RISK MANAGEMENT SOFTVER BAZIRAN NA AI I CPS PREDIKCIJI

DOI: *10.70329/2744-2403.2025.5.9.1*

Naučni rad

Edin Garaplija [1]
Muhamed Durakovic [2]

Sažetak:
Ovaj rad se fokusira na upotrebu mašinskog učenja i korištenje namjenskih baza podataka vještačke inteligencije u svrhu kreiranja rješenja zasnovanih na unaprijeđenom algoritmu za preventivno upravljanje rizicima i predikciju rizika u realnom vremenu. U radu se analiziraju postojeći standardi, njihovi nedostaci i moguća rješenja za unapređenje, kao i struktura i algoritamska osnova ovih sistema, te njihova integracija u postojeće sigurnosne arhitekture i platforme. Obuhvaćena je detekcija prijetnji na osnovu anomalija i analiza ustaljenog korisničkog ponašanja prema zadanim obrascima, procjena rizika i proaktivna detekcija napada. Pravovremena identifikacija i upravljanje rizicima postaju ključni faktori održivosti kompanija i sigurnosti poslovnih i informacionih sistema. Prediktivna analitika, zasnovana na vještačkoj inteligenciji, mašinskom učenju i analizi velikih skupova podataka, donosi transformacijske mogućnosti u oblastima poput industrije, finansija i zdravstva, koje su u savremenoj eri povezane sajber sigurnošću i predikcijom rizika, a koje pomažu donosiocima odluka da efikasnije upravljaju sistemima i zaštite ih. Integrativni pristup usklađivanju ovih tehnologija, posebno u kontekstu organizacione strukture i pravnog okvira, obuhvata pitanja pouzdanosti i transparentnosti modela, odgovornosti za automatizovane odluke, zaštite privatnosti i usklađenosti sa zakonodavstvom. Cilj rada je pružiti sveobuhvatan pregled tehnoloških i metodoloških inovacija u prediktivnoj zaštiti od sajber rizika, te identifikovati pravce budućeg razvoja sa posebnim fokusom na sigurnost, etiku i pouzdanost AI sistema.

Ključne riječi: *Rizik, AI Predikcija, Cyber sigurnost*

---

[1] Edin Garaplija, PhD in security Science, President of INZA Institute of the Risk Management
[2] Muhamed Durakovic, IT Eng., IT Development engineer of the INZA Group

1. Uvod

Upravljanje rizicima u sistemima kritične infrastrukture postaje sve zahtjevniji zadatak, posebno u kontekstu ubrzanog tehnološkog razvoja, povećane međusobne povezanosti samih sistema i sve sofisticiranijih sajber prijetnji. Dosadašnji pristupi, koji se najčešće oslanjaju na mjere koje zanemaruju prevenciju u najranijoj fazi, više nisu dovoljni da odgovore na savremene sigurnosne izazove u korporativnom okruženju. U tom kontekstu, vještačka inteligencija (AI) i mašinsko učenje nude nove perspektive i mogućnosti za unapređenje postojećih sigurnosnih sistema, prvenstveno kroz uvođenje prediktivnih modela koji omogućavaju pravovremeno prepoznavanje prijetnji prije nego što izazovu štetu.Poseban fokus biće stavljen na način integracije algoritama u postojeće procese, s ciljem unapređenja standardnih pristupa i omogućavanja blagovremenih reakcija u složenim okruženjima. Osim tehničkih aspekata, rad će se baviti i širim pitanjima koja prate primjenu ovih tehnologija, od etičkih i pravnih izazova, do pitanja transparentnosti, zaštite podataka i usklađenosti sa zakonima i internim regulativama. Ova dimenzija je ključna kako bi se osigurala odgovorna i dugoročno održiva upotreba AI sistema u poslovnoj praksi.Današnji procesi digitalne transformacije značajno doprinose većoj povezanosti i operativnoj efikasnosti, ali istovremeno otvaraju prostor za nove ranjivosti. Napadi na informacione sisteme sve više se oslanjaju na kombinaciju tehničkih propusta i ljudskih faktora. Stoga savremeni pristupi sigurnosti moraju prevazići tradicionalnu zaštitu mrežnih granica i obuhvatiti širu analizu rizika u svakodnevnom poslovanju. Potrebna je proširena vizija sigurnosti, koja povezuje tehničke, organizacione i ljudske faktore u jedinstven sistem za rano upozoravanje i preventivno djelovanje.Platforma INZA Risk Management za upravljanje rizicima razvijena je upravo s tom vizijom, kao odgovor na globalne izazove te nudi skalabilno i inteligentno rješenje koje se može prilagoditi specifičnim potrebama različitih organizacija u procesu upravljanja kritičnom infrastrukturom.

2. Teorijski okvir

U današnjem poslovnom okruženju, gdje digitalne tehnologije čine temelj gotovo svakog sektora, upravljanje rizicima sve više postaje sastavni dio šire strategije opstanka i rasta. Umjesto da se reaguje tek nakon što dođe do incidenta, sve veći naglasak stavlja se na pravovremeno prepoznavanje prijetnji i adekvatan odgovor na njih. Smatra se da spektakularan napredak u razvoju sajber-fizičkih sistema (CPS) i tehnologije interneta stvari (IoT) predstavlja osnovu za Industriju 4.0 (Whalster, W., 2013). Teorija CPS-a proistekla je iz teorije upravljanja i inženjerstva upravljačkih sistema, a fokusira se na međusobno povezivanje

fizičkih komponenti i upotrebu kompleksnih softverskih entiteta kako bi se uspostavile nove mrežne i sistemske mogućnosti. CPS-ovi povezuju fizičke i inženjerske sisteme te spajaju sajber svijet s fizičkim. Suprotno tome, teorija IoT-a proizašla je iz računarskih nauka i internetskih tehnologija, te je prvenstveno usmjerena na međusobnu povezanost, interoperabilnost i integraciju fizičkih komponenti putem interneta. Očekuje se da će s potpunom tržišnom integracijom IoT-a u narednoj deceniji doći do razvoja poput automatizacije CPS-ova putem IoT-a (Dworschak, B., Zaiser, H., 2014).

Ovo je posebno značajno u kontekstu sajber sigurnosti, gdje jedan jedini propust može izazvati ozbiljnu tehničku, ali i reputacijsku štetu. U svojoj suštini, upravljanje rizicima podrazumijeva identifikaciju prijetnji, njihovu procjenu, donošenje odluka o načinu odgovora i praćenje promjena tokom vremena. Standardi poput ISO 31000 nude koristan okvir, ali se u praksi često pokazuje da klasični modeli ne odgovaraju u potpunosti složenosti savremenog digitalnog okruženja. Oni se oslanjaju na procjene koje su ponekad subjektivne i teško prilagodljive brzini promjena.Pojava naprednih tehnologija, poput vještačke inteligencije, donijela je značajne promjene u ovom pristupu. Algoritmi danas mogu analizirati ogromne količine podataka, otkrivati obrasce koji su ranije ostajali neprimijećeni i upozoravati na potencijalne probleme prije nego što prerastu u ozbiljne incidente. Takvi sistemi su naročito korisni za prepoznavanje odstupanja u ponašanju; bilo korisnika, bilo uređaja – koja mogu ukazivati na greške, zloupotrebe ili sigurnosne napade.

Platforma INZA za upravljanje rizicima razvijena je na tim principima, ne funkcioniše samo kao alat za nadzor rizika, već kao sistem koji aktivno uči iz prethodnih iskustava i prilagođava se novim situacijama. Na osnovu stvarnih podataka i ponašanja korisnika, sistem može mnogo ranije upozoriti na sumnjive aktivnosti nego što bi to mogli klasični mehanizmi. Na taj način se značajno skraćuje vrijeme reakcije i smanjuju potencijalne štete.Osim toga, platforma koristi metode prediktivne analize, pristup koji omogućava izvlačenje korisnih obrazaca iz prošlih događaja za potrebe budućih procjena. To uključuje analizu situacije, procjenu tokom koje se predlažu preventivne mjere, kreiranje scenarija rizika, te na kraju ključnu analizu troškova i koristi, koja pokazuje koliko angažman u preventivne mjere u konačnici smanjuje mogućnost havarije, ali i koliko u ekonomskom smislu donosi koristi samoj organizaciji.

Na kraju, INZA Risk Management predstavlja spoj dugogodišnjeg iskustva i inovacije, a njena snaga ogleda se u sposobnosti prilagođavanja svakom okruženju, posebno onima koji su već zakoračili na put digitalizacije i traže načine da pametnije i dugoročnije zaštite svoje sisteme.

3. Sigurnosni sistemi bazirani na umjetnoj inteligenciji

Upotreba vještačke inteligencije u savremenim sigurnosnim sistemima postaje sve češći odgovor na izazove koje postavlja zaštita složenih informacionih mreža. Iako se klasične mjere poput vatrozida, antivirusnih alata i ručne kontrole pristupa i dalje koriste, praksa pokazuje da one često ne mogu pratiti brzinu i nepredvidivost savremenih napada. Današnji napadi nisu lako uočljivi; često se odvijaju kroz suptilne promjene i obrasce ponašanja koji mogu proći neopaženo. Zbog toga se sve veća pažnja usmjerava ka sistemima koji ne zavise od unaprijed definisanih pravila, već imaju sposobnost samostalnog prepoznavanja odstupanja u ponašanju.

Table 3 The applications and technologies related to artificial intelligence for CPS

Connection	SAAS	BDP, mCPS	CBM	Self-maintain
Conversion	LCM	HMI, MaC	PHM	Self-aware
	AMAT	LTTA, SDC		
Cyber (analytic solutions)	EaPS	RTD, FoM, AA, PtPM	CPS	Self-compare
Cognition	SCRM	POD, SOPS	DSS	Self-predict
	ISaDS	ACD, MLA, HPC, ISR		Self-optimise
Configuration	TaT	CoA	RCS	Self-organise
	FPR	KPI		
	AMaAC	CPPS		Self-configure

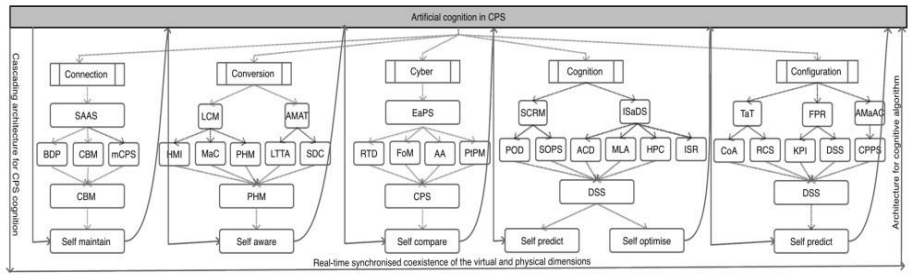


Fig. 2 Cascading framework for artificial intelligence for CPS

SN Applied Sciences
A SPRINGER NATURE journal

Slika 1.: Radanliev, P. (2020). *„Vještačka inteligencija i mašinsko učenje u dinamičkoj analitici sajber rizika na ivici mreže“*, SN Applied Science, časopis izdavača Springer Nature.

Kaskadni okvir prikazan na slici 2 predstavlja novi pristup u dizajniranju dinamičkih i automatiziranih prediktivnih sistema koji su podržani inteligencijom u realnom vremenu. Ovaj okvir omogućava procjenu potencijala za primjenu kognitivnih AI mehanizama u prikupljanju podataka i analitici s dinamičkim povratnim informacijama u realnom vremenu.

Takvi mehanizmi mogu omogućiti prediktivnu inteligenciju o učestalosti prijetnji i potencijalnoj veličini gubitaka koji iz njih proizilaze. Nesumnjivo je da se, kako

bi se osigurala ova funkcionalnost, algoritmi dubokog učenja moraju integrisati u kognitivne mehanizme kako bi formirali dinamičke intervale povjerenja i vremenski definisane granice na osnovu podataka u realnom vremenu. Kada se ove sposobnosti postignu, kaskadni okvir sa slike 2 postaje savremeni alat za analitiku rizika. (Radanliev, P., 2020)

Algoritmi vještačke inteligencije analiziraju velike količine podataka u realnom vremenu i traže znakove koji odstupaju od uobičajenog toka aktivnosti, čime omogućavaju otkrivanje prijetnji koje nisu evidentirane u postojećim bazama podataka. Korištene tehnike uključuju različite pristupe poput klasifikacije, klasterovanja podataka i neuronskih mreža, koje omogućavaju vrlo precizno prepoznavanje nepravilnosti u sistemu.

Napredni AI programi mogu brzo pregledati velike količine informacija kako bi prepoznali i odgovorili na potencijalne prijetnje te prema potrebi prilagodili sigurnosne mehanizme. Ove tehnologije koriste napredne algoritme za analizu velikih skupova podataka s ciljem identifikacije rizika, obrazaca i anomalija. Ovo poboljšanje u donošenju odluka i raspodjeli resursa može se uporediti s ulogom AI sistema u drugim oblastima, poput komunikacije o klimatskim promjenama, gdje su se AI glasovi pokazali jednako efikasnim kao i ljudski (Ni, B., 2023).

U okviru platforme INZA Risk Management, vještačka inteligencija se primjenjuje na više nivoa zaštite. Prvi sloj uključuje analizu stanja, gdje se stalno prate promjene u obrascima korištenja s ciljem otkrivanja neuobičajenih aktivnosti. Osim toga, sistem kontinuirano nadzire ponašanje svih komponenti kritične infrastrukture, bilježi njihove „normalne“ režime rada i prepoznaje odstupanja. Kada se pojavi takva situacija, sistem odmah reaguje, šalje obavijest i predlaže korake za preventivno djelovanje.

Posebna vrijednost INZA Risk Management sistema ogleda se u njegovoj sposobnosti povezivanja s vanjskim izvorima podataka, poput globalnih baza poznatih prijetnji i prethodnih incidenata, kao i u korištenju vlastite istorije kako bi bolje razumio specifičnosti okruženja u kojem se koristi. Na taj način, sistem reaguje ne samo na ono što vidi, već i na ono što zna, oslanjajući se na iskustvo kombinovano s aktuelnim podacima.

Automatizacija ima ključnu ulogu. Kada se rizik otkrije, sistem odmah obavještava odgovorne osobe i nudi preventivne mjere, čime se vrijeme reakcije svodi na minimum. Upravo ta brzina često odlučuje hoće li incident biti uspješno kontrolisan ili će se razviti u ozbiljan sigurnosni problem.Naravno, ovakav stepen automatizacije otvara i nova pitanja: Kako osigurati da su odluke sistema razumljive i provjerljive? I šta ako sistem pogriješi? Zbog toga INZA Risk Management uključuje mogućnost ljudske kontrole nad svakim automatiziranim

postupkom, čime se postiže ravnoteža između efikasnosti tehnologije i stručne procjene sigurnosnog tima. Na kraju, rješenja poput INZA Risk Management više nisu opcija – ona su postala nužnost.

4. Unaprijeđen algoritam predikcije rizika: primjeri i funkcionalnosti

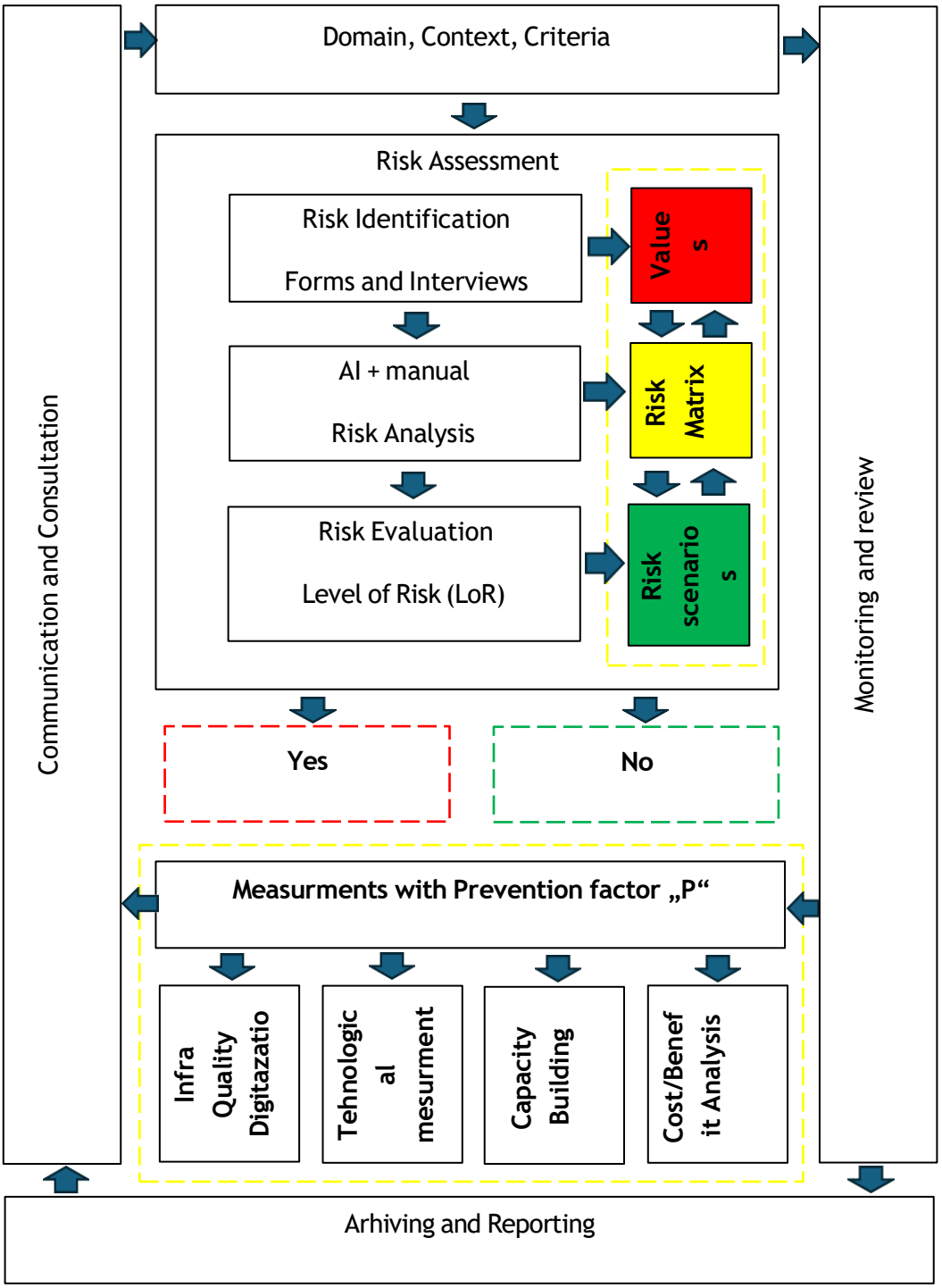
U samoj srži INZA Risk Management platforme za upravljanje rizicima nalazi se algoritam razvijen s ciljem rane detekcije sigurnosnih prijetnji u sistemima kritične infrastrukture. Za razliku od konvencionalnih pristupa koji se uglavnom oslanjaju na poznate obrasce, ovaj sistem koristi kombinaciju učenja iz podataka u realnom vremenu i analize anomalija kako bi kontinuirano prilagođavao svoje procjene i reagovao na nove situacije (Garaplija, 2022).

Jedna od njegovih ključnih prednosti jeste to što ne posmatra samo jedan izvor informacija, već istovremeno uzima u obzir različite aspekte: tehničke indikatore, način na koji je organizovana struktura kompanije i pravila pristupa, kao i samo ponašanje korisnika. U praksi to znači da sistem može prepoznati kada se neko ponaša drugačije nego inače, bilo da se radi o zaposleniku koji pokušava pristupiti osjetljivim podacima u neuobičajeno vrijeme, ili o iznenadnoj promjeni pristupnih prava.

Posebno je važan kontekst u kojem se te promjene dešavaju. Nije isto ako se administrator prijavljuje u sistem iz prostorija firme tokom radnog vremena ili ako se nepoznati korisnik prijavi s udaljene lokacije usred noći. Algoritam uzima u obzir ove razlike i, u zavisnosti od ozbiljnosti odstupanja, pokreće odgovarajuće upozorenje ili predlaže preventivne mjere.

Kako bi svoje procjene učinio što jasnijim i razumljivijim, INZA Risk Management koristi i vizuelne oznake rizika, određena boja i procenat prikazanina mapi označavaju nivo rizika, što korisnicima omogućava brz i intuitivan uvid u sigurnosnu situaciju bez potrebe da ulaze u tehničke detalje. (Garaplija, 2023)

INZA Risk Management softver za upravljanje rizicima usklađuje sajber i fizičku sigurnost povezivanjem različitih digitalnih protokola mjerenja i sigurnosnih senzora u jedinstvenu AI bazu podataka, što ne samo da ubrzava efikasnost donošenja odluka, već i razvija baze znanja za buduća istraživanja i razvoj.



Slika 2.: Unaprijeđeni algoritam za prevenciju rizika prema standardu ISO 31000, (Garaplija, 2022)

Teorija sajber-fizičkih sistema (CPS) potiče iz teorije upravljanja i inženjerstva upravljačkih sistema, te se fokusira na međusobno povezivanje fizičkih komponenti i upotrebu složenih softverskih entiteta za uspostavljanje novih mrežnih i sistemskih funkcionalnosti. Na taj način, CPS sistemi povezuju fizičke i inženjerske komponente, predstavljajući most između sajber svijeta i fizičkog svijeta.

Suprotno tome, teorija Interneta stvari (IoT) nastala je iz računarskih nauka i internet tehnologija, i prvenstveno se bavi međusobnom povezanošću, interoperabilnošću i integracijom fizičkih komponenti putem interneta. S potpunom tržišnom integracijom IoT-a u narednoj deceniji, očekuje se da će ova integracija rezultirati razvojem poput automatizacije CPS sistema putem IoT-a.

Ono što dodatno potvrđuje efikasnost algoritma INZA Risk Management sistema za upravljanje rizicima jeste način na koji se ponašao tokom testiranja u stvarnim uslovima. U više navrata, uspio je detektovati potencijalne rizike mnogo ranije nego što bi to učinio standardni sistem. Za razliku od mnogih generičkih rješenja koja se oslanjaju na unaprijed definisane šablone, INZA Risk Management je prilagođen lokalnim uslovima na terenu. Uzima u obzir specifične karakteristike tržišta, jezičkog okruženja, pravnog okvira i sigurnosnih izazova karakterističnih za određenu regiju.

Upravo ta sposobnost adaptacije čini ga posebno korisnim za kompanije i institucije širom svijeta, gdje često postoje nijanse koje strana rješenja jednostavno ne prepoznaju, što može dovesti do pogrešnih procjena i neadekvatnog odgovora.

5. Izazovi i ograničenja korporativne primjene

Integracija vještačke inteligencije u svakodnevne poslovne procese donosi brojne prednosti, ali istovremeno predstavlja i izazove, posebno kada se primjenjuje na osjetljiva područja poput procjene sigurnosnih rizika i upravljanja kritičnom infrastrukturom. Platforma INZA Risk Management, kao primjer takvog sistema, predstavlja snažan alat, ali njeno uklapanje u postojeće strukture kompanije često nije jednostavno, jer zahtijeva promjene koje se ne odnose samo na tehnologiju, već i na ljude, procese i organizacijsku kulturu.

Jedan od prvih problema koji se može pojaviti jeste pitanje spremnosti organizacije da prihvati takav sistem, budući da u mnogim okruženjima još uvijek dominira pristup u kojem se sve oslanja na ljudsku procjenu, dok automatizovani sistemi izazivaju opreznost, naročito kada se od njih očekuje davanje preporuka.

Ako uposlenici nisu upoznati s načinom na koji algoritam funkcioniše, može se javiti osjećaj nepovjerenja, pa čak i otpora. Situacija se dodatno komplikuje ukoliko nije jasno definisano ko snosi odgovornost za odluke koje sistem donosi – da li osoba koja ga nadgleda ili tim koji ga koristi.Tehnički aspekt integracije također može predstavljati ozbiljan izazov. Iako je INZA Risk Management dizajniran da bude fleksibilan, ipak zahtijeva pristup ključnim podacima, logovima, mrežnim zapisima i autentifikacijskim protokolima. Ako su ovi sistemi zastarjeli, zatvoreni ili nepovezani, integracija može zahtijevati dodatno vrijeme i resurse, što nije uvijek lako ostvariti u kratkom roku. Posebnu dimenziju predstavlja pitanje privatnosti. Da bi algoritam mogao ispuniti ono što se od njega očekuje, mora analizirati informacije koje mogu uključivati lične podatke – aktivnosti zaposlenika, pristup određenim datotekama, vrijeme i lokaciju prijave u sistem. Bez jasno definisanih granica, postoji rizik da se sigurnost pretvori u nadzor. Zbog toga je u sistem INZA Risk Management ugrađena kontrola pristupa podacima i princip ograničene obrade; analiziraju se samo podaci koji su zaista neophodni, a svaki korak koji sistem poduzme moguće je naknadno provjeriti.

Pored tehničkih i pravnih izazova, često postoji i suptilnija, ali jednako važna prepreka: ljudski faktor. Zaposlenici mogu osjećati nelagodu zbog uvođenja AI tehnologije u njihovo radno okruženje, ponekad je doživljavajući kao prijetnju sopstvenoj poziciji. Zbog toga uspješna implementacija mora ići dalje od pukog instaliranja softvera, potrebni su prije svega edukacija, otvoren dijalog i jasno objašnjenje kako ovakvi sistemi mogu donijeti dodatnu vrijednost. Pristup „korak po korak“, u kojem se ljudi kroz praksu postepeno upoznaju sa sistemom, pokazao se kao najefikasniji način za izgradnju povjerenja.

Pitanje standardizacije i formalne validacije ovakvih sistema dodatno komplikuje njihovu širu primjenu. Iako INZA Risk Management koristi provjerene modele i samoučeće algoritme, još uvijek ne postoji univerzalan okvir koji bi precizno definisao kako se ovakvi alati testiraju, odobravaju ili certificiraju, posebno u regulisanim industrijama poput bankarstva, zdravstva ili energetike, gdje nema prostora za pogrešne procjene.Uz sve to, neophodno je imati na umu da se ovakvi sistemi moraju redovno održavati, jer vještačka inteligencija nije statična, ako se ne ažurira, brzo zastarijeva i prestaje biti korisna. Modeli moraju pratiti nove podatke, učiti iz promjena i revidirati svoja pravila kako bi ostali relevantni, što znači da organizacija mora imati ne samo dobar početni plan, već i dugoročnu podršku: tehničku, kadrovsku i stratešku.Međutim, kada postoji iskrena spremnost, jasan plan implementacije i snažna podrška rukovodstva, iskustvo pokazuje da se ovakvi sistemi mogu uspješno integrisati. U takvom okruženju, INZA Risk Management ne samo da povećava nivo sigurnosti i ubrzava odgovor na incidente, već i pomaže promjeni organizacijske svijesti ka proaktivnijem pristupu upravljanju rizicima.

6. Zakonodavstvo, profesionalna etika i odgovornost

Razvoj tehnologija koje koriste vještačku inteligenciju za upravljanje rizicima, posebno u kontekstu korporativne sigurnosti, donosi ne samo tehnička, već i pravna i etička pitanja. Kada algoritmi počnu preuzimati zadatke koje su prethodno obavljali ljudi, analizirajući ponašanje i dajući preporuke, javlja se logična zabrinutost: šta ako sistem napravi grešku? I, još važnije, ko je tada odgovoran?

Implementacija rješenja poput platforme INZA Risk Management zahtijeva da se već od samog početka uzmu u obzir zakoni koji štite lične podatke i definišu granice automatizovanog odlučivanja. U Evropi se posebna pažnja posvećuje pravilima poput Opće uredbe o zaštiti podataka (GDPR), koja jasno propisuje da korisnici imaju pravo znati na koji način se donose odluke koje ih se tiču, te da u proces odlučivanja može biti uključen čovjek, kad god je to potrebno.Sistem INZA Risk Management je izgrađen tako da svaka akcija koju inicira sistem bude zabilježena, te da se može naknadno pregledati, objasniti i ako je potrebno na kraju osporiti. Cilj nije da se AI postavi iznad ljudi, već da pomogne timu da reaguje brže i efikasnije. No, pored zakona, važno je i profesionalno poštivanje etičkih principa. Osobe koje razvijaju i koriste ovakve sisteme imaju obavezu da djeluju pošteno, da poštuju granice i da ne koriste tehnologiju u svrhe koje nisu u skladu s njenom namjenom.

Na primjer, algoritmi se ne smiju koristiti za nadzor zaposlenih izvan jasno definisanog, opravdanog i poznatog okvira, niti smiju donositi automatske zaključke o nečijem ponašanju bez dodatne provjere i konteksta. INZA Risk Management je razvijen s ciljem da podrži „odgovornu upotrebu vještačke inteligencije“, ne da zamijeni ljudsku procjenu, već da je unaprijedi, ubrza i učini informisanijom.

Odgovornost je, naravno, i dalje osjetljivo pitanje. U tradicionalnim sistemima često je jasno, ako dođe do greške, zna se ko je postupao i gdje je pogreška nastala. Kod AI sistema ta granica nije toliko jasna. Da li je odgovorna osoba koja je kreirala model? Ili ona koja ga koristi? Ili možda sam sistem, iako pravno ne postoji kao „subjekt“? Zbog toga je važno da svaka organizacija koja koristi ovakva rješenja ima jasno definisan okvir: interne procedure, pravila upravljanja rizikom i dokumentaciju koja definiše postupanje u slučaju greške.

Ključ nije u prebacivanju odgovornosti, već u tome da svi znaju kako se ponašati u skladu s jasno utvrđenim pravilima. Još jedan važan aspekt je povjerenje, jer uposleni u organizaciji moraju znati da postoji sistem koji analizira njihove aktivnosti, ali i da znaju zašto, kako i u kojoj mjeri. Transparentnost se ne postiže samo kroz regulative i pravne formulacije, već i kroz iskren dijalog unutar tima.

Zato INZA Risk Management ne nudi samo tehničke mehanizme koji osiguravaju privatnost, već i podržava kulturu u kojoj se korisnici osjećaju informisano, a ne nadgledano. U konačnici, uspjeh ovakvih rješenja neće zavisiti samo od toga koliko su pametni algoritmi, već od toga kolika je spremnost organizacija da ih koriste odgovorno.Rješenja poput INZA Risk Management mogu biti izuzetno efikasna, ali samo ako se uklapaju u širi okvir koji uključuje zakonsku regulativu, interna vrijednosna načela i snažan osjećaj etičke odgovornosti. Kada se ti elementi spoje, sistem postaje praktičan alat koji doprinosi jačanju sigurnosti i podršci u donošenju informisanih odluka.

7. Sistemski pristup i dalji razvoj

Upravljanje rizicima u sistemima kritične infrastrukture zahtijeva mnogo više od jednog softverskog rješenja ili izolovanog sigurnosnog alata, potrebna je sveobuhvatna strategija koja objedinjuje tehnologiju, procese, ljude i zakonske obaveze u funkcionalan sistem sposoban da odgovori na vremenski promjenjive izazove.Platforma INZA Risk Management razvijena je upravo s tim ciljem, kao dio šireg sigurnosnog ekosistema, spremna da se prilagodi različitim sektorima, veličinama organizacija i stepenu digitalne zrelosti. Ono što INZA Risk Management čini drugačijom jeste njen pristup koji ne posmatra procjenu rizika kao krajnji cilj, već kao početak procesa koji se stalno razvija. Svaka identificirana prijetnja pokreće lanac aktivnosti, od analize i odgovora, do naknadnog učenja i prilagođavanja.Sistem „pamti“, procjenjuje vlastite reakcije i prilagođava se promjenama u okruženju, čime se izbjegava statički model i gradi okruženje u kojem sigurnost postaje dinamičan proces.

Već se razmatra niz novih mogućnosti u okviru daljih razvojnih planova, među kojima se izdvaja sposobnost da se dostupni resursi – bilo da se radi o ljudstvu, opremi ili vremenu, automatski usmjere tamo gdje su najpotrebniji, u zavisnosti od trenutnog nivoa rizika.Također se planira uvođenje simulacija i testova koji organizacijama omogućavaju da unaprijed provjere kako bi njihov sistem reagovao u slučaju ozbiljnog napada i na taj način na vrijeme otkriju svoje ranjivosti, prije nego ih neko iskoristi.U budućnosti će INZA Risk Management biti još tjesnije povezana s fizičkom infrastrukturom, putem IoT senzora, sigurnosnih kamera i drugih uređaja, kako bi slika o potencijalnim prijetnjama bila što potpunija i dostupna u realnom vremenu.Lokalizacija također igra veoma važnu ulogu. Platforma već sada podržava rad na različitim jezicima i unutar različitih pravnih okvira, što je od posebnog značaja za organizacije koje djeluju u više zemalja ili na tržištima sa specifičnim regulatornim zahtjevima.

Pored samog softvera, posebna pažnja se posvećuje i ljudima koji s njim rade, jer nijedna tehnologija neće dati očekivane rezultate ako oni koji je koriste nisu obučeni da je pravilno interpretiraju i primjenjuju.Zato INZA Risk Management uključuje podršku kroz interaktivne vodiče, objašnjenja odluka koje sistem predlaže i preporuke za dodatnu edukaciju, jer cilj nije da se korisnik izgubi u složenosti, već da sistem bude alat koji pomaže, a ne prepreka.Kada je riječ o usklađenosti s propisima, posebno onim koji tek dolaze, INZA Risk Management već sada prati regulative koje se razvijaju unutar Evropske unije, omogućavajući korisnicima da unapređuju svoje sigurnosne prakse, a da pritom ostanu usklađeni s pravnim očekivanjima i standardima koji će tek stupiti na snagu.

U narednim fazama, INZA Risk Management će otvoriti vrata ka još širem spektru saradnje, jer će zajednički rad na razvoju i testiranju novih modela dodatno pomoći platformi da se prilagodi različitim okruženjima i složenim izazovima, ne samo u digitalnom prostoru, već i u fizičkom i društvenom kontekstu.Suština sistemskog pristupa nije u pronalasku savršenog rješenja, već u osnaživanju organizacije da stalno prilagođava svoje mehanizme zaštite. INZA Risk Management je dizajniran da upravo to omogući, ne samo kao alat koji reaguje na prijetnje, već kao rješenje koje pomaže da se iz svake situacije nešto nauči, sistem stalno unapređuje, a organizacija iz dana u dan postaje otpornija.

8. Zaključak

Danas je izuzetno važno razmišljati unaprijed, djelovati preventivno te brzo spriječiti i reagovati. Ovaj rad je pokazao da vještačka inteligencija, ukoliko se razvija promišljeno i koristi odgovorno, može imati ključnu ulogu u takvom pristupu. Platforma INZA Risk Management upravo je takav primjer, jer se njena vrijednost ogleda ne samo u tehnološkim rješenjima koja koristi, već i u načinu na koji povezuje različite izvore informacija, uči kroz vrijeme i korisnicima pruža ono što im zaista treba: jasne uvide i preporuke koje se mogu odmah primijeniti.Postoje brojni tehnički izazovi, promjene unutar organizacije i niz pravnih pitanja koja prate svaki ozbiljan pokušaj digitalne transformacije.

Međutim, ti izazovi ne predstavljaju razlog za odustajanje, naprotiv, oni su poziv da se tehnologijom upravlja odgovorno i s razumijevanjem. Jasna pravila, usklađenost sa zakonodavstvom i etički pristup nisu opcija, već neophodna osnova za stabilnu i dugoročno održivu implementaciju ovakvih rješenja.U budućnosti će INZA Risk Management nastaviti svoj razvoj ka još boljoj povezanosti s drugim sistemima, većoj transparentnosti i jednostavnijoj upotrebi. Vizija nije samo tehnološki napredan alat, već partner koji raste, uči i zajedno s organizacijom sve bolje razumije složenost sigurnosnih izazova.

Na kraju, važno je jasno naglasiti: vještačka inteligencija neće zamijeniti čovjeka u donošenju odluka, ali ga može osnažiti – može mu pomoći da bolje razumije prijetnje, brže reaguje i donosi sigurnije odluke. U tom smislu, INZA Risk Management nije samo softver, već alat koji spaja ljudsku prosudbu i digitalnu preciznost u svrhu upravljanja rizicima u sistemima kritične infrastrukture.

LITERATURA

1. Dworschak, B., Zaiser, H. (2014). „Kompetencije za sajber-fizičke sisteme u proizvodnji – prvi nalazi i scenariji“, *Procedia CIRP*, 25:345–350.

2. Garaplija, E., Prguda, S. (2023). „Pametni gradovi za smanjenje rizika od katastrofa: korištenje tehnologije i inovacija za otpornu urbanu sredinu“, *Asocijacija za upravljanje rizicima*, www.zisjournal.com

3. Garaplija, E. (2024). „3D logički model integracije između metafizike i upravljanja rizicima od katastrofa“, *Asocijacija za upravljanje rizicima*, www.zisjournal.com

4. Ni, B., Wu, F., Huang, Q. (2023). „Kada vještačka inteligencija izražava ljudske brige: paradoksalni efekti AI glasa na percepciju klimatskih rizika i namjeru za proekološkim ponašanjem“, *International Journal of Environmental Research and Public Health*, 20(4), 3772.

5. Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Anthi, E. (2020). „Vještačka inteligencija i mašinsko učenje u dinamičkoj analitici sajber rizika na ivici mreže“, *SN Applied Science*, *Springer Nature Journal*.

6. Wahlster, W., Helbig, J., Hellinger, A., Stumpf, M. A. V., Blasco, J., Galloway, H., Gestaltung, H. (2013). „Preporuke za implementaciju strateške inicijative Industrija 4.0“, *Savezno ministarstvo za obrazovanje i istraživanje*, Njemačka.

7. Uredba (EU) 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti fizičkih osoba u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka, kojom se stavlja van snage Direktiva 95/46/EZ (Opšta uredba o zaštiti podataka – GDPR

8. ISO 31010:2019, Upravljanje rizikom – Tehnike procjene rizika, *Međunarodna organizacija za standardizaciju (ISO)*.

RISK MANAGEMENT SOFTWARE BASED ON AI AND CPS PREDICTION

DOI: *10.70329/2744-2403.2025.5.9.1*

Scientific article

Edin Garaplija [3]
Muhamed Duraković [4]

Abstract:
This paper focuses on the use of machine learning and the use of dedicated AI databases to create solutions based on an improved algorithm for preventive risk management, and real-time risk prediction. The paper analyses the existing standard, its shortcomings and solutions for improvement, and the structure and algorithmic basis of these systems, as well as their integration into existing security architectures and platforms. The work includes the detection of threats based on anomalies and the analysis of established user behavior according to given patterns, risk assessment and proactive detection of attacks. Timely identification and management of risks are becoming key factors in corporate sustainability and security of business and information systems. Predictive analytics, based on artificial intelligence, machine learning and big data analytics, bring transformational opportunities in areas such as industry, finance, healthcare, which in the modern era are connected by cybersecurity and risk prediction that help decision makers to manage systems more efficiently and protect them. An integrative approach to harmonizing these technologies, especially considering the organizational structure and legal framework, includes issues of reliability and transparency of models, as well as accountability for automated decisions, privacy protection and compliance with legislation. The aim of the paper is to provide a comprehensive overview of technological and methodological innovations in predictive protection against cyber risks, and to identify directions for future development with a special focus on the security, ethics and reliability of AI systems.

Keywords: *Risk, AI Prediction, Cyber Security*

---

[3] Edin Garaplija, PhD in security Science, President of INZA Institute of the Risk Management
[4] Muhamed Durakovic, IT Eng., IT Development engineer of the INZA Group

1. Introduction

Risk management in critical infrastructure systems is becoming an increasingly demanding task, especially in the context of accelerated technology development, increased connectivity of the systems themselves, and the growing sophistication of cyber threats. Current approaches based on measures, which usually omit prevention at the very beginning, are no longer sufficient to respond to modern corporate security challenges. In this context, artificial intelligence (AI) and machine learning offer new perspectives and opportunities for improving existing security systems, primarily through the introduction of predictive models that enable the recognition of threats before they cause damage in time. The focus will be on how algorithms are integrated into existing processes to improve standard approaches and enable timely reactions in complex environments. In addition to technical aspects, the paper will also address broader issues that accompany the application of these technologies, from ethical and legal challenges to issues of transparency and compliance with laws and internal regulations. This dimension is crucial to ensure the responsible and long-term sustainable use of AI systems in business practice. Today's digital transformation processes significantly contribute to greater connectivity and operational efficiency, but at the same time open up space for new vulnerabilities. Attacks on information systems are increasingly based on a combination of technical failures and human factors. Therefore, modern security approaches must go beyond traditional network boundary protection and encompass a broader risk analysis in everyday business. An expanded vision of security is needed, which connects technical, organizational, and human factors into a single early warning and preventive response system. The INZA Risk Management platform was developed with this vision in mind, in response to global challenges, offering a scalable and intelligent solution that can be adapted to the specific needs of different organizations in the management process of critical infrastructures.

2. Theoretical framework

In today's business environment, where digital technologies form the foundation of almost every sector, risk management is increasingly becoming part of a broader strategy for survival and growth. Instead of reacting only after an incident has occurred, increasing emphasis is placed on timely identification of threats and adequate responses to them.

It has been argued that the spectacular advancements in cyber-physical systems (CPSs) and internet of things (IoT) technology represent the foundation for Industry 4.0 (Whalster, W., 2013)CPS theory emerged from control theory and control systems engineering and focuses on the interconnection of physical components and use of complex software entities to establish new network and

systems capabilities. CPSs thus link physical and engineered systems and bridge the cyber world with the physical world.In contrast, IoT theory emerged from computer science and Internet technologies and focuses mainly on the interconnectivity, interoperability and integration of physical components on the Internet. With full IoT market adoption over the next decade, this integration work is anticipated to lead to developments such as IoT automation of CPSs (Dworschak, B., Zaiser, H., 2014)

This is especially true for cybersecurity, where a single failure can cause serious damage, both technical and reputational. At its core, risk management involves identifying threats, assessing them, making decisions about how to respond, and monitoring changes over time. Standards such as ISO 31000 offer a useful framework, but in practice it is often shown that classic models do not always correspond to the complexity of the modern digital environment. They rely on assessments that are sometimes subjective and difficult to adapt to the speed of change. The emergence of advanced technologies such as artificial intelligence has brought significant changes to this approach. Algorithms can now analyze huge amounts of data, detect patterns that previously went unnoticed, and warn of potential problems before they develop into serious incidents. Such systems are particularly useful for identifying deviations in behavior, whether of users or devices, which may indicate errors, abuses, or security attacks. The INZA Risk Management platform was developed on these principles, where it does not function only as a risk monitoring tool but as a system that actively learns from previous experiences and adapts to new situations.

Based on real data and user behavior, the system can warn of suspicious activities much earlier than classic mechanisms would. In this way, the reaction time is shortened, and damages can be significantly reduced. In addition, the platform uses predictive analysis methods, an approach that allows useful patterns to be extracted from past events for future assessments. This includes a situation analysis, an evaluation in which preventive measures are proposed, the creation of risk scenarios, and finally a crucial cost-benefit analysis that shows how much engaging in preventive measures ultimately reduces the possibility of a breakdown, as well as how much it brings, in economic terms, in benefits for the organization itself. Ultimately, INZA Risk Management is the product of a combination of years of experience and innovation, where its strength lies in its ability to adapt to any environment, especially those who have already embarked on the path of digitalization and are looking for ways to protect their systems in a smarter and longer-term way.

3. Security systems based on artificial intelligence

The use of artificial intelligence in modern security systems is becoming an increasingly common response to the challenges posed by the protection of complex information networks. Although classic measures such as firewalls, antivirus tools, and manual access control are still used, practice shows that they often cannot keep up with the speed and unpredictability of modern attacks. Today's attacks are not easily noticeable; they often occur through subtle changes and behaviors that can pass under the radar. Therefore, attention is increasingly being directed towards systems that do not depend on predefined rules but have the ability to recognize deviations in behavior themselves.

Table 3 The applications and technologies related to artificial intelligence for CPS

Connection	SAAS	BDP, mCPS	CBM	Self-maintain
Conversion	LCM	HMI, MaC	PHM	Self-aware
	AMAT	LTTA, SDC		
Cyber (analytic solutions)	EaPS	RTD, FoM, AA, PtPM	CPS	Self-compare
Cognition	SCRM	POD, SOPS	DSS	Self-predict
	ISaDS	ACD, MLA, HPC, ISR		Self-optimise
Configuration	TaT	CoA	RCS	Self-organise
	FPR	KPI		
	AMaAC	CPPS		Self-configure

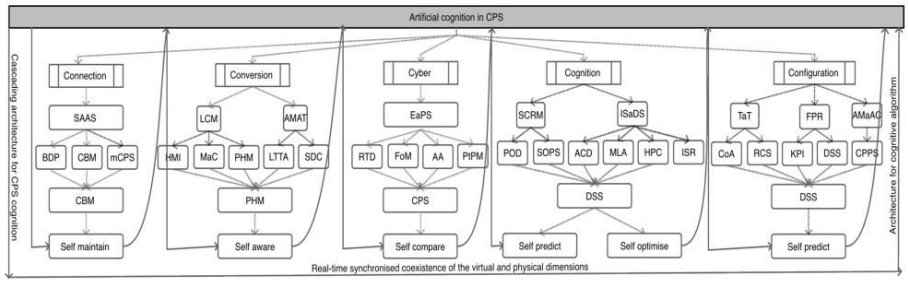


Fig. 2 Cascading framework for artificial intelligence for CPS

SN Applied Sciences
A SPRINGER NATURE journal

Fig.1.: Radanliev, P., (2020). „Artifcial intelligence and machine learning in dynamic cyber risk analytics at the edge“, SN Applied Science, Springer Nature Journal

The cascading framework in Fig. 2 presents a new way to design dynamic and automated predictive systems supported with real-time intelligence. This framework supports an assessment of the potential for adapting AI cognitive engines in data collection and analytics with dynamic real-time feedback. These engines might provide predictive intelligence on threat event frequency and the potential magnitude of resulting losses. Undoubtedly, to provide this

functionality, deep learning algorithms need to be adopted into cognitive engines to form dynamic confdence intervals and time bound ranges with real-time data. Once we have these abilities the cascading framework in Fig. 2 becomes a modern tool for risk analytics. (Radanliev, P., 2020)

Artificial intelligence algorithms analyze large amounts of data in real time and look for signs that deviate from the usual flow of activity, thus enabling them to detect threats that are not recorded in existing databases. The techniques used include various approaches, including classification, data clustering, and neural networks, which enable very precise recognition of irregularities in the system.

Advanced computer programs (AI) can quickly look through a lot of information to find and respond to potential threats, and change security methods as needed. These technologies utilize advanced algorithms to analyze large volumes of data and uncover potential risks, patterns, and anomalies. This enhancement in decision-making and resource allocation can be paralleled to the role of AI in other domains, such as climate change communication, where AI voices have shown to be as effective as human voices (Ni, B.,2023).

As part of the INZA Risk Management platform, AI is applied at multiple levels of protection. The first layer involves state analysis, where changes in usage patterns are constantly monitored in order to identify anything unusual. In addition, the system continuously monitors the behavior of all critical infrastructure components, records their "normal" operating modes, and recognizes when something deviates. When such a situation occurs, the system reacts immediately, sends a notification, and suggests steps for a preventive response. The special value of the INZA Risk Management system is reflected in its ability to connect to external data sources, such as global databases of known threats and previous accidents, and to use its own history to better understand the specifics of the environment in which it is used. This way, the system reacts not only to what it sees but also to what it knows, relying on experience combined with current data. In addition, automation plays a key role. When a risk is detected, the system immediately notifies the responsible persons and offers preventive measures, which shortens the reaction time to a minimum. It is this speed that often decides whether an incident will be successfully controlled or will develop into a serious security problem. Of course, such a degree of automation also opens up new questions: How to ensure that the system's decisions are understandable and verifiable, and what if the system makes a mistake? That is why INZA Risk Management includes the possibility of human control over each automated procedure, which achieves a balance between the efficiency of the technology and the professional assessment of the security team, and in the end, solutions like INZA Risk Management aren't more options, it's a necessity.

4. Improved risk prediction algorithm: examples and functionalities

At the core of the INZA Risk Management platform is an algorithm that was developed to help in the early detection of security threats in critical infrastructure systems. Unlike conventional approaches that mainly rely on known patterns, this system uses a combination of real-time data learning and anomaly analysis to continuously adjust its assessments and react to new situations (Garaplija, 2022).

One of its key advantages is that it does not look at just one source of information but simultaneously takes into account different aspects: technical indicators, the way the company structure is organized and access rules, and the behavior of the users themselves. In practice, this means that the system can notice when someone behaves differently than usual, whether it is an employee trying to access sensitive data at an unusual time or an unexpected change in access rights.

The context in which these changes occur is particularly important. It is not the same if an administrator logs into the system from the office premises during working hours or if an unknown user logs in from another location in the middle of the night. The algorithm takes these differences into account and, depending on the severity of the deviation, triggers an appropriate warning or offers preventive action. In order to be as clear as possible in its assessments, INZA Risk Management also uses visual risk labels; a certain color and percentage on the map show the level of risk, and in this way, people using the system quickly get an overview of the situation without having to go into technical details. (Garaplija, 2023).

Additionally, the system throws out what could happen if the observed problem is not resolved. Based on previous experiences and current analysis, the user is given three possible scenarios: realistic, most likely, and worst case. And what is more important, descriptions are written in a way that they can understand in their profession.

Great attention is also paid to preventive advice. When a threat is detected, the system suggests specific steps to be taken sometimes it is a technical intervention sometimes it is an organizational measure or employee education.

These recommendations are not random but are based on situations that have already occurred and have been successfully resolved in similar circumstances.

INZA risk management software has aligned Cyber and Physical Security by connecting various digital protocols of measurement and security sensors into a single AI database, which not only accelerates decision-making efficiency but also develops knowledge bases for future research and development.

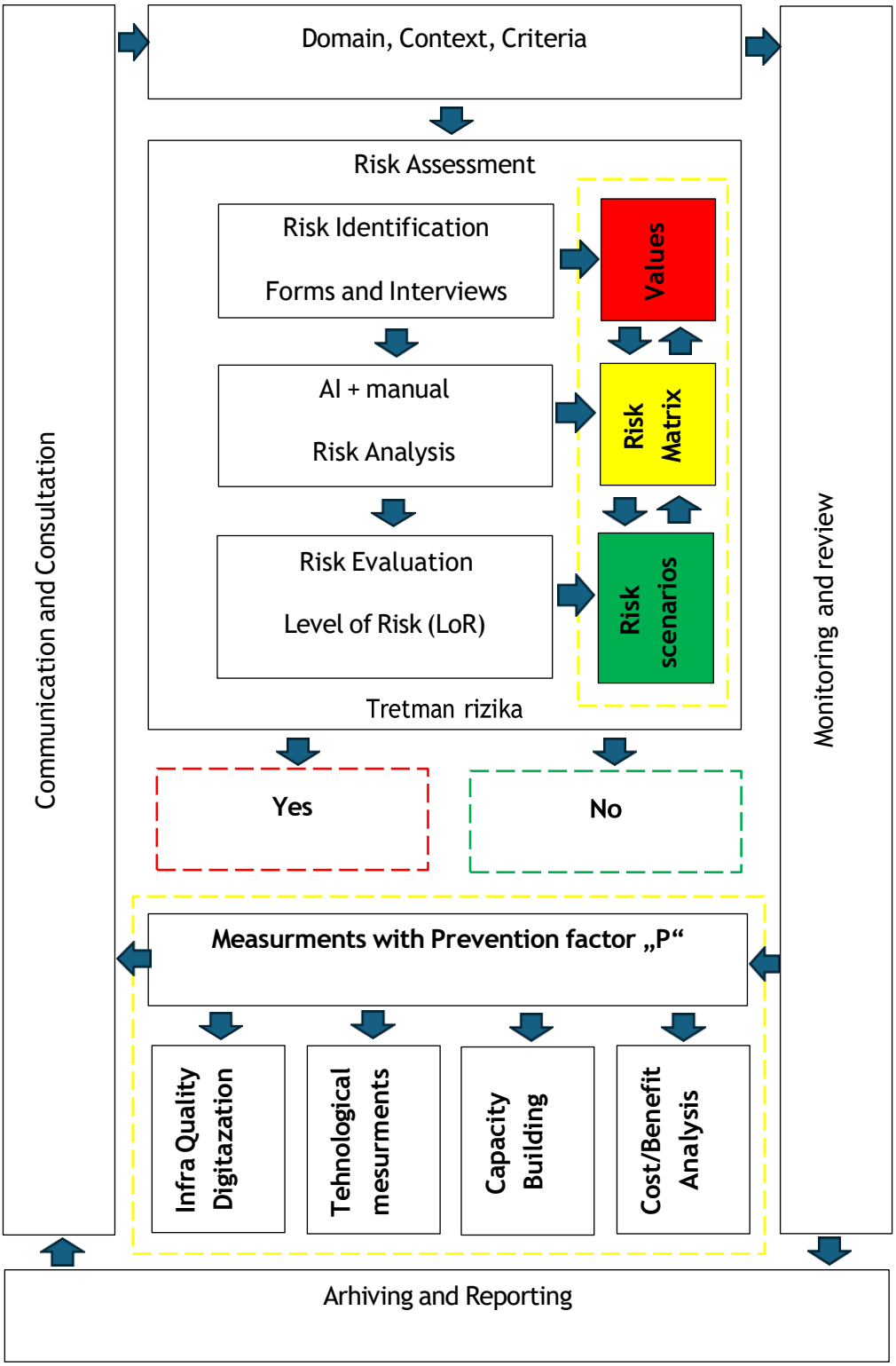


Fig.2: Improved ISO 31000 Risk Prevention Algorithm, (Garaplija, 2022)

CPS theory emerged from control theory and control systems engineering and focuses on the interconnection of physical components and use of complex software entities to establish new network and systems capabilities. CPSs thus link physical and engineered systems and bridge the cyber world with the physical world. In contrast, IoT theory emerged from computer science and Internet technologies and focuses mainly on the interconnectivity, interoperability and integration of physical components on the Internet. With full IoT market adoption over the next decade, this integration work is anticipated to lead to developments such as IoT automation of CPSs

What further confirms the efficiency of the INZA Risk Management algorithm is the way it reacted during testing in real conditions. In several cases, it managed to detect potential risks long before a standard system would have done so. Unlike many generic solutions that rely on predefined templates, INZA Risk Management is adapted to local conditions on the ground. It takes into account the specific characteristics of the market, language, legal framework, and security challenges that are characteristic of that region. It is precisely this ability to adapt that makes it particularly useful for companies and institutions around the world, where there are often nuances that foreign solutions simply do not recognize and then make incorrect assessments.

