 2019. Cooperation between the North Atlantic Alliance and Bosnia and Herzegovina. Sarajevo: Criminal Topics, 17-36.

6. Turković, B., 2006. NATO from a security alliance to modern challenges. Sarajevo: Center for Security Studies.

7. Vencl, K., Jamnić, S., & Pušeljić, M., 2021. Police as the foundation of security in the state. Sarajevo: Protection and Security. Year 1. Number 1, 19-34.

a. Other

8. Atlantic Initiative., 2010. Bosnia and Herzegovina and NATO. Sarajevo.

9. White Book of Defense of Bosnia and Herzegovina. 2005., available at: https://www.mod.gov.ba/files/file/dokumenti/Bijela-knjiga-bs.pdf . (Accessed: 7.10.2025.)

10. Partner. 2008. Monthly on Euro-Atlantic Integration, Defense and the Army. Issue 2, available at: http://www.mod.gov.me/files/1206620684.pdf . (Accessed: 10.11.2025.)

11. Presentation document. 2006. Partnership for Peace, available at: https://mod.gov.ba/files/file/nato/prez_dokum_hr.pdf . (Accessed: 10/16/2025)

12. https://www.mvp.gov.ba/vanjska_politika_bih/multilateralni_odnosi/sjevernoatlantski_savez_nato/bih_i_nato/?id=112, (Accessed: 21.10.2025)

13. https://www.tacno.net/polemika/zasto-je-opasno-forsirati-clanstvo-u-nato-paktu-bez-unutrasnje-koncenzusa-u-bih/. (Accessed: 10/15/2025)