5. Challenges and limitations of corporate application

Integrating artificial intelligence into everyday business operations offers numerous advantages, but it also presents challenges, particularly when applied to sensitive domains like security risk assessment and the management of critical infrastructure. The INZA Risk Management platform, as an example of such a system, represents a powerful tool, but its inclusion in existing company structures is often not easy, as it requires changes that relate not only to technology but also to people, processes, and work culture. One of the first problems that may arise is how ready the organization is to adopt such a system, because in many environments the approach in which everything relies on human judgment still prevails, and automated systems cause skepticism, especially when they are expected to make recommendations. If employees are not familiar with how the algorithm works, a feeling of distrust and even resistance may arise, and in this way the situation is further complicated if it is not clearly defined who bears responsibility for the decisions made by the system, whether it is the person who monitors it or the team that uses it. The technical aspect of integration can also pose a serious challenge. Although INZA Risk Management is designed to be flexible, it still requires access to key data—logs, network records, and authentication protocols. If these systems are outdated, closed, or disconnected,

integration can take time and require additional resources, which is not always easy to do in the short term. A separate dimension is the issue of privacy. In order for the algorithm to do what is expected of it, it must analyze information that may include personal data—employee activities, access to certain files, and time and location of logging. Without clearly defined boundaries, there is a risk that security will turn into surveillance. That is why the INZA Risk Management system has built-in data access control and the principle of limited processing—only what is really necessary is analyzed, and every step the system takes can be subsequently verified. Beyond the technical and legal challenges, there's often a more subtle yet equally important barrier: the human factor. Employees may feel uneasy about AI being introduced into their work environment, sometimes perceiving it as a risk to their position. That's why successful implementation must go beyond simply deploying software; it also requires education, honest dialogue, and a clear explanation of how these systems can add value. A "step-by-step" approach, in which people learn the system through practice, has proven to be the most effective way to build trust. The issue of standardization and formal validation of such systems further complicates wider implementation. Although INZA Risk Management uses proven models and self-trained algorithms, there is still no universal framework that would accurately define how such tools are tested, approved, or certified, especially in regulated industries such as banking, healthcare, or energy, where there is no room for misjudgments. Added to all this is the fact that these systems must be regularly maintained, because AI is not static; if we do not update it, it quickly becomes outdated and ceases to be useful. Models must adapt to new data, learn from changes, and revise their rules to remain relevant, which means that the organization must have not only a good initial plan but also long-term support: technical, human, and strategic. However, when there is genuine willingness, a clear implementation plan, and strong leadership support, experience shows that such systems can be successfully embedded. In these environments, INZA Risk Management not only enhances security and accelerates incident response but also helps shift organizational mindsets toward a more proactive approach to risk.

6. Legislation, professional ethics and responsibility

The development of technologies that use artificial intelligence for risk management, especially in the context of corporate security, brings not only technical but also legal and ethical issues. When algorithms start taking over tasks that were previously performed by people, analyzing behavior and making recommendations, a logical concern arises: what if the system makes a mistake? And more importantly, who is responsible then? The implementation of solutions such as the INZA Risk Management platform requires that laws that protect

personal data and define the boundaries of automated decision-making be taken into account from the very beginning. In Europe, special attention is paid to rules such as the GDPR, which clearly states that users have the right to know how decisions that affect them are made and that a human can be involved in the process whenever necessary. INZA Risk Management is built so that every action initiated by the system is recorded and can be subsequently reviewed, explained, and, if necessary, challenged. The goal is not to put AI above people but to help the team react better and faster, but in addition to the law, professional ethics are also important. People who develop and use such systems have an obligation to act fairly, to respect boundaries, and not to use technology for things that are not in accordance with its purpose. For example, algorithms should not be used to monitor employees outside of a framework that is clear, justified, and known to everyone, and they should not draw automatic conclusions about someone's behavior without additional verification and context. INZA Risk Management is developed to support the "responsible use of AI"—not to replace human judgment, but to improve it and make it faster and more informed. Liability, of course, remains a sensitive issue. In traditional systems, it is often clear that if an error occurs, it is known who acted and where the mistake was made.

With AI systems, this boundary is not so clear. Is the person who created the model responsible? Or the person who uses it? Or maybe the system itself, although it does not legally exist as a "subject"? Therefore, it is important that every organization that uses such solutions has a clear framework: internal procedures, risk management rules, and documents that define how to act in the event of an error. The key lies in this, not in shifting responsibility, but in ensuring that everyone knows how to behave in accordance with clearly defined rules. Another important aspect is trust, because people working in an organization must know that there is a system that analyzes their activity, but also that they know why, how, and to what extent. Transparency is not achieved only by regulations and legal formulations but by honest conversations within the team.

INZA Risk Management therefore offers technical mechanisms that ensure privacy but also supports a culture in which users feel informed, not monitored. Ultimately, the success of such solutions will not depend only on how smart the algorithms are but on how much organizations are willing to use them responsibly. The solution, like INZA Risk Management, can be highly effective, but only when it fits within a broader framework that includes legal regulations, internal values, and a strong sense of ethical responsibility. When these elements come together, the system becomes a practical tool that helps strengthen security and support more informed decision-making.

7. System approach and further development

Risk management in critical infrastructure systems requires more than a single software solution or isolated security tool, or rather a comprehensive strategy that combines technology, processes, people, and legal obligations into a functional system that can respond to time-changing challenges. The INZA Risk Management platform was developed with this very goal in mind as part of a broader security ecosystem, ready to adapt to different sectors, sizes of organizations, and degrees of digital maturity, and what makes INZA Risk Management different is its approach that does not view risk assessment as the end goal but as the beginning of a constantly evolving process. Each identified threat triggers a chain of activities, from analysis and response to subsequent learning and adaptation. The system remembers, evaluates its own reactions, and adapts to changes in the environment, thus avoiding a static model and creating an environment in which security becomes a dynamic process.

A number of new possibilities are already being considered in further development plans, one of which is the ability to automatically direct available resources, whether it is personnel, equipment, or time, to where they are most needed, depending on the current level of risk. It is also planned to introduce simulations and tests, which allow organizations to test in advance how their system would react in the event of a serious attack and thus discover where they are vulnerable before someone else takes advantage of it. In the future, INZA Risk Management will be even more closely connected to the physical infrastructure with IOT sensors, security cameras, and other devices so that the picture of potential threats is as complete as possible and available in real time. Localization also plays a very important role: the platform already supports work in different languages and legal frameworks, which is especially important for organizations operating in multiple countries or in markets with specific requirements. In addition to the software itself, special attention is paid to the people who work with it, because no technology will produce the expected results if those who use it are not trained to interpret and apply it correctly.

That is why INZA Risk Management includes support through interactive guides, explanations of decisions proposed by the system, and recommendations for additional training, because the goal is not for the user to get lost in complexity, but for the system to be a tool that helps, not an obstacle. When it comes to regulatory compliance, especially those that are yet to come, INZA Risk Management is already keeping pace with the regulations that are developing within the European Union, thus enabling users to improve their security practices while remaining in line with legislative expectations and standards that are yet to come into force. In the following phases, INZA Risk Management will open the door to an even wider range of cooperation, as joint work on the development and

testing of new models will help the platform to further adapt to different environments and complex challenges that arise not only in the digital space, but also in the physical and social context. The essence of a systems approach is not to find the perfect solution but to teach the organization how to constantly adapt its protection mechanisms. INZA Risk Management is designed to provide exactly that, not just a tool that reacts to threats, but a solution that helps to learn something from every situation, to constantly improve the system, and to make the organization more resilient day by day.

8. Conclusion

Today, it is very important to think ahead, act preventively, and prevent and react quickly. This work has shown that artificial intelligence, if developed thoughtfully and used responsibly, can play a key role in this approach. The INZA Risk Management platform is just such an example, because its value is reflected not only in the technological solutions it uses, but also in the way it connects different sources of information, learns over time, and gives users what they really need: clear insights and recommendations that can be applied immediately.

There are numerous technical obstacles, changes in the organization, and numerous legal issues, which are part of any serious attempt at digital transformation. But these challenges are not a reason to give up; on the contrary, they are a call to manage technology responsibly and with understanding. Clear rules, legal compliance, and an ethical approach are not options but a necessary foundation for the stable and long-term implementation of such solutions. In the future, INZA Risk Management will continue to develop towards even better connectivity with other systems, greater transparency, and easier use.

The vision is not just a technologically advanced tool but a partner that grows, learns, and better understands the complexity of security challenges together with the organization. Finally, it should be clear: artificial intelligence will not replace humans in decision-making, but it can empower them; it can help them better understand what threatens them, react faster, and make safer decisions. In this sense, INZA Risk Management is not just software but a tool that combines human judgment and digital precision for management in critical infrastructure systems.

LITERATURE

1. Dworschak B, Zaiser H (2014), "Competences for cyber-physical systems in manufacturing - frst fndings and scenarios", Procedia CIRP 25:345–350

2. Garaplija, E., Prguda, S., (2023), "Smart cities for disaster risk reduction: using technology and innovation for a resilient urban environment", Assosiation of Risk Management, www.zisjournal.com

3. Garaplija, E., (2024), „3D logical model of integration between metaphysics and Disaster Risk Management, Assosiation of Risk Management, www.zisjournal.com

4. Ni, B., Wu, F., Huang, Q. (2023), „When artificial intelligence voices human concerns: The paradoxical effects of AI voice on climate risk perception and pro-environmental behavioral intention. International Journal of Environmental Research and Public Health, 20(4), 3772.

5. Petar Radanliev, David De Roure, Rob Walton, Max Van Kleek, (2020), „Eirini Anthi4, Artifcial intelligence and machine learning in dynamic cyber risk analytics at the edge"m SN Applied Science, Springer Nature Journal

6. Wahlster W, Helbig J, Hellinger A, Stumpf MAV, Blasco J, Galloway H, Gestaltung H (2013) Recommendations for implementing the strategic initiative Industrie 4.0. Federal Ministry of Education and Research

7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)

8. ISO 31010:2019, Risk management - Risk assessment techniques, International Standard Organisation

UPRAVLJANJE POŽARNIM RIZICIMA NA GLAVNOJ GASNOJ KRITIČNOJ INFRASTRUKTURI U BOSNI I HERCEGOVINI - GASNI SISTEM KANTONA SARAJEVO

DOI: *10.70329/2744-2403.2025.5.9.2*

Stručni rad

Dr. sci. Haris Delić, mag. SIMS
Mr. sci. Kemal Bošnjaković, dipl. maš. ing.,

Sažetak:
Značaj energetske sigurnosti u zemljama Jugoistočne Europe, u kontekstu pouzdanosti i sigurnosti snabdijevanja je uvijek bio u fokusu nacionalne sigurnosti i nacionalne ekonomije država te regije. Ovo naročito u vrijeme sve većih rizika koji se odvijaju na međunarodnom planu u pogledu rata Ruske Federacije protiv Ukrajine, a gledajući kroz kontekst da se prirodni gas najvećim dijelom doprema na područja Jugoistočne Europe (pa i Europske unije) putem prav(a)ca iz Ruske Federacije. U ovom radu ćemo se bazirati na mikroprostor Bosne i Hercegovine, tačnije na najveću gasnu infrastrukturu u Bosni i Hercegovini, a to je gasni sistem Kantona Sarajevo. Kada se govori o gasnoj infrastrukturi prvi rizici po ovu infrastrukturu su požarni rizici, koji mogu dovesti do požarnih uzroka i posljedica, odnosno razvoja požara i eksplozija na gasnim postrojenjima i gasnoj mreži. Da do ovoga ne bi došlo ulaže se velika pozornost i ozbiljnost, te se provode mjere i aktivnosti na prevenciji i sprečavanju da požarni rizici pređu u požarne posljedice. To podrazumijeva da distributer gasa u saradnji sa partnerima, te nadležnim javnim organima i institucijama ulaže maksimum napora, radi praktičnog provođenja zakonskih, tehničkih i tehnoloških propisa i standarda, svojstvenih ovoj specifičnoj oblasti energetike i sigurnosti oblasti, a ta aktivnost se obavlja 24/7.

Ključne riječi*: Zaštita od požara, zaštita od eksplozija, gasna mreža, gasna postrojenja, rizici, upravljanje rizicima, prevencija, provođenje zakonskih odredbi, standardi, tehnička pravila.*

Uvod

U svjetskim odnosima gasna infrastruktura predstavlja sami vrh nacionalnih interesa zemalja Europske unije, ali i drugih zemalja Europe koji još nisu članicom EU, tu posebno misleći na Bosnu i Hercegovini. Bosna i Hercegovina je prije tačno 50 godina, krenula u generacijski projekat izgradnje gasne mreže kojom se tada htjelo riješiti zagađenje glavnog grada BiH, Sarajeva, te se osigurati doprema pouzdanog i ekološki prihvatljivog energenta za ljudsko zdravlje, stvaranje optimalne toplotne energije, zaštitu okoliša i izgradnju industrije tog perioda. Devedesetih godina prošlog vijeka, Sarajevo kao i cijela BiH su bili pogođeni strašnim ratom koji je pored stradanja ljudi jako pogodio i gasnu infrastrukturu u smislu njenog rastresanja i vibriranja unutar zemlje usljed djelovanja minsko-eksplozivnih naprava. Također, jedan dio mreže je (do)građen u ratu, što predstavlja poseban izazov na očuvanju i eksploataciji infrastrukture koja potiče iz ovog perioda. Aktuelno gledajući, najveći izazov i rizik po gasnu infrastrukturu trenutno u Kantonu Sarajevo predstavlja nelegalna (do)gradnja objekata, te provođenje nelegalnih aktivnosti u zaštitnom pojasu gasovoda, što stvara direktnu opasnost po one koji takve radove izvode, te druge ljude, imovinu, te samo gasni sistem u cjelini. Kada govorimo o ovoj temi, kontekst promatranja pojma upravljanja rizicima a samim tim i sigurnosti moramo gledati u kroz današnje događaje, na način da „sigurnost i sigurnosne znanosti pokrivaju mnoga područja i zahtijevaju sveobuhvatni, ali i multidisciplinarni pristup zbog raznovrsnosti tih područja. Ta činjenica posebno dolazi do izražaja u 21. stoljeću kad se fokus u području sigurnosti počinje sve više odmicati od tradicionalnih shvaćanja i ratnih djelovanja“ (Kadić, 2024).

Zakonska legislativa, tehnička regulativa, standardi – važnost i primjena

I dalje u periodu od preko 30 godina nakon samostalnosti, Bosna i Hercegovina nema usvojen zakon o gasu. Umjesto toga koriste se propisi entitetskog nivoa ili čak nižih nivoa. Konkretno kada je Kanton Sarajevo u pitanju temeljno referentni su slijedeći propisi za oblast gasne privrede i infrastrukture:

- Uredba o organizaciji i regulaciji sektora gasne privrede (Službene novine Federacije BiH, broj: 83/07),
- Pravilnik o preuzimanju i primjeni tehničkih propisa za oblast projektovanja, građenja, puštanja u pogon, eksploatacije i održavanja postrojenja i instalacija prirodnog gasa (Službene novine Federacije BiH, broj: 83/08),
- Uredba o snabdijevanju prirodnim gasom Kantona Sarajevo (Službene novine Kantona Sarajevo broj 22/16),

- Pravilnik o uslovima za nesmetanu i sigurnu distribuciju prirodnog gasa distributivnim gasnim sistemom pritiska do 16 bara (Službene novine Kantona Sarajevo broj 40/2017),
- Tehnička pravila,
- Standardi,
- Interne procedure distributera.

U pogledu sigurnosti, konkretno zaštite od požara, primarno su referentni slijedeći propisi i dokumenti:

- Zakon o zaštiti i spašavanju ljudi i materijalnih dobara od prirodnih i drugih nesreća (Službene novine Federacije BiH, broj: 39/03, 22/06 i 43/10),
- Zakon o zaštiti od požara i vatrogastvu (Službene novine Federacije BiH, broj 64/09),
- Podzakonska akta iz ove oblasti,
- Procjene i planovi zaštite i spašavanja od prirodnih i drugih nesreća,
- Procjene i planovi zaštite od požara.

Dosljednom primjenom i provođenjem ovih propisa, pravila, standarda i dokumenata se može osigurati optimalna sigurnost i pametno upravljanje požarnim rizicima. Međutim to nije uvijek slučaj u praksi, naročito kada govorimo o primjeni ovih propisa od strane trećih lica, koja svojim nepropisnim radom ugrožavaju gasni sistem, te ljude i materijalna dobra. Također jedan od velikih rizika po sigurnost gasne infrastrukture, ali i općenito kritične infrastrukture u Bosni i Hercegovini, predstavlja činjenica da Bosna i Hercegovina, ali ni Federacija BiH, nemaju zakon o kritičnoj infrastrukturi, čime do današnjeg dana nisu ispunjene obaveze u pogledu reguliranja ove oblasti u skladu sa Direktivom Europske unije (EU) 2022/25571 iz 2022. godine. Ovo predstavlja temeljni i suštinski nedostatak u efikasnom upravljanju rizicima na kritičnoj infrastrukturu, pa samim tim i požarnim rizicima. Naročito imajući u vidu činjenicu da: „prijetnje po infrastrukturu imaju antropogene, strateške, organizacijske, materijalne, i tehničko-tehnološke posljedice. Štete koje mogu nastati usljed realizacije rizika sem što prouzrokuju velike materijalne troškove, utiču i na sam ugled organizacije“ (Gavrilović, 2023).

[1] Direktiva Europske unije (EU) 2022/2557 Europskog parlamenta i vijeća od 14.12.2022. godine o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ

Požarni rizici u procesu distribucije prirodnog gasa

Požarni rizici predstavljaju najopasnije rizike po kritičnu infrastrukturu za distribuciju gasa. Kada je u pitanju njihovo stvaranje i posljedično kreiranje iz neke druge opasnosti i rizika, posebno mjesto zauzima slijedećih 7 uzroka ili rizika:

1. Prirodne i druge nesreće koje kreiraju požarni rizik (poplava, klizište i sl.),
2. Curenje prirodnog gasa (u najvećoj mjeri nekontrolisano),
3. Neispravna gasna ili elektro instalacija ili tehnički sistemi koji ih štite,
4. Rizici kod održavanja gasnih instalacija i postrojenja (prilikom održavanja pojavljivanje iskre, otvoreni plamen u blizini, korištenje iskrećeg alata, upaljena cigareta i sl.),
5. Sabotaže, diverzije ili teroristički napadi na gasnoj infrastrukturi,
6. Nepravilnosti kod zapunjavanja i pražnjenja gasnog sistem prirodnim gasom (prekid dotoka gasa zbog raznih razloga, politički, ekonomski i sl.),
7. Nepravilnost u procesu postavljanja instalacija i neredovno održavanje istih (kod krajnjeg korisnika, prepravke, neispravni krajnji uređaji i sl.).

U svakom ovom segmentu, ljudski faktor u preduprjeđenju da ne dođe do prelaska požarnog rizika u stvarnu prijetnju, a kasnije i posljedicu, igra ključnu ulogu.

Mjere i aktivnosti koje poduzima distributer glavne gasne infrastrukture u cilju pametnog upravljanja požarnim rizicima

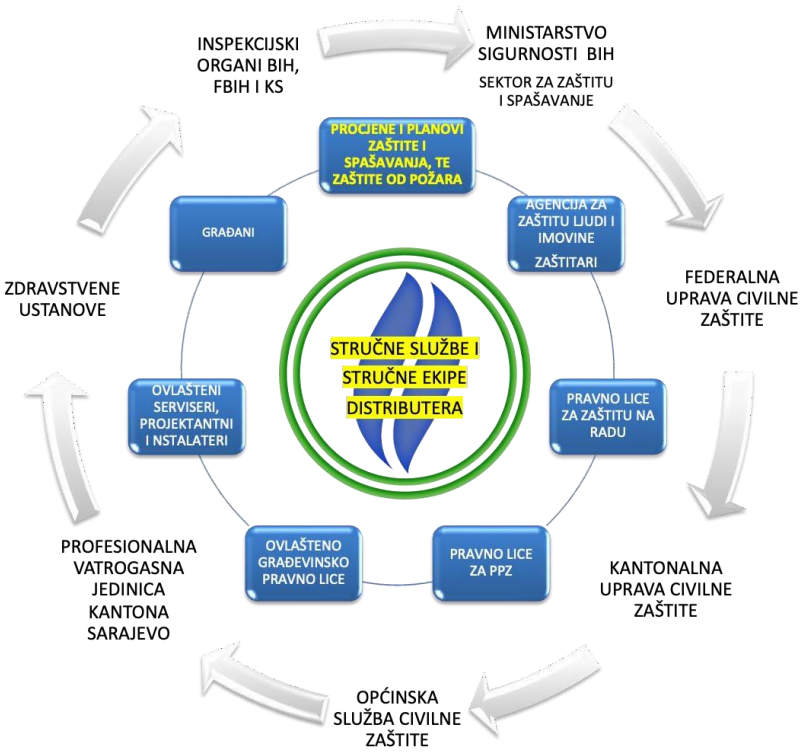
Baza svakog ozbiljnog posla na visokorizičnim i opasnim infrastrukturama je dosljedna, te kontinuirana primjena mjera zaštite od požara u 24 satnom režimu rada, sa posebnim osvrtom na primjenu dodatnih i posebnih mjera prilikom provođenja požarno visokorizičnih poslova u pogledu održavanja, sanacije, rekonstrukcije i izgradnje gasne mreže i postrojenja. Kada je u pitanju Kanton Sarajevo, gasna mreža Kantona Sarajevo ima dužinu od preko 1500 kilometara, na području cijelog Kantona u različitim smjerovima, različitog profila, a ova mreža je uvijek pod pritiskom. To znači da ispod Kantona Sarajevo imamo u svakom momentu visok rizik od od potencijalnog nastanka eksplozije i/ili požara, što uvijek nivo ozbiljnost diže na najviše mjesto na ljestvici. Pored propisa koje distributer gasa i upravljač ovim javnim dobrom (gasnim sistemom), Sarajevogas primjenjuje, on posjeduje visokokvalitetne kadrove koji su stručnjaci u oblasti mašinske, elektro, građevinske struke, zaštite na radu, zaštite od požara, te zaštite od prirodnih i drugih nesreća. Održavanje sistema u ispravnoj funkciji, njegova kontrola i održavanje su od presudnog značaja za sigurnu i pouzdanu distribuciju

gasa putem Gasnog sistema Kantona Sarajevo. Tu spada čitav niz preventivnih radnji:

- Nadzor i upravljanje gasnim sistemom, poseban nadzor nad parametrima pritiska gasa. Ova aktivnost se provodi putem Dispečerskog centra i putem ekipa na terenu, sa operativnošću 24/7.
- Odorizacija, dodavanje karakterističnog mirisa prirodnom gasu da bi se isti prepoznao u slučaju njegovog prisustva u prostoru gdje može u omjeru sa zrakom, formirati eksplozivnu smjesu.
- Redovno održavanje gasnih postrojenja, gasne mreže, provođenje nadzora nad radom ovlaštenih servisera, instalatera i projektanata unutrašnjih gasnih instalacija.
- Ugradnja sistema prevencije putem tehničke zaštite (sistemi aktivne zaštite od požara za dojavu dima i vatre, te sistemi aktivne zaštite od požara za dojavu prisustva zapaljivih gasova), kojima se pravovremeno i preventivno doznaje za prisustvo određenog rizika (dima, vatre, gasa), na mjestu i u količini koja može dovesti do posljedica.
- Tehnička i fizička zaštita gasnih postrojenja, poseban nadzor nad parametrima sigurnosti ovih postrojenja (fizička zaštita, vatrodojava, plinodojava, protuprovala, kontrola pristupa i videonadzor). Ova aktivnost se provodi putem Dojavnog-operativnog centra i putem mobilnih naoružanih ekipa na terenu, sa operativnošću 24/7. Predmetni centar posjeduje ovlaštenja i odobrenja izdate od strane Federalnog ministarstva unutrašnjih poslova i nadležnog kantonalnog ministarstva unutrašnjih poslova.
- Redovna, periodična *ad hoc* obuka vlastitih radnika za djelovanje u kriznim situacijama, izazvanih nekontrolisanim curenjem gasa, požarom ili eksplozijom, sa aspekta tehničko-tehnoloških mjera, preko mjera zaštite od požara, do mjera zaštite procesa redovnog snabdijevanja prirodnim gasom Kantona Sarajevo.
- Saradnja sa inspekcijskim organima sa nivo Kantona, Federacije i nivoa države BiH, u cilju kontrole, nadzora i pomoći distributeru da propisno i pravilno primjenjuje propise, tehnička pravila, standarde i pravila struke u svom radu.
- Podrška ovlaštenih pravnih lica za obavljanje poslova zaštite od požara, putem sistema ugovaranja.
- Protupožarna i protueksplozivna podrška lokalne profesionalne vatrogasne jedinice 24/7, sistemu rada i sigurnosti gasnog sistema Kantona Sarajevo.
- Pisane i slikovite smjernice putem znakova upozorenja, obavještenja i zabrana koji se nalaze na svim postrojenjima, na način da svim ljudima koji na bilo koji način dolaze u dodir ili susret sa gasnim postrojenjima,

daju jasne smjernice šta treba a šta ne treba raditi kada su u pitanju gasna postrojenja, sa aspekta zaštite od požara.

Na narednoj ilustraciji ćemo prikazati na koji način se odvija saradnja različitih subjekata i aktera sigurnosti, u cilju osiguranja pouzdane i sigurne distribucije gasa



Slika 1. Izvor: Sektor sigurnosti i općih poslova KJKP Sarajevogas d.o.o. Sarajevo, 2023. godina

Kao što i ilustracija prikazuje, distributer se primarno oslanja na vlastite kadrove i stručno osoblje koje posjeduje u redu vlastitih radnika. Kada zahtjevi i požarni rizici nadilaze kapacitete i nadležnosti distributera, isti se odmah (znači bez odlaganja) obraća eksternim pravnim osobama, organima i institucijama za podršku u oblasti upravljanje požarnim rizicima, i najveći dio aktivnosti se odvija u sferi prevencije. Ovaj sistem rada pokazuje važnost stručnosti i timskog rada u ovom poslovima zaštite od požara i zaštite od požarnih rizika, kroz javno-javno i javno-privatno partnerstvo. Ovaj pristup u aktuelnom trenutku daje rezultate, ali se uvijek iznova analizira u cilju obogaćivanja i proširenja saradnje, te pametnijeg i efikasnijeg upravljanja požarnim rizicima.

Zaključak

Gasna infrastruktura Kantona Sarajevo nije samo tehnički sistem podzemnih cijevi i postrojenja – ona je pulsirajući krvotok jedne urbane cjeline, temelj stabilnosti energetskog, ekonomskog i društvenog poretka. Njena sigurnost nije stvar rutinskog tehničkog održavanja, nego svakodnevne borbe protiv višeslojne strukture rizika – od fizičkih i tehnoloških, do pravnih, društvenih i strateških.

Upravljanje požarnim rizicima u kontekstu gasne infrastrukture zahtijeva daleko više od pukog ispunjavanja zakonskih normi. To je kontinuirani proces promišljenog balansiranja između prevencije i reakcije, između zakonodavnog vakuuma i stvarnih potreba sigurnosne prakse na terenu. Iako Kanton Sarajevo ima niz propisa koji se primjenjuju u regulaciji distribucije gasa, sistemska praznina koju ostavlja nepostojanje zakona o kritičnoj infrastrukturi – kako na nivou entiteta, tako i države – predstavlja ključnu slabost u lancu sigurnosti.

Uprkos institucionalnim izazovima, distributer gasa u Kantonu Sarajevo, KJKP Sarajevogas d.o.o., pokazuje visok nivo profesionalizma u prepoznavanju i upravljanju požarnim rizicima. Kroz operativni režim 24/7, obuku stručno-tehničkih kadrova, tehničku i fizičku zaštitu postrojenja, te široku mrežu saradnje s inspekcijskim organima, sigurnosnim institucijama i privatnim akterima, ovaj sistem ne samo da odgovara na rizike – on ih aktivno predviđa i predupređuje. U tom kontekstu, vidimo formu tzv. „žive sigurnosti“, gdje tehnika, zakon i ljudski faktor djeluju u sinergiji.

S druge strane, svakodnevna prijetnja od nelegalne gradnje, nestručnih radova trećih lica, i generalno nepostojanja optimalne spoznaje o značaju gasne mreže među građanima i institucijama, nameću potrebu za novim pristupima. Sigurnost gasne infrastrukture više se ne može promatrati kao izolovana tehnička oblast. Ona je sastavni dio koncepta „otporne zajednice“, gdje je svaki akter – od zakonodavca do građanina – odgovoran za sigurnost sistema koji u konačnici čuva normalan život građana, njihovu imovinu, poslove procese kompanija, te ono najvažnije zdravlje i živote ljudi.

U tom svjetlu, donošenje zakona o kritičnoj infrastrukturi u BiH i usklađivanje sa Direktivom EU 2022/2557 nisu samo evropske obaveze – one su egzistencijalni prioritet. Svaki dan bez tog zakona je dan sa više nepredvidivih rizika. Praksa Sarajevogasa može i treba poslužiti kao model drugim subjektima u BiH i regiji – ne samo po pitanju organizacije i tehničkog nadzora, već i po načinu na koji se sigurnost postavlja kao centralna vrijednost poslovanja.

LITERATURA

Udžbenici, stručni i naučni tekstovi:

1) Gavrilović, B., 2023. Scenario rizika i protivpožarna zaštita kod sistema mehaničke ventilacije. Zaštita i sigurnost, Objavljeno u Izdanju 1., Godina 3, str. 29,
2) Kadić, A., 2024. Mogućnost formiranja hrvatskog tima strukturnih inženjera unutar Europskog kapaciteta za odgovor na hitne situacije (EERC). Zaštita i sigurnost, Objavljeno u Izdanju 2., Godina 4, str. 96,

Propisi

1) Direktiva Europske unije (EU) 2022/2557 Europskog parlamenta i vijeća od 14.12.2022. godine o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ,
2) Zakon o zaštiti i spašavanju ljudi i materijalnih dobara od prirodnih i drugih nesreća (Službene novine Federacije BiH, broj: 39/03, 22/06 i 43/10),
3) Zakon o zaštiti od požara i vatrogastvu (Službene novine Federacije BiH, broj 64/09),
4) Uredba o organizaciji i regulaciji sektora gasne privrede (Službene novine Federacije BiH, broj: 83/07),
5) Pravilnik o preuzimanju i primjeni tehničkih propisa za oblast projektovanja, građenja, puštanja u pogon, eksploatacije i održavanja postrojenja i instalacija prirodnog gasa (Službene novine Federacije BiH, broj: 83/08),
6) Uredba o snabdijevanju prirodnim gasom Kantona Sarajevo (Službene novine Kantona Sarajevo broj 22/16),
7) Pravilnik o uslovima za nesmetanu i sigurnu distribuciju prirodnog gasa distributivnim gasnim sistemom pritiska do 16 bara (Službene novine Kantona Sarajevo broj 40/17),
8) Procjena ugroženosti od prirodnih i drugih nesreća KJKP Sarajevogas d.o.o. Sarajevo, 2023,
9) Procjena ugroženosti od požara KJKP Sarajevogas d.o.o. Sarajevo, 2023,
10) Plan zaštite ljudi i materijalnih dobara od prirodnih i drugih nesreća KJKP Sarajevogas d.o.o. Sarajevo, 2023,
11) Plan zaštite od požara KJKP Sarajevogas d.o.o. Sarajevo, 2023,

FIRE RISK MANAGEMENT ON MAIN GAS CRITICAL INFRASTRUCTURE IN BOSNIA AND HERZEGOVINA - THE GAS SYSTEM OF CANTON SARAJEVO

DOI: *10.70329/2744-2403.2025.5.9.2*

Professional article

Dr. sci. Haris Delić, M.Sc. SPS
Mr. sci. Kemal Bošnjaković, B.Sc. Mech. Eng.

Abstract:

The importance of energy security in Southeast European countries, particularly in terms of the reliability and safety of energy supply, has consistently been a central concern of both national security and national economic policy. This issue has become even more prominent in light of increasing geopolitical risks, especially following the Russian Federation's war against Ukraine. This context is particularly relevant given that natural gas is predominantly supplied to Southeast Europe via routes originating in the Russian Federation.

This professional paper focuses on the micro-level context of Bosnia and Herzegovina, specifically on the country's largest gas infrastructure system—the gas distribution system of Sarajevo Canton. When it comes to gas infrastructure, fire hazards are among the primary risks, as they can lead to significant consequences including fires and explosions in gas facilities and the gas distribution network. In order to prevent such incidents, significant attention is given to implementing preventive and mitigation measures aimed at managing fire risks before they escalate into actual fire-related events. This implies that the gas distributor, in cooperation with the competent inspection authorities, exerts maximum effort to ensure the practical implementation of legal, technical, and technological regulations and standards specific to this highly specialized area of energy and safety. These activities are carried out continuously, 24/7.

Keywords*: fire protection, explosion protection, gas network, gas facilities, risks, risk management, prevention, legal compliance, standards, technical regulations.*

Introduction

In global strategic relations, gas infrastructure occupies a top position among national interests—not only for European Union member states, but also for other European countries that are not yet part of the EU, particularly Bosnia and Herzegovina. Exactly fifty years ago, Bosnia and Herzegovina embarked on a generational project to build a gas distribution network with the goal of mitigating air pollution in the capital city, Sarajevo. The aim was to ensure the supply of a reliable and environmentally friendly energy source, contributing to public health, optimal thermal energy production, environmental protection, and industrial development at the time.

In the 1990s, Sarajevo and the entire country were devastated by war. In addition to the tragic human toll, the gas infrastructure was severely affected—displaced and destabilized by underground detonations caused by explosive devices. Furthermore, part of the network was built or expanded during wartime, presenting a specific challenge for preserving and operating infrastructure that originates from that period.

Today, one of the greatest risks facing the gas infrastructure in Sarajevo Canton is illegal construction and unauthorized activities within the gas pipeline protection corridor. These actions pose a direct danger not only to those carrying out such works, but also to the wider population, property, and the gas system as a whole.

When addressing this topic, it is essential to frame risk management—and safety in general—within the context of contemporary challenges. As Kadić (2024) points out, "security and security sciences encompass many fields and require a comprehensive, multidisciplinary approach due to their diversity. This fact is especially evident in the 21st century, as the focus in the field of security increasingly shifts away from traditional interpretations and wartime operations."

Legal Framework, Technical Regulations, and Standards – Importance and Implementation

More than thirty years after gaining independence, Bosnia and Herzegovina still has not adopted a state-level gas law. Instead, regulations are applied at the entity or even lower administrative levels. Specifically, for Sarajevo Canton, the following legal instruments represent the core regulatory framework for the gas sector and infrastructure:

- Regulation on the Organization and Regulation of the Gas Industry Sector (Official Gazette of the Federation of BiH, No. 83/07),
- Rulebook on the Adoption and Implementation of Technical Regulations for the Design, Construction, Commissioning, Operation, and Maintenance of Natural Gas Facilities and Installations (Official Gazette of the Federation of BiH, No. 83/08),
- Regulation on Natural Gas Supply in Sarajevo Canton (Official Gazette of Sarajevo Canton, No. 22/16),
- Rulebook on Conditions for the Safe and Uninterrupted Distribution of Natural Gas in Distribution Systems with Pressure up to 16 bar (Official Gazette of Sarajevo Canton, No. 40/2017),
- Technical Rules,
- Standards,
- Internal procedures of the gas distributor.

In terms of safety—specifically fire protection—the following laws and documents are primarily referenced:

- Law on the Protection and Rescue of People and Material Goods from Natural and Other Disasters (Official Gazette of the Federation of BiH, Nos. 39/03, 22/06, and 43/10),
- Law on Fire Protection and Firefighting (Official Gazette of the Federation of BiH, No. 64/09),
- Sub-legal acts in the field of fire protection,
- Risk assessments and protection and rescue plans against natural and other disasters,
- Fire protection assessments and fire safety plans.

Strict implementation and consistent application of these laws, rules, standards, and documents ensure optimal safety and effective fire risk management. However, this is not always the case in practice—especially when third parties violate these regulations through improper work practices, thereby endangering the gas system, human lives, and material assets.

A particularly significant risk to the safety of gas infrastructure—and to critical infrastructure in Bosnia and Herzegovina in general—is the absence of a law on critical infrastructure, both at the state level and within the Federation of BiH. As a result, the country has yet to fulfill its obligation to regulate this area in accordance with the European Union Directive (EU) 2022/2557 from 2022. This legislative gap constitutes a fundamental weakness in the efficient management of risks associated with critical infrastructure, including fire risks.

This is especially concerning given the fact that "threats to infrastructure can have anthropogenic, strategic, organizational, material, and technical-technological consequences. The damages resulting from risk realization not only incur significant material costs, but also affect the reputation of the organization" (Gavrilović, 2023).

Fire Risks in the Natural Gas Distribution Process

Fire risks represent the most serious threats to critical infrastructure in the natural gas distribution sector. These risks can arise directly or as a consequence of other hazards, with the following seven causes or risk factors being particularly significant:

1. Natural and other disasters that create fire hazards (e.g., floods, landslides, etc.),
2. Uncontrolled leakage of natural gas,
3. Defective gas or electrical installations or malfunctioning safety systems,
4. Risks associated with maintenance of gas installations and facilities (e.g., occurrence of sparks, presence of open flame, use of spark-generating tools, smoking near installations),
5. Sabotage, diversion, or terrorist attacks targeting gas infrastructure,
6. Improper procedures during gas system pressurization or depressurization (e.g., gas supply interruptions due to political, economic, or other causes),
7. Improper installation and irregular maintenance of internal gas systems (e.g., unprofessional modifications, faulty end-user appliances).

In all of these areas, the human factor plays a key role in preventing fire risks from escalating into actual threats and ultimately causing harmful consequences.

Measures and Activities Undertaken by the Distributor of the Main Gas Infrastructure for Smart Fire Risk Management

The foundation of any serious operation involving high-risk and hazardous infrastructures lies in the consistent and continuous implementation of fire protection measures around the clock, with special attention given to additional and specific measures during fire high-risk operations such as maintenance, repairs, reconstruction, and construction of the gas network and facilities.

Regarding the Canton of Sarajevo, the gas network extends over 1,500 kilometers across the entire canton, covering various directions and profiles, and is continuously under pressure. This inherently creates a constant high risk of potential explosion and/or fire incidents beneath the territory of Canton Sarajevo, which elevates the seriousness of safety management to the highest priority.

In addition to the regulations governing gas distributors and the operators of this public asset (the gas system), Sarajevogas employs highly qualified personnel who are experts in mechanical, electrical, and civil engineering disciplines, occupational safety, fire protection, as well as natural and other disaster protection fields. Maintaining the system in proper operational condition, its continuous monitoring, and upkeep are crucial for the safe and reliable distribution of gas through the Gas System of Canton Sarajevo. This includes a broad range of preventive measures:

- **Monitoring and control of the gas system**, with special attention to gas pressure parameters. This activity is carried out through the Dispatch Center and field teams operating 24/7.
- **Odorization** – the addition of a characteristic smell to natural gas to enable its detection in case it leaks into an area where it could form an explosive mixture with air.
- **Regular maintenance** of gas facilities and the network, including supervision of authorized service providers, installers, and designers of internal gas installations.
- **Installation of prevention systems through technical protection**, such as active fire protection systems for smoke and flame detection and active gas detection systems. These enable timely and preventive detection of hazards (smoke, fire, gas) at levels and locations that could lead to adverse consequences.
- **Technical and physical protection of gas facilities**, including close monitoring of safety parameters (physical protection, fire alarm, gas detection, anti-burglary measures, access control, and video surveillance). This is managed through the Alarm and Operations Center and mobile armed teams operating 24/7. This center holds official authorizations issued by the Federal Ministry of Internal Affairs and the relevant cantonal ministries.
- **Regular and ad hoc training** of in-house personnel for crisis response caused by uncontrolled gas leaks, fires, or explosions, covering technical and technological measures, fire protection protocols, and maintaining uninterrupted gas supply to the Canton.

- **Collaboration with inspection authorities** at the cantonal, federal, and state levels to ensure proper enforcement and application of regulations, technical rules, standards, and best practices in daily operations.
- **Support of authorized legal entities** for fire protection tasks via contractual engagement.
- **Fire and explosion protection support** from the local professional firefighting unit operating 24/7, ensuring the safety and operational continuity of the gas system in Canton Sarajevo.
- **Clear written and visual guidelines** through warning signs, notices, and prohibitions displayed on all facilities. These provide all personnel and visitors interacting with gas installations with explicit instructions on what actions to take or avoid concerning fire protection.

The subsequent illustration will demonstrate how various entities and actors collaborate to ensure the reliable and safe distribution of gas.

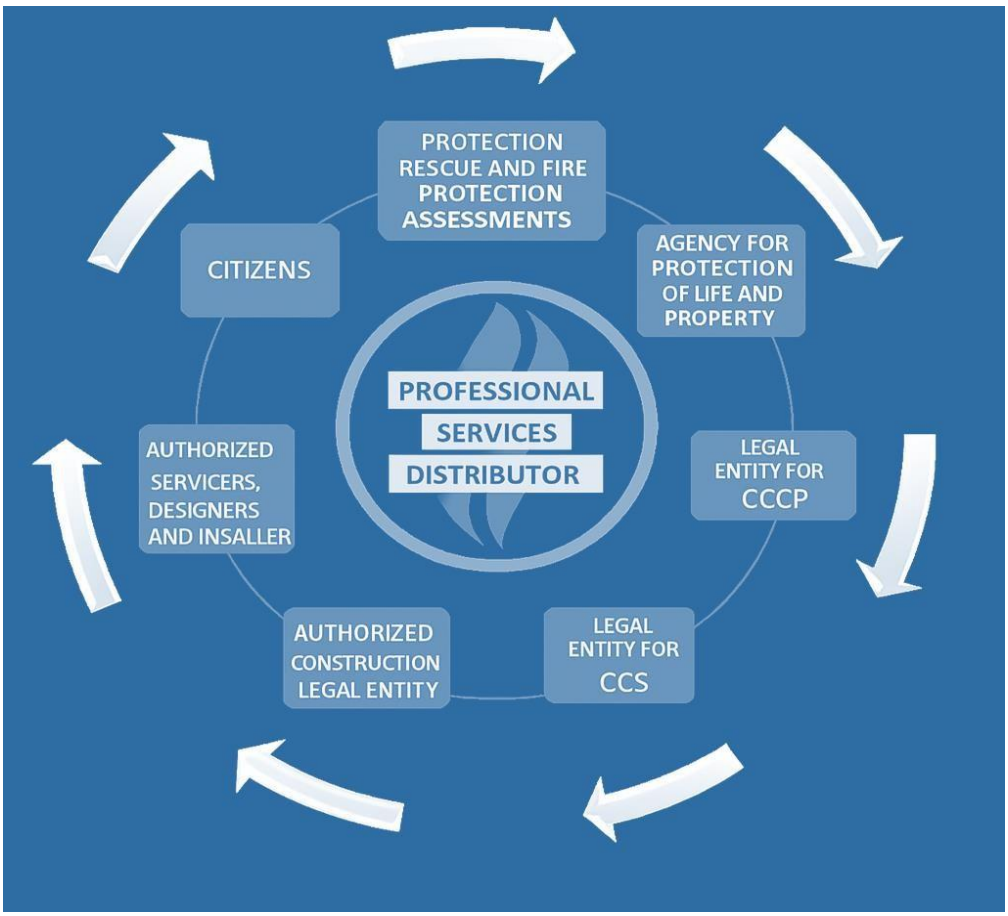


Figure 1. Source: Security and General Affairs Sector, Public Utility Company Sarajevogas d.o.o. Sarajevo, 2023.

As illustrated, the distributor primarily relies on its own qualified personnel and expert staff within its workforce. When demands and fire risks exceed the capacities and jurisdiction of the distributor, they immediately (without delay) engage external legal entities, authorities, and institutions to support fire risk management. The majority of activities take place within the realm of prevention. This operational model underscores the importance of expertise and teamwork in fire protection and fire risk management, through both public-public and public-private partnerships. While this approach currently delivers results, it is continually analyzed to enhance and expand cooperation for smarter and more efficient fire risk management.

Conclusion

The gas infrastructure of Canton Sarajevo is not merely a technical system of underground pipes and facilities — it is the pulsating bloodstream of an urban entity, the foundation of the energy, economic, and social order's stability. Its safety is not a matter of routine technical maintenance but a daily battle against a multilayered structure of risks — from physical and technological, to legal, social, and strategic.

Managing fire risks in the context of gas infrastructure demands far more than mere compliance with legal norms. It is a continuous process of thoughtful balancing between prevention and response, between legislative gaps and the actual needs of safety practice on the ground. Although Canton Sarajevo has numerous regulations governing gas distribution, the systemic void created by the absence of a critical infrastructure law — both at the entity and state levels — represents a key weakness in the safety chain.

Despite institutional challenges, the gas distributor in Canton Sarajevo, Public Utility Company Sarajevogas d.o.o., demonstrates a high level of professionalism in recognizing and managing fire risks. Through a 24/7 operational regime, training of technical experts, technical and physical protection of facilities, and an extensive network of cooperation with inspection bodies, security institutions, and private actors, this system not only reacts to risks — it actively anticipates and prevents them. In this context, we observe a form of so-called "living safety," where technology, legislation, and the human factor operate synergistically.

On the other hand, the daily threat of illegal construction, unqualified work by third parties, and a general lack of awareness about the significance of the gas

network among citizens and institutions call for new approaches. Gas infrastructure safety can no longer be viewed as an isolated technical issue. It is an integral part of the concept of a "resilient community," where every actor — from lawmakers to citizens — shares responsibility for the safety of the system that ultimately protects citizens' normal lives, their property, business processes, and, most importantly, their health and lives.

In this light, the enactment of a critical infrastructure law in Bosnia and Herzegovina and harmonization with EU Directive 2022/2557 are not only European obligations — they are existential priorities. Every day without such legislation is a day with increased unpredictable risks. The practice of Sarajevogas can and should serve as a model for other entities in BiH and the region — not only in terms of organization and technical supervision but also in how safety is established as a core business value.

REFERENCES

Textbooks, Professional and Scientific Papers:

1. Gavrilović, B., 2023. *Risk Scenarios and Fire Protection in Mechanical Ventilation Systems*. Zaštita i sigurnost, Issue 1, Vol. 3, pp. 29.
2. Kadić, A., 2024. *Possibility of Forming a Croatian Team of Structural Engineers within the European Emergency Response Capacity (EERC)*. Zaštita i sigurnost, Issue 2, Vol. 4, pp. 96.

Regulations:

1. European Union Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
2. Law on Protection and Rescue of People and Material Goods from Natural and Other Disasters (Official Gazette of the Federation of BiH, Nos. 39/03, 22/06, and 43/10).
3. Law on Fire Protection and Firefighting (Official Gazette of the Federation of BiH, No. 64/09).
4. Regulation on the Organization and Regulation of the Gas Industry Sector (Official Gazette of the Federation of BiH, No. 83/07).
5. Rulebook on Adoption and Application of Technical Regulations in the Field of Design, Construction, Commissioning, Operation, and Maintenance of Natural Gas Plants and Installations (Official Gazette of the Federation of BiH, No. 83/08).
6. Regulation on Natural Gas Supply in Canton Sarajevo (Official Gazette of Canton Sarajevo, No. 22/16).
7. Rulebook on Conditions for Uninterrupted and Safe Distribution of Natural Gas through Distribution Gas Systems up to 16 bar Pressure (Official Gazette of Canton Sarajevo, No. 40/17).
8. Risk Assessment of Natural and Other Disasters, KJKP Sarajevogas d.o.o. Sarajevo, 2023.
9. Fire Risk Assessment, KJKP Sarajevogas d.o.o. Sarajevo, 2023.
10. Protection Plan for People and Material Goods from Natural and Other Disasters, KJKP Sarajevogas d.o.o. Sarajevo, 2023.
11. Fire Protection Plan, KJKP Sarajevogas d.o.o. Sarajevo, 2023.

SLUŽBE SIGURNOSTI BOSNE I HERCEGOVINE

DOI: *10.70329/2744-2403.2025.5.9.3*

Stručni rad

Nemanja Doder, mr [1]

Sažetak:

Ovaj rad analizira institucionalni okvir službi sigurnosti u Bosni i Hercegovini, s posebnim osvrtom na njihove nadležnosti, strukturu i međusobnu koordinaciju. Fokus je stavljen na ključne aktere sigurnosnog sistema, uključujući Ministarstvo sigurnosti Bosne i Hercegovine, Obavještajno–sigurnosnu agenciju (OSA), Državnu agenciju za istrage i zaštitu (SIPA), Graničnu policiju i Direkciju za koordinaciju policijskih tijela (DKPT). Rad se osvrće i na pravne osnove djelovanja navedenih institucija, njihovu ulogu u zaštiti ustavnog poretka, borbi protiv terorizma i organizovanog kriminala, te provođenju međunarodnih obaveza. Analizom domaće legislative i dostupne literature, uključujući i radove objavljene u časopisu „Zaštita i sigurnost", identifikovani su glavni izazovi u funkcionisanju sigurnosnog sektora, kao što su nedovoljna koordinacija, politički uticaji i potreba za reformom institucionalnih kapaciteta. Poseban akcenat stavljen je na značaj međunarodne saradnje i integraciju sa evropskim sigurnosnim standardima. Cilj rada je da pruži pregled postojećeg stanja i doprinese boljem razumijevanju sigurnosne arhitekture Bosne i Hercegovine u savremenom kontekstu.

Ključne riječi: *službe sigurnosti, obavještajna djelatnost, koordinacija policijskih tijela, SIPA*

[1] Nemanja Doder, mr, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije. E-mail: doderrnemanja@gmail.com

1. UVOD

Sigurnost predstavlja temeljnu funkciju svake savremene države. Bez adekvatnog nivoa sigurnosti nije moguće govoriti o demokratskoj vladavini, vladavini prava, niti o stabilnosti društva u cjelini. Kao društvena potreba i normativni cilj, sigurnost je jedan od ključnih preduslova za funkcionisanje i egzistenciju zajednice (Masleša, 2007).

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. U kontekstu Bosne i Hercegovine, sistem sigurnosnih službi je posebno složen zbog unutrašnje strukture države, slojevitog nadležnog okvira i djelimično preklapajućih funkcija između različitih institucija.

Ovaj rad analizira pravni i institucionalni okvir službi sigurnosti Bosne i Hercegovine, uključujući njihove funkcije, nadležnosti, operativne zadatke i međusobnu saradnju. Poseban akcenat stavlja se na ulogu Državme agencije za istrage i zaštitu (SIPA), Obavještajno-sigurnosne agencije (OSA), Direkcije za koordinaciju policijskih tijela BiH (DKPT) i drugih relevantnih aktera. Takođe, razmatra se istorijski razvoj sigurnosnih službi u BiH, kao i njihova saradnja sa regionalnim i međunarodnim partnerima.

Analiza obuhvata ključne izazove u radu sigurnosnog sektora, uključujući nedovoljnu koordinaciju, političke uticaje i tehničke kapacitete, uz korištenje relevantne domaće i međunarodne literature. Kao važan doprinos u kontekstu aktuelnih prijetnji, koristi se i rad Lakića, Kovačevića i Kovačevića (2023), koji ukazuje na kompleksnost borbe protiv terorizma i potrebu za unapređenjem institucionalne saradnje.

2. MINISTARSTVO SIGURNOSTI BOSNE I HERCEGOVINE

Ministarstvo sigurnosti Bosne i Hercegovine predstavlja centralno tijelo državne uprave nadležno za unutrašnju sigurnost, saradnju u oblasti provođenja zakona, zaštitu granica, azil, civilnu zaštitu i druga sigurnosna pitanja. Osnovano je Zakonom o Vijeću ministara Bosne i Hercegovine, koji je stupio na snagu u decembru 2002. godine.[2]

U okviru svojih nadležnosti, Ministarstvo sigurnosti BiH obavlja sljedeće funkcije:

- zaštita međunarodnih granica i regulisanje prometa na graničnim prijelazima;

[2] Zakon o Vijeću ministara Bosne i Hercegovine, Službeni glasnik BiH, broj 30/03

- međunarodna saradnja u oblastima sigurnosti, uključujući saradnju s organizacijama poput INTERPOL-a, EUROPOL-a, SELEC i MARRI;
- zaštita lica i objekata od značaja za državu;
- sprječavanje i otkrivanje izvršilaca krivičnih djela kao što su terorizam, trgovina drogom, krivotvorenje valuta i trgovina ljudima;
- koordinacija aktivnosti entitetskih ministarstava unutrašnjih poslova i policije Brčko distrikta;
- prikupljanje i razmjena sigurnosno značajnih podataka;
- sprovođenje međunarodnih obaveza i koordinacija u oblasti civilne zaštite, uključujući planove reagovanja na prirodne i druge nesreće;
- upravljanje politikom useljavanja, azila i nadzor nad kretanjem i boravkom stranaca;
- podrška policijskim tijelima i stručno usavršavanje kadrova;
- forenzička ispitivanja i vještačenja.

Upravne organizacije koje djeluju u sastavu Ministarstva sigurnosti su: Direkcija za koordinaciju policijskih tijela BiH, Granična policija BiH, Državna agencija za istrage i zaštitu (SIPA), Agencija za forenzička ispitivanja i vještačenja, Agencija za školovanje i stručno usavršavanje kadrova, Agencija za policijsku podršku i Služba za poslove sa strancima.

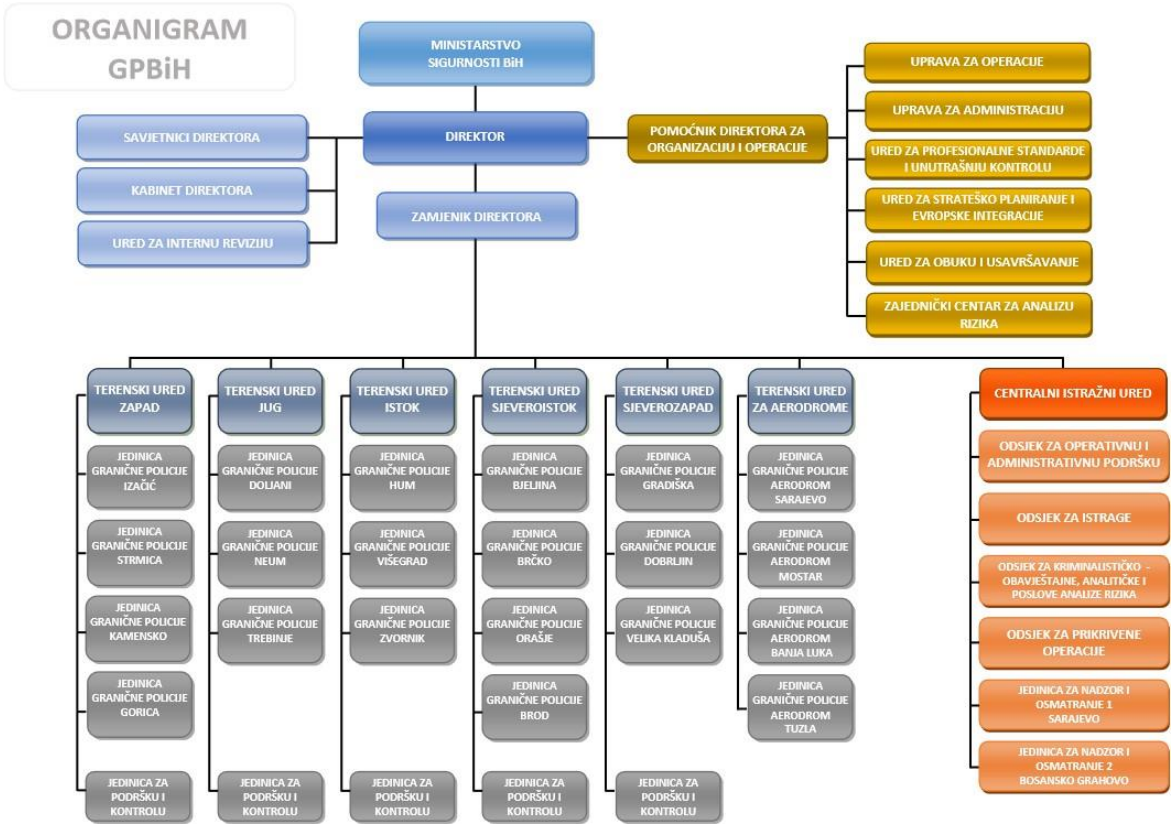
3. GRANIČNA POLICIJA BOSNE I HERCEGOVINE

Granična policija Bosne i Hercegovine predstavlja prvu multietničku policijsku agenciju formiranu na državnom nivou. Riječ je o upravnoj organizaciji u sastavu Ministarstva sigurnosti Bosne i Hercegovine, koja djeluje sa operativnom samostalnošću, a zadužena je za nadzor i kontrolu prelaska državne granice, kao i za druge poslove utvrđene zakonom.

Policija je uspostavljena na osnovu **Zakona o Državnoj graničnoj službi Bosne i Hercegovine**, koji je 13. januara 2000. godine donio visoki predstavnik u BiH. [3] Granična policija je otpočela sa operativnim radom formiranjem prve jedinice na Aerodromu Sarajevo, nakon čega je uslijedio etapni proces preuzimanja nadležnosti nad državnom granicom od entitetskih i kantonalnih ministarstava unutrašnjih poslova. Taj proces je završen krajem 2002. godine.

Danas Granična policija BiH ima ključnu ulogu u očuvanju sigurnosti državne granice, sprječavanju ilegalnih migracija, prekograničnog kriminala i trgovine ljudima, te učestvuje u međunarodnim operacijama i programima saradnje sa srodnim institucijama u regionu i šire.

[3] Zakon o Državnoj Graničnoj službi Bosne i Hercegovine, Službeni glasnik BiH, broj: broj 19/00.



Slika 1: Organizaciona struktura Granične policije Bosne i Hercegovine

4. OBAVJEŠTAJNO – SIGURNOSNA AGENCIJA BOSNE I HERCEGOVINE

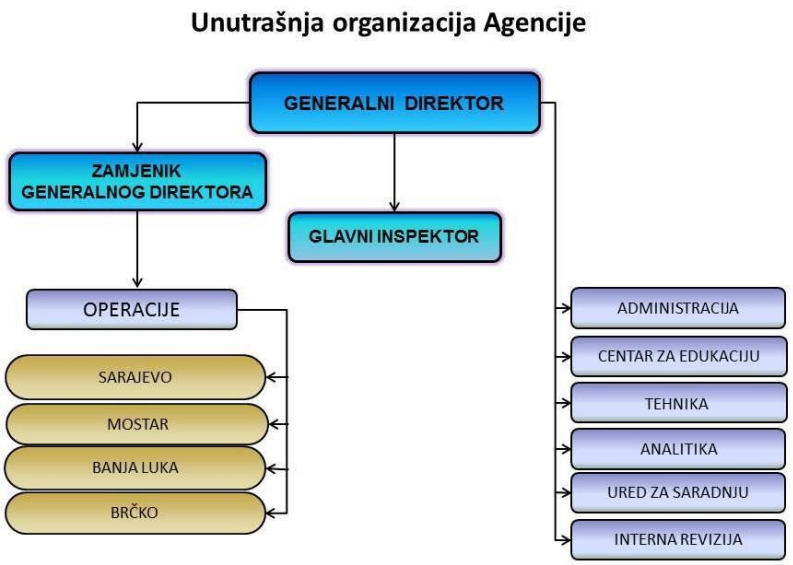
Obavještajno–sigurnosna agencija Bosne i Hercegovine (OSA BiH) predstavlja centralnu instituciju za obavještajnu djelatnost na državnom nivou. Sjedište agencije nalazi se u Sarajevu, a njene aktivnosti su usmjerene na zaštitu nacionalne sigurnosti, suvereniteta, teritorijalnog integriteta i ustavnog poretka Bosne i Hercegovine. OSA BiH je osnovana donošenjem **Zakona o Obavještajno–sigurnosnoj agenciji Bosne i Hercegovine** na sjednici Parlamentarne skupštine BiH 2004. godine.[4] Prema zakonskim odredbama, Agencija je odgovorna za prikupljanje, obradu, analizu i distribuciju obavještajnih podataka koji su od značaja za bezbjednost države i njenih građana. Njena

[4] Zakon o Obavještajno – sigurnosnoj agenciji Bosne i Hercegovine, Službeni glasnik BiH, broj 12/04

nadležnost obuhvata obavještajno djelovanje u vezi sa terorizmom, špijunažom, organizovanim kriminalom i drugim prijetnjama po ustavni poredak i sigurnost BiH.

Agencija djeluje nezavisno u operativnim poslovima, ali je njen rad podložan parlamentarnom nadzoru i ocjeni zakonitosti. Poseban akcenat se stavlja na usklađivanje sa međunarodnim standardima u oblasti zaštite ljudskih prava, obrade podataka i razmjene informacija s partnerskim službama. U sastav Agencije ušle su civilne obavještajno – sigurnosne institucije koje su ranije djelovale u entitetima – u Federaciji Bosne i Hercegovine i u RS-u. Zakonom je određeno da se na teritoriji Bosne i Hercegovine ne mogu osnivati ni djelovati nikakve druge civilne obavještajno – sigurnosne strukture. Finansijska sredstva za rad Agencije u cjelini se osiguravaju iz državnog budžeta, u skladu sa zakonom koji reguliše Trezor institucija Bosne i Hercegovine. [5]

Posebna pažnja posvećuje se usklađivanju obavještajnog rada sa međunarodnim normama zaštite ljudskih prava**,** zaštite privatnosti i zakonite obrade podataka. U tom smislu, rad Agencije je usmjeren na očuvanje ravnoteže između zaštite nacionalne sigurnosti i poštovanja osnovnih prava i sloboda građana.



Slika 2: Unutrašnja organizacija Agencije

[5] Preuzeto sa stranice www.osa-oba.gov.ba, (30.04.2025.)

5. DRŽAVNA AGENCIJA ZA ISTRAGE I ZAŠTITU – SIPA

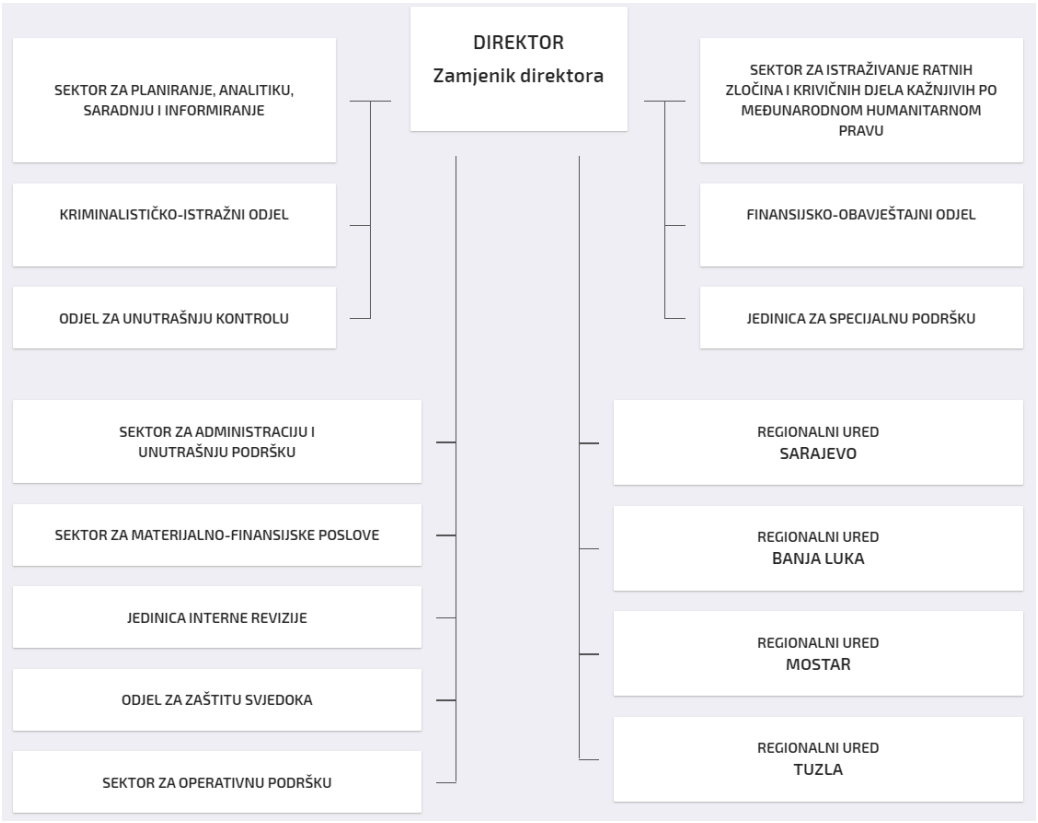
Državna agencija za istrage i zaštitu (SIPA) predstavlja jednu od ključnih agencija za provođenje zakona u Bosni i Hercegovini. Osnovana je usvajanjem **Zakona o Agenciji za informacije i zaštitu**, kao samostalna državna institucija nadležna za prikupljanje i obradu podataka od značaja za provođenje zakona, zaštitu ličnosti i objekata institucija Bosne i Hercegovine, te diplomatskih misija. [6]

U kasnijoj fazi razvoja, SIPA je transformisana u agenciju sa punim policijskim ovlaštenjima i operativnom samostalnošću. Njena nadležnost obuhvata teritoriju cijele Bosne i Hercegovine, čime je postala prva policijska agencija sa državnim kapacitetima u borbi protiv najtežih oblika kriminala.
Ključni zadaci SIPA-e uključuju:

- sprječavanje, otkrivanje i istraživanje krivičnih djela iz nadležnosti Suda Bosne i Hercegovine,
- fizičku i tehničku zaštitu štićenih osoba i objekata od državnog značaja,
- zaštitu svjedoka koji su ugroženi ili izloženi ozbiljnoj prijetnji,
- provođenje finansijskih istraga i otkrivanje pranja novca,
- borbu protiv terorizma, organizovanog kriminala i trgovine ljudima.[7]

SIPA takođe ima značajnu ulogu u saradnji s međunarodnim partnerima poput EUROPOL-a i INTERPOL-a, kao i u operacijama podržanim od strane EUBAM-a i drugih institucija Evropske unije. Kroz svoju strukturu organizacionih jedinica i specijalizovanih timova, Agencija doprinosi sigurnosnoj stabilnosti države i jačanju vladavine prava.

[6] Zakon o Agenciji za informacije i zaštitu, Službeni glasnik BiH, broj 27/04.
[7] Preuzeto sa www.sipa.gov.ba, (27.04.2025.)



Slika 3: Organizaciona struktura Državne agencije za istrage i zaštitu – SIPA

6. DIREKCIJA ZA KOORDINACIJU POLICIJSKIH TIJELA BiH (DKPT)

Direkcija za koordinaciju policijskih tijela Bosne i Hercegovine (DKPT) predstavlja upravnu organizaciju u sastavu Ministarstva sigurnosti Bosne i Hercegovine, osnovanu radi koordinacije aktivnosti policijskih tijela na državnom i nižim nivoima vlasti. Njena uloga ogleda se u jačanju efikasnosti, komunikacije i operativne povezanosti između entitetskih i kantonalnih policijskih struktura, kao i institucija Brčko distrikta.

Osnovne nadležnosti Direkcije obuhvataju:

- koordinaciju operativnog djelovanja državnih policijskih agencija
- praćenje i usklađivanje provođenja zakonskih i podzakonskih akata u oblasti sigurnosti,
- saradnju sa međunarodnim i regionalnim policijskim tijelima,
- zaštitu objekata institucija Bosne i Hercegovine i diplomatsko-konzularnih predstavništava,

- organizaciju i sprovođenje zajedničkih operacija policijskih agencija.

DKPT ima i nadležnost u oblasti logističke podrške policijskim tijelima, uključujući zajedničke planove obuka i unapređenja kapaciteta, kao i u razmjeni operativnih podataka i statistike. Posebno se ističe funkcija Direkcije u slučajevima vanrednih situacija i kriznog upravljanja, kada postaje centralna tačka za koordinaciju odgovora na sigurnosne prijetnje.

Iako su kapaciteti DKPT-a još uvijek predmet razvoja, ova institucija predstavlja važan instrument u uspostavljanju funkcionalnog i depolitizovanog sistema sigurnosti na nivou Bosne i Hercegovine, posebno u kontekstu kompleksne institucionalne strukture zemlje (Lakić, Kovačević i Kovačević, 2023).

7. ZAKLJUČAK

Navedene službe sigurnosti Bosne i Hercegovine itekako doprinose u stvaranju bolje i učinkovitije sigurnosti među građanima naše države. Svojom profesionalnošću, tehničkim i ljudskim resursima itekako se svrstavaju među vodeće službe u regionu, međutim konstantan pritisak od strane medija, ali i politički uticaj, ne dozvoljavaju im da u punom kapacitetu odgovore na sve izazove i zadatke koji se postave ispred njih. Službe sigurnosti Bosne i Hercegovine ostvaruju saradnju sa svim međunarodnim sigurnosnim službama, s ciljem suzbijanja kriminala koji je itekako prisutan na ovom području, naročito na Balkanu. Također službe sigurnosti ostvaruju međusobnu saradnju na području cijele države, te na taj način podižu stepen nacionalne sigurnosti na veći nivo. Stabilna sigurnost je garant vladavine prava u jednoj državi, stoga sve službe trebaju dati svoj maksimum da se isti osigura na pravi način. Postojanje jednog naroda i njegova egzistencija na određenom prostoru ne bi bila moguća bez kvalitetno pružene sigurnosti koju osiguravaju razne agencije za provedbu zakona, pa samim time ovo postaje potreba tog naroda, a ne samo formalno prisutna stvar.

Posebno bi se država trebala pozabaviti problemom u vezi sa finansiranjem navedenih institucija, što je posljednih godina itekako usporeno i ograničeno, jer opremajući svoju policiju, vojsku, službe sigurnosti itd., stvaramo bolji ugled među ostalim državama. Također konstantno podmlađivanje kadra navedenih institucija, ali i doškolovanje ostalih članova kroz razne seminare, radionice, obuke itd., doprinosi jačanju navedenih kapaciteta i ispunjavanju svakodnevnih zadataka.

8. LITERATURA

- Masleša, R. (2007). Teorije i sistemi sigurnosti. Univerzitet u Sarajevu, Fakultet kriminalističkih nauka;

- Lakić, Z., Kovačević, Z. i Kovačević, I., 2023. Terorizam – bezbjednosna prijetnja Zapadnom Balkanu. Zaštita i sigurnost, godina 4, broj 2, str. 191–211.

- Zakon o Vijeću ministara Bosne i Hercegovine, *Službeni glasnik BiH*, broj 30/03;

- Zakon o Obavještajno – sigurnosnoj agenciji Bosne i Hercegovine, *Službeni glasnik BiH*, broj 12/04;

- Zakon o Državnoj Graničnoj službi Bosne i Hercegovine, *Službeni glasnik BiH,* 19/00;

- Zakon o Agenciji za informacije i zaštitu, *Službeni glasnik BiH*, broj 27/04;

- Direkcija za koordinaciju policijskih tijela BiH, dostupno na: www.dkpt.gov.ba (28.11.2024.)

-Granična policija BiH (2025). *Organizaciona struktura*, dostupno na: www.granpol.gov.ba (Pristupljeno: 30.04.2025).

- Državna agencija za istrage i zaštitu – SIPA, dostupno na: www.sipa.gov.ba (Pristupljeno: 27.04.2025).

- Obavještajno-sigurnosna agencija BiH – OSA, dostupno na: www.osa-oba.gov.ba (Pristupljeno: 30.04.2025).

SECURITY AGENCIES OF BOSNIA AND HERZEGOVINA

DOI: *10.70329/2744-2403.2025.5.9.3*

Professional article

Nemanja Doder, MA

Abstract:

This paper analyzes the institutional framework of security services in Bosnia and Herzegovina, with a particular focus on their competencies, structure, and mutual coordination. Emphasis is placed on the key actors of the security system, including the Ministry of Security of Bosnia and Herzegovina, the Intelligence-Security Agency (OSA), the State Investigation and Protection Agency (SIPA), the Border Police, and the Directorate for Coordination of Police Bodies (DKPT). The paper also examines the legal basis for the operations of these institutions, their role in protecting the constitutional order, combating terrorism and organized crime, and fulfilling international obligations. Through an analysis of domestic legislation and available literature, including articles published in the journal "Zaštita i sigurnost" (Protection and Security), the main challenges in the functioning of the security sector have been identified, such as insufficient coordination, political influence, and the need for institutional capacity reform. Special attention is given to the importance of international cooperation and integration with European security standards. The aim of the paper is to provide an overview of the current situation and contribute to a better understanding of the security architecture of Bosnia and Herzegovina in the modern context.

Keywords: *security agencies, intelligence activities, coordination of police bodies, SIPA*

1. INTRODUCTION

Security represents a fundamental function of every modern state. Without an adequate level of security, it is impossible to speak of democratic governance, the rule of law, or the overall stability of society. As a social necessity and normative objective, security is one of the key prerequisites for the functioning and survival of any community (Masleša, 2007).

Security agencies play an essential role in preserving the constitutional order, protecting citizens, and combating contemporary threats, including terrorism, organized crime, and other forms of threats to public safety. In the context of Bosnia and Herzegovina, the system of security services is particularly complex due to the internal structure of the state, multilayered jurisdictional frameworks, and partially overlapping functions among various institutions.

This paper analyzes the legal and institutional framework of the security services of Bosnia and Herzegovina, including their functions, competences, operational tasks, and inter-agency cooperation. Special emphasis is placed on the role of the State Investigation and Protection Agency (SIPA), the Intelligence and Security Agency (OSA), the Directorate for Coordination of Police Bodies of BiH (DKPT), and other relevant actors. The paper also considers the historical development of security services in BiH, as well as their cooperation with regional and international partners.

The analysis includes the key challenges faced by the security sector, such as insufficient coordination, political influence, and limited technical capacities, based on relevant domestic and international literature. As a significant contribution in the context of current threats, the work of Lakić, Kovačević, and Kovačević (2023) is also utilized, highlighting the complexity of the fight against terrorism and the need to improve institutional cooperation.

2. MINISTRY OF SECURITY OF BOSNIA AND HERZEGOVINA

The Ministry of Security of Bosnia and Herzegovina is the central government body responsible for internal security, law enforcement cooperation, border protection, asylum, civil protection, and other security-related matters. It was established by the Law on the Council of Ministers of Bosnia and Herzegovina, which entered into force in December 2002.[8]

[8] **Law on the Council of Ministers of Bosnia and Herzegovina**, Official Gazette of BiH, No. 30/03.

Within its scope of authority, the Ministry of Security of BiH performs the following functions:

- Protection of international borders and regulation of traffic at border crossings;
- International cooperation in security matters, including collaboration with organizations such as INTERPOL, EUROPOL, SELEC, and MARRI;
- Protection of persons and facilities of importance to the state;
- Prevention and detection of perpetrators of criminal offenses such as terrorism, drug trafficking, counterfeiting of currency, and human trafficking;
- Coordination of activities of the entity ministries of interior and the police of the Brčko District;
- Collection and exchange of security-relevant information;
- Implementation of international obligations and coordination in the field of civil protection, including disaster response planning;
- Management of immigration policy, asylum, and oversight of the movement and stay of foreigners;
- Support for police bodies and professional training of personnel;
- Forensic examinations and expert analyses.

The administrative bodies operating under the Ministry of Security include:
the Directorate for Coordination of Police Bodies of BiH, the Border Police of BiH, the State Investigation and Protection Agency (SIPA), the Agency for Forensic Examinations and Expert Analyses, the Agency for Education and Professional Training of Personnel, the Agency for Police Support, and the Service for Foreigners' Affairs.

3. BORDER POLICE OF BOSNIA AND HERZEGOVINA

The Border Police of Bosnia and Herzegovina is the first multi-ethnic police agency established at the state level. It is an administrative body within the Ministry of Security of Bosnia and Herzegovina, operating with operational independence, and is responsible for the supervision and control of the state border crossing, as well as other duties defined by law. The agency was established based on the Law on the State Border Service of Bosnia and Herzegovina, enacted by the High Representative in BiH on January 13, 2000.[9]

[9] **Law on the State Border Service of Bosnia and Herzegovina,** Official Gazette of BiH, No. 19/00.

The Border Police began its operational work by forming its first unit at Sarajevo International Airport, after which a phased process of taking over jurisdiction over the state border from the entity and cantonal ministries of interior followed. This process was completed by the end of 2002.

Today, the Border Police of BiH plays a key role in maintaining the security of the state border, preventing illegal migration, cross-border crime, and human trafficking, and participates in international operations and cooperation programs with related institutions in the region and beyond.

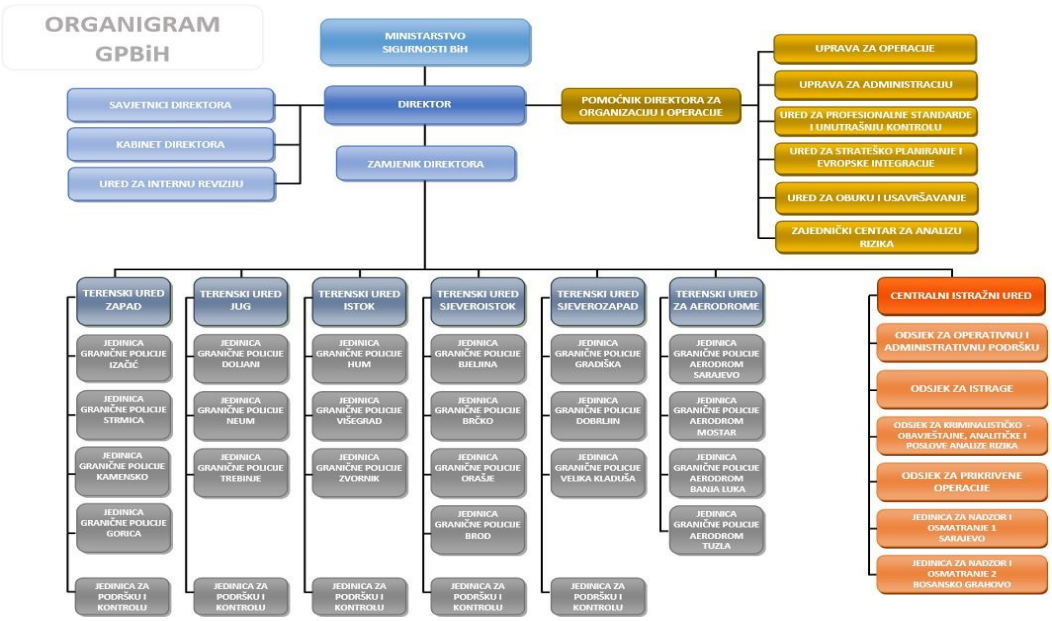


Figure 1: Organizational structure of the Border Police of Bosnia and Herzegovina

4. INTELLIGENCE AND SECURITY AGENCY OF BOSNIA AND HERZEGOVINA

The Intelligence and Security Agency of Bosnia and Herzegovina (OSA BiH) is the central institution for intelligence operations at the state level. The agency is headquartered in Sarajevo, and its activities are focused on protecting national security, sovereignty, territorial integrity, and the constitutional order of

Bosnia and Herzegovina. OSA BiH was established by the adoption of the Law on the Intelligence and Security Agency of Bosnia and Herzegovina, passed by the Parliamentary Assembly of BiH in 2004.[10]

According to the legal provisions, the Agency is responsible for collecting, processing, analyzing, and distributing intelligence data relevant to the security of the state and its citizens. Its jurisdiction includes intelligence activities related to terrorism, espionage, organized crime, and other threats to the constitutional order and security of BiH.

The Agency operates independently in its operational tasks but is subject to parliamentary oversight and legality assessment. Special emphasis is placed on alignment with international standards in the field of human rights protection, data processing, andinformation exchange with partner services. The Agency incorporated the previously existing civil intelligence and security institutions from the entities—the Federation of Bosnia and Herzegovina and Republika Srpska. The law stipulates that no other civil intelligence and security structures may be established or operate within the territory of Bosnia and Herzegovina.[11]

The Agency's financial resources are fully provided from the state budget, in accordance with the law governing the Treasury of the institutions of Bosnia and Herzegovina. Particular attention is given to harmonizing intelligence work with international norms for the protection of human rights, privacy, and the lawful processing of data. In this regard, the Agency's work is focused on maintaining a balance between protecting national security and respecting the fundamental rights and freedoms of citizens.

[10] **Law on the Intelligence and Security Agency of Bosnia and Herzegovina**, Official Gazette of BiH, No. 12/04.

[11] Retrieved from www.osa-oba.gov.ba (30 April 2025).

Figure 2: Internal Organization of the Agency

5. STATE INVESTIGATION AND PROTECTION AGENCY – SIPA

The State Investigation and Protection Agency (SIPA) is one of the key law enforcement agencies in Bosnia and Herzegovina. It was established with the adoption of the Law on the Agency for Information and Protection, as an independent state institution responsible for collecting and processing data relevant to law enforcement, the protection of persons and facilities of Bosnian institutions, as well as diplomatic missions.[12]

In its later development, SIPA was transformed into an agency with full police powers and operational independence. Its jurisdiction covers the entire territory of Bosnia and Herzegovina, making it the first police agency with national-level capacity to combat the most serious forms of crime.

SIPA's core tasks include:

- Preventing, detecting, and investigating criminal offenses under the jurisdiction of the Court of Bosnia and Herzegovina;
- Providing physical and technical protection of protected persons and state-level facilities;

[12] **Law on the Agency for Information and Protection,** Official Gazette of BiH, No. 27/04.

- Protecting witnesses who are endangered or exposed to serious threats;
- Conducting financial investigations and detecting money laundering;
- Combating terrorism, organized crime, and human trafficking.[13]

SIPA also plays a significant role in cooperation with international partners such as EUROPOL and INTERPOL, as well as in operations supported by EUBAM and other European Union institutions. Through its organizational units and specialized teams, the Agency contributes to the security and stability of the state and to strenghening the rule of law.

Figure 3: Organizational structure of SIPA

[13] Retrieved from www.sipa.gov.ba (27 April 2025).

6. DIRECTORATE FOR COORDINATION OF POLICE BODIES OF BOSNIA AND HERZEGOVINA (DKPT)

The Directorate for Coordination of Police Bodies of Bosnia and Herzegovina (DKPT) is an administrative organization within the Ministry of Security of Bosnia and Herzegovina, established to coordinate the activities of police bodies at the state and lower levels of government. Its role lies in enhancing efficiency, communication, and operational connectivity between the police structures of the entities, cantons, and the Brčko District.

The main responsibilities of the Directorate include:

- Coordinating the operational activities of state-level police agencies;
- Monitoring and harmonizing the implementation of legal and sub-legal acts in the field of security;
- Cooperating with international and regional police bodies;
- Protecting institutions of Bosnia and Herzegovina and diplomatic-consular missions;
- Organizing and conducting joint operations of police agencies.

DKPT is also responsible for providing logistical support to police bodies, including joint training plans, capacity building, and the exchange of operational data and statistics. The Directorate plays a particularly important role in emergency situations and crisis management, where it becomes the central coordination point in responding to security threats. Although the capacities of the DKPT are still in development, this institution represents an important mechanism for establishing a functional and depoliticized security system at the national level, especially in the context of the country's complex institutional structure (Lakić, Kovačević & Kovačević, 2023).

7. CONCLUSION

The aforementioned security services of Bosnia and Herzegovina significantly contribute to establishing better and more effective security for the citizens of our country. Through their professionalism, technical, and human resources, they are ranked among the leading services in the region. However, constant pressure from the media and political influence prevents them from fully responding to all the challenges and tasks placed before them.

The security agencies of Bosnia and Herzegovina maintain cooperation with all international security services, with the aim of combating crime, which is

especially prevalent in this region, particularly in the Balkans. Furthermore, the agencies cooperate with each other throughout the entire country, thereby raising the level of national security.

Stable security is a guarantee of the rule of law in any country; therefore, all agencies must give their maximum effort to ensure it in the right way. The existence of a nation and its survival in a certain territory would not be possible without the quality security provided by various law enforcement agencies. Thus, this becomes a necessity of the people, not merely a formal matter.

The state should especially address the issue of financing these institutions, which in recent years has been significantly slowed down and limited. By properly equipping its police, military, and security services, a country builds a better reputation among other states. Additionally, constant rejuvenation of personnel and further education of existing members through various seminars, workshops, and trainings contributes to strengthening institutional capacity and the successful fulfillment of daily task.

8. REFERENCES

- Lakić, Z., Kovačević, Z. and Kovačević, I. (2023). *Terrorism – A Security Threat to the Western Balkans*. *Zaštita i sigurnost*, 4(2), pp. 191–211.
- Masleša, R. (2007). *Theories and Systems of Security*. Sarajevo: University of Sarajevo, Faculty of Criminalistics.
- Law on the Council of Ministers of Bosnia and Herzegovina, *Official Gazette of BiH*, No. 30/03.
- Law on the Intelligence and Security Agency of Bosnia and Herzegovina, *Official Gazette of BiH*, No. 12/04.
- Law on the State Border Service of Bosnia and Herzegovina, *Official Gazette of BiH*, No. 19/00.
- Law on the Agency for Information and Protection, *Official Gazette of BiH*, No. 27/04.
- Directorate for Coordination of Police Bodies of BiH. Available at: https://www.dkpt.gov.ba (Accessed: 28 November 2024).
- Border Police of BiH (2025). *Organizational Structure*. Available at: https://www.granpol.gov.ba (Accessed: 30 April 2025).
- State Investigation and Protection Agency – SIPA. Available at: https://www.sipa.gov.ba (Accessed: 27 April 2025).
- Intelligence and Security Agency of BiH – OSA. Available at: https://www.osa-oba.gov.ba (Accessed: 30 April 2025).

SUPERHEROJI U STRIPOVIMA KAO SREDSTVO ZA SPRJEČAVANJE MALOLJETNIČKE DELINKVENCIJE: PRILAGOĐAVANJE ZAPADNIH PRAKSI BALKANSKOM KONTEKSTU

DOI: *10.70329/2744-2403.2025.5.9.4*

Stručni rad

Haris Memija, doktorant FPN UNSA

Sažetak:

Ovaj rad istražuje potencijal stripova o superherojima kao alata za sprječavanje maloljetničke delinkvencije, posebno na Balkanu. U svijetu oblikovanom tehnologijom i složenim etičkim pitanjima, novi načini rješavanja društvenih problema su neophodni. Oslanjajući se na bazu zapadnih praksi, ova studija sugerira da dobro izrađeni stripovi o superherojima mogu promovirati pozitivne vrijednosti, poboljšati pismenost i baviti se osjetljivim temama na način koji se povezuje s mladim ljudima. Naglašava važnost razumijevanja specifičnih izazova i kulture Balkana, uključujući njegovu ekonomsku situaciju, etničke tenzije i historiju sukoba. Rad se zalaže za saradnju s lokalnim umjetnicima, edukatorima i liderima zajednice kako bi se osiguralo da su stripovi relevantni i učinkoviti. Priznavanjem zabrinutosti zbog prevelikog pojednostavljenja i nenamjernih posljedica, te promoviranjem medijske pismenosti i promišljenog pripovijedanja, ovaj pristup se može odgovorno koristiti za ohrabriranje mladih ljudi i poticanje pozitivnih promjena.

Ključne riječi: *superheroji, strip, maloljetnička delikvencija, medijska pismenost*

1. Uvod

Porast maloljetničke delinkvencije predstavlja stalan izazov za društva širom svijeta, zahtijevajući inovativne i efikasne strategije prevencije. Na Balkanu, gdje socioekonomski faktori i nerazvijene demokratske institucije mogu pogoršati problem, potreba za novim pristupima je posebno izražena. Kako tehnologija prožima društvo u svim aspektima, pristup rješavanju problema delinkvencije treba biti inovativan i moderan. Čuljević je 2024. godine u svom radu "Maloljetničko prekršajno pravo u Bosni i Hercegovini – razvoj prekršajnog prava i analiza pravnog okvira " (Čuljević, 2024) navela da je maloljetnička delinkvencija društveni fenomen koji karakterizira društveno neprihvatljivo ponašanje maloljetnika i da uključuje ne samo krivična djela već i druge oblike poremećaja u ponašanju, tj. takozvana rizična ponašanja maloljetnika.

Stripovi superheroja, popularan i vizualno privlačan medij, imaju značajan potencijal da odjeknu kod mladih ljudi na Balkanu. Ovi stripovi, koji su osvojili društvo u savremenom dobu (Hening and Rusdiarti, 2020), nude jedinstvenu priliku za promociju pozitivnih vrijednosti, prosocijalnog ponašanja i vještina kritičkog mišljenja na način koji tradicionalne obrazovne metode možda ne mogu postići. Stripovi o superherojima mogu pokrenuti diskusiju i kritičko razmišljanje (Mitchell and George, 1996).

Ovaj pregledni članak tvrdi da stripovi o superherojima, crpeći inspiraciju iz iskustava i praksi sa Zapada, mogu poslužiti kao efikasno obrazovno sredstvo za prevenciju maloljetničke delinkvencije na Balkanu. Predstavljajući uspješne zapadne programe i inicijative, ovaj rad ima za cilj da pruži okvir za prilagođavanje i implementaciju akcija zasnovanih na stripovima u balkanskom kontekstu, uzimajući u obzir kulturne osjetljivosti i lokalne izazove. To će se postići definiranjem stripova kao medija, razumijevanjem psihološke privlačnosti superheroja, pregledom specifičnih primjera stripova na Zapadu i potencijalnih izazova usvajanja ovih praksi u balkanskom kontekstu. Krajnji cilj je pokazati kako stripovi o superherojima mogu doprinijeti izgradnji sigurnijeg i bezbjednijeg okruženja za mlade ljude u regiji, osnažujući ih da postanu odgovorni i angažirani građani.

2. Teorijski okvir

Da bismo razumjeli kako stripovi o superherojima mogu efikasno doprinijeti prevenciji maloljetničke delinkvencije, ključno je uspostaviti teorijski okvir. Ovaj

odjeljak će definirati strip kao medij, istražiti moć vizuelne pismenosti u tumačenju stripova i istražiti psihološku privlačnost superheroja.

Definiranje stripova kao medija

Stripovi su specifična vrsta jezika, vizuelni jezik, a mogu se smatrati i jedinstvenim oblikom komunikacije (Cerić 2013; Cohn 2003; Munitić 2006). Kao što Duncan i Smith sugeriraju, stripovi se mogu smatrati medijem masovne komunikacije, olakšavajući posredovanu interakciju između komunikatora i široke publike (Duncan i Smith, 2009). Da bismo u potpunosti shvatili potencijal ovog medija, korisno je pozvati se na Scott McCloudovo fundamentalno djelo "Understanding Comics: The Invisible Art" (Baetens i Frey, 2014), koje pruža sveobuhvatno istraživanje strukture i jezika stripova. McCloudov rad objašnjava kako stripovi koriste sekvencijalne slike, uparene s tekstom, kako bi prenijeli narative i ideje na jedinstven i zanimljiv način. Ovo preplitanje riječi i slika omogućava stripovima da prenesu višedimenzionalnost stvarnog života (Cerić, 2013; Cohn, 2003; Darnhofer, 2018).

Moć vizulne pismenosti

Stripovi zahtijevaju specifičan oblik pismenosti: vizualnu pismenost. To obuhvata sposobnost identificiranja veza između ikoničnih simbola i slika, procjene njihovog značaja, sinteze informacija koje prenose i kritičkog bavljenja njihovim značenjem (Cerić i Rašidagić, 2019). Vizualna pismenost je duboko isprepletena s konvencionalnom pismenošću (Cerić, 2013). Stoga, bavljenje stripovima o superherojima može poboljšati vještine vizualne pismenosti, koje su sve važnije u današnjem svijetu vođenom vizualnim svijetom (Cerić, 2013).

Psihološka privlačnost

Narativi o superherojima dotiču se temeljnih ljudskih želja i motivacija. Žanr superheroja jedinstven je po svom oslanjanju na zajednički narativni univerzum s kontinuitetom (Chambliss, 2012). Superheroji nude kulturno sredstvo za premošćivanje jaza između male grupe s kojom su se ljudska bića morala nositi i mnogo veće grupe koju podrazumijevaju moderni društveni aranžmani (Carney et al., 2014). Stripovi o superherojima mogu pokrenuti diskusiju i kritičko razmišljanje (Mitchell i George, 1996). Oni čitateljima pružaju uzore, nudeći inspiraciju i primjer inspirativne vrline (Pizarro i Baumeister, 2013). Priče često istražuju teme moralnog osnaživanja, pravde i prevladavanja nedaća, što duboko rezonira s mladom publikom koja se možda suočava s vlastitim izazovima (Fradkin et al., 2016).

3. Zapadne prakse: Stripovi o superherojima kao preventivno sredstvo

Na Zapadu su stripovi o superherojima prepoznati po svom potencijalu kao obrazovni alati, posebno u rješavanju pitanja relevantnih za mlade ljude. Ovaj dio će istražiti specifične primjere kako su stripovi korišteni u zapadnim kontekstima za promociju pozitivnih vrijednosti, poboljšanje pismenosti i sprječavanje rizičnih ponašanja, s fokusom na inicijative koje bi se mogle prilagoditi balkanskom kontekstu.

Promocija vrijednosti i prosocijalnog ponašanja

Stripovi o superherojima korišteni su za pokretanje diskusije i kritičkog mišljenja (Mitchell and George, 1996). Taj pristup je ponudio kulturno sredstvo za premošćivanje jaza između male grupe ljudi koji su razvili metod da se nose s problemom i mnogo veće veličine grupe koju podrazumijevaju i moderna društvena uređenja (Carney et al., 2014).

Poboljšanje pismenosti i obrazovanja

Osim promocije vrijednosti, stripovi su također pronašli mjesto u obrazovnim okruženjima za poboljšanje vještina pismenosti. Zanimljiva priroda stripa može motivirati nevoljne čitatelje i pružiti most prema tradicionalnijim oblicima književnosti (Cerić i Cerić, 2020). Upotreba stripa u obrazovanju usklađena je s naporima za promociju vizualne pismenosti. Po samoj svojoj prirodi, stripovi zahtijevaju specifičan oblik pismenosti (Cerić, 2013).

Rješavanje osjetljivih pitanja i promoviranje zdravih odluka

Stripovi su se pokazali kao vrijedan alat za rješavanje osjetljivih pitanja i promoviranje zdravog donošenja odluka među mladima. Na primjer, "The Native Comic Book Project" (Montgomery et al., 2012) pokazuje kako stripovi mogu biti odlično sredstvo za dosezanje i angažiranje mladih i promoviranje zdravih odluka (Montgomery et al., 2012).

Naučene lekcije i prilagodljive strategije

Ispitivanjem ovih zapadnih praksi postaje jasno da stripovi o superherojima nude fleksibilnu i zanimljivu platformu za rješavanje niza pitanja relevantnih za prevenciju maloljetničke delinkvencije. Ključ leži u prilagođavanju ovih strategija specifičnom kulturnom kontekstu Balkana, osiguravajući da sadržaj

odražava lokalne vrijednosti i da se bavi jedinstvenim izazovima s kojima se suočavaju mladi ljudi u regiji.

4. Prilagođavanje zapadnih praksi balkanskom kontekstu

Iako gore navedene zapadne prakse nude vrijedne uvide, njihovo direktno prenošenje na balkanski kontekst bilo bi neefikasno. Ovaj odjeljak će se baviti važnošću kulturne osjetljivosti, potrebom prilagođavanja sadržaja lokalnim izazovima i potencijalom za saradnju s lokalnim umjetnicima i edukatorima kako bi se osigurao uspjeh intervencija zasnovanih na stripovima na Balkanu.

Kulturna osjetljivost i lokalizacija

Balkanska regija ima bogato i raznoliko kulturno nasljeđe, s jedinstvenim vrijednostima, tradicijama i društvenim normama. Ključno je izbjegavati nametanje zapadnih ideala ili narativa koji u tom slučaju možda neće imati odjeka kod lokalne publike. Svaka akcija zasnovana na stripovima mora biti pažljivo prilagođena kako bi odražavala specifičan kulturni kontekst Balkana. Stripovi mogu navesti čitatelje da razmišljaju i analiziraju kulturne razlike (Fedotova et al., 2015). To uključuje razmatranje faktora kao što su:

Jezik: Osiguravanje da su stripovi prevedeni na lokalne jezike i dijalekte, koristeći kulturno prikladan jezik i izraze. U tom kontekstu, podsjetimo se na jedan uspješan primjer. U Jugoslaviji se 70-ih godina pojavio popularni strip „Alan Ford“ koji je zahvaljujući sjajnim prijevodom Nenada Brixyja postigao veću popularnost čak i od originalnog italijanskog tržišta.
Vrijednosti: Prilagođavanje narativa kako bi se uskladili s lokalnim vrijednostima i uvjerenjima, uz istovremeno promoviranje pozitivnih vrijednosti i prosocijalnog ponašanja.
Predstavljanje: Prikazivanje likova i okruženja koja odražavaju raznolikost balkanske regije, promovirajući inkluzivnost i razumljivo kulturološko predstavljanje.

Rješavanje lokalnih izazova

Izazovi s kojima se suočavaju mladi ljudi na Balkanu mogu se razlikovati od onih na Zapadu. Bitno je prilagoditi sadržaj stripa kako bi se riješili specifični lokalni problemi, kao što su:

Socioekonomski faktori: Rješavanje problema vezanih za siromaštvo, nezaposlenost i nedostatak prilika.

Etničke tenzije: Promocija tolerancije, razumijevanja i pomirenja između različitih etničkih grupa.
Korupcija i nedostatak povjerenja u institucije: Podsticanje građanskog angažmana, transparentnosti i odgovornosti.
Trauma i postkonfliktna pitanja: Pružanje podrške i resursa mladima pogođenim ratom i raseljavanjem.

Saradnja s lokalnim učesnicima

Da bi se osigurao uspjeh akcija zasnovanih na stripovima na Balkanu, neophodno je uključiti lokalne učesnike u proces razvoja i implementacije. To podrazumijeva:

Lokalni umjetnici i pisci: Saradnja s lokalnim umjetnicima i piscima stripova kako bi se stvorio kulturno relevantan i zanimljiv sadržaj.
Obrazovni sektor i omladinski radnici: Partnerstvo s edukatorima i omladinskim radnicima radi integracije stripova u obrazovne programe i inicijative u zajednici.
Lokalna vlast i organizacije zajednice: Angažovanje lidera i organizacija zajednice radi izgradnje podrške za projekat i osiguranja njegove održivosti. Usvajanje pametnih tehnologija i inovativnih pristupa u urbanim sredinama ima potencijal da značajno poboljša rezultate smanjenja rizika od katastrofa i izgradi otporne gradove (Garaplija i Prguda, 2023).

Davanjem prioriteta kulturnoj osjetljivosti, rješavanjem lokalnih izazova i podsticanjem saradnje s lokalnim zainteresovanim stranama, moguće je prilagoditi zapadne prakse i stvoriti efikasne akcije zasnovane na stripovima koje doprinose prevenciji maloljetničke delinkvencije u balkanskom kontekstu. Vrijedi napomenuti da sami stripovi nisu ideološki neutralan fenomen (Karadjov, 2022), što je još jedan razlog da se osigura prilagođavanje poruka. I podsjećamo na krucijalnu vrijednost stripa; stripovi se mogu koristiti za pokretanje diskusije i kritičkog mišljenja (Mitchell and George, 1996).

I za kraj ovog dijela rada, ponudit ćemo moguća rješenja putem pet konkretnih primjera kako bi se zapadne prakse mogle prilagoditi balkanskom kontekstu, nadograđujući se na prethodne tvrdnje:

Strip kao prevencija sigurnosnih izazova
Analizirajući događaje iz novije historije, možemo doći do zaključka da su različitim sigurnosnim izazovima prethodile društveno-političke krize kao svojevrsni inkubatori za razvoj osnovnih elemenata koji svojim individualnim ili sinergijskim djelovanjem mogu izazvati različite sigurnosne posljedice (Garaplija i Korajlić, 2023). Smještajući „krizu“ u početak dramaturškog zapleta i

detektujući „elemente“ kao „loše momke“ mogao bi biti osnov za kreiranje stripova, te na bazi navedene fabule dalje razvijati scenarije. Širenjem konteksta se rješavaju konflikti, te bi u tom smislu strip mogao odigrati ulogu preventivnog sredstva u sprječavanju sigurnosnih izazova.

Rješavanje traume i postkonfliktnih problema
U regiji obilježenoj prošlim sukobima, stripovi o superherojima mogu se koristiti za rješavanje traume i promoviranje pomirenja. Na primjer, priče bi mogle prikazivati likove koji su iskusili rat ili raseljavanje, pokazujući otpornost ljudi i ujedno nudeći poruke nade. Ovim pristupom stripovi mogu promovirati bolje razumijevanje različitih kultura (Fedotova et al., 2015) i to bi se razlikovalo od pasivnosti Zapadne Evrope prema događajima u bivšoj Jugoslaviji (Lowe, 2022).

Promoviranje tolerancije i razumijevanja
Stripovi se mogu koristiti za osporavanje stereotipa i promoviranje razumijevanja između različitih etničkih i vjerskih grupa na Balkanu. Priče bi mogle prikazivati likove iz različitih sredina koji rade zajedno na prevladavanju zajedničkih izazova, ističući važnost empatije i saradnje. Balkan je plodno tlo za primjenu ovog primjera, jer svi balkanski narodi gaje isti običaj o važnosti dobrosusjedskih i prisnih odnosa.

Rješavanje socioekonomskih problema
S obzirom na ekonomske izazove u dijelovima Balkana, stripovi bi se mogli baviti pitanjima poput siromaštva, nezaposlenosti i korupcije. Priče bi mogle prikazivati likove koji pronalaze kreativna rješenja za ekonomske probleme, ističući važnost poduzetništva, obrazovanja i građanskog angažmana.

Promoviranje građanskog aktivizma i demokratije
Stripovi se mogu koristiti za poticanje mladih ljudi da učestvuju u demokratskim procesima i da njihovi lideri postanu odgovorniji. Priče bi mogle sadržavati likove koji se bore protiv korupcije i nepravde, inspirirajući čitatelje da postanu aktivni i angažirani građani.

5. Rješavanje potencijalnih izazova i kritika

Iako upotreba stripova o superherojima kao preventivnog alata nudi značajan potencijal, ključno je prepoznati i riješiti potencijalne izazove i kritike. Ovaj odjeljak će istražiti zabrinutost vezanu za preveliko pojednostavljenje, kulturnu prikladnost i potencijal za neželjene posljedice, nudeći strategije za ublažavanje ovih rizika.

Preveliko pojednostavljenje i nijansiranje

Jedna uobičajena kritika stripova je da mogu previše pojednostaviti složena pitanja, svodeći ih na pojednostavljene narative o dobru protiv zla. Da bismo to izbjegli, ključno je:

Razviti nijansirane narative: Priče trebaju istraživati složenost maloljetničke delinkvencije, izbjegavajući pojednostavljena objašnjenja i stereotipe.
Promovirati kritičko mišljenje: Stripovi se mogu koristiti za pokretanje diskusije i kritičkog mišljenja (Mitchell and George, 1996). Uvesti prilike za čitatelje da razmišljaju o pitanjima pokrenutim u stripovima i uključe se u kritički dijalog.
Izbjegavati didaktizam: Umjesto da predstavljaju propisana rješenja, stripovi trebaju poticati čitatelje da istraže različite perspektive i razviju vlastita informirana mišljenja.

Kulturna prikladnost i predstavljanje

Kao što smo ranije spomenuli, kulturna osjetljivost je od najveće važnosti. Da bi se osiguralo da stripovi odjeknu kod lokalne publike i izbjegla kulturna neosjetljivost, bitno je:

Uključiti lokalne aktere: Sarađivati s lokalnim umjetnicima, piscima, edukatorima i liderima lokalne vlasti i zajednice kako bi se osiguralo da su stripovi kulturno prikladni i relevantni.
Promovirati raznolika predstavljanja: Predstavljati likove i priče koji odražavaju raznolikost balkanske regije, izbjegavajući stereotipe i promovirajući inkluzivnost.
Rješavati lokalna pitanja: Prilagoditi sadržaj stripa kako bi se riješili specifični lokalni izazovi i problemi.

Nenamjerne posljedice i strategije ublažavanja

Postoji rizik od promoviranja fetišizma robe i seksističkih, rasističkih i fašističkih "vrijednosti" u stripovima (Karadjov, 2022). Da bi se to ublažilo, važno je:

Promovirati medijsku pismenost: Naučiti mlade ljude kako kritički analizirati medijske poruke i identificirati potencijalne predrasude ili štetne stereotipe. Korištenje stripova kao alata za medijsku pismenost može pomoći u prevladavanju kulturnih ili jezičkih barijera i njegovati kritičko razmišljanje, kreativnost i empatiju (Tsene, 2022).
Pružiti kontekst i smjernice: Dopuniti stripove edukativnim materijalima i diskusijama kako bi se čitateljima pružio kontekst i smjernice.

Procijeniti uticaj i prilagoditi se: Redovno procjenjivati uticaj akcija zasnovanih na stripovima i prilagođavati ih na osnovu povratnih informacija čitatelja i zainteresiranih strana.

Rizik od "zaglupljivanja"

Postoji zabrinutost da bi se korištenje stripova moglo smatrati "zaglupljivanjem" važnih pitanja. Da bismo se pozabavili ovim, trebalo bi:

Naglasiti sofisticiranost medija: Istaknuti jedinstvene narativne i umjetničke mogućnosti stripa (Pedri, 2015).
Promovirati vizuelnu pismenost: Demonstrirati kako stripovi mogu poboljšati vizuelnu i medijsku pismenost (Cerić, 2013).
Koristiti stripove kao ulaz: Koristiti stripove kako bismo potaknuli interes za složenije teme, potičući čitatelje da dalje istražuju ova pitanja kroz druge medije.
Istaknuti izuzetnu umjetnost: Neki stripovi su se uzdigli do priznate i cijenjene umjetničke forme (Cerić, 2013; 2019; 2020).

Priznavanjem i rješavanjem ovih potencijalnih izazova i kritika, moguće je iskoristiti moć stripova o superherojima kao preventivnog alata, a istovremeno smanjiti rizike od neželjenih posljedica.

6. Zaključak

U eri koju definiraju brzi tehnološki napredak i složeni globalni izazovi, potreba za inovativnim i angažirajućim pristupima prevenciji maloljetničke delinkvencije hitnija je nego ikad. Kako tehnologija nastavlja prožimati svaki aspekt ljudskog postojanja, pitanja koja se tiču njenih etičkih implikacija, društvenog utjecaja i potencijalnih rizika zauzela su centralno mjesto. Ovo istraživanje tvrdi da stripovi o superherojima, kada se promišljeno prilagode i implementiraju, mogu poslužiti kao vrijedan alat u ovom nastojanju, posebno u kontekstu Balkana. Ovim radom provociramo stručno-naučnu javnost da razvija inovativne pristupe teorijskom određenju i definisanju stripa kao preventivnog alata protiv sve rastuće maloljetničke delikvencije.

Crpeći zapadne prakse i prilagođavajući ih specifičnim kulturnim nijansama i izazovima regije, stripovi mogu promovirati pozitivne vrijednosti, poboljšati pismenost i baviti se osjetljivim pitanjima na način koji odjekuje kod mladih ljudi. "The Native Comic Book Project" (Montgomery et al., 2012) i druge inicijative pokazuju potencijal stripova da angažiraju mlade i promoviraju zdrave odluke

(Montgomery et al., 2012). Stripovi mogu potaknuti čitatelje na razmišljanje, promišljanje i analizu kulturnih razlika (Fedotova et al., 2015).

Međutim, ključno je priznati i odgovoriti na potencijalne kritike vezane za preveliko pojednostavljenje, kulturnu prikladnost i nenamjerne posljedice. Razvojem nijansiranih narativa, promoviranjem raznolikog predstavljanja i njegovanjem medijske pismenosti (Tsene, 2022), ovi rizici se mogu ublažiti.

U konačnici, uspjeh akcija zasnovanih na stripovima ovisi o saradnji s lokalnim umjetnicima, edukatorima i liderima zajednice, osiguravajući da je sadržaj kulturno relevantan, zanimljiv i utjecajan. Kao što koristan tekst (What Superheroes Should Today's Tech Inspire?, 2012) sugerira, fikcija može stvoriti stvarnost, a iskorištavanjem moći pripovijedanja možemo inspirirati pozitivne promjene i ohrabriti mlade ljude da postanu aktivni i odgovorni građani. Zaključno, prihvatanjem kreativnosti, kulturne osjetljivosti i posvećenosti rješavanju lokalnih izazova, stripovi o superherojima mogu doprinijeti svjetlijoj budućnosti mladih ljudi na Balkanu i šire.

Literatura

1. Baetens, J., Frey, H., 2014. The graphic novel: an introduction. Cambridge: University Press

2. Carney, J., Dunbar, R., Machin, A., Dávid-Barrett, T., & Júnior, M.S., 2014. Social Psychology and the Comic-Book Superhero: A Darwinian Approach. Philosophy and Literature 38(1), A195-A215. https://dx.doi.org/10.1353/phl.2014.0019.
3. Cerić, H., 2013. Skandalon u oblačićima; kako koristiti strip u nastavi. Sarajevo: Dobra knjiga
4. Cerić, H., 2019. O edukativnom potencijalu stripa: prilozi etabliranju stripov-ne metode u nastavi. Sarajevo: Perfecta
5. Cerić, H., Cerić E., 2020. Strip kao medij filozofske poruke: stripozofski pristup nastavi filozofije. Sarajevo: Druga Gimnazija
6. Cerić, H., Rašidagić. E.K., 2019. Strip i karikatura u nastavi politologije. Sarajevo: Časopis za obrazovanje odraslih i kulturu Obrazovanje odraslih, godina 19, broj 2. str. 39-54.
7. Chambliss, J.C., 2012. Superhero Comics: Artifacts of the U.S. Experience. Juniata Voices. Sequential SmArt: A Conference on Teaching with Comics, May 19, 2012.
8. Christina, L., Ismaniati, C., 2019. Comics to Learn Characters of Care and Responsibility in Children. Proceedings of the 3rd International Conference on Current Issues in Education (ICCIE 2018). Atlantis Press. DOI: 10.2991/iccie-18.2019.55
9. Cohn, N., 2003. Early Writings on Visual Language. Carlsbad, CA: Emaki Production
10. Čuljević, I., 2024. Maloljetničko prekršajno pravo u Bosni i Hercegovini – razvoj prekršajnog prava i analiza pravnog okvira. Zaštita i sigurnost, godina 4., broj 1. str. 29-58.
11. Darnhofer, I., 2018. Using Comic-Style Posters for Engaging Participants and for Promoting Researcher Reflexivity. International Journal of Qualitative Methods, 17(1). https://doi.org/10.1177/1609406918804716
12. Duncan, R., Smith, M., 2009. The Power of Comics: History, Form & Culture. New York • London: Continuum
13. Fedotova O., Kotliarenko, I., Latun, V., 2015. Comics Projects of the International Cultural and Educational Organizations in Youth Forums Devoted to Anti-Terrorism's Issues. Procedia - Social and Behavioral Sciences, Volume 186, Pages 192-196. https://doi.org/10.1016/j.sbspro.2015.04.038.

14. Fradkin C., Weschenfelder, G.V., Yunes, M.A.M., 2016. Shared adversities of children and comic superheroes as resources for promoting resilience: Comic superheroes are an untapped resource for empowering vulnerable children. Child Abuse & Neglect, Vol. 51, 407-415. https://doi.org/10.1016/j.chiabu.2015.10.010.
15. Garaplija, E,. Prguda, S., 2023. Pametni gradovi za smanjenje rizika od katastrofa: korištenje tehnologije i inovacija za otporno urbano okruzenje. Zaštita i sigurnost, godina 3, broj 2. str. 70-92.
16. Garaplija, E., Korajlić, N., 2022. Društveno-političke krize kao inkubatori suvremenih sigurnosnih izazova i prijetnji po nacionalnu sigurnost - studija slučaja "Bosna i Hercegovina". XV. Međunarodna znanstveno-stručna konferencija: Dani kriznog upravljanja. Zbornik radova, str. 174-182.
17. Hening, I. and Rusdiarti S., 2020. Villain Figure's Ambivalence in the Comic Gundala: Destiny. Jurnal Lingua Idea, 11(2), 127-138.
18. Karadjov, B., 2022. The portrayal of the neighbour and the neighbour-hood in Macedonian graphic literature and comic book culture. Slavia Meridionalis, 22, Article 2674. https://doi .org /10.116 49/sm.2674
19. Lowe, P. 2022. Photography, Bearing Witness and the Yugoslav Wars, 1988–2021: Testimonies of Light. London • New York: Routledge
20. McCloud, S., 1993. Understanding Comics: The Invisible Art. New York: HarperCollins Publishers
21. Memija, H., 2015. Fotografija – ratni i postratni svjedok: značaj dokumentarne fotografije. Sarajevo: Časopis za odgoj i obrazovanje Novi muallim, godina 16. broj 62. str. 48-57.
22. Mitchell, J. P., and George, J. D. 1996. What do Superman, Captain America, and Spiderman have in Common? The Case for Comics Books. Gifted Education International, 11(2), 91-94.
23. Montgomery, M., Manuelito, B., Nass, C., Chock, T., Buchwald, D., 2012. The Native Comic Book Project: Native Youth Making Comics and Healthy Decisions. Journal of Cancer Education, 27 (Suppl 1), 41–46. https://doi.org/10.1007/s13187-012-0311-x
24. Munitić, R., 2006. Deveta umetnost, strip. Beograd: Mont Image i Fakultet primenjenih umetnosti
25. Pedri, N., 2015. Thinking about Photography in Comics. Image & Narrative, 16(2), 1–13. Retrieved from https://www.imageandnarrative.be/index.php/imagenarrative/article/view /802
26. Tsene, L., 2022. Using Comics as a Media Literacy Tool for Marginalised Groups: The Case of Athens Comics Library. Media and Communication. Vol 10, No 4 (2022): Inclusive Media Literacy Education for Diverse Societies. https://doi.org/10.17645/mac.v10i4.5716

27. What Superheroes Should Today's Tech Inspire?, 2012. Devian Art 25. Pristupljeno 16. maja, 2025. (https://www.deviantart.com/techgnotic/journal/What-Superheroes-Should-Today-s-Tech-Inspire-298464237)

SUPERHEROES IN COMICS AS A MEANS OF PREVENTING JUVENILE DELINQUENCY: ADAPTING WESTERN PRACTICES FOR THE BALKAN CONTEXT

DOI: *10.70329/2744-2403.2025.5.9.4*

Professional article

Haris Memija, doktorant FPN UNSA

Abstract:

This paper explores the potential of superhero comics as a tool for preventing juvenile delinquency, particularly in the Balkans. In a world shaped by technology and complex ethical questions, new ways to address social issues are essential. This study suggests that well-crafted superhero comics can promote positive values, improve literacy, and tackle sensitive subjects in a way that connects with young people. It emphasizes the importance of understanding the specific challenges and culture of the Balkans, including its economic situation, ethnic tensions, and history of conflict. The paper argues for collaboration with local artists, educators, and community leaders to ensure the comics are relevant and effective. By acknowledging concerns about oversimplification and unintended consequences, and by promoting media literacy and thoughtful storytelling, this approach can be used responsibly to empower young people and encourage positive change.

Keywords*: superheroes, comics, juvenile delinquency, media literacy*

1. Introduction

The rise of juvenile delinquency presents a persistent challenge to societies worldwide, demanding innovative and effective prevention strategies. In the Balkans, where socioeconomic factors and underdeveloped democratic institutions can exacerbate the problem, the need for fresh approaches is particularly acute. As technology permeates society, the approach to solving delinquency issues should be innovative and modern. In 2024, Čuljević stated in her paper "Juvenile Misdemeanor Law in Bosnia and Herzegovina - Development of Misdemeanor Law and Analysis of the Legal Framework" (Čuljević, 2024), that juvenile delinquency is a social phenomenon characterized by socially unacceptable behaviors of minors and that it includes not only criminal offenses but also other forms of behavioral disorders, i.e., so-called risky behaviors of minors.

Superhero comics, a popular and visually engaging medium, hold significant potential to resonate with young people in the Balkans. These comics, which have captivated society in the contemporary era (Hening and Rusdiarti, 2020), offer a unique opportunity to promote positive values, prosocial behavior, and critical thinking skills in a way that traditional educational methods may not achieve. Superhero comics may initiate discussion and critical thinking (Mitchell and George, 1996).

This review article argues that superhero comics, drawing on experiences and practices from the West, can serve as an effective educational tool for preventing juvenile delinquency in the Balkans. By showcasing successful Western programs and initiatives, this paper aims to provide a framework for adapting and implementing comics-based interventions in the Balkan context, taking into account cultural sensitivities and local challenges. This will be done by defining comics as a medium, understanding the psychological appeal of superheroes, reviewing specific examples of comics in the West and the potential challenges of adopting these practices to the Balkan context. Ultimately, the goal is to demonstrate how superhero comics can contribute to building a safer and more secure environment for young people in the region, empowering them to become responsible and engaged citizens.

2. The Theoretical Framework

To understand how superhero comics can effectively contribute to juvenile delinquency prevention, it's crucial to establish a theoretical framework. This

section will define comics as a medium, explore the power of visual literacy in interpreting comics, and delve into the psychological appeal of superheroes.

Defining Comics as a Medium

Comics are a specific type of language, a visual language, and they can also be considered a unique form of communication (Cerić 2013; Cohn 2003; Munitić 2006). As Duncan and Smith suggest, comics can be seen as a medium of mass communication, facilitating mediated interaction between communicators and a broad audience (Duncan and Smith, 2009). To fully appreciate this medium's potential, it's helpful to refer to Scott McCloud's seminal work, "Understanding Comics" (Baetens and Frey, 2014), which provides a comprehensive exploration of the structure and language of comics. McCloud's work illuminates how comics use sequential images, coupled with text, to convey narratives and ideas in a unique and engaging manner. This intermingling of words and images allows comics to convey the multidimensionality of real life (Cerić 2013; Cohn 2003; Darnhofer, 2018).

The Power of Visual Literacy

Comics require a specific form of literacy: visual literacy. This encompasses the ability to identify connections between iconic symbols and images, assess their significance, synthesize the information they convey, and critically engage with their meaning (Cerić and Rašidagić, 2019). Visual literacy is deeply intertwined with conventional literacy (Cerić, 2013). Engaging with superhero comics can therefore enhance visual literacy skills, which are increasingly important in today's visually driven world (Cerić, 2013).

Psychological Appeal

Superhero narratives tap into fundamental human desires and motivations. The superhero genre is unique in its reliance on a shared narrative universe with continuity (Chambliss, 2012). Superheroes offer a cultural means of negotiating the gap between the small group size that human beings have evolved to deal with, and the much larger group size that is entailed by modern social arrangements (Carney et al., 2014). Superhero comics may initiate discussion and critical thinking (Mitchell and George, 1996). They provide readers with role models, offering inspiration and exemplifying inspirational virtue (Pizarro and Baumeister, 2013). The stories often explore themes of empowerment, justice, and overcoming adversity, which resonate deeply with young audiences who may be facing their own challenges (Fradkin et al., 2015).

3. Western Practices: Superhero Comics as a Preventive Tool

In the West, superhero comics have been recognized for their potential as educational tools, particularly in addressing issues relevant to young people. This section will explore specific examples of how comics have been used in Western contexts to promote positive values, enhance literacy, and prevent risky behaviors, with a focus on initiatives that could be adapted for the Balkan context.

Promoting Values and Prosocial Behavior

Superhero comics have been used to initiate discussion and critical thinking (Mitchell and George, 1996). They offer a cultural means of negotiating the gap between the small group size that human beings have evolved to deal with, and the much larger group size that is entailed by modern social arrangements (Carney et al., 2014).

Enhancing Literacy and Education

Beyond value promotion, comics have also found a place in educational settings to improve literacy skills. The engaging nature of comics can motivate reluctant readers and provide a bridge to more traditional forms of literature (Cerić and Cerić, 2020). The use of comics in education aligns with efforts to promote visual literacy. By their very nature, comics require specific form of literacy (Cerić, 2013).

Addressing Sensitive Issues and Promoting Healthy Decisions

Comics have proven to be a valuable tool for addressing sensitive issues and promoting healthy decision-making among young people. For example, "The Native Comic Book Project" (Montgomery et al., 2012) demonstrates how comic books might be an excellent vehicle to reach and engage youth and promote healthy decisions (Montgomery et al., 2012).

Lessons Learned and Adaptable Strategies

By examining these Western practices, it becomes clear that superhero comics offer a flexible and engaging platform for addressing a range of issues relevant to juvenile delinquency prevention. The key lies in adapting these strategies to the specific cultural context of the Balkans, ensuring that the content resonates with local values and addresses the unique challenges faced by young people in the region.

4. Adapting Western Practices to the Balkan Context

While the Western practices outlined above offer valuable insights, directly transposing them to the Balkan context would be ineffective. This section will address the importance of cultural sensitivity, the need to tailor content to local challenges, and the potential for collaboration with local artists and educators to ensure the success of comics-based interventions in the Balkans.

Cultural Sensitivity and Localization

The Balkan region has a rich and diverse cultural heritage, with unique values, traditions, and social norms. It is crucial to avoid imposing Western ideals or narratives that may not resonate with local audiences. Any comics-based intervention must be carefully adapted to reflect the specific cultural context of the Balkans. The comic books can make the readers reflect and analyze the cultural differences (Fedotova et al., 2015). This includes considering factors such as:

Language: Ensuring that the comics are translated into the local languages and dialects, using culturally appropriate language and expressions. In this context, let's recall a successful example. In the 1970s, the popular comic "Alan Ford" appeared in Yugoslavia, which, thanks to Nenad Brixy's excellent translation, became even more popular than the original Italian market.
Values: Adapting the narratives to align with local values and beliefs, while still promoting positive values and prosocial behavior.
Representation: Featuring characters and settings that reflect the diversity of the Balkan region, promoting inclusivity and representation.

Addressing Local Challenges

The challenges faced by young people in the Balkans may differ from those in the West. It is essential to tailor the content of the comics to address specific local issues, such as:

Socioeconomic factors: Addressing issues related to poverty, unemployment, and lack of opportunity.
Ethnic tensions: Promoting tolerance, understanding, and reconciliation between different ethnic groups.
Corruption and lack of trust in institutions: Encouraging civic engagement, transparency, and accountability.
Trauma and post-conflict issues: Providing support and resources for young people affected by war and displacement.

Collaboration with Local Stakeholders

To ensure the success of comics-based interventions in the Balkans, it is crucial to involve local stakeholders in the development and implementation process. This includes:

Local artists and writers: Collaborating with local comic book artists and writers to create culturally relevant and engaging content.
Educators and youth workers: Partnering with educators and youth workers to integrate comics into educational programs and community initiatives.
Community leaders and organizations: Engaging with community leaders and organizations to build support for the project and ensure its sustainability. The adoption of smart technologies and innovative approaches in urban areas has the potential to significantly improve disaster risk reduction outcomes and build resilient cities (Garaplija and Prguda, 2023).

By prioritizing cultural sensitivity, addressing local challenges, and fostering collaboration with local stakeholders, it is possible to adapt Western practices and create effective comics-based interventions that contribute to juvenile delinquency prevention in the Balkan context. It's worth noting that comics themselves are not an ideologically neutral phenomenon (Karadjov, 2022), which is another reason to make sure the messages are adapted. And we remind you of the crucial value of comics; comics can be used to initiate discussion and critical thinking (Mitchell & George, 1996).

And to conclude this part of the paper, we will offer possible solutions through five concrete examples of how Western practices could be adapted to the Balkan context, building on the previous statements:

Comics as a prevention of security challenges
Analyzing events from recent history, we can come to the conclusion that various security challenges were preceded by socio-political crises as a kind of incubators for the development of basic elements that, through their individual or synergistic action, can cause various security consequences (Garaplija and Korajlić, 2023). Placing the "crisis" at the beginning of the dramaturgical plot and detecting the "elements" as "bad guys" could be the basis for creating comics, and on the basis of the aforementioned plot, further developing scenarios. Conflicts are resolved by expanding the context, and in this sense comics could play the role of a preventive tool in preventing security challenges.

Addressing Trauma and Post-Conflict Issues

In a region marked by past conflicts, superhero comics can be used to address trauma and promote reconciliation. For example, stories could feature characters who have experienced war or displacement, demonstrating resilience and offering messages of hope. These comics can promote better understanding of different cultures (Fedotova et al., 2015). This differs from the passivity of Western Europe toward the events in the former Yugoslavia (Lowe, 2022).

Promoting Tolerance and Understanding
Comics can be used to challenge stereotypes and promote understanding between different ethnic and religious groups in the Balkans. Stories could feature characters from diverse backgrounds working together to overcome common challenges, highlighting the importance of empathy and cooperation. The Balkans are fertile ground for the application of this example, because all Balkan peoples share the same tradition of the importance of good neighborly and close relations.

Addressing Socioeconomic Issues
Given the economic challenges in parts of the Balkans, comics could address issues such as poverty, unemployment, and corruption. Stories could feature characters who find creative solutions to economic problems, highlighting the importance of entrepreneurship, education, and civic engagement.

Promoting Civic Engagement and Democracy
Comics can be used to encourage young people to participate in democratic processes and hold their leaders accountable. Stories could feature characters who stand up against corruption and injustice, inspiring readers to become active and engaged citizens.

5. Addressing Potential Challenges and Criticism

While the use of superhero comics as a preventive tool offers significant potential, it's crucial to acknowledge and address potential challenges and criticisms. This section will explore concerns related to oversimplification, cultural appropriateness, and the potential for unintended consequences, offering strategies to mitigate these risks.

Oversimplification and Nuance

One common critique of comics is that they can oversimplify complex issues, reducing them to simplistic narratives of good versus evil. To avoid this, it's crucial to:

Develop nuanced narratives: Stories should explore the complexities of juvenile delinquency, avoiding simplistic explanations and stereotypes.
Promote critical thinking: Comics can be used to initiate discussion and critical thinking (Mitchell and George, 1996). Include opportunities for readers to reflect on the issues raised in the comics and engage in critical dialogue.
Avoid didacticism: Rather than presenting prescriptive solutions, comics should encourage readers to explore different perspectives and develop their own informed opinions.

Cultural Appropriateness and Representation

As discussed earlier, cultural sensitivity is paramount. To ensure that comics resonate with local audiences and avoid cultural insensitivity, it's essential to:

Involve local stakeholders: Collaborate with local artists, writers, educators, and community leaders to ensure that the comics are culturally appropriate and relevant.
Promote diverse representation: Feature characters and stories that reflect the diversity of the Balkan region, avoiding stereotypes and promoting inclusivity.
Address local issues: Tailor the content of the comics to address specific local challenges and concerns.

Unintended Consequences and Mitigation Strategies

There is a risk of promoting commodity fetishism and sexist, racist, and fascist "values" in comic books (Karadjov, 2022). To mitigate this, it's important to:

Promote media literacy: Teach young people how to critically analyze media messages and identify potential biases or harmful stereotypes. Using comics as a media literacy tool can help overcome cultural or language barriers and cultivate critical thinking, creativity, and empathy (Tsene, 2022).
Provide context and guidance: Supplement the comics with educational materials and discussions to provide context and guidance for readers.
Evaluate impact and adapt: Regularly evaluate the impact of the comics-based interventions and adapt them based on feedback from readers and stakeholders.

The Risk of "Dumbing Down"

There's a concern that using comics might be seen as "dumbing down" important issues. To address this:

Emphasize the sophistication of the medium: Highlight the unique narrative and artistic possibilities of comics (Pedri, 2015).
Promote visual literacy: Demonstrate how comics can enhance visual and media literacy (Cerić, 2013).
Use comics as a gateway: Use comics to spark interest in more complex topics, encouraging readers to explore these issues further through other mediums.
Feature exceptional art: Some comics have risen to a recognized and respected art form (Cerić 2013; 2019; 2020).

By acknowledging and addressing these potential challenges and criticisms, it's possible to harness the power of superhero comics as a preventive tool while minimizing the risks of unintended consequences.

6. Conlusion

In an era defined by rapid technological advancement and complex global challenges, the need for innovative and engaging approaches to juvenile delinquency prevention is more pressing than ever. As technology continues to permeate every facet of human existence, questions surrounding its ethical implications, societal impact, and potential risks have taken center stage. This exploration has argued that superhero comics, when thoughtfully adapted and implemented, can serve as a valuable tool in this endeavor, particularly within the Balkan context. With this work, we provoke the professional and scientific community to develop innovative approaches to the theoretical determination and definition of comics as a preventive tool against the ever-growing juvenile delinquency.

By drawing upon Western practices and tailoring them to the specific cultural nuances and challenges of the region, comics can promote positive values, enhance literacy, and address sensitive issues in a way that resonates with young people. "The Native Comic Book Project" (Montgomery et al., 2012) and other initiatives demonstrate the potential of comics to engage youth and promote healthy decisions (Montgomery et al., 2012). The comic books can make the readers think, reflect, analyze the cultural differences (Fedotova et al., 2015).

However, it is crucial to acknowledge and address potential criticisms related to oversimplification, cultural appropriateness, and unintended consequences. By developing nuanced narratives, promoting diverse representation, and fostering media literacy (Tsene, 2022), these risks can be mitigated.

Ultimately, the success of comics-based interventions hinges on collaboration with local artists, educators, and community leaders, ensuring that the content is culturally relevant, engaging, and impactful. As useful text (What Superheroes Should Today's Tech Inspire?, 2012) suggests, fiction can create reality, and by harnessing the power of storytelling, we can inspire positive change and empower young people to become active and responsible citizens. In conclusion, by embracing creativity, cultural sensitivity, and a commitment to addressing local challenges, superhero comics can contribute to a brighter future for young people in the Balkans and beyond.

Literature

7. Baetens, J., Frey, H., 2014. The graphic novel: an introduction. Cambridge: University Press
8. Carney, J., Dunbar, R., Machin, A., Dávid-Barrett, T., & Júnior, M.S., 2014. Social Psychology and the Comic-Book Superhero: A Darwinian Approach. Philosophy and Literature 38(1), A195-A215. https://dx.doi.org/10.1353/phl.2014.0019.
9. Cerić, H., 2013. Skandalon u oblačićima; kako koristiti strip u nastavi. Sarajevo: Dobra knjiga
10. Cerić, H., 2019. O edukativnom potencijalu stripa: prilozi etabliranju stripov-ne metode u nastavi. Sarajevo: Perfecta
11. Cerić, H., Cerić E., 2020. Strip kao medij filozofske poruke: stripozofski pristup nastavi filozofije. Sarajevo: Druga Gimnazija
12. Cerić, H., Rašidagić. E.K., 2019. Strip i karikatura u nastavi politologije. Sarajevo: Časopis za obrazovanje odraslih i kulturu Obrazovanje odraslih, godina 19, broj 2. str. 39-54.
13. Chambliss, J.C., 2012. Superhero Comics: Artifacts of the U.S. Experience. Juniata Voices. Sequential SmArt: A Conference on Teaching with Comics, May 19, 2012.
14. Christina, L., Ismaniati, C., 2019. Comics to Learn Characters of Care and Responsibility in Children. Proceedings of the 3rd International Conference on Current Issues in Education (ICCIE 2018). Atlantis Press. DOI: 10.2991/iccie-18.2019.55
15. Cohn, N., 2003. Early Writings on Visual Language. Carlsbad, CA: Emaki Production
16. Čuljević, I., 2024. Juvenile Misdemeanor Law in Bosnia and Herzegovina - Development of Misdemeanor Law and Analysis of the Legal Framework. Zaštita i sigurnost, Vol. 4., No. 1. pp. 29-58.
17. Darnhofer, I., 2018. Using Comic-Style Posters for Engaging Participants and for Promoting Researcher Reflexivity. International Journal of Qualitative Methods, 17(1). https://doi.org/10.1177/1609406918804716
18. Duncan, R., Smith, M., 2009. The Power of Comics: History, Form & Culture. New York • London: Continuum
19. Fedotova O., Kotliarenko, I., Latun, V., 2015. Comics Projects of the International Cultural and Educational Organizations in Youth Forums Devoted to Anti-Terrorism's Issues. Procedia - Social and Behavioral Sciences, Volume 186, Pages 192-196. https://doi.org/10.1016/j.sbspro.2015.04.038.
20. Fradkin C., Weschenfelder, G.V., Yunes, M.A.M., 2016. Shared adversities of children and comic superheroes as resources for promoting

resilience: Comic superheroes are an untapped resource for empowering vulnerable children. Child Abuse & Neglect, Vol. 51, 407-415. https://doi.org/10.1016/j.chiabu.2015.10.010.
21. Garaplija, E,. Prguda, S., 2023. Smart Cities for Disaster Risk Reduction: Leveraging Technology and Innovation for a Resilient Urban Environment. Zaštita i sigurnost, Vol. 3, No. 2. pp. 70-92.
22. Garaplija, E., Korajlić, N., 2022. Socio-political Crises as Incubators of Contemporary Security Challenges and Threats to National Security - Case Study "Bosnia and Herzegovina". XV. International Scientific and Professional Conference: Crisis Management Days. Conference Journal 2022, pp. 174-182.
23. Hening, I. and Rusdiarti S., 2020. Villain Figure's Ambivalence in the Comic Gundala: Destiny. Jurnal Lingua Idea, 11(2), 127-138.
24. Karadjov, B., 2022. The portrayal of the neighbour and the neighbour-hood in Macedonian graphic literature and comic book culture. Slavia Meridionalis, 22, Article 2674. https://doi .org /10.116 49/sm.2674
25. Lowe, P. 2022. Photography, Bearing Witness and the Yugoslav Wars, 1988–2021: Testimonies of Light. London • New York: Routledge
26. McCloud, S., 1993. Understanding Comics: The Invisible Art. New York: HarperCollins Publishers
27. Memija, H., 2015. Fotografija – ratni i postratni svjedok: značaj dokumentarne fotografije. Sarajevo: Časopis za odgoj i obrazovanje Novi muallim, godina 16. broj 62. str. 48-57.
28. Mitchell, J. P., and George, J. D. 1996. What do Superman, Captain America, and Spiderman have in Common? The Case for Comics Books. Gifted Education International, 11(2), 91-94.
29. Montgomery, M., Manuelito, B., Nass, C., Chock, T., Buchwald, D., 2012. The Native Comic Book Project: Native Youth Making Comics and Healthy Decisions. Journal of Cancer Education, 27 (Suppl 1), 41–46. https://doi.org/10.1007/s13187-012-0311-x
30. Munitić, R., 2006. Deveta umetnost, strip. Beograd: Mont Image i Fakultet primenjenih umetnosti
31. Pedri, N., 2015. Thinking about Photography in Comics. Image & Narrative, 16(2), 1–13. Retrieved from https://www.imageandnarrative.be/index.php/imagenarrative/article/view /802
32. Tsene, L., 2022. Using Comics as a Media Literacy Tool for Marginalised Groups: The Case of Athens Comics Library. Media and Communication. Vol 10, No 4 (2022): Inclusive Media Literacy Education for Diverse Societies. https://doi.org/10.17645/mac.v10i4.5716
33. What Superheroes Should Today's Tech Inspire?, 2012. Devian Art 25. Pristupljeno 16. maja, 2025.

(https://www.deviantart.com/techgnotic/journal/What-Superheroes-Should-Today-s-Tech-Inspire-298464237)

KRIVIČNOPRAVNI ASPEKT RAZBOJNIŠTVA

DOI: *10.70329/2744-2403.2025.5.9.5*

Pregledni znanstveni članak

Doc. dr. Zoran Kovačević[3]

Stručni savjetnik, Aida Šeta Čavčić[4]

Sažetak:

U ovom radu razmatra se problematika krivičnog djela razbojništava u Bosni i Hercegovini. Ova problematika je veoma kompleksna pa joj je bilo potrebno posvetiti posebnu pažnju, što i jeste jedan od ciljeva ovoga rada. Mi ovdje nastojimo da odnosnu temu razmatramo višedimenzionalno i da damo neke preporuke u oblasti sprečavanja odnosnih delikata. Iako se čini da se, na prvi pogled, radi o jednoj, prije svega, krivičnopravnoj temi, ova tema je prvenstveno kriminalistička i to operativno – taktička i metodička.

Primat rada je na krivičnopravnopravnom aspektu razbojništva, zakonskom okviru razmatranja odnosnog kriminaliteta, gdje se analiziraju odredbe krivičnih zakona i zakona o krivičnim postupcima, koji su u primjeni na prostoru Bosne i Hercegovine.

Ključne riječi*: razbojništvo, krivično djelo, upotreba sile.*

[3] Visoka poslovno tehnička škola Doboj, e-mail: zoran.kovacevic@dkpt.gov.ba

[4] Direkcija za koordinaciju policijskih tijela BiH, e-mail: aida.seta@dkpt.gov.ba

Uvod

Prema zakonskoj inkriminaciji, sadržaj krivičnog djela razbojništva sastoji se u oduzimanju tuđe pokretne stvari upotrebom sile protiv nekog lica ili prijetnjom da će se neposredno napasti na život ili tijelo, u namjeri da se njenim prisvajanjem sebi ili drugom pribavi protivpravna imovinska korist. Teži oblik ovog krivičnog djela će postojati ako je nekom licu umišljajno nanesena teška tjelesna povreda ili je djelo učinjeno od strane više lica ili je upotrijebljeno kakvo oružje ili opasno sredstvo, ili ako vrijednost oduzetih stvari prelazi iznos od 50.000 KM, odnosno još teži oblik akoje neko lice umišljajno lišeno života.[5] Sila ili prijetnja može biti upotrijebljena prema licu, a ne i prema stvarima, pa se i ne mora uvijek raditi o krivičnim djelima razbojništva. Sudska praksa takođe zauzima takvo stanovište, zaključujući da takve slučajeve treba kvalifikovati kao krivično djelo teške krađe izvršeno na drzak način. Neće postojati razbojništvo, već teška krađa u slučaju kada se oduzimanje stvari od oštećenog vrši trganjem iz njegovih ruku, bez ikakvog neposrednog ugrožavanja života ili tijela oštećenog, odnosno upotrebe neke sile protiv njega. Pri izvršenju krivičnog djela razbojništva učinioci upotrebljavaju razna sredstva pogodna za primjenu sile ili prijetnje, što zavisi od objekta napada, profesionalnosti i organizovanosti učinilaca. Najčešća sredstva izvršenja su: vatreno oružje (pištolji, revolveri, razno automatsko oružje), hladno oružje (nož, bodež, sjekira, razna sječiva), minsko eksplozivne naprave i sprejovi za onesposobljavanje. Pod silom se podrazumijeva i primjena omamljujućih sredstava (upotreba spreja) koji služi za onemogućavanje i onesposobljavanje otpora oštećenog. Kod uličnih razbojništava najčeće se koristi fizička snaga koju učinilac primjenjuje prema oštećenom.Oružana razbojništva spadaju u grupu najtežih krivičnih djela, ukoliko je došlo do težih posljedica i predstavljaju visok stepen društvene opasnosti. Učinioci krivičnih djela razbojništva uglavnom vrše prethodne detaljne pripreme na osnovu kojih detaljno planiraju izvođenje kriminalnog napada. Učinioci prikupljaju relevantne podatke koji se odnose na objekat napada, posebno obraćajući pažnju na način obezbjeđenja vrijednosti čijim oduzimanjem i prisvajanjem žele da pribave protivpravnu imovinsku korist. Krivično djelo razbojništva uglavnom vrše muškarci, ali se u posljednje vrijeme i žene pojavljuju kao samostalni učinioci ovih krivičnih djela. Inače, ova krivična djela najčešće vrše lica koja nisu u radnom odnosu, mada ima i suprotnih slučajeva. Izvršenjem krivičnog djela razbojništva učinioci žele da pribave imovinsku korist što veće vrijednosti, pa je logično da napadaju one objekte gdje su smještene takve stvari ili lica koja poseduju stvari takvih vrijednosti. Ostaje isti kriterijum: prisvajanje što veće imovinske vrijednosti.Za

[3] Krivični zakon Republike Srpske, „Sl. glasnik RS“ br. 64/2017, 104/2018 i 31/2025, član 227.

učinioce ovih krivičnih djela interesantni su sljedeći objekti: banke, pošte, mjenjačnice, prodavnice zlatnog nakita i druge vrijedne robe, benzinske stanice, razne agencije, robne kuće, ugostiteljski i turistički objekti, a u novije vrijeme sve više se i stanovi pojavljuju kao objekti napada izvršilaca ovog krivičnog dela. Od fizičkih lica, najčešći objekt napada su: blagajnici, prenosioci novca, poštari, kelneri, taksisti, pijana lica, prodavci robe na pijacama, trgovci na sajmovima i vašarima, homoseksualci.

1. KRIVIČNOPRAVNI ASPEKT RAZBOJNIŠTVA

1.1. Krivični zakon Republike Srpske

1) Ko upotrebom sile protiv nekog lica ili prijetnjom da će neposredno napasti na život ili tijelo oduzme tuđu pokretnu stvar u namjeri da njenim prisvajanjem sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se kaznom zatvora od jedne do deset godina.
2) Ako je pri izvršenju djela iz stava (1) ovog člana nekom licu umišljajno nanesena teška tjelesna povreda ili je djelo izvršeno od strane više lica ili je upotrijebljeno kakvo oružje ili opasno sredstvo ili ako vrijednost oduzetih stvari prelazi iznos od 50.000 KM, učinilac će se kazniti kaznom zatvora od pet do četrnaest godina.
3) Ako je pri izvršenju krivičnog djela iz stava (1) ovog člana neko lice umišljajno lišeno života, učinilac će se kazniti kaznom zatvora najmanje deset godina ili dugotrajnim zatvorom.[6]

1.2. Krivični zakon Federacije Bosne i Hercegovine

1) Tko upotrebom sile protiv neke osobe ili prijetnje da će izravno napasti na njezin život ili tijelo oduzme tuđu pokretninu s ciljem da njenim prisvajanjem pribavi sebi ili drugome protupravnu imovinsku korist ili da je protupravno prisvoji, kaznit će se kaznom zatvora od jedne do deset godina.
2) Ako je kaznenim djelom iz stavke (1) ovog članka neka osoba s namjerom teško tjelesno ozlijeđena, ili je to kazneno dijelo počinjeno u sastavu grupe ljudi, ili ako je upotrebljeno oružje ili opasno oruđe, počinitelj će se kazniti kaznom zatvora najmanje pet godina. Ako je pri počinjenju kaznenog djela iz stavke (1) ovog članka neka osoba s namjerom usmrćena,počinitelj će se kazniti kaznom zatvora najmanje deset godina ili kaznom dugotrajnog zatvora.[7]

[6] Krivični zakon Republike Srpske, „Sl. glasnik RS“ br. 64/2017, 104/2018 i 31/2025, član 227.
[7] Krivični zakon Federacije BiH, „Sl. novine FBiH“, br. 36/2003,21/2004, 69/2004, 18/2005; 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017 i 31/202, član 289.

1.3. Krivični zakon Distrika Brčko

1) Ko upotrebom sile protiv nekog lica ili prijetnjom da će direktno napasti na njegov život ili tijelo Ako je krivičnim djelom iz stava (1) ovog člana neko lice s namjerom teško tjelesno ozlijeđeno ili je to krivično djelo počinjeno u sastavu grupe ljudi ili ako je upotrebljeno oružje ili opasno oruđe, učinilac će se kazniti kaznom zatvora najmanje pet godina.[8]
Ako je pri učinjenju krivičnog djela iz stava (1) ovog člana neko lice s namjerom usmrćeno, učinilac će se kazniti kaznom zatvora najmanje deset godina ili kaznom dugotrajnog zatvora.
Iz sadržaja citiranih inkriminacija proizlazi da razbojništvo spada među krivična djela s elementima nasilja. Po pravnoj konstrukciji ono je složeno krivično djelo. Djelo se sastoji od obilježja krivičnog djela krađe (oduzimanje tuđe pokretne stvari) i upotrebe sile ili prijetnje (ozbiljne), dakle prinude, ne- posrednog napada na život ili tijelo neke osobe od koje se stvar želi oduzeti u namjeri pribavljanja protivpravne imovinske koristi. Riječ je o djelu znatne društvene štetnosti, koje može lako prerasti u krivično djelo nanošenja teške tjelesne povrede ili u lišenje života.Društvenu štetnost razbojništva zakonodavac je izrazio kroz zaprijećenu kaznu.
Sila ili prijetnja (prinuda) javljaju se kod razbojništava kao sredstva kojima se omogućava oduzimanje tuđe pokretne stvari i zato moraju prethoditi oduzimanju tuđe pokretne stvari. Cilj prinude je sprečavanje ili savladavanje otpora kojim bi se nastojalo spriječiti oduzimanje tuđe pokretne stvari. Pri tome sila ne mora prouzrokovati neku posljedicu kod oštećenog. Dovoljno je da je upotrijebljena kao sredstvo za ostvarivanje cilja, tj. oduzimanja tuđe pokretne stvari u namjeri da se njenim prisvajanjem pribavi protivpravna imovinska korist. Ukoliko je djelo izvršeno bez navedene namjere, ne radi se o krivičnom djelu razbojništva.
Pod *silom* kao elementom krivičnog djela razbojništva treba podrazumijevati stvarno nanošenje zla. Riječ je o primjeni snage prema nekoj osobi u namjeri da ta osoba nešto učini ili ne učini. Ta snaga može biti *tjelesna* ili *mehanička.* Silom se smatra i primjena hipnoze ili omamljujućih sredstava.
Prema svom *intenzitetu* sila može biti: *neodoljiva* (apsolutna, vis apsoluta) ili *psihička* (kompulzivna, vis compulsiva). Apsolutna ili materijalna sila postoji u onom slučaju, ako osoba prema kojoj se primjenjuje nije uopšte u mogućnosti da

[8] Krivični zakon Brčko distrikta BiH, „Sl. glasnik Brčko distrikta BiH“ br. 19/2020, 3/2024 i 14/2024, član 283.

donese odluku ili nije u mogućnosti da donesenu odluku realizuje. Sila je psihička ili moralna, ako osoba prema kojoj se primjenjuje može donositi odluke, ali su te odluke iznuđene psihičkom prisilom npr. u situacijama uzimanja talaca i ucjenjivanja njima. Sila za oduzimanje tuđe pokretne stvari ne mora biti znatna. Sila ili prijetnja moraju biti uperene protiv osobe od koje se oduzima pokretna stvar, a ne prema stvari.

Krivično djelo razbojništva postoji i kad žrtva ne vidi oduzimanje svoje pokretne stvari npr. kad je zaključana u nekoj prostoriji ili su joj povezane oči, kad je onesviještena ili omamljena i sl. U navedenim slučajevima bitno je da je odvajanje žrtve od mogućnosti da vidi oduzimanje svoje pokretne stvari rezultat upotrebe sile ili prijetnje od strane učinitelja.

kriminalističkoj i sudskoj praksi su sporni slučajevi kad je učinitelj istrgao ili iščupao predmet žrtvi iz ruke ili s tijela. Sudovi, po pravilu, ovakve slučajeve "otimačine" kvalifikuju kao tešku krađu izvršenu na naročito drzak način. Ukoliko je žrtva pružila otpor, treba ustanoviti njegov oblik i opseg. Ukoliko se slamanjem otpora ugrožava život ili tijelo žrtve, riječ je o razbojništvu. To znači da sila mora biti upravljena prema osobi od koje se želi oduzeti pokretna stvar, a u cilju da se spriječi ili onemogući njen otpor oduzimanju stvari. Ukoliko sila nije upravljena prema osobi u cilju da se spriječi ili onemogući njen otpor oduzimanju stvari, već je upotrijebljena u svrhu da se prekine fizička veza između stvari i njenog držaoca, riječ je o drskoj krađi. Ona je u takvom slučaju sastavni dio radnje oduzimanja stvari, a ne sredstvo da se ta radnja omogući. Takva sila nema karakter one sile koja je element krivičnog djela razbojništva. Otimanje torbe u sredstvima javnog prijevoza ili na ulici koje žrtve drže "ovlaš" prebačene preko ruku ili ramena, ili ih uopšte ne drže, pa čak nemaju ni pod vizuelnim nadzorom, ne smatra se oblikom otpora i ne radi se o krivičom djelu razbojništva. Čak i u slučajevima "natezanja" ili čak "male borbe" u cilju oduzimanja pokretne stvari, bez prinude u smislu napada na život ili tijelo žrtve, ne radi se o razbojništvu. Rečeno vrijedi samo pod pretpostavkom da razbojnik nije, osim sile potrebne da se istrgne pokretna stvar, upotrijebio još i neki drugi dodatni akt nasilja prema držaocu stvari u cilju savladavanja njegovog otpora i oduzimanja pokretne stvari, kad će se raditi o razbojništvu. Ukoliko se sila primjenjuje prema žrtvi, tada ona, kako je istaknuto, predmet ne mora držati, niti se on mora nalaziti na njoj, bitno je da se on nalazi pod kontrolom žrtve, da je u njenom vlasništvu. Pod kontrolom u navedenom smislu treba podrazumijevati pravo ili privilegij upotrebe predmeta na slobodan način od strane žrtve. Što više, u času oduzimanja predmet ne mora biti pod faktičnim vizualnim nadzorom žrtve, ako je ona onesposobljena na jedan od naprijed navedenih načina. (Filipov, A.G., Cemničev, AJ, 2007).

Pod *prijetnjom* treba podrazumijevati stavljanje u izgled nekog zla radi utjecaja na volju onoga kome se prijeti. Od naprijed navedene psihološke sile prijetnja se razlikuje po tome što se kod prve zlo primjenjuje, a kod druge samo stavlja

u izgled. Prijetnja je sredstvo za izvršenje razbojništva. Koji puta se može raditi o kvalifikovanoj prijetnji, tj. prijetnji određenim zlom.
Prijetnja neposrednim napadom na život ili tijelo osobe je usmjerena na sprečavanje ne samo slobode akcije, nego i slobode odlučivanja i kretanja.
Prilikom primjene prijetnje za postojanje razbojništva nije bitan pravni temelj po kome napadnuta osoba drži neki predmet, ali je potrebno da je žrtva prisutna na mjestu izvršenja djela. Zlo koje se stavlja u izgled prijetnjom, dakle određena opasnost, mora biti neposredna i istovremena. Prijetnja mora biti takva da je onaj prema kome je upućena shvaća ozbiljno i da učinitelj to hoće. Pri tome nije odlučujuće da li osoba koja prijeti (učinitelj) tu prijetnju objektivno može ostvariti npr. prijetnja pištoljem plašljivcem, bitno je da žrtva nije svjesna činjenice o kakvom pištolju se radi.Krivično djelo razbojništva postoji i u slučaju kad učinitelj ne oduzme tuđu pokretnu stvar sam, nego i kad oštećeni neposredno pod uticajem sile ili prijetnje preda pokretnu stvar učinitelju.
Prijetnja da će za neku osobu biti iznesen podatak da je npr. homoseksualne orijentacije, pronevjeritelj i sl. ne udovoljava pojmu prijetnje.
Što se tiče vrijednosti oduzete stvari, smatramo da, bez obzira na njenu vrijednost, postoji krivično djelo razbojništva, ako je prinuda izvršena. Stojimo na stanovištu da visina stvarno postignute protivpravne imovinske koristi primjenom sile ili prijetnje nije odlučna za pravnu kvalifikaciju djela. Mora se raditi o nasilnom oduzimanju tuđe pokretne stvari, čijim je prisvajanjem ispunjena namjera pribavljanja protivpravne imovinske koristi. Vrijedi pravilo da se uvijek radi o krivičnom djelu razbojništva, kad je učinitelj silom ili prijetnjom neposrednog napada na život ili tijelo, a u namjeri pribavljanja protivpravne imovinske koristi, žrtvi sam oduzeo pokretnu stvar ili ju je prinudio da mu stvar sama neposredno preda ili da stvar na licu mjesta neposredno napusti. U praksi se slučajevi kad je primijenjena samo prijetnja, bez primjene sile, dakle, kad nema objektivno vidljivih posljedica i kad se ne nađe sredstvo prijetnje, ako je korišteno ili oduzeta pokretna stvar, u načelu, teško dokazuju. U takvim slučajevima vještina istražitelja igra ključnu ulogu. On mora dobro poznavati istražiteljske tehnike (Aleksić, Ž, 1982).
Upotreba sile ili prijetnje mora prethoditi ili se udružiti s oduzimanjem pokretne stvari. Sila primijenjena da se zadrži oduzeta pokretna stvar (tuđa) čini krivično djelo razbojničke krađe. Kod prijetnje upotrebom sile žrtva ne mora biti uplašena do nivoa panike. Dovoljno je da ona shvaća da postoji mogućnost da bude ozlijeđena.
Upotreba sile ili prijetnje varira s obzirom na objektivne i subjektivne okolnosti svakog
konkretnog slučaja, pa čak i kad je riječ o istom učinitelju. Krivično djelo razbojništva je dovršeno oduzimanjem tuđe pokretne stvari. Ukoliko do oduzimanja nije došlo radiće se o pokušaju razbojništva.Prinuda kao obilježje krivičnog djela razbojništva postojaće i onda kad nije upotrijebljena sila ni izričita

prijetnja neposrednog napada na život ili tijelo, ako je samo manifestno ponašanje učinitelja ili njegovih saučesnika takvo da se njime izražava prijetnja neposrednog napada na život ili tijelo. Osoba prema kojoj se primjenjuje sila ili prijetnja može biti i osoba koja je pritekla u pomoć držaocu stvari. U izvršenju krivičnog djela razbojništva često sudjeluje više osoba uz nužnu podjelu rada. U takvim slučajevima neko od saučesnika upotrebljava silu, neko prijetnju, a neko oduzima tuđu pokretnu stvar. Razlika tih uloga u izvršenju djela ne utiče na kvalifikaciju krivičnog djela pojedinih učesnika, jer su svi učinioci krivičnog djela razbojništva u svojstvu suizvršilaca. Upravo činjenica da je razbojništvo izvršeno u sastavu skupine čini kvalifikatorni element tog krivičnog djela. Sredstva izvršenja u svakodnevnoj kriminalističkoj i pravnoj praksi variraju od slučaja do slučaja, od primjene same "gole" sile (fizičke snage) do primjene vatrenog i hladnog oružja, eksplozivnih naprava i sl. Vrsta primijenjenog sredstva izvršenja i način njegove primjene u svakom konkretnom slučaju (tehnički modus operandi), utiču na kvalifikaciju djela i o tome treba stalno voditi računa kod razrade taktike hapšenja učinioca.Pružanje ozbiljnog otpora žrtve napadaču može rezultirati teškom tjelesnom ozljedom ili lišenjem života žrtve. Mogućnost ozljeđivanja je veća što je više napadača, osobito ako je riječ o mlađim i agresivnim osobama ili osobama pod djelovanjem omamljujućih sredstava koja podstiču agresivnost. Pretjeranom upotrebom sile često se želi paralovati žrtvu ili posmatrače razbojništva.

Uvijek treba što detaljnije i tačnije utvrditi intenzitet i nanin primijenjene prinude kao i okolnosti, kao skup uslova, pod kojima je došlo do primjene prinude. Kad je riječ o strancima, pod pojmom "okolnost" može se podrazumijevati i nepoznavanje lokaliteta.

Pristajanje žrtve na neposrednu predaju pokretne stvari pod okolnostima razbojništva, je razbojništvo. Za postojanje razbojništva dovoljno je, kako je istaknuto, da se silom ili prijetnjom, sprečava otpor žrtve koji se tek očekuje i koji se ne mora slamati. To što koji put žrtve ne znaju što je stvarna svrha napada na njih, pa tek kasnije utvrde da im je oduzeta pokretna stvar, je irelevantno za postojanje krivičnog djela razbojništva (Petrović, A, 1981).
Za postojanje krivičnog djela razbojništva nije odlučno da li je oštećenik kome je oduzeta pokretna stvar njen vlasnik ili stvar drži po nekoj pravnoj osnovi ili čak protivpravno. Stvar ne smije biti od učinitelja. Pod tuđom pokretnom stvari treba podrazumijevati stvar koja je tuđa u odnosu na učinitelja djela. U pravnom smislu tuđa stvar je svaka stvar, na koju učinitelj djela nema pravo dispozicije, već se ona nalazi na raspolaganju druge osobe, bez obzira na kakvoj se pravnoj osnovi temelji to raspolaganje.

1.3.1 Teži oblici razbojništva

Vidljivo je da zakonodavac predviđa kao teži oblik razbojništva slučajeve kad je žrtvi nanesena teška tjelesna ozljeda, koja se može pripisati umišljaju učinitelja, bilo direktnom, bilo eventualnom. U slučaju te posljedice, koja je rezultat umišljaja, ne dolazi u obzir kvalifikacija razbojništva u stjecaju s krivičnimnim djelom teške tjelesne ozljede, jer se tu radi o slučaju konzumpcije.Teži oblik djela predlaže i ako je djelo izvršeno u sastavu skupine. Skupinu čine najmanje tri osobe. Riječ je o posebnom obliku zločinačkog udruženja, obično bez većeg stepena organizovanosti i povezanosti, koja može biti povremena i slučajna. Članovi skupine moraju biti organizovani u nekom smislu i to upravo za izvršenje određenih krivičnih djela, u našem slučaju razbojništva. Djela ne moraju biti unaprijed pobliže konkretizovana. Za kvalifikovani oblik ovog djela ne traži se ni prethodni dogovor, niti neki čvrsti sporazum među učiniteljima, već je bitno da oni sudjeluju u izvršenju djela na način koji je po prirodi ovog djela potreban za ostvarivanje cilja razbojništva. Ako je među sudionicima došlo do diobe rada pri izvršenju djela, onda je riječ o saizvršiocima. Kako je istaknuto za ovaj oblik kvalifikovanog razbojništva ne traži se postojanje prethodnog dogovora među sudionicima skupine, jer do skupnog čina razbojništva može doći i ad hoc, trenutačnom situacijskom odlukom najmanje tri osobe, ali je nužno da svi djeluju skupno u vrijeme izvršenja djela. To znači da se ne mora raditi o nekom većem stupnju međusobne organizovanosti, pa zato mora svaki od sudionika skupine pri skupnom izvršenju djela primijeniti prema napadnutoj osobi silu ili prijetnju, ali mora biti evidentno da on djeluje u sastavu skupine zbog postizanja zajedničkog cilja.Upotrebu kakvog oružja ili opasnog oruđa kao kvalifikovani oblik razbojništva, treba tumačiti kao prijetnju neposrednog napada na život ili tijelo napadnute osobe. Oružje ili opasno oruđe može biti vidljivo ili sakriveno, ali ga učinilac mora imati kod sebe, u svojoj vlasti u vrijeme prijetnje. On, ili neka druga s njim povezana osoba, mora prijetnju iz osnovnog djela razbojništva upravo upotrebom oružja ili opasnog oruđa učiniti ozbiljnom, za žrtvu tetom i opasnijom, te baš zbog toga težom i različitom od prijetnje kod običnog razbojništva. Riječ je o popularno zvanoj pljački pri kojoj se prijeti oružjem ili opasnim oruđem, ali još ne dolazi do njihove primjene. To je na Zapadu poznati „Hold Up“ (Modly, D, 1999).

Čovjeka i ljudsko društvo pitanje sigurnosti zaokuplja od njihova postanka. Sigurnost shvaćamo kao jedan od egzistencijalnih ljudskih problema, koji do punog izražaja dolazi tek onda kad se čovjek nađe u kritičnim opasnim okolnostima (Vencel, K., Jamnić S., Pušeljić M, 2021). Bosna i Hercegovina ima složenu organizaciju policijskog sistema sa mješavinom različitih organizacionih rješenja što je čini unikatnim primjerom (Kovačević, Z., Lakić Z, 2023).

Zaključak

Na snovu sprovedenog istraživanja može se zaključiti da je zakonodavac predvidio kao teži oblik razbojništva, za koji je propisao i najtežu kaznu, slučaj kad je pri izvršenju osnovnog djela razbojništva neka osoba s umišljajem lišena života. Takođe je istaknuto da svako oduzimanje tuđe pokretne stvari s namjerom pribavljanja protivpravne imovinske koristi, ako je izvršeno silom prema nekoj osobi, predstavlja krivično djelo razbojništva. Sila može poprimiti različiti intenzitet i opseg, pa se može manifestovati i u lišenju života neke osobe, žrtve djela razbojništva. Ona je sredstvo za savladavanje otpora i kod razbojništva mora biti obuhvaćena umišljajem učinioca. Umišljaj može biti i potpuno konkretan, tj. obuhvatiti silu u njezinom stvarnom intezitetu. Može se raditi o direktnom ili eventualnom umišljaju. Na osnovu navedenog mora se voditi računa o elementima načina izvršenja krivičnog djela razbojništva. U najširem smislu u te elemente spadaju:

- opšte i posebne okolnosti i uzročnici koji stvaraju uslove za izvršenje djela,
- stepen recidivizma, tragovi i predmeti djela,
- metode i načini prikrivanja djela,
- mjesto izvršenja; - sredstvo izvršenja,
- vrijeme izvršenja; - objekt napada.

Ako posebno posmatramo krivično djelo razbojništva, evidentno je, i iz teorije, ali i iz prakse, da ovo krivično djelo nije na adekvatan način istraženo i objašnjeno, odnosno dosadašnje posmatranje problematike razbojništva nije u skladu sa opasnošću koju ovo krivično djelo stvarno i predstavlja u našem društvu.

Za kvalitetno, efikasno i zakonito postupanje policijskih službenika, osnovna je pretpostavka postojanja koheretnog sistema kriminalističkih procedura, zasnovanih na zakonskim i podzakonskim normama. Traži se „ kvalitetan spoj“ dobrog zakona i „dobrog ovlaštenog službenog lica“, jer iluzorno bi bilo tražiti kvalitetno postupanja ovlaštenih službenih lica, ako su kriminalističke procedure neadekvatne, i obrnuto. Tako, zbog svoje prirode, aktivnosti ovlaštenih službenih lica moraju biti znatno ograničene pozitivnim zakonskim i podzakonskim aktima.

LITERATURA

1. Aleksić, T, 1982, Naučno otkrivanje zločina, Beograd.
2. Filipov, A.G, Cemniĉev, A.J, 2007, Ključni problemi metodike istraživanja krivičnih djela, Zagreb.
3. Modly, D, 1999, Metodika istraživanja razbojništava, Sarajevo, FKN
4. Petrović, A, 1978, Kriminalistička metodika, Beograd.
5. Krivični zakon Bosne i Hercegovine („Sl. glasnik BiH“ br. 3/03, 32/03, 37/03, 54/04, 61/04 i 30/05).
6. Krivični zakon Federacije BiH, „Sl. novine FBiH“, br. 36/2003,21/2004, 69/2004, 18/2005; 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017 i 31/202.
7. Krivični zakon Republike Srpske, „Sl. glasnik RS“ br. 64/2017, 104/2018 i 31/2025.
8. Krivični zakon Brčko distrikta BiH („Sl. glasnik Brčko distrikta BiH“ br. 19/2020, 3/2024 i 14 /2024).
9. Zaštita i sigurnost, godina 1., broj 1. (2021).
10. Zaštita i sigurnost, godina 3., broj 2.(2023).

THE CRIMINAL LAW ASPECT OF ROBBERY

DOI: *10.70329/2744-2403.2025.5.9.5*

Review scientific article

Assoc. Prof. Dr. Zoran Kovačević[9]

Expert Advisor, Aida Šeta Čavčić[10]

Abstract:

This paper explores the issue of criminal offence of robbery in Bosnia and Herzegovina. The subject matter is very complex, thus it was necessary to give particular attention to it, which is one of the goals of this paper. We have attempted to view this topic from multiple aspects and to provide some recommendations when it comes to preventing these types of crime. Although, at first glance, it seems like a criminal law topic, this is primarily a topic related to criminology, i.e. operational-tactical and methodical topic.

The focus of the paper is on the criminal law aspect of robbery, on the legal framework for examining this type of crime, analyzing provisions of criminal laws and criminal procedure laws, applicable on the territory of Bosnia and Herzegovina.

Key words: *robbery, criminal offence, use of force.*

Doboj Business and Technical College, e-mail: zoran.kovacevic@dkpt.gov.ba

Directorate for Coordination of Police Bodies of Bosnia and Herzegovina, e-mail: aida.seta@dkpt.gov.ba

Introduction

According to legal incrimination, a criminal offence of robbery consists of taking away movable property of another by use of force against a person or by threatening to instantly attack his/her life or limb with the intention of obtaining unlawful material gain for oneself or for someone else, by appropriating it. A more serious form of this criminal offence exists when a serious bodily injury has been intentionally inflicted on a person of if the offence has been committed by several persons of if a weapon or dangerous instrument has been used of if the value of the stolen property exceeds 50.000,00 BAM, or even more serious form if a person has been murdered intentionally. [11] Force or threat can be used against a person but not against property thus it does not always have to be a criminal offence of robbery. Case law also takes this position and comes to a conclusion that such cases should be qualified as the criminal offense of aggravated theft committed in a particularly brazen manner. In a case when the seizure of property from the injured party is carried out by snatching it from their hands, without any direct threat to the life or limb of the injured party, or without use of any force against him/her, it will not be qualified as a robbery, but as an aggravated theft. While committing the criminal offence of robbery, perpetrators use various means suitable to use force or threat, depending on the object of an attack, professionalism and organization of perpetrators. The most common means of perpetrating the criminal offence are: firearms (pistols, revolvers, various automatic weapons), close-combat weapons (knife, dagger, axe, various blades), mine explosive devices and incapacitating sprays. Force also includes the use of intoxicants (use of spray) to disable and incapacitate the victim. In street robberies, physical force is most often used by the perpetrator against the victim. If with serious consequences, armed robberies fall into the group of the gravest forms of serious criminal offences characterized by a high degree of social danger. Perpetrators of robberies generally make detailed preparations in advance, based on which they plan the execution of the criminal offence/attack in detail. The perpetrators collect relevant data with regards to the object of the attack, paying particular attention to the method of securing the values they are seizing and appropriating in order to obtain unlawful material gain. The criminal offence of robbery is mostly committed by men, but recently women have also emerged as independent perpetrators of these crimes. Usually, these crimes are most often committed by persons who are not employed, although there are also cases proving the opposite. By committing criminal offence of robbery, perpetrators want to obtain property of the greatest possible value, so it is logical that they

[3] Criminal Code of the Republic of Srpska, „Official Gazzette of RS“, br. 64/2017, 104/2018 and 31/2025, Article 227.

attack those facilities where such things are located or persons who possess things of such value. The criterion remains the same: appropriating as much material gain as possible. The following facilities are of interest to perpetrators of these criminal offences: banks, post offices, exchange offices, jewelry stores and other stores selling valuable goods, gas stations, various agencies, department stores, catering and tourist facilities, and more recently, apartments have increasingly appeared as targets of attacks by perpetrators of this crime. Among individuals, the most common targets of attacks are: cashiers, money transmitters, postmen, waiters, taxi drivers, drunk people, sellers of goods at markets, traders at fairs and homosexuals.

1. THE CRIMINAL LAW ASPECT OF ROBBERY

1.1. Criminal Code of the Republic of Srpska

(1) Whoever, by use of force against another person or by threatening to immediately attack against his life or body, takes away another person's personal property with the intent to gain material benefit to himself or to another by doing so, shall be punished by imprisonment for a term between one and ten years.
(2) If, during the commission of the criminal offence referred to in Paragraph 1 of this Article, grievous bodily injury has been intentionally inflicted on a person, or if the offense has been committed by a group or if firearms or dangerous implements were used or if the value of stolen property exceeds 50,000 KM, the perpetrator shall be punished by imprisonment for a term between five and fifteen years.
(3) If, during the commission of the criminal offence referred to in Paragraph 1 of this Article, a person has been intentionally killed, the perpetrator shall be punished by imprisonment for not less than ten years or by long term imprisonment.[12]

1.2. Criminal Code of the Federation of Bosnia and Herzegovina

(1) Whoever, being caught in the perpetration omission of criminal offence of theft, and with an aim of retaining possession of the stolen property, uses force against a person or threatens instant attack on his life or limb, shall be punished by imprisonment for a term between one and ten years.
(2) If, by the criminal offence referred to in paragraph 1 of this Article, a serious bodily injury is inflicted on a person with intent, or if the criminal offence is

[12] Criminal Code of Republika Srpska, „Official Gazzete“no. 64/2017, 104/2018 and 31/2025, Article 227.

perpetrated within a group of people, or a weapon or dangerous instrument is used, the perpetrator shall be punished by imprisonment for a term not less than five years.
(3) If, in perpetrating the criminal offence referred to in paragraph 1 of this Article, a life of person is taken with intent, the perpetrator shall be punished by imprisonment for a term not less than ten years or by long-term imprisonment.[13]

1.3. Criminal Code of the Brcko District of Bosnia and Herzegovina

(1) A person who uses force against another person, or threatens to directly attack his life or body in order to seize another's movable piece of property intending thereby to obtain an unlawful property gain for himself or another, shall be sentenced to prison from one to ten years.
(2) If, while committing the offence referred to in Paragraph 1 of this Article, a person inflicted severe bodily injury to another with premeditation, or the offence was committed by several persons, or if certain weapon or a dangerous object was used, the perpetrator shall be sentenced to at least five years in prison.
(3) If a person was killed deliberately in committing the offence referred to in Paragraph 1 of this Article, the perpetrator shall be sentenced to prison of at least ten years or long-term imprisonment.[14] From the content of the cited incrimination, robbery is a criminal offence with elements of violence. According to the legal construction, it is a complex criminal offence. This criminal offence consists of elements of the criminal offence of theft (taking someone else's movable property) and the use of force or threat (serious), i.e. coercion, a direct attack on the life or body of a person from whom the property is to be taken with the intention of obtaining unlawful material gain. The offence poses significant social harm which can easily escalate into a criminal offence of causing grievous bodily injury or deprivation of life. The legislator expressed the social harm of robbery through possible punishment.
Force or threat (coercion) occurs in robberies as means of enabling the taking away another person's movable property and must therefore precede the seizure of another person's movable property. The goal of coercion is to prevent or overcome resistance aiming to prevent seizure taking away someone else's movable property. In this case, the force does not have to cause any consequences for the injured party. It is sufficient that it was used as a means to achieve the goal, i.e. to seize someone else's movable property with the intention of obtaining unlawful gain through its appropriation. If the offence was committed without the stated intention, it is not the case of robbery.

[13] Criminal Code of Federation of BiH, „Official Gazzete"no. 36/2003,21/2004, 69/2004, 18/2005; 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017 i 31/202, član 289
[14] Criminal Code of the Brcko District BiH, „Official Gazzete of Brcko Districta BiH" no. 19/2020, 3/2024 and 14/2024, Article 283.

Force as an element of robbery should mean the actual infliction of harm. It is the application of force against a person with the intention of making that person do or don't do something. That force can be physical or mechanical. The use of hypnosis or soporifics is also considered force.
According to its intensity, force can be: irresistible (absolute, vis absoluta) or psychological (compulsive, vis compulsiva). Absolute or material force implies that the force applied is so overwhelming that it negates the individual's ability to make a free choice or to implement the decision made. Force is psychological or moral if the person against whom it is applied can make decisions, but those decisions are forced by psychological coercion, for example in situations of hostage-taking and blackmail.
The force required to take away another person's movable property does not have to be significant. The force or threat must be directed against the person from whom the movable property is taken and not towards the property itself.
The crime of robbery also exists in cases when the victim does not see the taking away of his/her movable property, e.g. when the victim is locked in a room or blindfolded, when is unconscious or under the influence of opiates, etc. In the mentioned cases, it is important to stress that the disabling the victim to see his/her movable property being taken away is the result of use of force or threats by the perpetrator.

In criminal and judicial practice, cases where the perpetrator ripped an object from the victim's hand or body are controversial. Typically, courts qualify such cases of "plunder" as aggravated theft committed in a particularly brazen manner. If the victim offered any resistance, its form and extent should be established. If the life or body of the victim is endangered by breaking the resistance, it is a case of robbery. This means that the force must be directed against the person from whom the movable property is to be taken, with the aim of preventing or disabling their resistance to it. If the force is not directed against a person with the aim of preventing or disabling their resistance to take away the property, but is used for the purpose of breaking the physical connection between the property and its holder, it is a case of brazen theft. In such a case, theft is an integral part of the act of taking things, and not a means of enabling that act. In such a case, force is an integral part of the act of taking things, not a means to enable that action. Such force does not have the traits of the force that is an element of the criminal offence of robbery. The theft of a bag on public transportation or on the street, which a victim is holding loosely over the arms or shoulders, or not holding at all, or even not looking at it, is not considered a form of resistance and is not considered to be criminal offence of robbery. Even in cases of "nudge" or even "small struggle" in order to take away movable property, it is not the case of robbery if there is no coercion in the sense of an attack on the life or body of the victim. What has been said is valid only on the assumption that the robber did not, apart from the force necessary to tear off the movable object, also used some other additional act of

violence against the owner of the object in order to overcome his/her resistance and take away the movable object, then it is a case of robbery. If force is applied to a victim, then, as pointed out, the does not have to hold the object, nor does it have to be on the victim; what is important is that it is under the victim's control, that it is in the victm's possession. Being under control, as stated above, is the right or privilege of using the object in a free way by the victim. Moreover, at the time of seizure, the object does not have to be under the actual visual supervision of the victim, if the victim is incapacitated in one of the aforementioned ways. (Filipov, A.G., Cemničev, AJ, 2007, Ključni problemi metodike istraživanja krivičnih djela/ Key problems in criminal investigation methodology, „Izbor", Zagreb).

Threat should imply probability of some sort of evil in order to influence the will of a person being threatened. The threat differs from the above-mentioned psychological force, the former being the evil is applied, while in the latter it is only likely to happen.

Threat is a means to commit robbery. Sometimes it can be a qualified threat, i.e. a threat of specific evil. The threat of a direct attack on a person's life or body is aimed at preventing not only freedom of action, but also freedom of decision and movement. When applying threat, the legal basis according to which the attacked person is holding an object is not important for the existence of robbery, but it is necessary that the victim is present at the crime scene. Evil that is presented as a threat, i.e. some sort of danger, must be immediate and simultaneous. The threat must be such that the person toward whom it is directed takes it seriously and that the perpetrator has that intention. It is not crucial whether the person making a threat (perpetrator) can really carry out the threat, e.g. threatening with a flare gun; what is important is that the victim is unaware of the fact of what kind of gun it is. The criminal offence of robbery also exists in cases where a perpetrator does not take someone else's movable property himself, but when the injured party, directly under the influence of force or threat, hands over the movable property to the perpetrator. The threat that information about a person will be disclosed, for example, that he/she is a homosexual, an embezzler, etc., does not meet the definition of a threat.

As for the value of the seized item, we believe that regardless of its value, it is a criminal offence of robbery if coercion was committed. We are of the opinion that the amount of illegal property benefit actually obtained through the use of force or threat is not decisive for the legal qualification of the offence. It has to be forcible seizure of someone else's movable property, the appropriation of which fulfills the intention of obtaining an illegal property benefit. When a perpetrator commits a direct attack on life or body by force or threat with the intention of obtaining an illegal property benefit, if the perpetrator takes away a movable thing from the victim or forces the victim to hand it over or to leave it on the spot, it is always considered a criminal offence of robbery.

In practice, cases where only a threat was applied without the use of force, i.e. when there are no visible consequences and when no means of threat is found, if a movable object was used or taken, are, in general, difficult to prove. In such cases, investigator' skill plays a crucial role. The investigator must be well versed in investigative techniques (Aleksić, Ž, 1982, Naučno otkrivanje zločina/Scientific Crime Detection, Beograd).
The use of force or threat must precede or be combined with the seizure of movable property. Force applied to keep seized movable property (belonging to someone else) constitutes a criminal offence of robbery. When threatened with the use of force, a victim does not have to be frightened to the point of panic. It is sufficient for the victim to realize that there is a possibility of being hurt. The use of force or threat varies depending on the objective and subjective circumstances of each specific case, even when it comes to the same perpetrator. The crime of robbery is completed by taking away someone else's movable property. If the seizure does not take place, it is an attempted robbery.

Coercion as a feature of the criminal offence of robbery exists even when force or an explicit threat of direct attack on life or body is not used, if the behavior of the perpetrator or his accomplices is such that it expresses a threat of direct attack on life or body. A person against whom force or threat is applied may also be the person who is trying to help the victim. Multiple people often participate in the commission of the criminal offence of robbery with a necessary division of tasks. In such cases, one of the accomplices uses force, another uses threats, and another takes away someone else's movable property. The difference in these roles in the commission of the crime does not affect the qualification of the criminal offence of individual participants, because all perpetrators of the criminal offence of robbery are co-perpetrators. It is exactly the fact that the robbery was committed as part of a group that constitutes a qualifying element of this criminal offence. The means of commission in everyday criminal and legal practice vary from case to case, from the use of "bare" force (physical force) to the use of firearms and cold weapons, explosive devices, etc. Methods used for commission of criminal offence and the manner of its application in each specific case (technical modus operandi) affect the crime qualification and it should always be taken into account when developing tactics for arresting the perpetrator.

The victim's significant resistance to the attacker may result in serious bodily injury or loss of life. The possibility of getting injured is greater the more attackers there are, especially if they are younger and violent or under the influence of intoxicants that simulates violence. Excessive use of force is often intended to paralyze the victim or witnesses of a robbery.
It is always necessary to determine the intensity and manner of the applied coercion as precisely as possible, as well as the circumstances and conditions,

under which the coercion has been applied. When it comes to foreigners, the term "circumstance" can also imply unfamiliarity with the place.

The victim's consent to hand over a movable property under the circumstances of robbery is robbery. As pointed out, for robbery to exist it is sufficient that the victim's resistance, which is yet to be expected and does not have to be broken, is prevented by force or threat. The fact that sometimes the victims do not know the real purpose of the attack against them, and only later find out that their movable property was taken, is irrelevant to the existence of the crime of robbery (Petrović, A, 1981, Kriminalistička metodika/Criminal Methodology, Zemun). For the criminal offense of robbery to exist, it is not decisive whether the injured party from whom the movable property was seized is its owner or holds the property on some legal basis or even illegally. The property must not belong to the perpetrator. Another person's movable property should be perceived as the property that belongs to someone else and not the perpetrator. In legal sense, someone else's property is any property that the perpetrator of the offence does not have the right to dispose of, but is at the disposal of another person, regardless of the legal basis on which that disposal is based.

1.3.1. Serious Forms of Robbery

When a victim is inflicted with serious bodily injury, which can be attributed to the perpetrator's intent, either direct or potential, it is evident that the legislator foresees these cases as a more serious form of robbery. In the case of this consequence, which is the result of intent, the qualification of robbery in conjunction with the criminal offence of serious bodily injury is out of the question, because this is a case of consummation. A more serious form of the crime is also proposed if the crime has been committed as part of a group. The group consists of at least three people. It is a special form of criminal association, usually without a greater degree of organization and connection, which can be occasional and accidental. The members of the group must be organized in some sense, precisely for the commission of certain criminal offences, in our case robbery. The offences do not have to be specified in detail in advance. For the qualified form of this crime, neither prior agreement nor a firm agreement between the perpetrators is required, however it is important that they participate in the commission of the crime in a manner that is by the nature of the crime necessary to achieve the goal of robbery. If there was a division of tasks among the participants during the commission of the crime, then we are talking about co-perpetrators. As previously indicated, this form of qualified robbery does not require prior agreement among the group members, because a collective offence

of robbery can also occur ad hoc, by a momentary situational decision of at least three people, but it is necessary that everyone acts together at the time of the crime. This means that it does not have to be a greater degree of mutual organization, and therefore each of the group participants must use force or threats against the attacked person when committing the offence together, but it must be evident that they are acting as part of the group to achieve a common goal. The use of a weapon or dangerous instrument, as a qualified form of robbery, should be interpreted as a threat of direct attack on the life or body of the attacked person. A weapon or dangerous instrument can be visible or hidden, but the perpetrator must have it in his/her possession at the time of the threat. Specifically, by using a weapon or tool dangerous for the victim, he/she or some other person connected with him must make the threat from the basic offence of robbery more serious, difficult and dangerous, and precisely due to this, different from the threat related to ordinary robbery. This is popularly called robbery, in which a person is threatened with a weapon or dangerous tool but it is not yet used. This is the "Hold Up"as known in the West. (Modly, D, 1999, Metodika istraživanja razbojništava/Robbery Research Methodology, FKN, Sarajevo).
The issue of security has preoccupied humans and human society since their inception. We understand security as one of the existential human problems, which comes to full expression only when a person finds himself in critical dangerous circumstances (Vencel, K., Jamnić S., Pušeljić M, 2021). Bosnia and Herzegovina has a complex organization of the police system with a mixture of different organizational solutions, which makes it a unique example (Kovačević, Z., Lakić Z, 2023).

Conclusion

On the basis of the conducted research, it can be deduced that the legislator foreseen a case when a person is intentionally deprived of life during the commission of the basic offence of robbery as a more serious form of robbery for which he/she also prescribed the most severe punishment. It was also emphasized that any seizure of another's movable property with the intention of obtaining unlawful material gain, if carried out by force against a person, constitutes the criminal offense of robbery. Force can take on different intensity and scope, and can also manifest itself in the deprivation of a person's life, a victim of a robbery. It is a means of overcoming resistance and when it comes to robbery, must be included in the perpetrator's intent. It could be a direct or possible premeditation. Based on the above, the manner in which a criminal offense of robbery was committed must be taken into account. Based on the above, all elements of a committed criminal offense of robbery must be taken into account. In the broadest sense, these elements include:

- general and special circumstances and causes creating conditions for the commission of a crime,
- degree of recidivism, traces and objects of a crime,
- methods and ways of concealing a crime,
- place of commission; - means of commission,
- time of commission; - object of an attack.

If we look specifically at the criminal offence of robbery, it is evident, both from theory and practice, that this crime has not been adequately researched and explained, i.e. the current observation of the issue of robbery is not in line with the danger this crime actually poses to our society. For high-quality, efficient and lawful actions of police officers, the existence of a coherent system of criminal procedures, based on legal and by-law norms, is essential. It is necessary to have a “quality combination” of an adequate law and "adequate authorized official", for it would be delusional to demand quality actions by authorized officials if criminal procedures are inadequate, and vice versa. Thus, due to their nature, activities of authorized officials must be significantly limited by positive legal and regulatory acts.

LITERATURE

11. Aleksić, T, 1982, Naučno otkrivanje zločina/ Scientific Crime Detection, Beograd.
12. Filipov, A.G, Cemniĉev, A.J, 1982, Ključni problemi metodike istraživanja krivičnih djela/ Key problems in criminal investigation methodology, Zagreb.
13. Modly, D, 1999, Metodika istraživanja razbojništava/ Robbery Research Methodology, Sarajevo, FKN
14. Petrović, A, 1978, Kriminalistička metodika/ Criminal Methodology, Beograd.
15. Criminal Code of Bosnia and Herzegovina (Official Gazette of BiH" no. 3/03, 32/03, 37/03, 54/04, 61/04 i 30/05);
16. Criminal Code of Federation of Bosnia and Herzegovina, „Official Gazette FBiH", no. 36/2003,21/2004, 69/2004, 18/2005; 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017 i 31/202.
17. Criminal Code of the Republic of Srpska, „Official Gazzete of RS" no. 64/2017, 104/2018 i 31/2025.
18. Criminal Code of Brsko District of BiH (Official Gazzete of Brcko District of BiH" no. 19/2020, 3/2024 i 14 /2024).
9. Protection and Security, Year 1, Issue 1 (2021).
10. Protection and Security, Year 3, Issue 2 (2023).

ZLOUPOTREBA LAŽNIH DOJAVA O BOMBAMA PRIJETNJA STVARNOJ SIGURNOSTI

DOI: *10.70329/2744-2403.2025.5.9.6*

Pregledni znanstveni članak

Doc.dr. Zoran Lakić [(1)]
Doc.dr. Zoran Kovačević [(2)]

Sažetak:

Lažne dojave o postavljenim eksplozivnim napravama predstavljaju sve izraženiji sigurnosni izazov u savremenom društvu. Iako na prvi pogled mogu djelovati kao bezazlene smetnje, ovakve radnje u stvarnosti izazivaju širok spektar posljedica, od narušavanja osjećaja sigurnosti građana do ozbiljnog opterećenja resursa sigurnosnih i hitnih službi. Činjenica da se ovakve dojave ne mogu odmah klasifikovati kao neosnovane zahtijeva hitnu i sveobuhvatnu reakciju nadležnih institucija, pri čemu se nerijetko angažuju specijalizovane jedinice i oprema visoke vrijednosti. U ovome radu razmatra se na koji način zloupotreba sistema dojavljivanja utiče na operativnu spremnost sigurnosnih struktura i kakve dugoročne implikacije ostavlja na javne i finansijske tokove. Također, biće analizirani statistički podaci Ministarstva unutrašnjih poslova Kantona Sarajevo za 2023. i 2024. godinu, s ciljem dubljeg razumijevanja dinamike ovog problema i njegovog uticaja na svakodnevni život građana i institucionalni odgovor.

Ključne riječi*: Lažne dojave, specijalni timovi, sigurnost, terorizam, ugrožavanje javne sigurnosti.*

[(1)]. Viktoria Internacionalni Univerzitet Mostar, e-mail: e-mail: zoran.lakic@viu.ba
[(2)]. Visoka poslovno tehnička škola Doboj, e-mail: zoran.kovacevic@dkpt.gov.ba

1. UVOD

Lažne dojave o postavljenim eksplozivnim napravama postale su ozbiljan bezbjednosni problem, s potencijalom da prerastu u rašireni društveni fenomen s višestrukim negativnim posljedicama. Sve češće motivisane različitim razlozima, ove dojave ne samo da iscrpljuju resurse sigurnosnih službi, već izazivaju i psihološki stres među građanima, što u velikoj mjeri narušava povjerenje u institucije nadležne za očuvanje javne sigurnosti. U savremenom kontekstu, u kojem je brzina protoka informacija od ključnog značaja, ovakve dojave mogu značajno poremetiti rad institucija koje su zadužene za reagovanje na stvarne prijetnje. Iako naizgled bezopasne, lažne dojave mogu izazvati širok društveni haos, uznemirenje građana i preusmjeravanje značajnih resursa ka pretragama koje se, na kraju, pokažu kao neopravdane. Problem ne leži samo u izazivanju panike, već i u stvaranju iluzije opasnosti, pri čemu stvarne prijetnje mogu ostati zanemarene. Lažno dojavljivanje ne predstavlja samo nesporazum ili bezazlenu šalu, već je riječ o namjernoj radnji sa ciljem izazivanja straha, panike i destabilizacije sistema. Takve dojave se mogu uputiti putem različitih kanala, uključujući telefonske pozive, anonimne elektronske poruke i objave na društvenim mrežama.

Poseban izazov predstavlja upotreba savremenih tehnologija za širenje dezinformacija, što dodatno otežava identifikaciju stvarnih prijetnji i adekvatno reagovanje nadležnih institucija. Iako lažna dojava ne znači da je eksplozivna naprava zaista postavljena, ona u znatnoj mjeri ometa svakodnevni život, izaziva osjećaj nesigurnosti i stvara iskrivljenu sliku o stvarnoj opasnosti. Ovaj fenomen ne može se smatrati bezopasnim činom, naprotiv nerijetko se koristi kao sredstvo političkog ili socijalnog protesta. Iako motivi variraju, posljedice su konkretne i ozbiljne, uključujući visoke troškove angažovanja specijalizovanih jedinica, kao što su timovi za deminiranje, koji su zaduženi za detekciju i neutralizaciju potencijalnih prijetnji. Osim materijalne štete, učestale uzbune mogu dovesti do slabljenja ozbiljnosti institucionalnog odgovora u trenucima kada stvarna prijetnja zaista postoji. Preopterećenost službi zbog ponavljajućih lažnih uzbuna vodi ka umanjenju njihove efikasnosti i eroziji povjerenja građana u sistem zaštite. Svaka nova lažna dojava dodatno otežava razlikovanje između stvarne i izmišljene prijetnje. Posebnu pažnju treba posvetiti preciznom definisanju pojma lažne dojave. Lažna dojava predstavlja svjesno i namjerno obmanjivanje nadležnih organa o postavljenom eksplozivnom sredstvu, bez postojanja stvarne prijetnje. Motivacija može biti politička, ideološka, socijalna, psihološka ili čak trivijalna, poput potrebe za pažnjom ili izazivanjem nereda. Bez obzira na uzrok, posljedice ostaju ozbiljne i višeslojne. U tom kontekstu, treba pomenuti i improvizovana eksplozivna sredstva (engl. Improvised Explosive Devices – IED), koja, iako nisu industrijski proizvedena, imaju kapacitet da izazovu veliku materijalnu štetu i ljudske žrtve. Takva sredstva često se koriste u terorističkim

napadima, a čak i lažne dojave o njihovoj upotrebi mogu poslužiti kao instrument političkog pritiska, zastrašivanja ili destabilizacije.

Lažna dojava o postavljenom eksplozivnom sredstvu obuhvata svijestan i namjeran pokušaj izazivanja panike, straha ili uznemirenosti među ljudima, čime se bez potrebe mobilizuju resursi koji bi u suprotnom bili usmjereni na stvarne prijetnje. Ove dojave mogu doći u različitim oblicima od telefonskih poziva do anonimnih emailova ili poruka na društvenim mrežama, pri čemu je posebno zabrinjavajuća tendencija korišćenja savremene tehnologije i medijskih kanala za širenje dezinformacija (Smith, R. T., 2017). Kada se razmatra fenomen lažnih dojava o eksplozivnim napravama, od ključne je važnosti razumjeti potrebu za razvojem efikasnih strategija prevencije i odgovora, u cilju smanjenja štetnih posljedica i bolje zaštite resursa sigurnosnih službi. Brza identifikacija lažnih prijetnji omogućava da se stvarne opasnosti ne zanemare, čime se direktno štite ljudski životi i očuvava stabilnost sigurnosnog sistema. Procjenjivanje rizika, tj. ugroženosti se provodi u skladu s Matricom procjene rizika prema opštim kriterijama nivoa rizika odnosno vjerovatnoće i posljedice u odnosu na isti (Hasović, L., 2021).

2. TEORIJSKI OKVIR I PROBLEMATIKA

Lažne dojave o postavljenim improvizovanim eksplozivnim sredstvima (IED), kao i druge vrste lažnih uzbuna, stvaraju pravu sigurnosnu dilemu. U društvu koje je sve više suočeno s brzim informativnim tokovima, lažne dojave postaju ozbiljan problem, ne samo zbog narušene sigurnosti, nego i zbog panike koju izazivaju. Ovaj fenomen nije samo pitanje prepoznavanja prijetnji, jer radi se o složenoj situaciji u kojoj je ključno balansirati između prepoznavanja stvarnih opasnosti i suzbijanja štete koju izazivaju neistiniti pozivi. Kada sagledamo postojeće istraživanje na ovu temu, dolazimo do jasnog zaključka da su lažne dojave su odraz širih društvenih i psiholoških problema. Značajan broj istraživača bavio se motivima koji stoje iza ovih incidenata, ali i posljedicama koje one ostavljaju na društvo. Nisu svi radovi u ovoj oblasti usmereni samo na tehničke i sigurnosne aspekte; mnogi istraživači, kao što su Garrison i McManus, razmatraju psihološke i socijalne korene koji podstiču ljude na donošenje takvih odluka (Garrison, J., & McManus, T. , 2014). Ispostavlja se da iza većine lažnih dojava stoje problemi koji nisu uvek očigledni na prvi pogled i često su povezani sa ličnim, političkim ili čak ideološkim razlozima. Pitanje kako zakon reaguje na ovakve postupke nije manje bitno. Većina zemalja, uključujući Bosnu i Hercegovinu, ima jasno postavljene kazne za lažno prijavljivanje opasnosti. U našem zakonodavnom okviru, lažna dojava o postavljenim eksplozivnim sredstvima može rezultirati kaznom zatvora do 5 godina, uz ogromne troškove koji prate angažovanje specijalizovanih timova. A troškovi nisu samo novčani, jer

dugoročne posljedice u smislu gubitka vremena i resursa nisu zanemarive. Sjećanja na istorijske incidente, poput onog iz 2001. godine u New Yorku, gde je lažna dojava izazvala evakuaciju više od 10.000 ljudi, podsećaju nas koliko dalekosežne posledice ovakvi incidenti mogu imati. Iako su brojni, takvi događaji su i dalje izazovni za analizu, jer sa svakim novim slučajem uočava se i šira upotreba tehnologija, pretežno društvenih mreža, kao načina za širenje dezinformacija. Nekoliko slučajeva u poslednjih nekoliko godina pokazuje kako lažne dojave postaju sve češće. 2019. godine, u Italiji su se dogodile brojne lažne dojave o eksplozivima postavljenim u školama, što je uzdrmalo obrazovni sistem i izazvalo dodatni pritisak na policijske snage. Kada podaci i obavještenja ukazuju da postoje osnovi sumnje (Korajlić, 2003) da je izvršeno krivično djelo za koje se goni po službenoj dužnosti, postupanje policije mora da ima sistematski karakter i da se odvija kroz evidentiranje podataka i obavještenja, njihovo stručno procjenjivanje, donošenje odluke o postupanju, kao i provjeravanju podataka i obavještenja, u cilju prikupljanja materijalnih i drugih dokaza. Prijetnje koje nisu stvarne često nemaju dovoljno konkretnih informacija, što usmerava bezbjednosne resurse u pogrešnom pravcu. Čak i u slučajevima kada je lažna dojava očigledna, posledice, poput panike ili prekomernog angažovanja resursa, mogu biti ozbiljne. Da bi se ovi problemi minimizirali, neophodno je razviti preciznije mehanizme za identifikaciju i prepoznavanje lažnih dojava, kao i ulagati u obuku timova za suočavanje sa sličnim izazovima. Zajedno s naprednom tehnologijom, koja je u stanju da poveća brzinu prepoznavanja prijetnji, trebalo bi da se osigura da društvo bude bolje pripremljeno za suočavanje sa svim vrstama sigurnosnih izazova. Na primjer, autori kao što su Garrison i McManus istražuju psihološke motive koji vode do zloupotrebe sistema javljanja, naglašavajući da često u pozadini takvih dojava stoje socijalni problemi, ali i političke i ideološke ambicije (Garrison, J., & McManus, T., 2014).

3. SISTEM POD OPSADOM DEZINFORMACIJA - FUNKCIONALNA SLABOST I REAKCIJA

Lažne dojave o bombama možda zvuče kao stara fraza, ali realnost je daleko ozbiljnija. Takvi incidenti nisu samo "zloupotreba sistema", oni su udarac na njegovu srž. I svaki put kad neko digne lažnu uzbunu, pokrene se mašinerija koja troši vrijeme, resurse i strpljenje. Neki to rade iz bijesa ili frustracije, neki zbog pažnje. Neki jer žele skrenuti fokus sa nečeg drugog. Ima i onih koji igraju malo ozbiljniju igru, hoće da zaustave neku firmu, izazovu štetu konkurenciji ili poremete događaj. Ipak, bez obzira na razlog, posljedice su uvijek stvarne. Prva linija udara su policija i sigurnosne službe. Svaka dojava, bez izuzetka, mora biti ozbiljno shvaćena. I to znači da se protivdiverzini timovi angažuju, saobraćaj i ulice zatvaraju, škole, sudovi, tržni centri evakuišu. A kad se ispostavi da je sve bilo "ništa" svejedno ostane račun, ali i nervoza iznad kojeg lebdi osjećaj

nesigurnosti. Problem je i u tome što ovakvi slučajevi opterećuju sistem. Policajci koji su mogli raditi na stvarnim prijetnjama, sada gube sate na nešto što ne postoji. A što ih je možda namjerno odvuklo u pogrešnom smjeru. Svaka lažna dojava je, u suštini, neka vrsta sabotaže ne samo sistema, nego i zdravog razuma. PDZ timovi zahtijevaju specijalizovanu opremu, stalnu obuku, mobilnost. Ništa od toga nije jeftino. Organizacija terenskih intervencija, smještaj, logistika o ostale aktivnosti, sve to ulazi u budžetski minus. I uz sve to, tu su i druge službe koje se paralelno angažuju: lokalna policija, medicinske ekipe, jer svi moraju biti spremni, čak i kad nije stvarno. A šteta se ne mjeri samo u novcu. Lažne dojave remete svakodnevni život. Zatvaraju se škole, firme, tržni centri. Ljudi se izbacuju iz rutine, širi se panika, atmosfera nesigurnosti lagano puzi kroz pukotine svakodnevice. I što je najgore navikavanje na takve stvari može biti još opasnije od samih dojava. Zbog toga je potrebna je kombinacija svega kroz institucionalni odgovor, zakoni koji se ne šale, edukacija koja ide ispod površine. Jer ovo nije problem koji će se riješiti sam od sebe. Možda je najveći problem u tome što sistem još uvijek reaguje kao da vjeruje svakome. A to je i lijepo, i opasno. Lijepo jer pokazuje da ne ignorišemo prijetnje. Opasno jer oni koji to znaju koriste. U trenutku kad sistem prestane vjerovati, svi gubimo.

4. VEZA IZMEĐU LAŽNIH DOJAVA I TERORIZMA

Terorizam kao pojam nema jednu univerzalnu definiciju, ali se najčešće opisuje kao upotreba nasilja ili ozbiljne prijetnje nasiljem nad civilima, radi ostvarivanja političkih, ideoloških ili vjerskih ciljeva. Suština terorističkog djelovanja zapravo nije samo u izazivanju fizičke štete, već u kreiranju atmosfere straha, nesigurnosti i pritiska na vlasti ili širu javnost da promijene svoje ponašanje, zakone ili stavove. Stručnjaci za terorizam i države koje se bore protiv terorizma saglasni su u ocjeni da će biti vrlo teško odrediti definiciju terorizma koju bi priznale sve zemlje svijeta, ali su takođe saglasni o tome da se bez nje ne može voditi uspješna internacionalna borba protiv terorizma (Lakić, Z., Kovačević Z, 2024). U tom svjetlu, lažne dojave o bombama mogu se, u određenim okolnostima, posmatrati i kao dio šireg bezbjednosnog problema. One ne nose eksploziv, ali mogu razoriti povjerenje i kapacitete sistema. Naizgled banalne, te dojave zapravo remete rad institucija, troše resurse i otežavaju prepoznavanje stvarnih prijetnji. Kada službe bezbjednosti budu zatrpane istragama koje se na kraju pokažu lažnim, povećava se rizik da stvarna opasnost prođe ispod radara.

Jedan od ozbiljnih problema jeste i to što se vremenom stvara efekat „lažne uzbune“, te svaka naredna dojava može biti shvaćena s manje ozbiljnosti. A upravo to može iskoristiti neko ko planira stvarni napad. Sistem postaje zasićen, pažnja otupi, a to je idealno tlo za iznenađenje. Preplavljenost sistema lažnim dojavama može dovesti do smanjenja sposobnosti vlasti da reaguje na stvarne

prijetnje, stvarajući tako ranjivost za terorističke napade (Hoffman, B., 2006). Nije nepoznato da se uoči izbora, posebno tokom politički napetih perioda, broj lažnih dojava zna povećati. Neki analitičari vide u tome pokušaj destabilizacije, usmjeravanje pažnje javnosti, pa čak i svjesno izazivanje nepovjerenja prema institucijama. Kada se to poklopi s danima glasanja ili ključnim političkim događajima, sumnja u pozadinske motive nije bez osnova. Takođe, lažne dojave u tim trenucima mogu biti alat manipulacije ili čak diverzije.

Dok se bezbjednosne službe bave evakuacijama i pretragama, neka druga radnja može ostati ispod radara. U svakom slučaju, efekat je isti: sistem je opterećen, a povjerenje građana načeto. Lica koja šalju lažne dojave o bombama najčešće nisu „klasični kriminalci“. Mnogi od njih dolaze iz pozadine emocionalne nestabilnosti, lične frustracije ili društvene isključenosti. Motivacija im može biti raznolika, od potrebe za pažnjom, preko želje za osvetom, pa sve do pokušaja da testiraju sistem. U nekim slučajevima, riječ je o adolescentima ili mladim osobama koje ne sagledavaju težinu svog čina. U drugim, radi se o planskim i ciljanim pokušajima da se izazove haos ili odvrati pažnja sa nečeg drugog.

Nerijetko se može govoriti i o tzv. "operativnom narcizmu", pojedinci koji se lažno predstavljaju kao borci protiv nepravde, ali zapravo instrumentalizuju haos da bi se osjećali moćno. U političkim ili socijalno polarizovanim društvima, ovi motivi se lako zapale, pa nije čudno da broj lažnih dojava raste kad je društvena temperatura visoka. Ukoliko se ovom problemu priđe ozbiljno, mora se posmatrati u svim dimenzijama i to: bezbjednosnoj, političkoj, psihološkoj i društvenoj. One su ogledalo stanja u kojem se društvo nalazi, tj.koliko je ranjivo, koliko vjeruje institucijama, i koliko smo spremni da reagujemo zrelo. A borba protiv toga nije samo stvar zakona i kazni. Potrebno je obrazovanje, odgovorno izvještavanje, efikasna koordinacija službi i što je možda najteže stvaranje kulture u kojoj sigurnost nije samo tuđa odgovornost.

5. STATISTIČKI POKAZATELJI MUP-A KANTONA SARAJEVO ZA 2023. I 2024. GODINU

U toku 2023. godine evidentirano je 120 slučajeva anonimnih dojava o postavljanju eksplozivne naprave, a odnosile su se na sudove, tužilaštva, opštine, obrazovne ustanove, ugostiteljske objekte, banke i hotele. Nakon PDZ pregleda utvrđeno je da su dojave bile lažne, osim anonimne dojave o postavljenoj eksplozivnoj napravi u jednom ugostiteljskom objektu, gdje su PDZ pregledom u podrumskim prostorijama pronađene dvije ručne bombe. Od ukupno 120 anonimnih dojava o postavljenim eksplozivnim napravama rasvijetljeno je šest događaja, i to četiri iz mjeseca aprila i po jedan iz juna i jula ove godine. Zbog postojanja osnova sumnje da su učestvovali u izvršenju navedenih događaja

prijavljeni su mldb. Ć.H. (2010), kao i O.M. (1995), Đ.E. (1999), Č.E. (1969), B.M. (1974) i T.A. (1981). Preduzimaju se aktivnosti na rasvjetljavanju ostalih događaja i pronalaženju počinioca (MUP KS-Izvještaj o radu UP za 2023. godinu).

U 2024. godini evidentirano je 569 anonimnih dojava o postavljenim eksplozivnim napravama (449 ili 374,2% više u odnosu na 2023. godinu), od čega se 541 odnosila na osnovne i srednje škole na području Kantona Sarajevo, 10 na sudove na području općina Centar i Novi Grad od čega su se dvije odnosile i na zgradu Kantonalnog tužilaštva Kantona Sarajevo, pet na Dom zdravlja Ilidža, tri na ugostiteljske objekte na području općina Vogošća i Ilidža, tri na tržne centre na području općina Centar i Novo Sarajevo, dvije na prostoriju Fondacije Konrad Adenauer, jedna na stambeni objekat na području općine Stari Grad, dok su se preostale četiri odnosile na: osnovne škole na području Federacije Bosne i Hercegovine dvije, na zgradu Predsjedništva BiH i Međunarodni aerodrom Sarajevo – po jedna. Za navedene događaje izvršena su 443 PDZ pregleda u kojima je utvrđeno da su dojave bile lažne (MUP KS-Izvještaj o radu UP za 2024. godinu).

Najčešće mete ovih dojava bile su pravosudne i obrazovne institucije, zdravstvene ustanove i ugostiteljski objekti. Policija je do sada rasvijetlila sedam krivičnih dijela, a neki od počinilaca su već procesuirani. Kada se priča o lažnim dojavama, važno je ne gledati ih kao pojedinačne slučajeve koji se dešavaju nasumično. U stvarnosti, često postoji obrazac, a oni koji se time bave ozbiljno, znaju koliko je korisno tragati za tim ponavljanjima. Statistika tu zna biti vrlo rječita. Primjećeno je, recimo, da se lažne dojave češće javljaju u određenim danima u sedmici ili u tačno određenim dijelovima dana kao da neko cilja trenutke kada su institucije najranjivije ili kada se očekuje najveća reakcija.

Nisu rijetke ni sezonske oscilacije. U školskim ustanovama, na primjer, "bombe" se nekim čudom pojavljuju baš u vrijeme testova ili ispita. Geografski gledano, postoje lokacije koje su očigledno "popularnije" za ovakve manipulacije. Tržni centri, škole, opštinske zgrade, sudovi sve su to mete koje izazivaju maksimalnu pažnju javnosti i institucija. Analizom lokacija može se naslutiti i vrsta motiva, pa čak i moguće pozadinske namjere. Kada se lažne dojave podudaraju sa važnim događajima recimo, velikim političkim skupovima, osjetljivim sudskim procesima ili predizbornim kampanjama teško je povjerovati da je u pitanju slučajnost. Ponekad je cilj da se odvuče pažnja, a nekad da se izazove haos baš kada društvo pokušava da funkcioniše na visokom stepenu organizacije.

6. ZAKLJUČAK

Lažne dojave o postavljenim eksplozivnim napravama predstavljaju ozbiljan sigurnosni izazov koji prevazilazi okvir pojedinačnih incidenata, zadirući u samu strukturu javne sigurnosti. Iako formalno spadaju u domenu krivičnih djela protiv javnog reda i mira, njihova funkcionalna šteta mnogo je dublja: remete operativne kapacitete interventnih službi, izazivaju kolektivnu anksioznost i narušavaju institucionalni autoritet. U kontekstu savremenih sigurnosnih prijetnji, posebno onih koje dolaze iz sfere terorizma, ovakve dojave dodatno komplikuju operativnu realnost ne samo da resursi bivaju raspršeni, već se gubi dragocjeno vrijeme koje bi, u situacijama stvarne ugroženosti, moglo predstavljati razliku između prevencije i tragedije. Uočen je i snažan korelativni odnos između porasta ovakvih incidenata i specifičnih društvenih okolnosti predizborni periodi, sudski procesi visokog profila, te važne društvenopolitičke manifestacije nerijetko služe kao vremenski okidači za aktivaciju lažnih prijava. Cilj je skretanje pažnje, izazivanje panike ili narušavanje funkcionalnosti institucionalnih mehanizama. Etiologija ovog fenomena nije jednoznačna. Uočavaju se različiti motivacioni obrasci od adolescenata koji kroz antisocijalne akte traže pažnju, preko pojedinaca sa psihopatološkim poremećajima, do svjesnih aktera sa jasnim instrumentalnim ciljevima. Takvi činovi, osim što mogu predstavljati element manipulativne taktike u okviru političkoideoloških konflikata, često nose i implikacije koje nadilaze domet prvobitne namjere.

U cilju minimizacije ovih incidenata, neophodno je sprovesti višeslojnu strategiju prevencije. To podrazumijeva unapređenje obuke profesionalnog kadra iz oblasti forenzike i kriznog upravljanja, uvođenje savremenih softverskih alata za procjenu vjerodostojnosti prijetnji i uspostavljanje strožih zakonskih mehanizama represije i sankcionisanja. Pored institucionalne odgovornosti, neophodna je i aktivnija uloga medija. Neodgovorno i senzacionalističko izvještavanje dodatno podiže prag straha, umanjuje osjećaj kontrole kod građana i doprinosi društvenoj fragmentaciji. Zato medijski prostor mora biti tretiran kao instrument bezbjednosti, a ne kao arena za poticanje panike. Naposljetku, bezbjednost nije isključivo domen institucija, već zajednički društveni projekat. Potrebno je jačati kolektivnu svijest o ozbiljnosti lažnih dojava i educirati populaciju, naročito kroz formalne obrazovne kanale, o pravnim i etičkim reperkusijama ovakvog ponašanja. Ukoliko želimo dugoročno očuvati otpornost društva na sigurnosne devijacije, važno je da se osim represivnih razvijaju i proaktivne politike. One uključuju razvoj prediktivnih modela za identifikaciju visokorizičnih obrazaca ponašanja, kao i promociju kulture odgovornosti na svim nivoima. Borba protiv lažnih dojava ne počinje u trenutku kada telefon zazvoni ona počinje u kulturi, obrazovanju i institucionalnoj spremnosti da razlikuje šalu od strategijski plasirane prijetnje.

LITERATURA

1. Bishop, C.M. (2006), Pattern Recognition and Machine Learning, Springer
   Nature.
2. Garrison, J., McManus, T. (2014). The Psychology of False Threats: Understanding the Social and Political Motivations. Journal of Security Studies.
3. Hoffman, B. (2006). Inside Terrorism. Columbia University Press.
4. Hastie, T., Tibshirani, R., Friedman, J. (2001), The Elements of Statistical Learning, Springer Nature.
5. James, G., Witten, D., Hastie, T., Tibshirani, R. (2013). Introduction to Statistical Learning, Springer Nature.
6. Korajlić, N., 2003. Kriminalistička obrada kod ubistva, Fakultet kriminalističkih nauka, Sarajevo: Magistrat.
7. LaFree, G., Dugan, L. (2007). The Impact of Terrorism on the Public's Trust in Government, Journal of Politics,
8. Smith, R. T. (2017) Terrorism and CounterTerrorism: A Security and Intelligence Perspective, Routledge.
9. Zaštita i sigurnost, godina 1., broj 1. (2021).
10. Zaštita i sigurnost, godina 4., broj 2. (2024).

Elektronski izvori:

1. Ministarstvo unutrašnjih poslova Kantona Sarajevo, Izvještaj o radu UP za 2023. godinu, str.11, (https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/202502/informacija preuzeto 16.2.2025. godine).
2. Ministarstvo unutrašnjih poslova Kantona Sarajevo, Izvještaj o radu UP za 2024. godinu, str.11, (https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/202502/preuzeto 18.2.2025. godine).

ABUSE OF FALSE BOMB THREATS A THREAT TO REAL SECURITY

DOI: *10.70329/2744-2403.2025.5.9.6*

Review scientific article

Doc.dr. Zoran Lakić [(1)]
Doc.dr. Zoran Kovačević [(2)]

Abstract:

False reports of planted explosive devices represent an increasingly pronounced security challenge in modern society. Although at first glance they may seem like harmless disturbances, such actions in reality provoke a wide range of consequences from undermining citizens' sense of security to seriously straining the resources of security and emergency services. The fact that such reports cannot be immediately classified as unfounded requires a prompt and comprehensive response from the relevant institutions, often involving specialized units and high value equipment. This paper examines how the abuse of the reporting system affects the operational readiness of security structures and what long term implications it has on public and financial flows. Also, statistical data from the Ministry of Internal Affairs of Sarajevo Canton for 2023 and 2024 will be analyzed, with the aim of gaining a deeper understanding of the dynamics of this issue and its impact on the daily lives of citizens and institutional response.

Keywords*: False alerts, special teams, security, terrorism, public safety threats.*

[(1)]. Victoria International University Mostar, email: zoran.lakic@viu.ba
[(2)]. Higher Business Technical School Doboj, email: zoran.kovacevic@dkpt.gov.ba

1. INTRODUCTION

False reports of planted explosive devices have become a serious security problem, with the potential to escalate into a widespread social phenomenon with multiple negative consequences. Increasingly motivated by various reasons, these reports not only drain the resources of security services but also cause psychological stress among citizens, which significantly undermines trust in the institutions responsible for maintaining public safety. In a modern context, where the speed of information flow is crucial, such reports can significantly disrupt the work of institutions tasked with responding to real threats. Although seemingly harmless, false reports can cause widespread social chaos, citizen unrest, and the diversion of significant resources towards searches that ultimately prove unjustified. The problem lies not only in causing panic but also in creating an illusion of danger, while real threats may be overlooked. False reporting is not just a misunderstanding or a harmless joke; it is an intentional act aimed at instilling fear, panic, and destabilizing the system. Such reports can be made through various channels, including phone calls, anonymous electronic messages, and social media posts. A special challenge is the use of modern technologies to spread disinformation, which further complicates the identification of actual threats and the adequate response of relevant institutions. Although a false alarm does not mean that an explosive device is really placed, it significantly disrupts daily life, causes a sense of insecurity, and creates a distorted picture of the real danger. This phenomenon cannot be considered a harmless act; on the contrary, it is often used as a means of political or social protest. Although the motives vary, the consequences are concrete and serious, including high costs of engaging specialized units, such as demining teams, which are responsible for detecting and neutralizing potential threats. In addition to material damage, frequent alarms can weaken the seriousness of institutional response at times when a real threat actually exists. The overload of services due to repeated false alarms leads to a decrease in their efficiency and an erosion of public trust in the protection system. Each new false report further complicates the distinction between real and imagined threats. Special attention should be paid to precisely defining the concept of a false report. A false report represents the conscious and intentional deception of authorities regarding the placement of an explosive device, without any real threat present. The motivation can be political, ideological, social, psychological, or even trivial, such as the need for attention or provoking disorder. Regardless of the cause, the consequences remain serious and multifaceted. In this context, it is also important to mention improvised explosive devices (IEDs), which, although not industrially manufactured, have the capacity to cause significant material damage and human casualties.

Such means are often used in terrorist attacks, and even false alarms regarding their use can serve as instruments of political pressure, intimidation, or destabilization. A false report of a planted explosive device encompasses a conscious and intentional attempt to provoke panic, fear, or distress among people, thereby unnecessarily mobilizing resources that would otherwise be directed towards real threats. These reports can come in various forms from phone calls to anonymous emails or messages on social media, with a particularly concerning trend of using modern technology and media channels to spread misinformation (Smith, R. T., 2017). When considering the phenomenon of false reports about explosive devices, it is crucial to understand the need for the development of effective prevention and response strategies in order to reduce harmful consequences and better protect the resources of security services. Rapid identification of false threats allows real dangers not to be neglected, thereby directly protecting human lives and preserving the stability of the security system. Risk assessment, i.e. threats is carried out in accordance with the Risk Assessment Matrix according to the general criteria of the level of risk, i.e. probability and consequences in relation to it (Hasović, L., 2021).

2. THEORETICAL FRAMEWORK AND ISSUES

False reports of planted improvised explosive devices (IEDs), as well as other types of false alarms, create a real security dilemma. In a society increasingly faced with rapid information flows, false reports become a serious problem, not only due to compromised safety but also because of the panic they provoke. This phenomenon is not merely a matter of threat recognition, as it involves a complex situation where it is crucial to balance between identifying real dangers and mitigating the harm caused by false calls. When we examine the existing research on this topic, we come to a clear conclusion that false reports reflect broader social and psychological issues. A significant number of researchers have addressed the motives behind these incidents, as well as the consequences they have on society. Not all works in this field are aimed solely at technical and security aspects; many researchers, such as Garrison and McManus, consider the psychological and social roots that drive individuals to make such decisions (Garrison, J., & McManus, T., 2014). It turns out that behind most false alarms are problems that are not always obvious at first glance and are often connected to personal, political, or even ideological reasons. The question of how the law responds to such actions is no less important. Most countries, including Bosnia and Herzegovina, have clearly defined penalties for making false danger reports. In our legislative framework, making a false report about planted explosive devices can result in a prison sentence of up to 5 years, along with enormous costs associated with the engagement of specialized teams. And the costs are not only monetary, as the long-term consequences in terms of loss of time and resources

are significant. Memories of historical incidents, such as the one from 2001 in New York, where a false alarm triggered the evacuation of more than 10,000 people, remind us of how far-reaching the consequences of such incidents can be. Although numerous, such events remain challenging to analyze, as with each new case, there is a broader use of technologies, primarily social media, as a means of spreading misinformation. Several cases in recent years show how false alarms are becoming more frequent. In 2019, there were numerous false alarms about explosives planted in schools in Italy, which shook the education system and put additional pressure on law enforcement. When data and information indicate that there are grounds for suspicion (Korajlić, 2003) that a criminal offense has been committed for which prosecution is mandatory, police action must be systematic and carried out through the recording of data and information, their expert assessment, making decisions on actions, as well as verifying data and information, with the aim of collecting material and other evidence. Threats that are not real often lack sufficient concrete information, which directs security resources in the wrong direction. Even in cases where false alarms are obvious, the consequences, such as panic or excessive resource mobilization, can be serious. To minimize these problems, it is essential to develop more precise mechanisms for identifying and recognizing false alarms, as well as to invest in training teams to confront similar challenges. Together with advanced technology, which is capable of increasing the speed of threat recognition, it should be ensured that society is better prepared to face all kinds of security challenges. For example, authors such as Garrison and McManus explore the psychological motives that lead to the abuse of reporting systems, emphasizing that often behind such reports lie social problems, as well as political and ideological ambitions (Garrison, J., & McManus, T., 2014).

3. SYSTEM UNDER SIEGE OF DISINFORMATION - FUNCTIONAL WEAKNESS AND REACTION

False bomb threats may sound like an old phrase, but the reality is far more serious. Such incidents are not just "abuse of the system"; they strike at its core. And every time someone raises a false alarm, machinery is set in motion that consumes time, resources, and patience. Some do it out of anger or frustration, some for attention. Some want to divert focus from something else. There are also those who play a more serious game, wanting to stop some company, cause damage to the competition, or disrupt an event. Nevertheless, regardless of the reason, the consequences are always real. The first line of impact is the police and security services. Every report, without exception, must be taken seriously. And that means anti-diversion teams are deployed, traffic and streets are closed, schools, courts, and shopping centers are evacuated. And when it turns out that it was all "nothing," there is still a bill to be paid, along with the stress above which

hovers a sense of insecurity. The problem is that such cases burden the system. Police officers who could be working on real threats are now losing hours on something that doesn't exist. And which may have intentionally diverted them in the wrong direction. Every false alarm is essentially a kind of sabotage not only of the system but also of common sense. Special teams require specialized equipment, ongoing training, and mobility. None of this is cheap. Organizing field interventions, accommodation, logistics, and other activities all contribute to a budget deficit. On top of all this, there are other services that are engaged in parallel: local police, medical teams, because everyone must be ready, even when it's not real. And the damage is not just measured in money. False alarms disrupt everyday life. Schools, businesses, and shopping centers are closed. People are thrown out of their routines, panic spreads, and an atmosphere of insecurity slowly seeps through the cracks of everyday life. And worst of all, getting used to such things can be even more dangerous than the alarms themselves. Therefore, a combination of everything is needed through an institutional response, laws that are not to be taken lightly, education that goes beneath the surface. Because this is not a problem that will resolve itself. Perhaps the biggest problem is that the system still reacts as if it trusts everyone. And that's both beautiful and dangerous. Beautiful because it shows that we do not ignore threats. Dangerous because those who know how to exploit that do so. The moment the system stops trusting, we all lose.

4. THE CONNECTION BETWEEN FALSE ALERTS AND TERRORISM

Terrorism as a concept does not have a single universal definition, but is most commonly described as the use of violence or serious threats of violence against civilians, in order to achieve political, ideological, or religious goals. The essence of terrorist action is not only in causing physical harm but in creating an atmosphere of fear, insecurity, and pressure on authorities or the wider public to change their behavior, laws, or attitudes. Terrorism experts and countries fighting terrorism agree that it will be very difficult to determine a definition of terrorism that would be recognized by all countries of the world, but they also agree that without it, a successful international fight against terrorism cannot be waged (Lakić, Z., Kovačević Z, 2024). In this light, false bomb threats can be, under certain circumstances, viewed as part of a broader security problem. They do not carry explosives, but can undermine trust and the capacities of the system. Seemingly trivial, these alerts actually disrupt the work of institutions, waste resources, and complicate the identification of real threats. When security agencies are overwhelmed with investigations that ultimately turn out to be false, the risk increases that a real danger goes unnoticed. One of the serious problems

is that over time, a 'false alarm' effect is created, so each subsequent report may be taken less seriously. And that is exactly what someone planning a real attack can exploit. The system becomes saturated, attention dulls, and that is ideal ground for surprise. Overloading the system with false reports can reduce the authorities' ability to respond to real threats, thus creating vulnerability to terrorist attacks (Hoffman, B., 2006). It is not uncommon for the number of false reports to increase before elections, especially during politically tense periods. Some analysts see this as an attempt at destabilization, redirecting public attention, and even deliberately provoking distrust in institutions. When this coincides with voting days or key political events, suspicion of underlying motives is not unfounded. Additionally, false reports at such times can be a tool of manipulation or even diversion. While security services are busy with evacuations and searches, other actions may go under the radar. In any case, the effect is the same: the system is overwhelmed, and citizens trust is shaken. Those who send fake bomb threats are often not classic criminals. Many of them come from backgrounds of emotional instability, personal frustration, or social exclusion. Their motivations can be diverse, ranging from a need for attention, a desire for revenge, to attempts to test the system. In some cases, they are adolescents or young individuals who do not grasp the gravity of their actions. In others, they are planned and targeted attempts to provoke chaos or distract from something else. It is also often referred to as operational narcissism, where individuals falsely present themselves as fighters against injustice, but actually instrumentalize chaos to feel powerful. In politically or socially polarized societies, these motivations can easily ignite, so it's not surprising that the number of false reports rises when the social temperature is high. If this problem is approached seriously, it must be viewed in all dimensions: security, political, psychological, and social. They reflect the state of society, that is, how vulnerable it is, how much trust it has in institutions, and how ready we are to respond maturely. And the fight against this is not just a matter of laws and penalties. Education, responsible reporting, efficient coordination of services, and perhaps most difficult, the creation of a culture in which safety is not just someone else's responsibility, are needed.

5. STATISTICAL INDICATORS OF THE MINISTRY OF INTERIOR OF SARAJEVO CANTON FOR 2023 AND 2024

During the year 2023, 120 cases of anonymous reports about the placement of explosive devices were recorded, relating to courts, prosecutor's offices, municipalities, educational institutions, hospitality establishments, banks, and hotels. After the special teams inspection, it was determined that the reports were false, except for the anonymous report about an explosive device placed in a hospitality establishment, where special teams found two hand grenades in the

basement premises. Out of the total of 120 anonymous reports about placed explosive devices, six incidents were clarified, namely four from April and one each from June and July of this year. Due to the existence of grounds for suspicion that they participated in the execution of the mentioned incidents, the following individuals were reported: juvenile Ć.H. (2010), as well as O.M. (1995), Đ.E. (1999), Č.E. (1969), B.M. (1974), and T.A. (1981). Activities are being undertaken to clarify the other events and to locate the perpetrators (MUP KS- Report on the work of the UP for 2023. In the year 2024, 569 anonymous reports of planted explosive devices were recorded (449 or 374.2% more compared to the year 2023), of which 541 referred to primary and secondary schools in the Sarajevo Canton, 10 to courts in the municipalities of Centar and Novi Grad, of which two referred to the building of the Cantonal Prosecutor's Office of Sarajevo Canton, five to the Health Center Ilidža, three to hospitality establishments in the municipalities of Vogošća and Ilidža, three to shopping centers in the municipalities of Centar and Novo Sarajevo, two to the premises of the Konrad Adenauer Foundation, one to a residential building in the municipality of Stari Grad, while the remaining four referred to: two primary schools in the Federation of Bosnia and Herzegovina, one to the building of the Presidency of Bosnia and Herzegovina, and one to Sarajevo International Airport. For the reported incidents, 443 special teams inspections were carried out, which determined that the reports were false (Ministry of Internal Affairs KS - Report on the work of the UP for 2024). The most common targets of these reports have been judicial and educational institutions, health care facilities, and hospitality establishments. The police have so far solved seven criminal offenses, and some of the perpetrators have already been prosecuted. When talking about false reports, it is important not to view them as individual cases happening randomly. In reality, there is often a pattern, and those who deal with this seriously know how useful it is to look for these repetitions. Statistics can be very telling in this regard. For example, it has been noticed that false reports are more frequently made on certain days of the week or at specific times of the day, as if someone is targeting moments when institutions are most vulnerable or when the greatest reaction is expected. Seasonal fluctuations are not rare either. In educational institutions, for instance, 'bombs' mysteriously appear exactly during test or exam times. Geographically, there are locations that are obviously 'more popular' for such manipulations. Shopping centers, schools, municipal buildings, courts - all of these are targets that attract maximum attention from the public and institutions. Analyzing the locations can also suggest the type of motives, and even possible underlying intentions. When false alarms coincide with important events, for instance, major political gatherings, sensitive court processes, or election campaigns, it is hard to believe that it is a coincidence. Sometimes the goal is to distract attention, and sometimes to cause chaos precisely when society is trying to function at a high level of organization.

6. CONCLUSION

False reports of planted explosive devices represent a serious security challenge that transcends the framework of individual incidents, intruding into the very structure of public safety. Although they formally fall under the domain of criminal offenses against public order and peace, their functional damage is much deeper: they disrupt the operational capacities of response services, provoke collective anxiety, and undermine institutional authority. In the context of modern security threats, especially those arising from the sphere of terrorism, such reports further complicate the operational reality; not only are resources dispersed, but precious time is also lost, which, in situations of real danger, could make the difference between prevention and tragedy. A strong correlational relationship has been observed between the increase in such incidents and specific social circumstances, such as election periods, high-profile court trials, and significant socio-political events, which often serve as temporal triggers for activating false reports. The aim is to draw attention, provoke panic, or disrupt the functionality of institutional mechanisms. The etiology of this phenomenon is not uniform. Various motivational patterns can be seen, ranging from adolescents seeking attention through antisocial acts, to individuals with psychopathological disorders, to conscious actors with clear instrumental goals. Such acts, besides potentially representing an element of manipulative tactics within political-ideological conflicts, often carry implications that go beyond the scope of the original intention. In order to minimize these incidents, it is necessary to implement a multi-layered prevention strategy. This includes enhancing the training of professional staff in the fields of forensics and crisis management, introducing modern software tools for assessing the credibility of threats, and establishing stricter legal mechanisms for repression and sanctioning. In addition to institutional responsibility, a more active role for the media is also necessary. Irresponsible and sensationalist reporting further raises the threshold of fear, diminishes the sense of control among citizens, and contributes to social fragmentation. Therefore, the media space must be treated as a security instrument, not as an arena for inciting panic. Finally, security is not solely the domain of institutions but a collective societal project. It is necessary to strengthen the collective awareness of the seriousness of false alarms and to educate the population, especially through formal educational channels, about the legal and ethical repercussions of such behavior. If we want to preserve the resilience of society to security deviations in the long term, it is important to develop not only repressive but also proactive policies. These include the development of predictive models for identifying high-risk behavioral patterns, as well as promoting a culture of responsibility at all levels. The fight against false alarms does not begin the moment the phone rings; it starts in culture, education, and institutional readiness to distinguish between a joke and a strategically placed threat.

LITERATURE

1. Bishop, C.M. (2006), Pattern Recognition and Machine Learning, Springer Nature.
2. Garrison, J., McManus, T. (2014). The Psychology of False Threats: Understanding the Social and Political Motivations. Journal of Security Studies.
3. Hoffman, B. (2006). Inside Terrorism. Columbia University Press.
4. Hastie, T., Tibshirani, R., Friedman, J. (2001), The Elements of Statistical Learning, Springer Nature.
5. James, G., Witten, D., Hastie, T., Tibshirani, R. (2013). Introduction to Statistical Learning, Springer Nature.
6. Korajlić, N., 2003. Criminal Investigation in Homicide, Faculty of Criminal Sciences, Sarajevo: Magistrate.
7. LaFree, G., Dugan, L. (2007). The Impact of Terrorism on the Public's Trust in Government, Journal of Politics.
8. Smith, R. T. (2017) Terrorism and CounterTerrorism: A Security and Intelligence Perspective, Routledge.
9. Protection and security, year 1, number 1 (2021).
10. Protection and security, year 4, number 2 (2024).

Electronic sources:

1. Ministry of Internal Affairs of Sarajevo Canton, Report on the work of the UP for the year 2023, p.11, (https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/202502/information retrieved on February 16, 2025).

2. Ministry of Internal Affairs of Sarajevo Canton, Report on the work of the UP for the year 2024, p.11, (https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/202502/retrieved on February 18, 2025).

PSIHOLOŠKE OPERACIJE NA DRUŠTVENIM MREŽAMA – PRIMJERI, TEHNIKE, TAKTIKE I PROCEDURE

DOI: *10.70329/2744-2403.2025.5.9.7*

Naučni rad

Emir Muhić, MA

Sažetak:

Ovaj rad istražuje transformaciju ratovanja i sigurnosnih sukoba pod utjecajem savremenih tehnoloških dostignuća, s posebnim naglaskom na ulogu društvenih mreža u provođenju psiholoških operacija (PSYOP). Analiziraju se 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, rad raspravlja o sigurnosnim implikacijama za nacionalne institucije i demokratski poredak. Također se predlažu smjernice i preporuke za izgradnju otpornosti društva na psihološke prijetnje koje proizlaze iz informacijskog prostora. Cilj rada je pružiti dublje razumijevanje uloge društvenih mreža u suvremenom psihološkom ratovanju i ukazati na potrebu za proaktivnim institucionalnim odgovorima.

Ključne riječi*: psihloške operacije, specijalni rat, propaganda, dezinformacije, nekonvencionalno ratovanje*

Uvod

Moderno tehnološko vrijeme, uveliko je promijenilo načine borbe i vođenja rata. Konvencionalni pristup ratu, zasnovan samo na oružju i velikim bitkama nikada nije bio dovoljan, te su komandanti težili da prije glavnog napada, utječu psihloški, kako na neprijatelja, tako i na svoje vojnike. Značaj psihološkog stanja i statusa neprijatelja u pogledu njegove volje za borbom je kolosalan, te se shodno njemu važne bitke dobijaju ili gube. Evolucijom ljudske civilizacije i tehnologije, desio se „transfer" ljudskog života iz realnog u apstraktni cyber prostor, koji je postao neizostavan i važan dio funkcionisanja stanovništva širom planete Zemlje. Internet tehnologija omogućava spajanje udaljenih, širenje vijesti i informacija, ali se u navedenom krije i mogućnost manipulacije umom i načinom razmišljanja svakog misaonog bića. Stoga, uloga društvnih mreža nije samo da spoji, približi i informiše, već i da utječe na stavove i mišljenja. U posljednjem desetljeću, društvene mreže su postale jedno od značajnijih oružja iz domena savremenog psihološkog ratovanja i operacija (u nastavku teksta kao PSYOP).

Društvene mreže igraju ključnu ulogu u savremenim psihološkim operacijama, omogućavajući brzo širenje dezinformacija i manipulaciju percepcijom ciljane publike. Korištenje društvenih mreža za psihološke operacije značajno utječe na oblikovanje javnog mišljenja i stavova ciljane publike pri čemu se omogućava provođenje agresivnih državnih ili nedržavnih politika. Strategije i taktike na društvenim mrežama u psihološkim operacijama razvijaju se u skladu s promjenama u digitalnom okruženju i vanjskoj politici države te se prilagođavaju promjenama u algoritmima i pravilima društvenih mreža. Zbog navedenog, sigurnosne institucije, kao i državni rukovodni kadrovi, moraju razviti sveobuhvatne strategije za borbu protiv psiholoških operacija na društvenim mrežama kako bi zaštitili državu i društvo.

1. Psihološke operacije i društvene mreže

Psihološke operacije predstavljaju značajan aspekt vojne doktrine i strategije usmjerene protiv neprijatelja. Historijski gledano, ne postoji niti jedan period u kojem plemena, carstva ili imperije nisu koristile određeni oblik utjecaja na vlastitu vojsku i stanovništvo ili na neprijatelja. Danas, psihološke operacije koriste drugačije moduse, te su bazirane na varijablama kao što su tehnologija, politika, kultura, narativi. Bez upotrebe psiholoških operacija i pratećih aktivnosti, ne bi bilo moguće pobijediti neprijatelja te nametnuti vlastitu volju.

1.1. Definisanje i razumijevanje aktivnosti psiholoških operacija

Kada se govori o definisanju psiholoških operacija, postoji mnoštvo definicija koje su specifične za državne i nedržavne aktere širom svijeta. Zbog standardizacije termina i boljeg razumijevanja onoga o čemu se govori, u svrhu istraživanja će se koristiti navedene definicije:

1. Psihološke operacije (PSYOP) su planirane operacije koje koriste selektirane informacije i povratne mehanizme kako bi utjecale na osjećaje, stavove, percepciju i ponašanje ciljane publike kako bi podržale postizanje ciljeva državne politike, vojnih ciljeva i planova te kako bi promicale zajedničke interese (U.S. Department of Defense, 2014).
2. Psihološke operacije (PSYOPS) su namjerno planirane aktivnosti koje se provode kako bi se ciljanoj publici prenijela određena poruka, promijenio njezin stav prema određenim pitanjima ili potaknula na određene akcije (NATO Standardization Agency , 2013).
3. Planirane, kulturno osjetljive, istinite i pripisive aktivnosti koje koriste metode komunikacije usmjerene na politički odobrenu ciljnu publiku, kako bi se utjecalo na percepcije, stavove i ponašanje u potpori postizanja političkih i vojnih ciljeva EU-a (European External Action Service (EEAS), 2020).

Kada se govori o zapadnom konceptu PSYOP-a, američki *policy makeri* su shvatili da termin „psihološke operacije" imaju negativnu konotaciju ili da nisu u skladu sa modernim vremenom, te je izvršeno preimenovanje. Američko Ministarstvo odbrane je preko institucije Zajedničkog načelnika štaba[1] izvršilo reviziju termina psiholoških operacija u operacije vojne informacijske potpore (MISO) koje predstavljaju: *planirane operacije prenošenja odabranih informacija i pokazatelja stranoj publici kako bi se utjecalo na njihove emocije, motive, objektivno razmišljanje i na kraju na ponašanje stranih vlada, organizacija, skupina i pojedinaca na način koji je povoljan za ciljeve autora* (Joint Chiefs of Staff (JCS), 2010).

Kada se posmatra Rusija, tu dolazi do jezičkog i ideološkog razilaženja. Naime, Rusi ne koriste zapadni termin „psihološke operacije", već termin „informacijsko - psihološke aktivnosti" (Thomas, 1997) i termin informaciono ratovanje koji predstavlja širi spektar djelovanja i poduzimanja aktivnosti iz domena informacijskog i informativnog (Giles, 2016). Kako navodi Mshvidobadze (2011) za Radio slobodna Europa, ovaj koncept u sebi nosi operacije računalne mreže uz discipline kao što su psihološke operacije (PsyOps), strateške komunikacije, utjecaj, zajedno s "obavještajnim radom, protuobavještajnim radom, *maskiranjem*, dezinformacijama, elektroničkim ratovanjem, slabljenjem komunikacija, degradacijom navigacijske podrške, psihološkim pritiskom, i uništavanje neprijateljskih računalnih sposobnosti." Shodno tome, to čini "cjelinu sistema, metoda i zadataka za utjecaj na percepciju i ponašanje neprijatelja, stanovništva i međunarodne zajednice na svim razinama" (Selhorst, 2016).

[1] Zajednički načelnici štabova – predstavlja tijelo je najviših uniformiranih čelnika unutar Ministarstva odbrane Sjedinjenih Država, koje savjetuje predsjednika Sjedinjenih Država, ministra odbrane, Vijeće domovinske sigurnosti i Vijeće nacionalne sigurnosti o vojnim pitanjima.

Specifična svrha psiholoških operacija (PSYOP) je utjecati na percepciju strane publike i naknadno ponašanje kao dio odobrenih programa podrške američkoj politici i vojnim ciljevima. PSYOP profesionalci slijede promišljen proces koji usklađuje zapovjednikove ciljeve s analizom okoline; odabrati relevantnu ciljnu publiku; razvijati usmjerene, kulturno i ekološki usklađene poruke i akcije; koristiti sofisticirana sredstva za isporuku medija i proizvesti vidljive, mjerljive reakcije ponašanja (Joint Chiefs of Staff (JCS), 2010). Također, zvanični web sajt američke Komande za specijalne operacije (US Army Special Operations Recruiting, 2023) govori na sljedeći način o aktivnostima PSYOP jedinica: „*Oni analiziraju operativna okruženja, fizičke mete i ciljanu publiku; savjetovati o psihološkim učincima; opcije utjecaja na plan; razviti radnje i poruke usmjerene na psihološke ranjivosti; dostaviti radnje i poruke u optimalno vrijeme; i procijeniti učinkovitost utjecaja. Djelujući u malim, autonomnim timovima, PSYOP jedinice provode operacije vojne informacijske potpore; Obmanjujuće aktivnosti Ministarstva obrane; izgraditi sposobnost utjecaja partnera; i, kada to predsjednik zatraži, pružiti informacijsku podršku civilnim vlastima*."

Dakle, psihološke operacije imaju jedan cilj, a to je utjecati na mišljenje stanovništva, bilo vlastitog, neprijateljskog ili neutralnog.

1.2. Primjeri psiholoških operacije kroz historiju

Psihološke operacije su u konceptu ratovanja predstavljale snažan i odlučujući faktor za pobjedu svake vojske. Svrha psiholoških operacija može biti izazovanje straha kod protivnika, umanjenje njegove želju za borbom i stvoriti kompleks inferiornosti u odnosu na protivnika. Modernizacijom i razvojem tehnologije, egzotične životinje (slonovi koje je koristio Hanibal Barka u borbi protiv Rima), kao i metode mučenja (nabijanja na kolac od strane Valda Tepeša) nisu mnogo izazivale strah kod pritivnka, te je bilo potrebno promijeniti pristup istom. Navedeno se nastojalo postignuti novim oružjem, ali i pisanom riječju, naročito u periodu Prvog i Drugog svjetskog rata. Kada je riječ o oružju, strah kod protivnika se izazivao korištenjem bojnih otrova od strane Njemačke ili upotrebe sačmarica u rovovima od strane Amerikanaca. Kada se govori o nenasilnim metodama, primat su imali Britanci koji su nastojali da pamfletima i drugom propagandom utječu na borbeni duh Njemaca (Fridman, Kabernik, & Granelli, 2022). Usmjerenje britanske vlade u ovom ratnom periodu je bilo na tri *fronta*: prema vlastitom stanovništvu, saveznicima i neutralnim akterima, te neprijatelju. Britanska vlada u početku se usredotočila na patriotsku propagandu kod kuće, dok je istovremeno pripremala zemlju za rat i borila se protiv domaće antiratne opozicije (Fridman, Kabernik, & Granelli, 2022). Na ovaj način je omogućeno da vlastito stanovništvo ne poklekne duhom, te da se održi nacionalni integritet i jedinstvo. Ukoliko se navedeno ne bi održalo, antiratni krugovi i neprijateljski agenti od utjecaja bi izvojevali pobjedu bez velikih materijalno-tehničkih

ulaganja. Odnosno, prema riječima Sun Cua, postigli bi najsavršeniju pobjedu, onu koja podčinjava neprijatelja bez oružane borbe.

Primjer iz Drugog svjetskog rata koji je ukazao na važnost propagandnog djelovanja na tradicionalnim medijima – radiju, bila je operacija „Aspidistra" izvedena od strane tijela nazvanog *Political Warfare Executive*. Operacija je bila zasnovana na obmani, širenju tzv. crne propagande. Britanci su se predstavljali kao njemci, dajući lažne informacije. Drugi dio operacije se zasnivao na vojnoj obmani, te kao dio svojih strategija pogrešnog usmjeravanja njemačkih lovaca, operateri RAF-a[2] koji govore njemački oponašali su te njemačke operatere zemaljske kontrole, šaljući lažne upute noćnim lovcima (Newton, 2019). Usmjeravali su noćne lovce da slete ili da se premjeste u pogrešne sektore. Ovo ometanje neprijateljskih radio i bežičnih transmisija bilo je poznato pod kodnim imenom "Dartboard" (RAF Upwood, 2002).

Naredni primjer psihološke operacije jeste upotreba muzike, što je bilo karakteristčno za američke trupe u Vijetamu, Panami i Iraku. Kada se govori o Vijetnamu, prije i u toku zračnog desanta, američke trupe su puštale rok muziku na razglasima koji su se nalazili na helikopterima. Ovaj akt je bio više usmjeren ka ohrabrivanju vlastitih trupa, nego zastrašivanju ideološki jakih vijetnamskih komunista. Drugi način psihološkog utjecaja na protivnika je bio i puštanje sablasnih krikova noću, usmjerenih prema neprijatelju. Snimka, poznata kao *Ghost Tape Number 10*, odigrala je središnju ulogu u operaciji *Wandering Soul*, psihološkoj operaciji koja je nastojala slomiti moral sjevernovijetnamskih vojnika iskorištavanjem njihovih umova i njihovih najdubljih strahova (Humphrey, 2023). Snimka se zasnivala na kricima i rečenicama: „*Moje tijelo je nestalo. Ja sam mrtav, moja obitelj. Tragično, kako tragično! Prijatelji moji, vraćam se da vam javim da sam mrtav. Ja sam mrtav. Ja sam u paklu. ... Prijatelji, dok ste još živi ... idite kući! ... Idite kući, prijatelji moji — prije nego što bude prekasno*. (Humphrey, 2023) " Izbor ovih riječi se zasnivao na kulturološkim i religijskim postavkama, odnosno na budističkom vjerovanju da duše onih koji nisu sahranjeni na adekvatan način, lutaju među živima u boli cijelu vječnost.

Druga upotreba zvuka i muzike je bila karakteristična za Panamu i Irak, kada su američke trupe puštale glasnu glazbu u pokušaju da navedu panamskog predsjednika Manuela Norriegu na predaju, korištenje "akustičnog bombardiranja" postalo je standardna praksa na bojištima u Iraku, a specifično glazbeno bombardiranje pridružilo se senzornoj deprivaciji i seksualnom ponižavanju među ne-smrtonosna sredstva pomoću kojih se zatvorenici od Abu Ghraiba do Guantanama mogu prisiliti da odaju svoje tajne bez kršenja američkog zakona (Cusick, 2006).

[2] RAF - Royal Air Force.

Sovjetski primjeri su također značajni zbog svoje obimnosti i utjecaja na širu javnost. Jedna od najpoznatijih psiholoških operacija, odnosno „psihološko – informativnih aktivnosti“ kako su to nazivali Sovjeti, jeste plasiranje laži da su bolest AIDS i virus HIV-a kreiran u američkoj vojnoj labaratoriji. Navedena aktivnost je nazvana „Operacija Denver“ i predstavlja dio sovjetskih aktivnih mjera kojima se nastojalo izazvati otklon prema SAD-u, a samim time i država trećeg svijeta u kojima je harala ova bolest i virus. Navedena operacija je razotkrivena dolaskom do KGB-ovog telegrama broj 2955. i broj broj 2742. prema bugarskom KGB-u i telegram istočno-njemačkog Stasija također prema bugarskom KGB-u (Kramer, 2020).

Psihološke i psihološko – informativne operacije nastoje ne samo da utječu na pojedinca u određenom manjem ili većem geografskom regionu kao što je džunga u Vijetnamu, ili gradić u Panami, već imaju za cilj da djeluju globalno vršeći utjecaj i pritisak na globalne i regionalne sile, kao i druge regionalne aktere. Navedeno uvijek započinje utjecajem na pojedince i grupe, pri čemu se isto širi poput virusa.

1.3. Društvene mreže kao sredstvo psiholoških operacija

Pojava Interneta je prirodno uslovila i kreiranje društvenih mreža kao sistema približavanja ljudi i informacija širom planete Zemlje. Povezivanje različitosti i udaljenih krajeva svijeta, kao i širenje informacija. Kada se govori o definiciji društvenih mreža, one se mogu predstaviti kao: *web stranica ili aplikacija koja omogućuje ljudima da se međusobno povežu na zajedničkoj platformi. Korisnici mogu dijeliti informacije, izražavati mišljenja, istraživati zajedničke interese, tražiti poslove, promovirati svoje poslovanje, stvarati odnose i na drugi način komunicirati jedni s drugima. Oni koji sudjeluju u društvenoj mreži često dijele širok raspon informacija i sadržaja, uključujući fotografije, video zapise, zvučne isječke, dokumente, vijesti, marketinške materijale ili poveznice na druge izvore. Društvene mreže obično pružaju mehanizme za objavljivanje sadržaja kao što su fotografije, videozapisi, blogovi ili poveznice na druge stranice. Ostali korisnici mogu komentirati ili ocjenjivati sadržaj, kao i preporučiti ga drugim korisnicima.* (Goulart, 2024).

Neke od poznatijih društvenih mreža su: Facebook, 4Chan, X (bivši Twitter), Reddit, YouTube, Instagram, TikTok, Snapchat, Tumblr i tako dalje. Ove društvene mreže su zasnovane na konceptu dijelenja informacije – video, audio, tekstualne ili kombinacije navedenih vidova. Cilj društvenih mreža je povezati ali i dati određenu informaciju, što se postiže upravo kroz audio-vizualne i tekstualne sadržaje.

Širenje sadržaja na društvenim mrežama kao što je Reddit, X (Twitter), Instagram, YouTube i ostalim, može da ima obrazovno-informativni karatker. Tako utjecajni akteri – influenseri, prenose svoje stavove i mišljenja širem auditorijumu, kako

vlastitih pratilaca, tako i onih kojima algoritam predloži video, fotografiju ili tekstualni sadržaj. U prošlosti navedeni zadatak su provodili državno sponzorirani mediji – televizijske kuće, radio stanice i prinatne novine, pri čemu je uvjek bio primjetan državni propagandni element. Društvene mreže navedeni element zamagljuju i pružaju iluziju različitosti mišljenja, međutim, ona ne može postojati zbog upotrebe raznih aktera od utjecaja i kontrolirajućih elemenata. Ukoliko za primjer uzmemo društvenu mrežu Reddit, koja je zasnovana na „subredditima", odnosno tematskim podforumima u kojima se daju informacije i dijeli sadržaj, primjetna je velika kontrola od strane moderatora, koji najčešće besplatno i po ideološkom ubjeđenju djeluju i ograničavaju širenje informacija. Reddit kao društvena mreža najčešće za moderatore ima ekstremne ljevičare i druge grupe povezane sa ovim političkim identitetom. Kontrola subbredita se zasniva na ograničavanju sadržaja koji propituje navedene narative, ideje i identitete, čime se onemogućava bilo kakva diskusija, već dogmatično slijeđenje uvjerenja koje imaju moderatori. Tako na primjer, moderatori „banuju" one korisnike koji nemaju ista, najčešće ekstremna ljevičarska uvjerenja kao i oni, pri čemu stvaraju takozvani „echo chamber" u kojem korisnici jednog subreddita imaju isto konformističko i politički usmjereno mišljenje, što se može širiti i na druge tematske subreddite. To se postiže uvidom u historiju komentara i objava korisnika, na osnovu čega moderatori nekog subreddita mogu da kazne, odnosno izbace korisnik iz svog subreddita jer ima suprotno mišljenje u odnosu na neku treću stvar (politika, religija, ideologija, natalitet i tako dalje). Ovakva psihološko – ideološka „klima" omogućava jednostranost i uniformnost, dajući pretpostavku da postoji samo jedna istina, te da su svi ostali u krivu, što daje sliku totalitarnog uređenja jedne društvene mreže. S druge strane, društvene mreže bez moderatora poput 4Chana, ne ograničavaju šta se može reći, bez obzira da li je to politički korektno ili ne, zbog čega je moguća diskusija i razmjena mišljenja, a ne stvaranje *echo chambe*r*a*. Ovakav način funkcionisanja omogućava provođenje raznih cyber propagandnih djelovanja kao što je *spam* određenih političkih ideja usmjerenih za ili protiv neke grupe, identiteta ili nacije, međutim, najčešće se to radi objavljivanjem pornografije na tematskim podforumima kako bi se smanjio broj korisnika u datom momentu, te prekinula svaka diskusija koja ne ide u željenom smjeru.

2. Uloga društvenih mreža u psihološkim operacijama

Društvene mreže kao novum tehnologije i neizostavni dio svakodnevnog ljudskog života imaju veliki značaj i ulogu u provođenju psiholoških operacija. Zamjenom tradicionalnih medija kao što su televizija, radio i printane novine kod mladih ili onih kojima isto nije dostupno, društvene mreže predstavljaju jedini i osnovni način informisanja, što znači da omogućavaju davanje onih informacija i sadržaja koje agresivni akter želi da se prime u umove ciljane publike. Društvene mreže su značajan pokazatelj života određene osobe i kao takve se trebaju u potpunosti

iskoristiti (Muhić, 2024). Poslednjih godina, sa napretkom velikih podataka i tehnika rudarenja podataka, istraživačka zajednica je primetila da otvoreni podaci predstavljaju moćan izvor analize društvenog ponašanja i dobijanja relevantnih informacija (Chen, Chiang, & Storey, 2012).

2.1. Načini upotrebe društvenih mreža za psihološke operacije

S obzirom da društvene mreže predstavljaju značajan aspekt borbe za umove, one se mogu koristit na različite načine, sve s ciljem obmanjivanja, zastrašivanja i demoralizacije neprijatelja, ali i kontrole narativa koji postaju društveno prihvatljivi i ulaze u sferu konformizma. Društvene mreže su zamijenile standarne i tradicionalne vidove širenja informacija, te stoga predstavljaju zanačajan *force multiplier* prilikom izvođenja obavještajnih, vojnih ili drugih operacija koje mogu biti kinetičkog ili nekinetičkog karaktera. U nekim slučajevima isto bi se moglo porediti sa terorizmom. On u svom korijenu sadrži esencijalno nasilje i njemu konačni cilj nisu samo ljudske žrtve i materijalna šteta koju nanese, već potvrda i simbolika prenošenja zastrašujućih poruka prema stanovništvu, gdje se planski udara na psihu čovjeka (Lakić, Kovačević, & Kovačević, 2024).

2.1.1. Širenje propagande i dezinformacija

Propagandne i dezinformacijske aktivnosti predstavljaju jedan od osnovnih aktivnosti agresivnih aktera na društvenim mrežama. Propaganda je uvijek prisutna u ljudskom društvu i životu, te pojava društvenih mreža i transfer na njih sa tradicionalnih medija, omogućio je da ona postane dostupnija, sadržajnija i superiornija u odnosu na druge metode. Propagand se definiše kao tehnika utjecanja na ljudsko djelovanje manipulacijom reprezentacija koje mogu poprimiti govorni, pisani, slikovni ili zvučni oblik (Lasswell, 1995). Također, Cambridg dictionary (2023), propagandu definiše i kao informacije, ideje, mišljenja ili slike, često samo jedan dio argumentacije, koje se emitiraju, objavljuju ili na neki drugi način šire s namjerom da se utječe na mišljenje ljudi. Utjecaj na mišljenje ljudi se primarno poduzima sa određenim informacijama ili sadržajima koji će izazvati specifična osjećanja, u zavisnosti od potrebe, targetirane skupine i kranjeg cilja. U navedenom će se najčešće koristiti dezinformacije, odnosno obmane kojima se kreira jedan poptuno novi narativ.

Upotrebom dezinformacija na društvenim mrežama, moguće je izazvati poptuni haos među targertiranom publikom, naročito ako se dezinformacijska i propagandna kampanja adekvatno planira i organizuje. Navedeno zahtjeva poznavanje kulturoloških, religijskih, ideoloških i političkih čimbenika nekog društva, kako bi se audio-vizuelnim i tekstualnim sadržajem načinila značajna šteta. Također, akter od utjecaja koji dijeli (dez)informacije, treba da ima određenu publiku koja mu vjeruje. Ukoliko navedni akteri konstantno šire laži, onda oni gube kredibilitet, a samim time i publiku koja će im vjerovati. Ono što se može primjetiti na društvenim mrežama jeste da akteri najčešće dijele istinu i poluistinu, a u veoma rijetkim situacijama apsolutno lažne vijesti. Drugim

riječima, moglo bi se reći da je oko 80% propagandnog sadržaja istina, dok je preostalih 20% poluistina ili poptpuna laž kreirana s ciljem obmane.

2.1.2. Odabir targetirane publike

Da bi se ostvarili traženi ciljevi, neophodno odrediti publiku kojoj će se predočiti propaganda i dezinformacije. Prije svega, neophodno je odlučiti prema kome će se primjenjivati propaganda, baš kao što je to bilo ključno za britansku vladu u Prvom svjetskom ratu. Dakle, propaganda i dezinformacije se mogu kreirati za tri grupe: vlastito stanovništvo, neprijatelja, te saveznike i neutralne aktere. Publika mora biti odabrana kako bi se prema njoj kreirala specifična propaganda. U periodu američkih predsjedničkih izbora 2015. godine, Cambridge Analityca je na osnovu istraženih preferensi različitih demografskih skupina (rasnih, etničkih, spolnih, seksualnih) predlagala bivšem predsjedniku Trumpu načine vođenja kampanje (Hern, 2018). To znači da je Trumpova kampanja bila najviše orjentirana prema onima koji su njegovi ideološki protivnici i oni koji su neodlučni, dok je skupina istomišljenika i vjernih pratilaca imala pasivniji tretman. To proizilazi iz pretpostavke da će sljedbenici uvijek da slijede, te da se resursi moraju usmjeriti ka pridobijanju onih koji su neodlučni ili su kategorički protiv njegovih politika.

Za uspješno provedenu psihološku operaciju važna su dva faktora:

1. pažljivo odabrana publika;
2. društvena mreža koju preferira odabrana publika.

Navedeno je potrebno utvrditi zbog različitosti u preferensama dobnih skupina i trendova koji vladaju među djecom, adolescentima, odraslima i onima u odmakloj starosnoj dobi. Na primjer, vizuelno dominantne društvene mreže poput TikToka preferiraju djeca i mladi, dok primarno tekstualne i foto-tekstualne preferiraju stariji. Navedeno u sebi ima ključne faktore poput nivoa pažnje i koncentracije koji je sve manji kod mladih (popularno nazvano *Gen Z*) i traje 8 sekundi (Noor, i dr., 2022) za razliku od staijih generacija kod kojih je to duže. Također, za *Gen Z* se mora izvršiti prilagodba formata sadržaja koja je kratka i u obliku video formata. Upotreba poznatih osoba od utjecaja - influensera za širenje ili regaovanje na navedeni sadržaj igra veliku ulogu u njegovoj diseminaciji i popularnosti. U ovom procesu je bitan i obavještajni ciklus koji usmjerava kreatora operacije, te je on *vrlo dinamičan, kontinuiran i beskrajan* (Muhić, 2024).

2.1.3. Kreiranje lažnih profila

Kreiranje lažnih profila predstavlja način manipulacije na društvenim mrežama kao sredstvo prikazivanja određene ideje kao favorabilne ili opće prihvatljive. To znači da grupa koja se bavi propagandnim i dezinformacijskim djelovanjem kreira mnoštvo naizgled legitimnih naloga na specifičnoj društvenoj mreži ili mrežama,

te kreirajući objave, pišući komentare i dijeljeći tuđe obavje, isto čini dostupnim većem broju ljudi. Lažni profili također mogu da služe i u druge svrhe, kao što je na primjer napad na određene javne ličnosti kroz uvrede ili prijetnje, ali i podrška drugim akterima i influenserima, bilo kroz dijeljenje i komentiranje njihovog sadržaja kako bi se potaknula rasprava, a samim time i algoritam za viralnost. Lažni profili se također mogu koristiti i za infiltriranje i prikupljanje informacija unutar interesnih grupa na internetu. Na primjer, kroz adekvatno „prilagođen" lažni nalog na društvenim mrežama, može se pristutpiti određenim grupama i tako prikupljati informacije, ometati rad, stvarati određene zavjere unutar zajdnice i izvršiti atomizaciju grupe. Postizanjem statusa administratora moguće je u potpunosti pristupiti svim informacijama članova grupe, kao i razgovorima, uklanjati članove grupe ili u određenom slučaju u potpunosti zatvoriti / ukloniti grupu prilikom čega se uništavaju gotovo sve veze koje su ostvarene online i na datoj društvenoj mreži ali ne postoje u fizičkom, materijalnom svijetu.

2.1.4. Korištenje algoritama

Korištenje algoritama za viralnost omogućava da propaganda i dezinformacije postanu dostupni većem broju korisnika društvenih mreža. Svaki algoritam radi na osnovu određenih setova pravila koji konstantno evoluiraju Zbog navednog platforme društvenih medija koriste posebno kreirane algoritme kao inteligentne vodiče koji imaju zadatak da pažljivo sortiraju i povezuju sadržaj s publikom koja ima slične preferense. To se može iskoristiti ukoliko se ciljana grupa treba izložiti određenoj propagandi ili dezinformacijama. Na primjer, ukoliko ciljana grupa pripada adolescentnoj dobi, i voli određene muzičke zvijezde ili filmove, moguće je kreirati video sadržaj koji u sebi inkorporira ili određenu muzičku ili filmsku zvijezdu ili insert filma, te u njega utisnuti određene poruke, ili koristiti sadržaj koji podjseća na određeni insert. Za diseminaciju propagande i političkih poruka, koriste se i vizuelno zanimljivi sadržaji sa određenom porukom i privlačnim akterima. Direktni primjer toga je djelovanje Izraelskih odbrambenih snaga (IDF), koje za širenje propagande i iskorištavanje algoritma najčešće koriste vojnike, pretežno plavokose žene, koje plešu ili izvode određene radnje koje su u datom trenutku trend na društvenim mrežama poput TikToka ili Instagrama. Na ovaj način se ostvaruju dva cilja: a) viralnost, i b) stvaranje simpatija prema IDF-u. Ovaj sadržaj je usmjeren ka speicifčnoj publici, najčešće muškarcima koji su neopredjeljeni ili ne daju podršku Izraelu, a nalaze se u poodmakloj starosnoj dobi. Pojednostavljeno, u ovom slučaju žene se koriste kao objekat privlačnosti putem kojeg se prenose političke poruke široj publici.

2.1.5. Iskorištavanje i produbljivanje društvene polarizacije

Akteri koji provode propagandne operacije usmjerene protiv određene grupe, države ili regije, često se koriste društvenim podjelama i nemirima. Društvene podjele i nemiri zasnovani na različitosti u religiji, politici ili nekom drugom sektoru, mogu da se iskoriste za promicanje određenih ideja. Navedene ideje se

kreiraju tako pojačavaju razlike između dvije ili više suprostavljenih grupa, te nije rijekta upotreba i *false flag* operacija. Drugim riječima, kreirat će se radikalni i ekstremistički sadržaj koji poziva na obračun, ubistva, etničko čišćenje i genocid jedne grupe, pri čemu se kreatori predstavljaju kao pripadnci onih koji pozivaju na to. Kreatori ovih operacija često su pripadnici stranih obavještajnih službi onih država koje imaju određenu korist u unutrašnjem sukobu jedne države. Za ostvarivanje navedenog, potrebno je ostvariti inicijalnu prednost kroz viralnost sadržaja, nakon čega mase svojevoljno prihvataju viralne ekstremističke i radikalne ideje.

2.2. Primjeri i studije slučaja psiholoških operacija na društvenim mrežama

2.2.1. Cambridge Analytica i predsjednički izbori

Predsjednički izbori u Sjedinjenim Američkim Državama održani 2016. godine predstavljaju jedan od najupečatljivijih primjera provođenja psiholoških operacija, kako od strane Republikanske stranke, tako i od strane Demokratske stranke. Kada je riječ o Republikancima i njihovom predsjedničkom kandidatu Donaldu J. Trumpu, njegova predizborna kampanja istaknula se sofisticiranim pristupom, naročito zahvaljujući angažmanu britanske kompanije Cambridge Analytica, koja je razvila efikasne strategije za osvajanje srca i umova birača širom Sjedinjenih Država. Otkrivanje metoda koje su korištene u kampanji, a koje su postale javne 2018. godine, pokazalo je na koji način lični podaci korisnika društvenih mreža – konkretno Facebooka – mogu biti upotrijebljeni za precizno ciljanje političkih poruka i oglasa, čime se direktno utiče na izborni proces. U ovom kontekstu, predmet analize nije legalnost, etičnost ili moralnost navedenih aktivnosti, već način njihove realizacije i njihova operativna učinkovitost.

Cambridge Analytica je politička konsultantska tvrtka koja se specijalizirala za korištenje tehnika rudarenja podataka kako bi pomogla svojim klijentima proširiti potencijalne biračke baze (Cadwalladr & Graham-Harrison, 2018). Skandal je uključivao iskorištavanje „sirovih podataka“ više od 87 miliona Facebook profila koje Facebook nije adekvatno zaštitio (Solon, 2018). Nedostatak adekvatne zaštite podataka – ili njihova eventualna prodaja – omogućio je kreiranje sofisticiranih informacijskih i psiholoških operacija usmjerenih na indoktrinaciju širokih društvenih slojeva, čime je ostvaren utjecaj na tok predsjedničkih izbora. U martu 2018. godine, Facebook je bio uhvaćen u velikom skandalu s kršenjem podataka u kojem je politička konzultantska tvrtka - Cambridge Analytica - izvukla lične podatke više od 87 miliona korisnika Facebooka bez njihovog pristanka (Cadwalladr & Graham-Harrison, 2018). Podaci su navodno korišteni u korist kandidata za predsjednika SAD-a, Donalda Trumpa, tokom izbora 2016 (Cadwalladr & Graham-Harrison, 2018).

Anketa koju je izradio Aleksandr Kogan, britanski akademski istraživač koji je koristio Facebook u istraživačke svrhe, poslana je 3 miliona Amerikanaca

(Cadwalladr & Graham-Harrison, 2018). Ova anketa, koja se činila bezopasnom i za koju su ispitanici dobijali simboličnu novčanu naknadu, uključivala je 125 pitanja o osobinama ličnosti s kojima su se ispitanici mogli složiti ili ne, i kombinirana je s podacima korisnika na Facebooku kako bi se stvorio psihometrijski model, sličan profilu ličnosti (Cadwalladr & Graham-Harrison, 2018). Ovi podaci su potom kombinirani s biračkim evidencijama i poslani Cambridge Analytici (Cadwalladr & Graham-Harrison, 2018). Obrada podataka je ukazala na to kojim se demografskim skupinama – bjelim muškarcima/ženama, latino muškarcima/ženama, crnim muškarcima/ženama, etničkim i seksualnim manjinama, kao i dugogodišnjim R/ D glasačima treba usmjeriti pažnja.

Navedeni skandal doveo je do pada vrijednosti dionica kompanije Facebook za 17%, te je izazvao intenzivne javne i institucionalne pozive na usvajanje strožijih zakonskih okvira u pogledu zaštite ličnih podataka koje prikupljaju i koriste tehnološke kompanije (Solon, 2018). Kompanija Meta, vlasnik Facebooka, pristala je isplatiti 725 miliona dolara u cilju rješavanja pravnih sporova proisteklih iz ovog slučaja (Solon, 2018). Skandal je, osim Facebooka, utjecao i na druge tehnološke kompanije koje su bile primorane redefinirati svoje politike privatnosti i upotrebe korisničkih podataka. Uprkos tome, navedeni događaji i dalje ukazuju na značajan rizik zloupotrebe ličnih podataka od strane trećih aktera u privatne ili političke svrhe, uz napomenu da će se slične prakse u budućnosti vjerovatno provoditi s većim oprezom i dodatnim sigurnosnim mjerama. Slučaj Cambridge Analytica predstavlja prekretnicu u razmatranju odnosa između društvenih mreža, privatnosti i digitalne sigurnosti. Ovaj slučaj je pokazao koliko su lični podaci korisnika društvenih mreža ranjivi i kako se ti podaci mogu zloupotrijebiti. Također je pokazao važnost zaštite privatnosti korisnika i potrebu za boljim regulativama u digitalnom prostoru.

Međutim, skandal nije označio kraj trgovine ličnim podacima koje posjeduju velike tehnološke korporacije – naprotiv, ukazao je na postojanje ozbiljnih i kontinuiranih prijetnji kada je riječ o neetičkoj komercijalizaciji digitalnih tragova korisnika. Kada se govori o političkim izborima, i republikanci i demokrati surađuju s tvrtkama koje se bave podacima kako bi stvorili nacionalne baze podataka biračkih dosjea, prikupljajući informacije iz mnogih izvora kako bi izradili detaljne profile birača s hiljadama podatkovnih točaka i izgradili modele koji predviđaju stavove ljudi o pitanjima ili kandidatima (Culliford, 2020).

U tom kontekstu ostaje otvoreno pitanje – da li ovakvi oblici političkog djelovanja predstavljaju prihvatljiv standard demokratske borbe, te da li je politička utakmica utemeljena na načelima pravičnosti i transparentnosti.

2.2.2. Operacija „Blacktivist“

Period predsjedničkih izbora u Sjedinjenim Američkim Državama bio je izuzetno složen i karakteriziran dubokim društvenim tenzijama. Antagonistički akteri, prije svega Rusija, nastojali su dodatno destabilizirati američko društvo izazivanjem i produbljivanjem postojećih društvenih podjela. Primarni cilj takvih aktivnosti bio je oslabiti unutrašnju koheziju SAD-a, čime bi se indirektno utjecalo i na njihovu međunarodnu poziciju. Kao što je i ranije historijski dokumentirano, ruske obavještajne službe su koristile slične metode destabilizacije. Primjer za to je operacija „PANDORA“, koju je 25. jula 1971. godine naložio načelnik Prvog (sjevernoameričkog) odjela FCD-a, Anatoli Tikhonovich Kireyev, izdavši naređenje KGB-ovoj rezidenciji u New Yorku da postavi eksplozivne naprave s odgođenim dejstvom u afroameričkom dijelu grada. Za Kirejeva je preferirana meta bio jedan od afroameričkih fakulteta, kako bi se izazvao snažniji međuetnički sukob, prvenstveno između afroameričke i jevrejske zajednice. Nakon eksplozije, naređeno je anonimno pozivanje nekoliko afroameričkih organizacija uz tvrdnju da je za napad odgovorna Jevrejska odbrambena liga (Andrew & Mitrokhin, 2000).

Savremeni pandan ovim starim taktikama predstavlja operacija „Blacktivist“, sofisticirana psihološka i dezinformacijska kampanja koju su na društvenim mrežama proveli ruski akteri. Cilj ove operacije bio je intenzivirati postojeće rasne napetosti u SAD-u i podstaći nerede, naročito u kontekstu predstojećih izbora i narativa o policijskoj brutalnosti (Levin, Did Russia fake black activism on Facebook to sow division in the US?, 2017). Podizanju napetosti su odgovarali predsjednički izbori koji su se trebali održati, ali i rasni neredi koji su nastali zbog navodne policijske brutalnosti.

Ove aktivnosti se pripisuju akterima povezanim s ruskim sigurnosnim aparatom, uključujući FSB, GRU i tzv. Agenciju za istraživanje interneta (IRA). Kao konkretan instrument korišten je lažni Facebook profil pod nazivom „Blacktivist“, koji se predstavljao kao dio autentičnog pokreta podrške „Black Lives Matter“ (Levin, Solon, & Walker, 2017). Ovaj profil je brzo stekao veliki broj pratitelja, čak preko 330 hiljada, ali nitko nije znao tko ga zapravo vodi. Ruski operativci su ga koristili za koordinaciju i promociju protesta protiv policijske brutalnosti. Koristili su autentične fraze poput “*COPS RAID WRONG HOME AND ASSAULTED PREGNANT WOMAN,”*, *“INSANE! COPS PULVERIZED HANDCUFFED MAN*” i slične autentične komentare kako bi potaknuli korisnike da se uključe u diskusiju i podijele objave (Levin, Did Russia fake black activism on Facebook to sow division in the US?, 2017). Korištenjem emocionalno provokativnih izraza i grafičkih prikaza brutalnosti, operacija je uspješno mobilizirala dio populacije, doprinoseći eskalaciji protesta i povećanju društvenih tenzija. Takva strategija cilja tzv. afektivnu polarizaciju, gdje se društvene skupine sve više definiraju negativnim osjećanjima prema drugima, a ne vlastitom političkom pripadnošću. U kontekstu psiholoških operacija, ovo

predstavlja efikasan način generisanja unutrašnje nestabilnosti bez direktnog vojnog angažmana. Prema izvještaju Odbora za obavještajne poslove američkog Senata, tisuće računa na platformama poput Facebooka, Twittera, Instagrama i YouTubea, koje je kreirala IRA, imale su za cilj sabotirati kampanju Hillary Clinton i indirektno podržati Donalda Trumpa. Više od 66% oglasa koje je objavila ova „fabrika trolova" sadržavalo je termine povezane s rasnim pitanjima (BBC News, 2019). Navedeno pružanje podrške bivšem predsjedniku Trumpu je služilo samo za pokušaj njegove diskreditacije, i stvaranja unutrašnjih problema u SAD-u.

Operacija „Blacktivist" ostavila je značajan trag u javnom diskursu Sjedinjenih Američkih Država. Iako je teško kvantitativno izmjeriti njen ukupni efekat, jasno je da je doprinijela radikalizaciji javne sfere i produbljivanju političkih i identitetskih podjela. Nastala je oštra dihotomija u percepciji političkih aktera – glasači Donalda Trumpa često su označavani kao ekstremni desničari, dok su s druge strane progresivni aktivisti percipirali širu bijelu populaciju kroz prizmu kolektivne krivnje i zahtjeva za reparacijom. Upravo ovaj primjer ilustrira kako društvene mreže mogu biti instrumentalizirane za provođenje tzv. „false flag" operacija – kada se operativci predstavljaju kao pripadnici jedne strane s ciljem kompromitacije iste. U takvim okolnostima, ključnu ulogu igra sposobnost aktera da razumije kulturološke, rasne, političke i ideološke tenzije ciljanog društva.

Efikasna borba protiv takvih operacija zahtijeva ne samo tehničke mehanizme detekcije, već i verifikaciju identiteta administratora i kreatora sadržaja. U slučaju operacije „Blacktivist", pravovremena identifikacija stvarnih upravljača profilom nije bila moguća, a broj pratilaca je služio kao zamjena za vjerodostojnost.

2.2.3. Ukrajinske psihološke operacije na društvenim mrežama – Ghost of Kiev
Period ruske invazije na Ukrajinu, započet krajem februara 2022. godine, predstavljao je prekretnicu u upotrebi društvenih mreža u kontekstu savremenog ratovanja. One su postale ključan instrument u oblikovanju javnog mnijenja, mobilizaciji podrške, podizanju morala vlastitih snaga, kao i demoralizaciji neprijatelja. Jedan od najznačajnijih primjera psihološke operacije koju su izvele ukrajinske snage jeste narativ o tzv. "Duhu Kijeva" — navodnom pilotu borbenog aviona MiG-29 Fulcrum, koji je, prema tvrdnjama, uništio veliki broj ruskih letjelica u prvim danima invazije.

Ova priča, iako kasnije razotkrivena kao konstrukcija i psihološka operacija, imala je jasan cilj: podizanje borbenog duha ukrajinskih snaga i građanstva, uz istovremeno izazivanje panike i nesigurnosti među ruskim pilotima. Prvi izvještaji o "Duhu Kijeva" počeli su da se šire društvenim mrežama odmah nakon početka invazije, potaknuti snimcima borbenih aviona u ukrajinskom zračnom prostoru. Prema tim navodima, pilot je tokom prvih 30 sati sukoba samostalno oborio šest ruskih aviona. Ova tvrdnja je ubrzo postala viralna, pri čemu su

zvanični ukrajinski vladini nalozi na društvenim mrežama, naročito na platformi Twitter, aktivno širili priču i time dodatno pojačali njen utjecaj. Međutim, već dva mjeseca nakon inicijalnog širenja, Ukrajinsko ratno zrakoplovstvo priznalo je da je narativ o "Duhu Kijeva" mit, pozivajući pritom građane na odgovorno ponašanje u digitalnom prostoru i poštovanje osnovnih principa informacijske higijene, uključujući provjeru izvora informacija prije njihovog daljnjeg dijeljenja (Bubola, 2022). kreiranju i održavanju ovog narativa važnu ulogu su odigrali i brojni OSINT nalozi na Twitteru, koji su svojim analizama i objavama doprinosili uvjerenju o postojanju misterioznog pilota.

Iako "Duh Kijeva" nije bio stvarna osoba, narativ koji je stvoren oko njega imao je snažan psihološki učinak, posebno u prvim danima rata, kada je postojala potreba za simbolima otpora i herojstva. S druge strane, kasnije otkrivanje da se radi o propagandnoj konstrukciji može imati negativne posljedice, poput gubitka povjerenja, pada morala i preispitivanja istinitosti ostalih informacija koje plasira vlast.

Ova operacija jasno demonstrira kako društvene mreže omogućavaju brzo i široko širenje neprovjerenih informacija, posebno kada su te informacije podržane objavama s verificiranih naloga — uključujući vladine račune na platformama poput X-a (bivši Twitter), Telegrama, Facebooka i Instagrama — ali i neverificiranih izvora s visokim stepenom utjecaja i reputacije, poput pojedinih OSINT zajednica. Operacija "Duh Kijeva" ujedno oslikava kako dezinformacije mogu biti strateški iskorištene u funkciji manipulacije javnim mišljenjem i povećanja borbene spremnosti vlastitih snaga u kontekstu oružanih sukoba. Također, širenje mitova o pilotu koji navodno obara moderne neprijateljske avione može imati ozbiljan psihološki utjecaj na protivnika, naročito na elemente zapovjedno-kontrolnog (C2) sistema, koji takve informacije mogu tumačiti kao rezultat intervencije vanjskih sila. To može podrazumijevati prisustvo sofisticirane strane vojne pomoći u obliku naprednih projektila, moderniziranih verzija borbenih aviona ili do tada nepoznatih PZO sistema (npr. napredni surface-to-air missile – SAM).

Ovaj slučaj ističe dvostruki značaj psiholoških operacija u savremenom ratu: s jedne strane, potrebu za zaštitom informacijskog prostora kroz borbu protiv dezinformacija, a s druge, njihovu ogromnu moć u oblikovanju percepcije i ponašanja – kako kod vlastitog stanovništva i oružanih snaga, tako i kod neprijatelja. Efikasnost ovakvih operacija naročito dolazi do izražaja kada se sprovode koordinirano, putem više platformi, i kada uključuju širok spektar aktera — od državnih institucija i medija do nezavisnih digitalnih influensera i OSINT zajednica – čime se osigurava lokalna, regionalna i globalna dostupnost i utjecaj.

2.2.4. Izraleske dezinformacije o Palestini

Izraelska invazija na Gazu koja je započela 27. oktobra 2023. godine predstavlja primjer koordinacije kinetičkih i nekinetičkih – psiholoških aktivnosti u fizičkom, cyber i kognitivnom prostoru. Ono što je specifično za navedenu agresiju i genocid jeste rat na društvenim mrežama koji se provodi od strane JIDF-a, odnosno Jevrejskih internet odbrambenih snaga i drugih aktera koji djeluju samovoljno posredstvom vlastitog ideološkog uvjerenja ili čak u određenoj mjeri centralizirano sa jasnim liderima i koncipiranim operacijama. U ovoj agresiji, u medije su plasirane lažne priče i dezinformacije o brutalnosti Hamasa kako bi se smanjla simpatija prema Palestincima i omogućilo okončanje Palestinskog pitanja, odnosno potpunog etničkog čišćenja i genocida nad njima. U ovu svrhu su korištene razne laži i dezinformacije, specijalno kreirane za zapadnu publiku koja ih je ipak raskrinkala i odbacila kao neosnovane.

Za psihološku operaciju usmjerenu prema Zapadu, Izrael je koristi mnoge narative u medijiima i na društvenim mrežama koje propagira preko agenata od utjecaja na društvenim mrežama, ali i političara na Zapadu. U nastavku će se navesti dva primjera od mnogih koji su rezultat izraelske propagandno – dezinformacijske mašinerije.

- Hamas je izvršio dekapitaciju 40 jevrejskih beba

Priča o obezglavljenim bebama proizašla je iz izvješća na izraelskoj stranici i24News novinarke Nicole Zedeck, iz njenog intervjua s izraelskim rezervnim vojnikom Davidom Ben Zionom. Max Blumenthal i Alexander Rubinstein izvijestili su 11. oktobra da je Ben Zion ozloglašeni radikalni vođa u izraelskom pokretu doseljenika na Zapadnoj obali. Između ostalog, ranije ove godine pozvao je razularene naoružane doseljenike da zbrišu palestinsko selo Harawa, koje su doseljenici napali i spalili nekoliko puta (Khouri, 2023). Izraelske vlasti i apolegete poput Ben Shapira i sličnih nikada nisu pružile dokaze o navedenom, te konstano odbijaju da prikažu dokaze koristeći *ad hominem* komentare prema onima koji to zahtjevaju. Čak u više navrata je IDF opovrgao navedenu laž (Solmaz & Call, 2023), ali se ona konstantno ponavlja kao istina na mnogim procionističkim nalozima na društvenim mrežama.

- Palestinski islamski džihad je sam raketirao bolnicu Al-Ahli Arab / prijevremena eksplozija njihove rakete je uništila bolnicu

Jedan od nezvaničnih izraelski glasnogovornika @HanayaNaftali je objavio tweet u kojem slavi IAF-ovo bombardovanje Al-Ahli bolnice, a nakon osuda javnosti je isto izbrisao[3], da bi se nakon nekog vremena pojavio „zvanični“ narativ da je to zapravo djelo Palestinskog islamskog džihada. Snimke uživo s Al Jazeere

[3] Vidjeti više na Naftalijevom X nalogu.

pokazale su 18. oktobra 2023. godine oko 19 sati po lokalnom vremenu jarku svjetlost koja se diže na nebu i dvaput bljesne prije nego što drastično promijeni smjer i eksplodira. Zatim se vidi eksplozija na tlu u daljini, a zatim druga mnogo veća eksplozija bliže kameri (Al Jazeera Staff, 2023). U satima nakon napada, @Israel, službeni izraelski račun na X (Twitter), objavio je video za koji tvrdi da je dokaz da je eksplozija bila rezultat pogrešno vođene rakete koju su lansirali militanti Islamskog džihada. Ali za nekoliko minuta, Aric Toler, bivši istraživač Bellingcata koji sada radi za The New York Times, istaknuo je da vremenska oznaka na videu pokazuje 20 sati po lokalnom vremenu, pun sat nakon što se eksplozija dogodila (Gilbert, 2023). Nalog @Israel je izbrisao objavu nakon ovog fact-checka.

Zpadni, britanski i američki mediji poput CNN-a i Fox News-a, kao i ostali, snažno podržavaju izraelski narativ, te često daju kontradiktorne informacije, ili opravdavaju izraleske napade na civile i civilnu infrastrukturu. Osnova medijskog izvještavanja koja mora biti zasnovana na principu objektivnosti i tačnosti je izostavljena, te medijske kuće postaju propagandno – dezinformacijski elementi, usmjereni na formiranju ili učvršćivanju stavova javnosti. Državno ili partijski sponzorirani mediji često su označeni kao slobodni mediji, ali ipak imaju veliku privženost određenim akterima, te nastoje da kreiraju specifične narative. Navedeno se može ogledati u političkom, ideološkom ili religijskom opredjeljenju koje imaju zaposlenici i menadžemnt, kao i stvarnim finansijerima. Također, britanski medij CNN je u svom izvještavanju bio isuviše pristrasan, pa je tako upotrebljavao semantičke greške, pri čemu su Palestinci bili mrtvi, a jevreji ubijeni. Na ovaj subliminalan način se nastojao kreirati naratv „ko je žrtva“ i izvršiti zamjena teza o žrtvi i agresoru, kao i izazvati određene simpatije. Ono što u potpunosti uništava narativ državno i politički sponzoriranih medija jesu društvene mreže poput X-a koji omogućava da se vidi i „druga strana“, odnosno realna situacija koju palestinci proživljavaju sa konstantnim bombardovanjem i ubijanjem koje ima velike naznake genocida kojem potpomažu upravo mediji kroz dehumanizaciju.

Razni procionistički inflienseri na društvenim mrežama djeluju ofanzivno, direktno pozivajući na genocid nad Palestincima. Navedeni često isto opravdavaju citirajući razne jervrejske spise koji govore o potpunom uništenju Amaleka. Također, prominentni influenseri poput Ben Shapira, Gaad Saada i sličnih, sve više i više gube podršku, dok na vidjelo izlaze propalestinski infulenseri. Ono što je specifično i unikatno za psihološke operacije na društvenim mrežama jeste upravo moć koji imaju određni akteri da kreiraju stavove i mišljenja drugih. U psihološkim operacijama, infulenseri predstavljaju oštricu mača, te su im podređeni ostali elementi (farme trolova i botova, lažna opozicija, false flag narativi). Procionistič infulenseri i agenti od utjecaja poput spomenutog Ben Shapira, imaju veliku bazu sljedbenika, koji svojevoljno šire laži

i dezinformacije, kreiraju nove, ili provode false flag operacije kao što je ranije spomenuta „Blacktivist“ kako bi prikupili informacije ili novac od simpatizera ili proizveli unutrašnji razdor. Navedeno se postiže koordiniranim napadima i preciznim „igranjem uloga“ kako bi se prižio osjećaj legitimnosti i istinitosti svakog aktera od utjecaja.

Izraelska agresija na Plestinu, kao i etničko čišćenje i genocid koji se čini, postaju stavljeni u drugi plan zbog jakih psiholoških operacija koje se provode od strane izraelske vlade, vojske i proizraleskih influensera. Pokušaj kontrole narativa se zasniva na plasianju laži i dezinformacija koje su kreirane tako da kod zapadne publike izazovu gnušanje i osudu prema Palestincima. Međutim, zbog postojanja društvenih mreža poput X-a koji ne cenzuriraju istinu, i omogućavaju svakoj strani da iznese dokaze i činjenice, sve više i više svjetske javnosti uviđa izraelske zločine i etničko čićenje koje se provodi „online“. Danas, kontrola stanovništva preko medija više nije u značajnoj mjeri moguća zbog građanskog novinarstva koje omogućava objektivnost i tačnost.

2.3. Utjecaj društvenih mreža na percepciju i ponašanje ciljane publike

Društvene mreže kao neizostavni dio ljudskog društva i ličnog života pojedinca, imaju značajne ujtecaje na donošenje svakodnevnih odluka te formiranja stavova i mišljenja. Internet i zajednice koje postoje na njemu poput društvenih mreža, transformirale su potrošače, društva i korporacije sa širokim pristupom informacijama, boljim društvenim umrežavanjem i poboljšanim komunikacijskim sposobnostima. Povezanost različitih individua u određenu grupu koja je orjentirana ka specifičnoj ideji je veoma bliska sa društvenim vezama u stvarnom životu. Uspostavljanje osjećaja društvene povezanosti sastavni je aspekt ljudskog života i onaj koji poboljšava različite aspekte psihološke dobrobiti (Mauss, i dr., 2011), pri čemu uspostavljanje društvenih veza u *online* prostoru može da bude ekvivalentno onom u stvarnom životu.

Način djelovanja društvenim mreža je ekvivalentan marketingu konzumerističkih proizvoda, pri čemu se u ovom slučaju ne prodaju fizički, već idejeni i misaoni proizvodi – *psihološki proizvodi*. Čak i način djelovanja ostaje isti, određena ideja se mora približiti specifično targetiranoj skupini kako bi oni postali njeni primarni konzumenti. Navedena ideja mora biti prilagođena demografiji skupine koja se nastoji tretirati, pri čemu je važno izučavanje kulturoloških, religijskih, društvenih i drugh trendova vezanih za metu. Na primjer, ukoliko se u svrhe političke kampanje tretiraju osobe afričkog porijekla (afro-amerikanci, afro-britanci, afro-francuzi i tako dalje) kao ciljana skupina, prema njima se mora kreirati sasvim drugačiji pristup od na primjer grupa azijskog ili blisko-istočnog porijekla koji je zasnovan primarno na kulutrološkim elementima, a zatim se grupa dijeli na više identitetskih podgrupa gdje se vrši usmjereno djelovanje u odnosu na: rod, spol, seksualnu orjetnaciju, religiju, kulturu, ranije političko opredjeljenje i drugo. Pored rasnog identiteta, postoje i drugi, kao što su oni koji se odnose na zdravlje

i zdravstvene probleme, na primjer osobe koje boluju od dijabetisa ili kancera, pri čemu se navedene grupe mogu koristiti na primjer kao jaka baza glasača ukoliko politički kandidat zagovara određne zdravstvene reforme u domenu navedenih bolesti.

Tretiranjem različitih rasnih, etničkih, religijskih ili nekih drugih grupa na isti način neće moći pružiti adekvatne rezultate u psihološkim kampanjama i borbi za kontrolu narativa. Samim time, ideja koja se propagira u domenu psihološke operacije, ima sve karakteristike brenda, te se mora prilagoditi i modificirati za svaku demografsku (i drugu) kategoriju i podkategoriju, odnosno spol, starosnu dob, seksualnu orjentaciju, političke preference i druge faktore. Na taj način se omogućava stvaranje prividne percepcije da su targetirane i tretirane grupe bitne donosiocu odluka (predsjedniku, predsjedničkom kandidatu, vladajućoj stranci ili opoziciji, nevladinim organizacijama i tako dalje) i da se on zalaže i bori za njih, kao i da je ostvario određenu vrstu emotivne konekcije sa njima.

Pored uloge društvenih mreža u izbornom procesu i predsjedničkim kampanjama, one svoju primjenjivost imaju i u domenu velikih nacionalnih netrpeljivosti i priprema za rat. U ovom slučaju, društvene mreže će biti korištene kao mjesto za širenje propagande, kako od državnih aktera – ministarstva odbrane i vojske koji će kreirati vlastiti video ili foto sadržaj koji nastoji da privuče određene grupe, najčešće muškarce[4], mada su ponekad ove kampanje usmjerene i prema netradicionalnim grupama – ženama i LGBT skupinama.[5] Razlozi za specifičnost reklama za regrutaciju je stvar državne politike u ratu i miru. Ono što je primjetno jeste da su za vrijeme rata reklamne kampanje inkluzivne i usmjerene prema seksualnim i drugim manjinama, dok je u vrijeme rata ili neposredne ratne opasnosti, fokus na muškarcima i tradicionalnim modelima muškosti – snazi, moći, očinstvu, bratstvu i drugom. Trenutačna geopolitička situacija u svijetu u kojem je moguć novi sukob na Bliskom Istoku, uakazala je na nizak nivo regruta u američkoj vojsci (Putterman, 2023), jer su upravo prethodne reklamne kampanje bile usmjerena prema seksualnim (LGBTQ+) i rasnim (BIPOC) manjinama koje tradicionalno nisu zainteresovane za državu i njenu nacionalnu sigurnost. Ta vrsta favorizma je uslovila kod heteroseksualnih bjelaca otklon prema vojsci, koji su često bili žrtve diskriminacije kada je riječ o napredovanjima i povlasticama koje su zaslužene na osnovu obavljenih zadataka, edukacija, misija i tako dalje. Usmjerenost i favorizacija seksualnih i rasnih manjina se može protumačiti kroz političke igre i borbu za glasove, što direktno šteti vojnoj mašineriji u kojoj nema mjesta inkluzivnosti i liberalnim shvatanjima civilnog svijeta jer je u vojnom svijetu sve bazirano na modelima zasluge, a ne privilegije

[4] Vidjeti primjer: First Jump | Be All You Can Be | U.S. Army; https://www.youtube.com/watch?v=luc9saxt_YQ (07.11.2023.)

[5] Vidjeti primjer: EMMA | THE CALLING | GOARMY; https://www.youtube.com/watch?v=MIYGFSONKbk (04.05.2021)

i tolerancije. Navedeni društveno – politički fenomen inkluzivnosti, tolerancije i apatije prema svemu je popularno nazvan „woke“, te ga mnogi optužuju za slabljenje SAD-a i umanjenje njene vojne moći i dominacije.

3. Razvoj i Strategije na Društvenim Mrežama

3.1. Kako se razvijaju i implementiraju psihološke operacije na društvenim mrežama

Razvoj psiholoških operacija, kao i njihovo implementiranje na društvenim mrežama kao nosiocima operacije, predstavlja veoma složen i sofisticiran proces. Taj proces se zasniva na prepoznavanju više ključnih faktora koji su neophodni za uspjeh same operacije, kao i posljedica koje će nastati njenom uspješnom implementacijom.

Kao osnova za razvoj svake psihološke operacije jeste identifikacija mete koja će biti tretirana i protiv koje će se poduzimati određene aktivnosti. Identifikacija kao osnovni korak procesa proizvodi osnovne pretpostavke za uspjeh same operacije, te se na njoj zasniva cjelokupni proces koji može imati veći ili manji broj elemenata i faza procesa koji zavise od kreativnosti i uspješnosti implementacije ideja.

Kao primjer provđenja uspješne psihološke operacije može se navesti sljedeći ciklus i njegovi elementi:

Identifikacija ciljane publike

Identifikacija ciljane publike predstavlja osnov za bilo koje propagandno, psihološko i drugo djelovanje koje za cilj ima proizvesti učinak na društveno – političkom nivou. Bez identifikacije onih prema kojima će se provoditi aktivnosti nije moguće uspješno ni provesti operaciju zbog nemogućnosti slanja prave poruke. Stoga, primarni cilj za svako djelovanje jeste odabir publike koja će biti tretirana. To može biti rasna, etnička, nacionalna ili religijska grupa, te je fokus na generalnim skupinama, nakon čega će se kroz profiliranje izvoditi usmjereno djelovanje na podgrupe.

Razvoj strategija

Razvoj strategija je usko povezan sa identifikacijom ciljane publike. On direktno korelira sa kulturološkim trendovima, tradicijama, običajima i načinima razmišljanja publike. U zavisnosti na demografske elemente poput spola, rase, regligije i drugih elemenata, neophodno je razviit pristupe koji će svjesno i podsvjesno utjecati na odabranu publiku. Strategije mogu biti zasnovane na identitetima – nacionalnost, seksualna orjentacija, dogmi – religiji ili kulturološkim i društvenim trendovima. Taokđer, svaka strategija mora imati elemente kao što su: a) jasni ciljevi operacije, b) odabir osnovnih poruka i tema

koje su u fokusu i c) planiranje i razvoj taktika za svaku društvenu mrežu i nosioc informacije pojedinačno. Navedeno možemo posmatati kroz *top down* proces strategija – operativa – taktika.

Segmentacija i podjela publike

Zbog previše generalnog i opšteg koje proizilazi iz masovnosti publike, kao i mnogobrojnosti identiteta, neophodno je specificirati svako djelovanje. Osnovu za uspjeh čini identifikacija publike, ali i njeno dublje razumjevanje koje proizilazi iz analize koje to grupe, podgrupe, kulture, subkulture i kontrakulture čine publiku. Zbog raznovrsnosti u društvu, svaka identificirana grupa koja čini publiku, mora imati specifično kreiranu i prenesenu poruku, koja zavisi od strateškog cilja koji može biti – umirivanje, podsticanje na djelovanje i djelovanje. Svaka grupa treba biti posebno tretirana sukladno načinu na koji ona najviše reaguje – video sadržaj na društvenim mrežama (kratki video klipovi, podcasti, fotografije), printani sadržaji (knjige, časopisi, naučni radovi i publikacije), tekst (noivnski članci na portalima, statusi i objave na društvenim mrežama), muzički sadržaj (muzički spotovi, radio, performansi na ulici). Svaka podgrupa ima određeni medijum iz kojeg crpi informacije zbog čega se on mora pronaći i iskoristiti.

Psihološko profiliranje

Psihološko profiliranje se zasniva na praćenju identificiranih grupa i podgrupa ciljane publike. Svaka grupa i podgrupa ima drugačije reakcije na određeni događaj i vijest, zbog čega je neophodno bilježenje, klasficiranje i analiziranje istog. Psihološko profiliranje se najlakše ostvaruje praćenjem komentara i reakcija na određene vijesti ili događaje koji su predmet rasprve na drušvenim mrežama. Na primjer, analiziranjem komentara ispod novog reklamnog videa za regrutaciju u pješadiju može se zaključiti stav određenih grupa i podgrupa. Također, potrebno je uvidjeti i reakcije drugih korisnika mreže na navedeni komentar – slaganje, neslaganje ili neutralnost. U navedenom pomaže i sistem valorizacije – like/dislike, repost, upvote/downvote ili neki drugi oblik kojim drugi korisnici izražavaju svoje slaganje ili neslaganje sa komentarom ili objavom. Korisnici se nakon toga klasificiraju u grupe zasnovane na demografiji (spol, rasa, nacionalnost, etnicitet, religija), te sfereama interesa i popularnim kulturološkim trendovima.

Kreiranje usmjerenog sadržaja

U zavisnosti od svake kulture, trenda i interesne sfere grupe i podgrupe koja se tretira, nastoji se kreirati i sadržaj koji će privući pažnju, potaknuti na razmišljanje, ali i subliminalno umetnuti određene ideje. Propaganda u samom početku djelovanja treba biti suptilna, neprimjetna i dvosmislena, da bi u daljim fazama operacije ona mogla biti direktnija, otvorenija i jasnija. Sadržaj se kreira

tako da izazove određene emocije kod konzumenta, najčešće ljutnju, međutim, potrebno je obratiti pažnju na to da sadržaj ne bude demoralizirajućeg karaktera zbog čega bi skupinakoja se pozitivno tretira i usmjerava na akciju postala apatična i tolerantna.

Optimizacija algoritma viralnosti

Da bi određena informacija i sadržaj bili usvojeni, neophodno je da postanu viralni, odnosno dostupni većem broju ljudi, odnosno pripadnicima targetirane skupine. Viralnost se može postići na dva načina: a) umjetnim putem kroz upotrebu botova i drugih metoda za postizanje viralnosti; b) stvarnim postizanjem viralnosti kroz kvalitet sadržaja. Za početak, neophodno je koristiti kombinaciju navedene dvije metode, odnosno kreirati kvalitetan upadljiv sadržaj koji će biti podržan upotrebom botova i lažnih profila. S ozbirom na mogućnost algoritma da prepozna djelovanje botova, neophodno je resurse usmjeriti u kreiranje kvalitetnog sadržaja koji korelira sa ciljanom publikom i grupama.

Upotreba botova i trollova

Za postizanje viralnosti i održavanje narativa općeprihvaćenosti neke ideje, neophodno je na vještački način ukazati na postojanje većeg broja ljudi koji se slažu sa navedenim porukama. To se postiže kroz upotrebu botova – računara i umjetne inteligencije koja imitira stvarnog korisnika, i trolova, odnosno stvarnih ljudi koji preko lažnih naloga na društvenim mrežama šire određene ideje, započinju diskusije ili kompromitiraju suparničku grupu kroz false flag aktivnosti[6]. Za veće i obimnije djelovanje, moguće je koristit farme trolova i botova, odnosno plaćenih aktera, koji će usmjereno djelovati na društvenim mrežama, interent forumima i novinskim portalima.

Implementacija sadržaja

Implementacija sadržaja, odnosno psihološko – propagandnog materijala i aktivnosti se provodi u tačno određenom vremenu. Navedeno vrijeme, odnosno vremenski period koji traje od nekoliko sedmica do nekoliko mjeseci, mora da korelira sa određenim društveno – političkim događajima kao što je na primjer predsjednička kampanja ili priprema za rat. Specifičnost implementacije sadržaja se nalazi u ideji raspodjele djelovanja na tri faze: a) faza prije događaja, b) faza za vrijeme događaja, c) faza nakon okončanja događaja. U navedenim periodima će se modificirati intenzitet i obim djelovanja, kako bi se postigao traženi efekat. Sama psihološka operacija ne okončava kad i društveno-politički događaj ili proces, već se ona kontinuirano nastavlja bez obzira na ishod događaja. Na

[6] Nosilac aktivnosti se predstavlja kao svoj ideološki protivnik te širi radikalni i ekstremistički sadržaj. Koristi se kao sredstvo odvraćanja neutralnih i umjerenih aktivista, te dehumanizaciju i demonizaciju suparnika.

primjer pobjeda ili poraz favorita za presjednika države ne znači okončanje psiholoških operacija, već njen kontinuitet i prilagodbu novonastaloj situaciji.

Mjerenje učinka i posljedica

Mjerenje učinka se može promatrati na dva načina, kvantitativno i kvalitativno. Kvantitativno se postiže evidencijom i obradom reakcija na društvenim mrežama (like/dislike, upvote/downvote, repost), komentara, dijeljenja i drugih prigodnih načina. Moguće je dodijeliti i određenu vrijednost komentarima koji su ekvivalentni od potpunog slaganja /pružanja podrške do potpunog neslaganja /odsustva podrške. Isto tako, moguće je provoditi i online ankete usmjerene ka specifičnim grupama koje se tretiraju, kako bi se dobila jasnija slika, međutim, navedeno istraživanje mora biti sprovedeno na način da se ne otkrije nalogodavac i prava svrha anketiranja.

Kada se govori o kvalitativnom istraživanju, navedeno se može postitći obradom komentara i objava, odnosno praćenjem emocionalnih reakcija, dubine angažmana korisnika, relevantnosti sadržaja, promjene u stavovima korisnika (kroz praćenje njihove ranije historije objava i reakcija) i tako dalje.

Prilagodba sadržaja

Prilagodba sadržaja označava i posljednju fazu koja ima za svrhu analizu ranijh koraka te učenje iz njih. U ovoj fazi, vršit će se modifikacije pristupima, načinu dijeljenja i kreiranja sadržaja kao i određivanja novih ciljanih grupa i metoda koje će biti usmjerene prema njima. Neophodno je izvršiti verifikaciju hipoteza o tome šta zapravo funkcioniše, a šta ne, te koji oblik djelovanja i prema kome daje najviše učinka u formiranju novih narativa. Nije loše ni implementirati nove strategije do kojih se došlo promatranjem procesa ili zbog promjena u društvenim i političkim dinamikama. Prilagodba sadržaja je ključna kako bi psihološka operacija mogla biti uspješno sprovedena u dužem vremenskom periodu i iz nje je moguće doći do nephodnih zaključaka, lekcija i nalaza za buduće psihološke operacije.

3.2. Analiza strategija i taktika sa primjerima

Kada se govori o analizi strategija i taktika za uspješno provođenje psiholoških operacija na društvenim mrežama, neophodno je razumjeti da su one mnogobrojne i promjenjive, te da zavise od datog trenutka, duštvenih procesa. One usko koreliraju i sa prethodno navedenim ciklusom djelovanja, te iz njega crpe osnovu djelovanja.

Strategije i taktike koje se primjenjuju u psihološkim operacijama su sljedeće:

1. False flag narativi;
2. Doxxing;
3. Upotreba lažnih identiteta;

4. Korištenje memova kao nosioca informacije;
5. Širenje teorija zavjera
6. Dezinformisanje.

3.2.1. False flag narativ

Ovi narativi predstavljaju strategiju neophodnu za podjelu javnosti i ciljanih grupa. Navedeno razbijanje jedinstva i uniformnosti u idejama omogućava specifičan narativ *rata svih protiv svih* i borbe za vlast. False flag narativi se provode kreiranjem lažnih naloga koji se predstavljaju kao pripadnici određene grupe, stiču njihovu podršku, te u ključnom momentu započinju diseminaciju lažnih vijesti i narativa. Osnovni zadatak je lažni narativ predstaviti kao ideju neke grupe, pri čemu nije značajno bitno da li će se otkriti da je navedeni narativ lažan. Pri tome je cilj izvršiti diskreditaciju i kompromitaciju ciljane grupe kako bi se smanjio njen utjecaj i podrška javnosti.

Primjer: Maliciozni akter koji nastoji narušiti ugled grupe koja se bori za prava građana će kreirati nalog na društvenim mrežama, te kroz značajnu aktivnost steći veliki broj pristalica. Ponekad je moguće da navedeni nalog bude podržan botovima i trolovima koji će mu dati kredibilitet. Nakon stjecanja podrške publike, nalog će započeti sa širenjem vijesti koje su dvosmislene, djelimično istinite ili su u potpunosti istinite ali se stavljaju u negativan kontekst. U početnoj fazi djelovanja laži koje se diseminiraju je teško uočiti. Nakon širenja laži, moguće je započeti i sa ekstremnijim aktivnostima poput ekstremizma i radikalizma, pri čemu se poziva na nasilje i mržnju prema državi i njenim institucijama, ili drugim grupama građana. Sa navedenim se postiže polaritet te diskredituju stvarni napori ciljane grupe da skupe podršku drugih građana i stvore pogodnu promjenu. Agitatori u ovom slučaju mogu u potpunosti diskredititrat i grupu građana koja se bori za ljudska prava, zatim pokrenuti val nasilja na koji će država odgovoriti silom i u potpunosti onemogućiti bilo kakav oblik druge borbe za prava. Naravno, šira javnost će se odmah ograditi od navedene grupe, povući svoju podršku i prestati sa bilo kakvim aktivnostima borbe za svoja prava.

3.2.2. Doxxing

Doxxing predstavlja efikasnu strategiju za utišavanje, zastrašivanje i fizičko ugrožavanje onih koji se ne priklanjaju određenim narativima ili koji postaju smetnja zbog svog političko - društvenog utjecaja na društvenim mrežama i drugim medijima. Doxxing predstavlja OSINT proces u kojem se prikupljaju privatni podaci subjekta ili grupe kao što su adresa stanovanja, broj članova porodice i informacije o njima (gdje rade, gdje idu u školu, zdravstveno stanje),

IP adresu[7], privatne fotografije i drugo. Iznošenjem privatnih podataka na društvene mreže ili određene servise, nastoji se zastrašit meta kroz ukazivanje na to da je njihov privatni život podložan infiltraciji drugih. Iznošenjem privatnih stvari poput zdravstvenog i finansijskog stanja ili porodičnih (ne)prilika, nastoji se diskreditirati lice (korištenje *argumentum ad hominem*) pri čemu ono može izgubiti značajan broj sljedbenika i tako umanjiti svoje poruke vezane za građanska prava ili ukazivanje djelovanja agresivnih aktera koji ugrožavaju nacionalnu sigurnost.

Primjer: Aktivista koji se bori ljudska prava i slobode postaje meta doxxera, koji nadziranjem njegovih društvenih mreža i servisa koje koristi upotrebom OSINT alata, dolaze do podataka o njegovom mjestu stanovanja kroz pribavljanje IP adrese[8], *data miningom*[9] njegovih naloga na društvenim mrežama ili jednostavnom evidencijom dnevnih aktivnosti ukoliko je korisnik aktivan na društvenim mrežama poput Instagrama, Twittera ili TikToka gdje objavljuje događaje iz privatnog života. Nakon što se prikupe ovi podaci, oni se iznose na društvenim mrežama, najčešće koordinirano od strane više lažnih naloga s ciljem zastrašivanja. Ukoliko se pronađu „prljavi detalji" kao što su razni fetiši, porodični problemi i slično, oni se preuveličavaju ili se u potpunosti fingiraju i grade na već postojećim činjenicama.

3.2.3. Upotreba lažnih identiteta

Lažni identiteti se upotrebljavaju u svakodnevnom online prisustvu, a naročito za stvaranje polarizacije prilikom diskusije na društvenim mrežama ili kao sredstvo podrške agitatoru i agresivnom akteru kako bi se njegovo mišljenje i stav pokazali prihvatljvim. Lažni identiteti mogu se koristiti i za druge aktivnosti kao što je dezinformiranje, špijunažu drugih, prikupljanje određenih podataka u interesnim grupama, širenje propagande, kreiranje botovskih mreža, izvođenje prevara i tako dalje. Mogućnosti i svrhe upotrebe lažnog identiteta su beskonačne, te se mogu međusobno isprepletati.

Primjer: nalog na nekoj društvenoj mreži koji prikazuje atraktivnu žensku osobu može da stekne značajnu popularnost, nakon čega se provodi dezinformiranje, širenje propagande ili prevara (razne donacije na servisima poput CashApp, Apple Cash, Xbon i tako dalje). Lažni identitet se može koristiti i u false falg

[7] IP adresa (Internet protokol) je jedinstveni broj koji identificira uređaj na Interenetu ili lokalnoj mreži. U biti, IP adrese su identifikator koji omogućuje slanje informacija između uređaja na mreži: one sadrže podatke o lokaciji i čine uređaje dostupnima za komunikaciju.

[8] Navedeno pribavljanje IP adrese nije značajna prepreka za pripadnike obavještajnih službi ili paralelnih – paradržavnih sigurnosnih sistema.

[9] Data mining /rudarenje podataka je proces sortiranja velikih skupova podataka kako bi se identificirali obrasci i odnosi koji mogu pomoći u rješavanju poslovnih problema analizom podataka.

narativima za evidenciju, praćenje i nadzor pristalica određenih ideja, pokreta i narativa.

3.2.4. Korištenje memova kao nosioca ideje

Pojavom interenta i širenja informacija na društvenim mrežama, omogućeno je kreiranje i specifičnih nosioca informacije - mema. Meme je istovremeno jednostavno ali i teško definisati. Svi neprestano gledamo memeove na društvenim mrežama i jednostavno ih definišem kao „šaljive slike sa natpisom“, međutim, njihova uloga i značaj su dosta veći odpukog nasmijavanja. U Evolutionary Psychology, Memes and the Origin of War (2006), Keith Henson je definirao meme kao "*repliciranje informacijskih obrazaca: načina da se nešto učini, naučenih elemenata kulture, uvjerenja ili ideja*." Sam meme se pojavljuje i u razmatranjima vojnih stručnjaka poput potpukovnika Prossera (2005), za koga memovi predstavljaju značajan alat američke vojske u psihološkim (PSYOP) i informativnim (IO) operacijama i strateškom komuniciranju unutar nelinearnog ratovanja, jer se putem njih utječe na stavove (neprijatelja, saveznika i neutralnih aktera). Meme kao „šaljiva slika“ zapravo šalje određenu informaciju i uspostavlja trend zasnovan na činjenici ili preptostavci kroz ironiju, sarkazam ili cinizam. Putem njih je moguće postaviti temelje za izgradnju društveno-političkog trenda ili formirati stavove o prihvatanju ili odbacivanju političkog kandidata / stranke ili određenog političkog procesa. Može se koristiti i za promociju nacionalizma, mržnje ili ideologije. Ono što je specifično za memove jeste da kvalitetni memovi ne mogu nastati vještačkim putem od strane državnog službenika koji je zadužen za njih od svog nadređenog i lično ne poznaje određene internet trendove i kulture. Naveden kulture i trendovi na interentu se ne mogu naučiti kroz prezentacije, brifinge ili obavještajne analize. One su nešto što korisnik interneta prirodno usvaja i kreira kroz svoje aktivnosti na društvenim mrežama. Za navedeno postoje i dokazi, jer su mnoge operacije državnih institucija propale zbog toga što su njihovi agenti bili diskreditirani u komentarima kao „feds“[10] zbog memova koji odišu birokratijom i vještačkim duhom, pisanjem i kreiranjem. To proizilaz iz generacijskog jaza i razumijevanja internet kulture između dvije grupe: boomera[11] sa jedne strane i milenijalaca[12] i

[10] Kolokvijalni internet naziv za policiju – kratica riječi Federal police, a ponekad se odnosi i na agente FBI i drugih obavještajnih agencija. Ponekad se koristi i riječ *spooks* – odnosno utvare / prikaze, za agente CIA-e, NSA, FBI i drugih službi koje djeluju aktivno na društvenim mrežama. Vidjeti primjere na Twitter nalogu: Posts By Feds (@SuspectFed).

[11] Boomer (baby boomer) predstavlja naziv za demografsku kohortu rođenih u periodu 1946-1964. godine, ali zbog svog ciničnog i ironičnog značenja povezanog sa nerazumijevanjem interent kulture i tehnologije, ponekad je oznaka i za sve one koji su rođeni prije 90-ih godina prošlog stoljeća.

[12] Milenijalac, izraz koji se koristi za opisivanje osobe rođene između 1981. i 1996. godine, mada su od strane generacije Z prozvani i kao boomeri (najčešće zbog svoje starosti). Riječnici ne definišu ko je boomer ili milenijalac, već to rade interent korisnici kao dominantni akter internet kulture.

generacija Z[13] sa druge strane. Da bi memovi bili uspješni u prenošenju poruke i da bi postigli viralnost, oni moraju biti „organski“, odnosno moraju biti kreirni od nekoga ko dobro poznaje Internet kulturu i trendove i ko je odrastao u njoj. Također, viralnost se postiže kroz njihov kvalitet koji korelira sa kratkom ali suštinski jakom i sadržajnom porukom. Ono što je specifično za memove kao nosioce ideja jeste da su politički desno orjentirane grupe uspješnije u kreiranju memova, dok ideološka ljevica previše ulaže u objašnjavanje ideje (koriste puno teksta koji diskreditira ideju i kreatora). Danas prosječni adolescent korištenjem memova može napraviti kvalitetnu viralnu kampanju za regrutaciju u vosjku ili favoriziranje određenih političkih ličnosti korištenjem mobilnog telefona i aplikacija društvenih mreža (Instagram, Tiktok) da kreira bolji propagandni video nego školovani i obrazovani scenaristi. Navedeni video sadržaji sa sufiksom – *wave*[14], *core*[15] i drugo mogu da budu simpatični korisniku koji se positovjećuje sa idejom, likom ili djelom onoga ko je predmet meme-a ili video sadržaja.

Primjer: Ukoliko se želi promovirati određeni politički akter, standardni porpagandni posteri sa porukom čine kontraefekat. Veći učinak se postiže kroz satiru i ironiju koja ističe i naglašava određene osobine kandidata i čini ga ili ljudskim ili značajno superiornijim od običnog čovjeka (poistovjećivanje sa superherojima i tako dalje). Također, kroz memove se može vršiti i omalovažavanje pritivnika što nekada ima veći učinak nego valorizacija vlastitog favorita. Da bi meme bio uspješan, mora se prvenstveno obaviti istraživanje trenda koji se posmatra i koristi za slanje poruke.

3.2.5. Kreiranje i diseminacija teorija zavjere

Teorije zavjere predstavljaju specifičan koncept kojim se šalju određene poruke, ali i izazivaju emocije kod šire publike. Teorije zavjere nikada ne mogu biti uspješne ukoliko se ne provode u sadejstvu sa drugim online aktivnostima poput dezinformisanja, kontrole narativa, pravljenja memova i tako dalje. Ono što je specifično za teorije zavjere jeste da su one viralno sredstvo za stavljanje u pokret inertnih masa, kao i sredstvo za širenje panike ili mržnje.

Ono što teorije zavjera čini odličnim sredstvom za kontrolu narativa jeste njihova dvostruka upotreba i svrha. Prvi koncept se zasniva na kreiranju i širenju zavjera kako bi se izazvali strah i panika, te zastrašio protivnik ili vlastito stanovništvo. U historiji postoje različiti primjeri korištenja teorija zavjera za stvaranje panike i oni se brzo otkriju kao laž. Drugi koncept predstavlja dublju psihološku

[13] Collinsov riječnik definira generaciju Z kao "pripadnike generacije ljudi rođene između sredine 1990-ih i sredine 2010-ih..

[14] Navedeni termin je sufiks za mikrožanr ironične popkulture koji proizilazi iz unikatnih, specifičnih trendova.

[15] Slično terminu –wave, ali se zasniva na određenoj aktivnosti ili stilu života oko koje se formira ličnost pojedinca. Npr: *techcore*, *militarycore*, *pilotcore*, *techbrocore*, *financialbrocore* i tako dalje.

operaciju koja služi za razbijanje kredibiliteta nekog pojedinca ili grupe koji imaju insajderske informacije o nekom događaju ili nekom entitetu (korporaciji, vladi, instituciji, organizaciji ili pojedincu) i njihovim ilegalim, nemoralnim ili neetičkim aktivnostima. Navedena operacija se poduzima kroz kreiranje lažnog ili stvarnog naloga na društvenim mrežama uz pomoć botova koji podržavaju navedeni glavni nalog. Zatim se plasiraju određene informacije koje su usko povezane sa tačnim informacijama vezanim za navedeni entitet ili subjekta, s tim da su informacije očito nerealne i netačne. Zatim se u dužem vremenskom periodu pojavljuju slični nalozi sa istim ili modifikovanim modusom djelovanja. Šira publika će ove deluzione subjekte vidjeti upravo kao takve, te će i prave *whistle blowere* svrstati u istu kategoriju. Što je više naloga koji se bavi navedenim pitanjem koje je iznio *whistle blower*, to će suludije izgledati prava informacija, te će društvo početi da je zanemaruje ili odbacuje kao lažnu.

3.2.6. Dezinformisanje

Dezinformisanje predstavlja jednu od najpopularnijih strategija i taktika djelovanja unutar medijskog i informativnog prostora koja svoje korijeme ima još u vremenu Prvog i Drugog svjetskog rata, kao i perioda blokvoske podjele svijeta. Kada se govori o definisanju ovog fenomena, on se može smatrati blažim oblikom lažnih vijesti, a u nekim slučajevima je rezultat nepreciznog ili nepotpunog prenošenja vijesti, čime se mijenja njeno izvorno značenje i navodi na pogrešne zaključke o temi ili pojavi o kojoj se izvještava (Raskrinkavanje, 2019). Cilj agresivnog i malicioznog aktera nikada nije da pusti u eter potpuno netačnu ili lažnu informaciju koja se može otkriti, jer bi to samo našteilo kreatorima kampanje. Stoga, dezinformacija koja se diseminira uvijek u sebi ima određeni postotak istinitosti, te se konzumentu preprušta zaključivanje kroz sublimianlnu argumentaciju upotrebom sintakse i emotivno nabijenih riječi. Konzument ove deziformacije može da doprinese njenom širenju kroz njeno shvatanje kao istine i dijeljenje iste sa drugima. Ovo razumijevanje dezinformacije kao istine i njeno dalje širenje se u literaturi naziva još i misinformacija.

Manipulacija informacijama u medijskom prostoru nikada nije bila zastupljenija, raširenija i dostupnija većem broju ljudi nego sada. Društvene mreže su omogućile širenje neprovjerenog, neverifikovanog, netačnog i poluistinitog sadržaja koji može biti potvrđen / verificiran od strane aktera koji ima određenu političko – društvenu agendu. Same dezinformacijske kampanje koje provode unutar medijskog prostora imaju za cilj da stvore polaritet, radikaliziraju, postaknu na nasilje ili mržnju, ili da izazovu strah i paniku.

Upotreba dezinformacija na društvenim mrežama predstavlja zanačajan i bitan aspekt psiholoških operacija. Same dezinformacije mogu biti usmjerene kako prema neprijatelju kako bi se narušio njegov moral, tako i prema vlastitom stanovništvu kako bi formiralo određene stavove. Navedeni stavovi su produkt neprimjetne manipulacije koja se provodi kroz laži u medijskom prostoru. Claire

Wardle (2016) navodi šest tipova lažnih informacija, a koje se mogu koristiti u psihološkim operacijama: autentični materijal korišten u pogrešnom kontekstu, sajtovi za lažne vijesti dizajniran da izgledaju kao brendovi koje već poznajemo, lažne vijesti, lažne informacije, manipulirani sadržaj, parodijski sadržaj. Na osnovu postojećih informativnih materijala, dezinformacijski akteri djeluju tako što će kroz kontroverzne naslove i modifikaciju konteksta informacije nastojati da pošalju subliminalne poruke.

3.3. Suradnja između državnih aktera i malicioznih grupa

Provođenje psiholoških operacija na društvenim mrežama s ciljem promjene narativa ili stvaranja novih društveno – političkih trendova zahjteva značajnu potporu i podršku, kako materijalnu i finansijsku, tako i ideološku, organizacijsku i kontraobavještajnu – sigurnosnu. Operacije nedržavnih, malicioznih aktera i grupa koje se provode u online prostoru da bi bile uspješne, efektivne i učinkovite, zahtjevaju postojanje veze, imperativno tajne, državnim institucijama, organizacijama i visoko hijerarhijski pozicioniranim državničkim subjektima. Uspješnost psiholoških operacija uveliko ovisi o snazi navedene veze, jer se maliciozne grupe pojavljuju kao „izvođači radova“, dok državni akteri samo daju naloge za djelovanje i finansiraju operacije.

Kada se govori o državnim akterima, njihovi ciljevi su zasnovani na ugrožavanju, uništavanju ili stavljanju pod kontrolu svoju metu i ciljanu publiku, te psihološke operacije u ovom slučaju predstavljaju alat nekonvencionalnog rata. Da bi se uspješno utjecalo na druge (neprijatelja, neutralnog aktera ili saveznika i vlastito stanovništvo), potrebno je uložiti značajne količine sredstava i resursa, prvenstveno novca kojim se kupuju materijalno – tehnička sredstva ali i profesionalni kadrovi, te „radna snaga“, odnosno aktivisti. Također, državni akteri (institucija, organizacija, partija, političar) su istinski kreatori ideja i narativa, te na osnovu njih daju zadatke malicioznim grupama. Ideološka indoktrinacija i ideološka kompatibilinost su imperativ za uspjeh navedenih operacija, ali da bi se u konačnici operacija provela uspješno, potrebni su profesionalizirani kadrovi unutar maliciozne grupe. Ovi kadrovi prvenstveno trebaju razumjeti zadatke, te samostalno pronaći način kako da ih realiziraju. Kreativnost je također veoma bitan „resurs“ koji se ne može kupiti, te svakodnevna prilagodba društveno-političkoj situaciji i kapitalizacija novonastalih događaja proizvodi efektivne učinke.

Posebno je važno istaknuti kontraobavještajnu aktivnost, odnosno zaštitu grupe ili pojedinca koji provode psihološke operacija. To nalaže obustavljanje ili opstruiranje bilo kakvih istraga koje bi se mogle provoditi protiv njih. Isto tako, neophodno je osigurati da navedeni akteri na online prostoru ne budu predmet nadzora obavještajnih službi ili određenih cyber sektora kriminalističke policije. S obzirom da aktivnosti psihološkog djelovanja mogu biti uočljive i postaju predmet interesovanja, kontrola sigurnosnih aktera (obavještajne službe, policije,

cyber policije itd.) omogćava smanjenje mogućnosti od kompromitacije i povećava uspješnost utjecaja. Stoga, borba protiv psiholoških operacije postaje izrazito teška, te gotovo nemoguća ukoliko se ne identificiraju metode, mjere i akteri, te poduzmu vlastite kontrapsihološke operacije.

4. Utjecaj psiholoških operacija na nacionalnu sigurnost i borba protiv njih

Zaštita nacionalne sigurnosti u modernom vremenu nije više rezervirano samo na fizičke prijetnje, već i one koje egzistiraju u nematerijalnom svijetu. Borba protiv nekonvencionalnih prijetnji, kao što su neprijateljske psihološke operacije na društvenim mrežama, zahtjevaju angažiranje cjelokupnog sigurnosnog sektora, ili kreiranje posebnih elemenata koji će se baviti tom tematikom.

Posljedice koje mogu nastati neprijateljskim djelovanjem su mnogostruke, suštinski uništavaju društvo i naciju, slabe državnu politiku, te mogu dovesti do većih negativnih ili katastrofalnih posljedica kao što su pobune ili građanski ratovi. Kada se govori posljedicama i rizicima koji nastaju slobodnim i neograničenim djelovanjem malicioznih aktera, na prvom mjestu uvijek stradaju demokratski procesi. Utjecaj na javno mijenje kroz dugoročne psihološke operacije i kampanje kojim se stvaraju novi narativi, značajno će utjecati na odluke stanovništva i činiti ih podložnijim utjecaju drugih, stranih, politički agresivnih aktera. Ponovno na vidjelo izlaze socijalna nestabilnost i društvene podjele kao rezultat kontinuiranog, decentraliziranog i višesektorskog malicioznog djelovanja aktera, ali i prirodne pojave rađanja opozicije i novih političkih struja koje se bore za vlast.

Efektivna borba protiv psiholoških operacija na društvenim mrežama zahtjeva kolosalni angažman državnog sigurnosnog sektora, te nevladnih organizacija koje se bore za ljudska i građanska prava. Državni sektor, ondosno obavještajna / kontraobavještajna služba, te cyber odjeli policije[16], mora da kontinuirano provodi monitoring na društvenim mrežama, te da određene aktere označava kao moguće strane agente. Zbog senzibilnosti u zadiranje u ljudska prava i slobode, kao i ograničavanje govora, naveden aktivnosti moraju biti dokumentovane, evidentirane, te podložne promjenama i reviziji etičkih *ad hoc* ili stalnih komiteta. Pored monitoringa sumnjivog malicioznog ponašanja, potrebno je vršiti evidencije grupa ili pojedinaca koje šire iste ili slične ideje, pratiti njihov sadržaj, te kreirati adekvatne procjene rizika i mogućnost širenja malicioznih ideja koje mogu proizvestu unutrašnji razdor i podjele.

Kreiranje posebnih državnih tijela koja surađujuju sa nevladinim organizacijama predstavlja imperativ borbe protiv psiholoških operacija i agresivnih kampanja na

[16] U zavisnost od državnog i društvenog uređenja neke države. Koncept nije uslovljen samo na Bosnu i Hercegovinu.

društvenim mrežama. Ova posebna tijela bi trebala imati formu obavještajno-kriminlističke službe koja nadgleda aktivnosti korisnika na društvenim mrežama, prikuplja podatke, utrvđuje činjenice te prati sumnjive aktivnosti poput djelovanja botova i trolova stranog agresivnog aktera. Također, uz suradnju sa nevladinim organizacijama, moguće je provesti kontrapsihološke kampanje i operacije koje bi za cilj imale kompromitaciju malicioznih aktera, te povećavanje rezilijentnosti građana na neprijateljsko djelovanje. Navedeno se može postići koordiniranim kampanjama povećanja svijesti, objavljivanjem publikacija u kojima se daju dokazi i činjenice o neprijateljskom djelovanju, te aktivno djelovanje na društvenim mrežama – naročito u formi podcasta i emisija sa raznim stručnjacima koji vrše demistifikaciju i razotrkivaju maliciozne i agresivne operacije. Ključ uspjeha borbe protiv psiholoških operacija na društvenim mrežama jeste njihovo razotrkivanje, te provođenje vlastitih kontrapsiholoških i kontrapropagandnih operacija.

Zaključci i preporuke

Moderno tehnološki superiorno vrijeme je u potpunosti promijenilo paradigmu modernog rata. Rat više nije moguće dobiti samo oružanim putem, već je potrebno u potpunosti potčiniti targetiranu naciju i društvo, što se čini uz pomoć pruštvenih mreža i psihološkim operacijama n anjima. Ljudski um je postao novo bojno polje na kojem se vode bitke i operacije, pri čemu se otvorila Pandorina kutija novih prijetnji i sredstava ugrožavanja. Navedena evolucija u razumijevanju rata i ratnih operacija zahtjeva poduzimanje određenih mjera kojima se onemogućava neprijateljsko djelovanje na umove građana koj su više nego ikada izloženi neprijateljskom agresivnom i malicioznom djelovanju. Speciifčnost ovoga se nalazi u upotrebi moderne tehnologije i socijalnih trendova kao što su društvene mreže. Kreiranje i širenje video/audio i tekstualnog sadržaja u koji se mogu inkorporirati informacije koje imaju za cilj stvaranje unutrašnjih podjela, straha, mržnje i drugog. Danas, informacije imaju značajno veći utjecaj na ljudski život, naročito zbog svoje viralnosti, ali i percepcije onih koji su primarne mete i konzumenti. Informacije, odnosno manipulisani sadržaji i šire operacije utjecaja mogu da proizvedu socijalne nemire i omoguće neprijateljskim agresivnim akterima da postignu destabilizaciju države i nacije bez upotrebe konvencionalnih metoda - vojnih, političkih, diplomatskih, ekonomskih ili nekih drugih. Međutim nekonvencionalne, psihološke operacije mogu biti i izvođene u sadejstvu sa konvencionalnim metodama destabilizacije, pri čemu je njihov utjecaj još veći.

Napad na um čovjeka i cjelokuponog društva danas predstavlja efektivno sredstvo za ostvarivanje agresivnih ciljeva, zbog čega je neophodno poduzeti značajne aktivnosti kako bi se to onemogućilo. Društvene mreže predstavljaju pogodno sredstvo i alat za agresivno djelovanje malicioznih aktera na um čovjeka. Zbog toga, neophodno je izučavanje istih, kako društvenih mreža, tako i njihove

primjenjivosti u psihološkim operacijama stranih državnih i nedržavnih aktera koji kontinuirano prijete. Pored izučavanja, neophodno je poduzimati kontraPSYOP aktivnosti, kojima se onemogućava agresvinom i malicioznom akteru da formuliše i održava njemu pogodan narativ koji se sa društvnih mreža prenosi u realnost.

Zbog navedenog, neophodno je navesti preporuke za efektivnu borbu protiv ove prijetnje:

- Kreiranje samostalnih organizacionih jedinica pri Ministarstvima sigurnosti, odbrane ili njihovim ekvivalentima koje se bore protiv neprijateljskih psiholoških i informativnih operacija;
- Formiranje istraživačkih centara koji se bave problematikom psiholoških operacija i informacionog ratovanja;
- Izvođenje kontraPSYOP operacija;
- Evidencija, klasifikacija i nadzor agresivnih i malicioznih aktera koji djeluju u online prostoru;
- Kontinuirani cyber nadzor nad malicioznim i agresivnim akterima;
- Kreiranje baze podataka agresivnih aktera i njihovih PSYOP operacija kako bi se izvršila identifikacija i klasifikacija;
- Izučavanje strategija, operacija i taktika psiholoških operacija na društvenim mrežama;
- Cyber kontrola na društvenim mrežama;
- Suradnja sa nevladinim organizacijama koje se bore za građanska i ljudska prava;
- Edukacija širih društvenih skupina, naročito djece i adolescenata;
- Aktivno djelovanje na društvenim mrežama u različitim formatima;
- Objavljivanje publikacija i raskrinkavanje agresivnih i malicioznih aktera i njihovih psiholoških operacija na društvenim mrežama;
- Redovito izvještavanje javnosti putem medija;
- Otvoreni kanal veze za građane kako bi ukazali na specifične dezinformacijske trendove;
- Kontrola i nadzor cyber prostora u odnosu na maligne aktivnosti.

Ove aktivnosti poduzete od državnih agencija će omogućiti smanjenje ili potpuno uklanjanje agresivnog i malicioznog djelovanja neprijateljskih aktera, koji fokus svoje borbe zasnivaju na primjeni nekonvencionalnih sredstava i metoda. Ograničavanjem djelovanja na cyber nivou, uveliko se sprječava širenje agresivne propagande, indoktrinacije te dezinformacije, a samim time i podložnost društva da postane potčinjeno neprijateljskom agresivnom akteru.

Literatura

Al Jazeera Staff. (20. 10 2023). *Investigations reveal discrepancies in Israel's Gaza hospital attack claims.* Preuzeto od Al Jazeera: https://www.aljazeera.com/news/2023/10/20/what-have-open-source-videos-revealed-about-the-gaza-hospital-explosion

Andrew, C., & Mitrokhin, V. (2000). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of KGB.* Basic Books.

BBC News. (09. 10 2019). *Russian trolls' chief target was 'black US voters' in 2016*. Preuzeto od BBC News: https://www.bbc.com/news/technology-49987657

Bubola, E. (01. 05 2022). *Ukraine acknowledges that the 'Ghost of Kyiv' is a myth*. Preuzeto od The New York Times: https://www.nytimes.com/2022/05/01/world/europe/ghost-kyiv-ukraine-myth.html

Cadwalladr, C., & Graham-Harrison, E. (17. 03 2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* Preuzeto od The Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cambridge Dictionary. (2023). *Propaganda*. Preuzeto od Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/propaganda

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact",. *MIS Quarterly*, 1165-1188.

Culliford, E. (12. 10 2020). *How political campaigns use your data*. Preuzeto od Reuters: https://www.reuters.com/graphics/USA-ELECTION/DATA-VISUAL/yxmvjjgojvr/

Cusick, S. G. (2006). Music as torture / Music as weapon. *Sociodad de Etnomusicologia TRANS 10*.

European External Action Service (EEAS). (2020). *EUMC Glossary of acronyms and definitions - Revision 2019.* Brussels: European Union Military Committee (EUMC).

Fridman, O., Kabernik, V., & Granelli, F. (2022). *Info Ops - From World War I to the Twitter Era.* London: Lyne Reinner.

Gilbert, D. (18. 10 2023). *Who's Responsible for the Gaza Hospital Explosion? Here's Why It's Hard to Know What's Real*. Preuzeto od Wired:

https://www.wired.com/story/al-ahli-baptist-hospital-explosion-disinformation-osint/

Giles, K. (2016). *Handbook of Russian Information Warfare.* Rome, Italy: NATO Defense College.

Goulart, K. (2024). *Social network*. Preuzeto 07. 11 2023 iz TechTarget: https://www.techtarget.com/searchcio/definition/social-network

Henson, K. (2006). Evolutionary psychology, memes and the origin of war. *Mankind Quarterly*, 443-459.

Hern, A. (06. 05 2018). *Cambridge Analytica: how did it turn clicks into votes?* Preuzeto od The Guardian: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Humphrey, C. (16. 09 2023). *The Ghostly Legacies of America's War in Vietnam*. Preuzeto od The Foreign Policy: https://foreignpolicy.com/2023/09/16/vietnam-war-psyops-ghosts/

Joint Chiefs of Staff (JCS). (2010). *Joint Publication 3-13.2 - Psychological Operations.* Washington DC: Joint Chiefs of Staff (JCS).

Khouri, R. G. (13. 10 2023). *Watching the watchdogs: Babies and truth die together in Israel-Palestine.* Preuzeto od Al-Jazeera: https://www.aljazeera.com/opinions/2023/10/13/watching-the-watchdogs-babies-and-truth-die-together-in-israel-palestine

Kramer, M. (26. 05 2020). *Lessons From Operation "Denver," the KGB's Massive AIDS Disinformation Campaign*. Preuzeto od The MIT Press Reader: https://thereader.mitpress.mit.edu/operation-denver-kgb-aids-disinformation-campaign/

Lakić, Z., Kovačević, Z., & Kovačević, I. (2024). Terorizam - bezjednosna prijetnja Zapadnom Balkanu. *Zaštita i sigurnost, godina 4., broj 2.*, 191-201.

Lasswell, H. D. (1995). Propaganda. U R. Jackall, *Propaganda* (str. 13). New York : New York University Press.

Levin, S. (30. 09 2017). *Did Russia fake black activism on Facebook to sow division in the US?* Preuzeto od The Guardian: https://www.theguardian.com/technology/2017/sep/30/blacktivist-facebook-account-russia-us-election

Levin, S., Solon, O., & Walker, S. (21. 10 2017). *'Our pain for their gain': the American activists manipulated by Russian trolls*. Preuzeto od The guardian: https://www.theguardian.com/world/2017/oct/21/russia-social-media-activism-blacktivist

Mauss, I. B., Shallcross, A. J., Troy, A. S., John, O. P., Ferrer, E., Wilhelm, F. H., & Gross, J. J. (2011). Don't hide your happiness! Positive emotion dissociation, social connectedness, and psychological functioning. *Journal of Personality and Social Psychology*, 738–748.

Merriam - Webster. (2019). *Disinformation*. Preuzeto od Merriam - Webster: https://www.merriam-webster.com/dictionary/disinformation

Mshvidobadze, K. (21. 03 2011). *The Battlefield On Your Laptop*. Preuzeto od Radio Free Europe: https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, godina 4., broj 2.*, 314-339.

NATO Standardization Agency . (2013). *NATO Glossary of Terms and Definitions.* Brussels, Belgium: NATO Standardization Agency .

Newton, K. (08. 08 2019). *Aspidistra: The wartime breakthrough you've never heard of.* Preuzeto od History of government: https://history.blog.gov.uk/2019/08/08/aspidistra-the-wartime-breakthrough-youve-never-heard-of/

Noor, A. S., Hosen, N., Hassan, N., Ismail, A. S., Rahim, F. N., & Tarmidi, Z. (2022). Active learning: Game-changer to short attention span in Gen Z. *New Academia Learning Innovation 2022*, (str. 369-371). Johor Bahru, Malaysia.

Prosser, M. (2005). *Memetics: A Growth Industry in US Military operations.* Quantico, Virginia: USMC, School of Advanced Warfighting, Marine Corps University.

Putterman, S. (25. 09 2023). *Politicians blame 'wokeism' for low military recruitment. The problem is more complex.* Preuzeto od PolitiFact: https://www.politifact.com/article/2023/sep/25/politicians-blame-wokeism-for-low-military-recruit/

RAF Upwood. (02 2002). *Radar and Radio*. Preuzeto od R.A.F. UPWOOD: http://www.rafupwood.co.uk/radarandradio.html

Raskrinkavanje. (2019). *Dezinformacija*. Preuzeto od Medijska pismenost: https://medijskapismenost.raskrinkavanje.ba/oblici-manipulacija-i-kome-se-obratiti-ako-ih-uocite/koji-sve-oblici-medijskih-manipulacija-postoje/dezinformacija/

Selhorst, A. (2016). Russia's Perception Warfare - The development of Gerasimov's doctrine in Estonia and Georgia and it's application in Ukraine. *Militaire Spectator*, 148-164.

Solmaz, M., & Call, E. (11. 10 2023). *Despite refutations from Israeli military, headlines that Hamas 'beheaded babies' persist*. Preuzeto od Anadolu Agency: https://www.aa.com.tr/en/middle-east/despite-refutations-from-israeli-military-headlines-that-hamas-beheaded-babies-persist/3016167

Solon, O. (19. 03 2018). *Facebook's value falls $37bn amid backlash from Cambridge Analytica data scandal*. Preuzeto od The Guardian: The Guardian. https://www.theguardian.com/news/2018/mar/19/facebook-value-declines-data-scandal

Thomas, T. L. (1997). Russian Information-Psychological Actions: Implications for U.S. PSYOP. *Special Warfare*, 12-19.

U.S. Department of Defense. (2014). *Joint Publication 3-13.3, Psychological Operations.* Washington DC: U.S. Department of Defense.

US Army Special Operations Recruiting. (2023). *Psychological operations.* Preuzeto 07. 11 2023 iz https://www.goarmysof.army.mil/PO/

Wardle, C. (18. 11 2016). *6 types of misinformation circulated this election season*. Preuzeto od Columbia Journalism Review: https://www.cjr.org/tow_center/6_types_election_fake_news.php

PSYCHOLOGICAL OPERATIONS ON SOCIAL NETWORKS - EXAMPLES, TECHNIQUES, TACTICS AND PROCEDURES

DOI: *10.70329/2744-2403.2025.5.9.7*

Scientific article

Emir Muhić, MA

Absract:

This paper explores the transformation of warfare and security conflicts influenced by contemporary technological advancements, with a particular focus on the role of social networks in conducting psychological operations (PSYOP). It examines the techniques, tactics, and procedures employed to shape public opinion, manipulate perceptions, and disseminate disinformation through digital communication platforms. By providing an in-depth analysis of the strategies used on social media, the study discusses the implications for national security and democratic governance. It also offers recommendations and strategic guidelines for strengthening societal resilience against psychological threats emerging from the information space. The primary aim is to foster a deeper understanding of the pivotal role that social networks play in modern psychological warfare and to highlight the necessity of proactive institutional responses.

Keywords: *psychological operations, special warfare, propaganda, disinformation, unconventional warfare*

Introduction

The modern technological era has significantly changed the ways of conducting war and conflict. The conventional approach to warfare, based solely on weapons and large-scale battles, has never been sufficient. Commanders have always aimed to psychologically influence both the enemy and their own soldiers before launching a main attack. The psychological condition and morale of the enemy, especially regarding their will to fight, plays a crucial role—important battles are often won or lost based on it. With the evolution of human civilization and technology, there has been a "transfer" of human life from the physical world into the abstract cyber space, which has become an essential part of daily functioning for people across the globe. Internet technologies allow people to connect over long distances and enable the fast spread of news and information. However, they also open up the possibility of manipulating thoughts and influencing the way people think. Therefore, the role of social media is not only to connect, inform, and bring people closer, but also to shape opinions and attitudes. In the past decade, social media has become one of the most significant tools in the domain of modern psychological warfare and operations (referred to in this text as PSYOP). Social media plays a key role in contemporary psychological operations, allowing for the rapid spread of disinformation and manipulation of the target audience's perception. The use of social media in PSYOP significantly affects the formation of public opinion and the attitudes of target groups, making it possible to carry out aggressive political strategies by both state and non-state actors. Strategies and tactics used on social media in psychological operations evolve in line with changes in the digital environment and a state's foreign policy, and they adjust to shifts in social media algorithms and policies. Because of this, security institutions and government leadership must develop comprehensive strategies to counter psychological operations on social media in order to protect the state and society.

1. Psychological Operations and Social Media

Psychological operations (PSYOP) represent a significant aspect of military doctrine and strategy aimed at opposing adversaries. Historically, there has not been a single period in which tribes, empires, or kingdoms did not use some form of influence—either on their own army and population or on the enemy. Today, psychological operations use different modes and are based on variables such as technology, politics, culture, and narratives. Without the use of psychological operations and accompanying activities, it would not be possible to defeat the enemy or impose one's own will.

1.1 Defining and Understanding Psychological Operations Activities

When it comes to defining psychological operations, there are numerous definitions that vary across state and non-state actors around the world. For the purpose of standardizing terminology and achieving a better understanding, the following definitions will be used in this research:

1. **Psychological operations (PSYOP)** are planned operations that use selected information and feedback mechanisms to influence the emotions, attitudes, perceptions, and behavior of target audiences in order to support national policy goals, military objectives, and plans, and to promote shared interests (U.S. Department of Defense, 2014).
2. **Psychological operations (PSYOPS)** are deliberately planned activities conducted to deliver a specific message to a target audience, aiming to change their attitudes toward certain issues or to encourage specific actions (NATO Standardization Agency, 2013).
3. **Planned, culturally sensitive, truthful, and attributable activities** that use communication methods aimed at a politically approved target audience, in order to influence perceptions, attitudes, and behavior in support of achieving the political and military goals of the EU (European External Action Service (EEAS), 2020).

In the context of the Western concept of PSYOP, U.S. policymakers realized that the term "psychological operations" carried negative connotations or was outdated, leading to a renaming of the concept. The U.S. Department of Defense, through the Joint Chiefs of Staff[17], revised the term "psychological operations" to **Military Information Support Operations (MISO)**. These represent: *planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives* (Joint Chiefs of Staff (JCS), 2010).

When examining Russia, a linguistic and ideological divergence becomes evident. Specifically, the Russians do not use the Western term *"psychological operations"*, but instead refer to *"information-psychological activities"* (Thomas, 1997) and the broader concept of *information warfare*, which includes a wider range of actions in both the informational and media domains (Giles, 2016). According to Mshvidobadze (2011), in an interview for Radio Free Europe, this

[17] **The Joint Chiefs of Staff** – is a body consisting of the highest-ranking uniformed leaders within the United States Department of Defense, which advises the President of the United States, the Secretary of Defense, the Homeland Security Council, and the National Security Council on military matters.

concept includes computer network operations alongside disciplines such as psychological operations (PsyOps), strategic communication, and influence, together with *"intelligence work, counterintelligence, camouflage, disinformation, electronic warfare, communication disruption, navigation support degradation, psychological pressure, and the destruction of enemy computer capabilities."* Accordingly, this represents *"an integrated system of tools, methods, and objectives aimed at influencing the perception and behavior of the enemy, the population, and the international community at all levels"* (Selhorst, 2016).

The specific purpose of psychological operations (PSYOP) is to influence the perception and subsequent behavior of foreign audiences as part of approved programs that support U.S. policy and military objectives. PSYOP professionals follow a carefully planned process that aligns the commander's objectives with an analysis of the environment; selects the relevant target audience; develops targeted messages and actions that are culturally and environmentally appropriate; uses sophisticated media delivery tools; and aims to generate visible, measurable behavioral responses (Joint Chiefs of Staff (JCS), 2010). Additionally, the official website of the U.S. Army Special Operations Command (US Army Special Operations Recruiting, 2023) describes PSYOP unit activities as follows: *"They analyze operational environments, physical targets, and target audiences; advise on psychological effects; plan influence options; develop actions and messages focused on psychological vulnerabilities; deliver actions and messages at the optimal time; and assess the effectiveness of the influence. Operating in small, autonomous teams, PSYOP units conduct military information support operations; Department of Defense deception activities; build partner influence capabilities; and, when requested by the President, provide information support to civil authorities."* Therefore, psychological operations have a clear and singular goal—to influence public opinion, whether of the domestic population, the enemy, or a neutral audience.

1.2 Examples of Psychological Operations Throughout History

In the context of warfare, psychological operations have often represented a powerful and decisive factor in achieving military victory. The purpose of psychological operations can include creating fear among opponents, reducing their willingness to fight, and instilling a sense of inferiority compared to their adversaries. With modernization and technological advancement, exotic animals (such as the elephants used by Hannibal Barca in his battles against Rome) and torture methods (like impalement used by Vlad the Impaler) no longer provoked the same level of fear among enemies. A new approach was therefore needed. This was pursued through the use of advanced weaponry, but also through written

words, particularly during World War I and World War II. In terms of weaponry, fear was induced by the Germans through the use of chemical weapons, or by the Americans using shotguns in trench warfare. When it comes to non-violent methods, the British led in this area, using pamphlets and other forms of propaganda to influence the fighting spirit of German troops (Fridman, Kabernik, & Granelli, 2022). The British government focused on three target audiences during the war: its own population, allies and neutral actors, and the enemy. At first, the government concentrated on patriotic propaganda at home, while also preparing the population for war and countering the domestic anti-war opposition (Fridman, Kabernik, & Granelli, 2022). This helped prevent a collapse of public morale and ensured national unity and integrity. Without such efforts, anti-war circles and hostile influence agents could have secured victory without major material or technical efforts. In other words, in the words of Sun Tzu, they would have achieved the most perfect victory—the one in which the enemy is subdued without fighting.

An important World War II example of propaganda through traditional media, especially radio, was **Operation Aspidistra,** carried out by the **Political Warfare Executive**. The operation was based on deception and the spreading of so-called black propaganda. The British posed as Germans and distributed false information. The second part of the operation focused on military deception: as part of a strategy to mislead German fighter pilots, German-speaking RAF[18] operators imitated German ground control officers and gave false instructions to night fighters (Newton, 2019). These pilots were directed to land or move to incorrect sectors. This disruption of enemy radio and wireless transmissions was known under the codename **"Dartboard"** (RAF Upwood, 2002).

Another example of psychological operations was the use of music, a tactic employed by American troops in **Vietnam, Panama,** and **Iraq**. In Vietnam, before and during air assaults, U.S. forces would broadcast rock music over loudspeakers mounted on helicopters. This act was more aimed at boosting the morale of their own troops rather than frightening the ideologically committed Vietnamese communists. Another method used to psychologically influence the enemy was the broadcasting of eerie screams at night. A recording known as **Ghost Tape Number 10** played a central role in **Operation Wandering Soul,** a psychological campaign that aimed to break the morale of North Vietnamese soldiers by exploiting their cultural beliefs and deepest fears (Humphrey, 2023). The recording featured cries and phrases such as: *"My body is gone. I am dead, my family... Tragic, how tragic! My friends, I have returned to tell you that I am dead. I am dead. I am in hell... Friends, while you are still alive... go home! Go*

[18] Royal Air Force.

home, my friends — before it is too late." (Humphrey, 2023) The choice of words was based on cultural and religious beliefs—specifically, the Buddhist idea that souls of those who are not properly buried wander the Earth in pain for eternity.

Another use of sound and music was characteristic in **Panama** and **Iraq**, where U.S. troops played loud music in an attempt to force Panamanian President **Manuel Noriega** to surrender. The use of "acoustic bombardment" became a standard practice on the battlefields in Iraq, and musical bombardment was combined with **sensory deprivation** and **sexual humiliation** as part of the **non-lethal tools** used to extract secrets from prisoners—from **Abu Ghraib** to **Guantanamo Bay**—without technically violating U.S. law (Cusick, 2006).

Soviet examples are also significant due to their scale and influence on the general public. One of the most well-known psychological operations—referred to by the Soviets as "psychological-informational activities"—was the spreading of the false claim that **AIDS and the HIV virus** were created in a U.S. military laboratory. This operation was called **Operation Denver** and was part of the Soviet Union's "active measures" aimed at generating hostility toward the United States—particularly in **Third World countries** where the disease was widespread. The operation was uncovered after the discovery of **KGB telegrams no. 2955 and 2742** sent to the Bulgarian KGB, as well as a telegram from East Germany's **Stasi** to the Bulgarian KGB (Kramer, 2020).

Psychological and psychological-informational operations aim not only to influence individuals in specific geographical regions—such as the jungles of Vietnam or a small town in Panama—but to have a **global impact**, putting pressure on major world powers, regional forces, and other geopolitical actors. This always begins by influencing individuals and groups, with the effect then spreading like a **virus**.

1.3 Social Media as a Tool of Psychological Operations

The emergence of the Internet naturally led to the creation of social media as a system for bringing people and information closer together across the globe. It enabled the connection of diverse individuals and distant parts of the world, as well as the rapid spread of information. Social media can be defined as *websites or applications that allow people to connect with each other on a shared platform. Users can share information, express opinions, explore shared interests, search for jobs, promote their businesses, build relationships, and otherwise communicate with one another. Those who participate in a social network often share a wide range of information and content, including photos, videos, audio clips, documents, news, marketing materials, or links to other sources. Social media platforms usually provide mechanisms for posting content such as photos,*

videos, blogs, or links to other sites. Other users can comment on or rate this content and recommend it to others (Goulart, 2024).

Some of the most well-known social media platforms include Facebook, 4Chan, X (formerly Twitter), Reddit, YouTube, Instagram, TikTok, Snapchat, Tumblr, and others. These platforms are based on the concept of sharing information—whether video, audio, text, or a combination of these formats. The goal of social media is not only to connect people but also to deliver certain types of information, which is achieved through audiovisual and textual content. The distribution of content on social media platforms such as Reddit, X (Twitter), Instagram, YouTube, and others can have an educational or informational character. Influential actors—known as influencers—share their opinions and views with a broader audience, including both their followers and those who are shown content by the algorithm. In the past, this role was performed by state-sponsored media—TV stations, radio broadcasters, and printed newspapers—where state propaganda was clearly visible. Social media blurs this propaganda element and creates the illusion of opinion diversity. However, real diversity often cannot exist due to the influence of certain actors and controlling elements. For example, Reddit is a social media platform based on "subreddits," or thematic subforums where users share content and information. However, there is significant control by moderators, who often act voluntarily and ideologically, limiting the spread of information. Reddit moderators are frequently aligned with extreme leftist political identities. Subreddit control is based on restricting content that questions dominant narratives, ideas, or identities, effectively preventing any discussion and enforcing dogmatic belief systems held by the moderators. For instance, moderators may ban users who do not share the same (often extreme) leftist beliefs, creating an "echo chamber" in which users within one subreddit hold conformist and politically uniform opinions. This mindset can easily spread to other topic-specific subreddits.

This is achieved by reviewing users' comment and post histories, based on which moderators may punish or ban someone from a subreddit simply for holding an opposing view on a completely unrelated topic (such as politics, religion, ideology, birthrates, and so on). Such a psychological and ideological "climate" leads to one-sidedness and uniformity, suggesting that there is only one truth and that all other views are wrong, thus giving the impression of a totalitarian system within a social media platform. On the other hand, social media platforms without moderators, such as 4Chan, do not restrict what can be said—regardless of whether it is politically correct—allowing for discussion and the exchange of ideas rather than the creation of echo chambers. This way of functioning enables various forms of cyber propaganda, such as spamming specific political ideas in support of or against certain groups, identities, or nations. However, a common

method is posting pornography in thematic subforums in order to reduce user activity at a given moment and to interrupt any discussion that is not going in the desired direction.

2. The Role of Social Media in Psychological Operations

Social media, as a technological novelty and an essential part of daily human life, plays a major role in the execution of psychological operations. By replacing traditional media such as television, radio, and printed newspapers—especially among young people or those without access to such media—social media has become the only and primary source of information. This means that it enables the delivery of the specific content and information that an aggressive actor wants to implant in the minds of the targeted audience. Social networks are a significant indicator of a person's life and as such should be fully utilized (Muhić, Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa, 2024). In recent years, with the advancement of big data and data mining techniques, the research community has noticed that open data represents a powerful source for analyzing social behavior and obtaining relevant information (Chen, Chiang, & Storey, 2012).

2.1 Methods of Using Social Media for Psychological Operations

Since social media represents a significant element in the battle for minds, it can be used in various ways to deceive, intimidate, and demoralize the enemy, as well as to control narratives that become socially accepted and enter the sphere of conformism. Social media has replaced standard and traditional methods of information dissemination, making it a significant force multiplier when conducting intelligence, military, or other operations—whether kinetic or non-kinetic in nature. In some cases the same could be compared to terrorism. At its root, it contains essential violence, and its ultimate goal is not only human victims and the material damage it causes, but the confirmation and symbolism of conveying terrifying messages to the population, where it deliberately strikes at the human psyche (Lakić, Kovačević, & Kovačević, Terorizam - bezjednosna prijetnja Zapadnom Balkanu, 2024).

2.1.1 Spreading Propaganda and Disinformation

Propaganda and disinformation activities are among the main strategies used by aggressive actors on social media. Propaganda has always been present in human society, and the transition from traditional media to social media has made it more accessible, richer in content, and more effective than other methods. Propaganda is defined as a technique of influencing human behavior through the manipulation of representations, which may take verbal, written, visual, or audio form (Lasswell, 1995). Similarly, the Cambridge Dictionary (2023) defines propaganda as information, ideas, opinions, or images—often just one side of an argument—

disseminated with the intention of influencing public opinion. The aim of influencing public opinion is typically achieved through specific information or content designed to trigger targeted emotions, depending on the needs, the audience, and the ultimate objective. Disinformation—false or misleading information—is often used to build an entirely new narrative.

By using disinformation on social media, it is possible to create complete chaos among a targeted audience, especially if the campaign is properly planned and executed. This requires knowledge of the cultural, religious, ideological, and political factors of a society, in order to inflict damage through audiovisual and textual content. Additionally, an influential actor who shares (dis)information must have an audience that trusts them. If such actors continuously spread lies, they will lose credibility—and with it, their followers. What can be observed on social media is that actors often share a mix of truth and partial truth, while fully false content is relatively rare. In other words, it could be said that approximately 80% of propaganda content is true, while the remaining 20% consists of half-truths or complete fabrications designed to deceive.

2.1.2 Selecting the Target Audience

In order to achieve the desired objectives, it is necessary to define the audience to whom propaganda and disinformation will be directed. First of all, it is essential to determine who the propaganda is aimed at—just as it was crucial for the British government during World War I. Propaganda and disinformation can be created for three types of groups: the domestic population, the enemy, and allies or neutral actors. The audience must be selected in order to tailor specific propaganda to them. During the 2015 U.S. presidential elections, **Cambridge Analytica**, based on its research into the preferences of different demographic groups (racial, ethnic, gender, and sexual), advised former President **Trump** on how to lead his campaign (Hern, 2018). This means that Trump's campaign focused mainly on ideological opponents and undecided voters, while supporters and loyal followers received less direct attention. This strategy was based on the assumption that loyal followers would support him anyway, and that resources should be directed toward persuading those who were undecided or opposed to his policies.

A successful psychological operation depends on two key factors:

1. a carefully selected audience, and
2. the social media platform preferred by that audience.

This must be determined because different age groups have different preferences and trends. For example, visually oriented platforms such as **TikTok** are more popular among children and young people, while older users prefer primarily text-

based or image-text platforms. Attention span is another crucial factor—among younger generations (commonly referred to as **Gen Z**), attention spans average around **8 seconds** (Noor et al., 2022), which is significantly shorter than in older generations. Therefore, content aimed at Gen Z must be adapted to short, video-based formats. The use of popular and influential individuals—**influencers**—to spread or react to content plays a major role in how widely that content is shared and how influential it becomes. In this process, the intelligence cycle that directs the creator's operations is also important, and it is very dynamic, continuous and endless (Muhić, Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa, 2024).

2.1.3 Creating Fake Profiles

Creating fake profiles is a method of manipulation on social media used to present certain ideas as favorable or widely accepted. This means that a group engaged in propaganda and disinformation creates a large number of seemingly legitimate accounts on one or more social media platforms. Through these accounts, they post content, write comments, and share other posts, making the material more visible and accessible to a broader audience. Fake profiles can also serve other purposes, such as attacking public figures with insults or threats, or supporting other actors and influencers by sharing and commenting on their content to stimulate discussion—and thus, trigger the platform's algorithm to increase its visibility. Additionally, fake profiles can be used to infiltrate and collect information within online interest groups. For example, through a well-crafted fake profile, an actor can gain access to specific groups and gather information, disrupt activities, create internal divisions, and fragment the group. By achieving **administrator status**, the actor can gain full access to member information and conversations, remove members, or in some cases, completely shut down or delete the group. This destroys nearly all the connections that were formed online, especially if they do not exist in the physical, material world.

2.1.4 Use of Algorithms

The use of algorithms for achieving virality allows propaganda and disinformation to reach a wider audience on social media platforms. Each algorithm operates based on a set of rules that constantly evolve. Because of this, social media platforms use specially designed algorithms as intelligent guides, with the task of carefully sorting and linking content to users who have similar preferences. This feature can be exploited when a targeted group needs to be exposed to specific propaganda or disinformation. For example, if the targeted group consists of adolescents who are fans of certain music stars or movies, it is possible to create video content that incorporates a celebrity or a movie scene, embedding specific messages or using visuals that resemble well-known clips. Visually engaging content with embedded political messages and attractive

individuals is often used to distribute propaganda. A direct example of this is the activity of the **Israeli Defense Forces (IDF)**, who often use soldiers—mostly blonde women—performing dances or engaging in trending activities on platforms like TikTok or Instagram to spread propaganda and exploit algorithmic virality. This strategy achieves two goals: a) content becomes viral, and b) it creates sympathy for the IDF. Such content is directed toward a specific audience, most often middle-aged or older men who are undecided or do not currently support Israel. Simply put, in this case, women are used as objects of attraction through which political messages are communicated to a broader audience.

2.1.5 Exploiting and Deepening Social Polarization

Actors conducting propaganda operations against a specific group, state, or region often take advantage of existing social divisions and unrest. Social divisions based on religion, politics, or other sectors can be exploited to promote particular ideas. These ideas are crafted to deepen the divide between two or more opposing groups, and it is not uncommon for **false flag operations** to be used. In other words, radical and extremist content is created that calls for violence, killings, ethnic cleansing, or genocide against a particular group—while the creators of the content pose as members of that same group. These operations are often carried out by members of foreign intelligence services from countries that have an interest in internal conflict within the targeted state. To successfully execute such a strategy, an initial advantage must be gained through the **virality** of the content. Once the content spreads, large groups of people voluntarily adopt these extremist and radical ideas simply because they appear popular or widely supported.

2.2 Examples and Case Studies of Psychological Operations on Social Media

2.2.1 Cambridge Analytica and the Presidential Elections

The 2016 presidential elections in the United States represent one of the most striking examples of psychological operations, carried out by both the Republican and Democratic parties. When it comes to the Republicans and their candidate Donald J. Trump, his campaign stood out for its sophisticated approach, especially due to the involvement of the British company Cambridge Analytica, which developed effective strategies for winning the hearts and minds of voters across the country. The methods used in the campaign, which became public in 2018, demonstrated how personal data from social media—specifically Facebook—could be used to precisely target political messages and ads, directly influencing the election process. In this context, the focus of analysis is not on the legality, ethics, or morality of these activities, but on their execution and operational effectiveness.

Cambridge Analytica was a political consulting firm specialized in using data mining techniques to help its clients expand their potential voter bases (Cadwalladr & Graham-Harrison, 2018). The scandal involved the misuse of raw data from more than 87 million Facebook profiles, which Facebook had failed to protect properly (Solon, 2018). The lack of proper data protection—or the possible sale of that data—enabled the creation of sophisticated informational and psychological operations aimed at indoctrinating broad segments of the population and influencing the course of the presidential election. In March 2018, Facebook was caught in a major data breach scandal in which Cambridge Analytica harvested the personal data of over 87 million Facebook users without their consent (Cadwalladr & Graham-Harrison, 2018). The data was allegedly used to benefit presidential candidate Donald Trump during the 2016 election (Cadwalladr & Graham-Harrison, 2018).

A survey created by Aleksandr Kogan, a British academic researcher who used Facebook for research purposes, was sent to 3 million Americans (Cadwalladr & Graham-Harrison, 2018). The survey, which appeared harmless and offered a symbolic financial reward, included 125 personality questions where respondents could agree or disagree, and was combined with users' Facebook data to create a **psychometric model**, similar to a personality profile (Cadwalladr & Graham-Harrison, 2018). This data was then combined with voter records and forwarded to Cambridge Analytica (Cadwalladr & Graham-Harrison, 2018). Data processing revealed which demographic groups—white men/women, Latino men/women, Black men/women, ethnic and sexual minorities, as well as long- time Republican/Democrat voters—should be the focus of campaign efforts.

The scandal led to a 17% drop in Facebook's stock value and sparked intense public and institutional calls for stricter legal frameworks regarding the protection of personal data collected and used by tech companies (Solon, 2018). Meta, the parent company of Facebook, agreed to pay 725 million USD to settle legal disputes arising from the case (Solon, 2018). The scandal affected other tech companies as well, forcing them to redefine their privacy policies and how they handle user data. Nonetheless, the case pointed to a significant risk of personal data misuse by third-party actors for private or political purposes. It also highlighted that such practices will likely continue in the future—with more caution and additional security measures. The **Cambridge Analytica case** marked a turning point in considering the relationship between social media, privacy, and digital security. It showed how vulnerable social media users' personal data is, and how easily it can be abused. It also emphasized the importance of protecting user privacy and the need for better regulation of the digital space.

However, the scandal did not signal the end of the trade in personal data by major tech corporations—on the contrary, it revealed the existence of serious and ongoing threats related to the unethical commercialization of users' digital footprints. In the context of political elections, both Republicans and Democrats work with data firms to build national voter databases, collecting information from many sources to create detailed voter profiles with thousands of data points and developing models that predict people's opinions on issues or candidates (Culliford, 2020).

In this context, one important question remains: do such forms of political activity represent an acceptable standard of democratic competition, and is the political process truly based on fairness and transparency?

2.2.2 Operation "Blacktivist"

The period of the U.S. presidential elections was extremely complex and marked by deep social tensions. Antagonistic actors—most notably Russia—sought to further destabilize American society by provoking and deepening existing societal divisions. The primary goal of such actions was to weaken the internal cohesion of the United States, thereby indirectly undermining its international standing. As previously documented in history, Russian intelligence services have used similar methods of destabilization. One such example is **Operation PANDORA**, launched on July 25, 1971, by Anatoli Tikhonovich Kireyev, head of the First (North American) Department of the KGB's Foreign Counterintelligence Directorate. He ordered the KGB's New York office to plant time-delayed explosive devices in an African American neighborhood. Kireyev's preferred target was one of the historically Black colleges, in an effort to spark a stronger inter-ethnic conflict, particularly between the African American and Jewish communities. Following the explosion, anonymous calls were to be made to several African American organizations claiming that the **Jewish Defense League** was responsible for the attack (Andrew & Mitrokhin, 2000). A modern version of these old tactics is **Operation "Blacktivist"**, a sophisticated psychological and disinformation campaign carried out by Russian actors on social media. The goal of this operation was to intensify existing racial tensions in the United States and provoke unrest, particularly in the context of the upcoming elections and narratives around police brutality (Levin, *Did Russia fake black activism on Facebook to sow division in the US?*, 2017). The growing tension aligned with both the approaching elections and racial unrest sparked by allegations of police violence.

These activities have been attributed to actors connected to the Russian security apparatus, including the **FSB, GRU**, and the so-called **Internet Research Agency (IRA)**. A specific tool used in the campaign was a fake Facebook profile

named *"Blacktivist,"* which posed as part of the authentic *Black Lives Matter* movement (Levin, Solon & Walker, 2017). This profile quickly amassed over 330,000 followers, although no one knew who actually ran it. Russian operatives used it to coordinate and promote protests against police brutality. They used emotionally charged phrases like *"COPS RAID WRONG HOME AND ASSAULTED PREGNANT WOMAN"* and *"INSANE! COPS PULVERIZED HANDCUFFED MAN"* to provoke user engagement and encourage sharing (Levin, 2017). By using emotionally provocative language and graphic depictions of violence, the operation successfully mobilized parts of the population, contributing to the escalation of protests and increased social tension. This strategy aimed at **affective polarization**, where social groups define themselves more by negative feelings toward others than by their own political identity. In terms of psychological operations, this represents an effective way of generating internal instability without direct military involvement. According to the U.S. Senate Intelligence Committee report, thousands of accounts on platforms such as Facebook, Twitter, Instagram, and YouTube—created by the IRA—were designed to sabotage Hillary Clinton's campaign and indirectly support Donald Trump. More than **66% of the ads** published by this "troll factory" contained content related to racial issues (BBC News, 2019). The apparent support for Trump was primarily meant to discredit him and to create internal conflict within the United States.

Operation "Blacktivist" left a significant mark on public discourse in the United States. Although it is difficult to quantify its overall effect, it clearly contributed to the radicalization of the public sphere and the deepening of political and identity divisions. A sharp divide emerged in the perception of political actors—Trump supporters were often labeled as far-right extremists, while progressive activists viewed the broader white population through a lens of collective guilt and demands for reparations. This case illustrates how social media can be instrumentalized for **false flag operations**—where operatives pretend to represent one side in order to discredit it. In such cases, the actor's ability to understand the cultural, racial, political, and ideological tensions of the target society plays a key role.

Effectively countering such operations requires not only technical tools for detection, but also mechanisms for verifying the identities of content creators and page administrators. In the case of Operation "Blacktivist," timely identification of the true operators was not possible, and the number of followers served as a substitute for credibility.

2.2.3 Ukrainian Psychological Operations on Social Media – Ghost of Kyiv

The period of Russia's invasion of Ukraine, which began in late February 2022, marked a turning point in the use of social media in the context of modern warfare. Social media became a crucial tool for shaping public opinion, mobilizing support, boosting the morale of Ukrainian forces, and demoralizing the enemy. One of the most significant psychological operations carried out by Ukrainian forces was the narrative of the so-called *"Ghost of Kyiv"* — an alleged MiG-29 Fulcrum fighter pilot who, according to claims, shot down numerous Russian aircraft during the early days of the invasion.

Although this story was later revealed to be a fabrication and a psychological operation, its purpose was clear: to lift the fighting spirit of Ukrainian forces and civilians, while simultaneously causing panic and uncertainty among Russian pilots. The first reports about the "Ghost of Kyiv" began circulating on social media immediately after the invasion started, driven by videos of fighter jets in Ukrainian airspace. According to these reports, the pilot allegedly shot down six Russian aircraft within the first 30 hours of conflict. The claim quickly went viral, and official Ukrainian government accounts—especially on Twitter—actively promoted the story, further amplifying its reach and influence. However, just two months later, the Ukrainian Air Force acknowledged that the "Ghost of Kyiv" was a myth and urged citizens to behave responsibly in the digital space, emphasizing the importance of information hygiene and the need to verify sources before sharing them further (Bubola, 2022). Numerous OSINT accounts on Twitter also played an important role in creating and sustaining this narrative, sharing analyses and posts that contributed to the belief in the existence of the mysterious pilot.

Even though the "Ghost of Kyiv" was not a real person, the narrative built around him had a powerful psychological effect, especially during the early days of the war, when symbols of resistance and heroism were desperately needed. On the other hand, the later revelation that it was a propaganda construct may have negative consequences, such as a loss of trust, a drop in morale, and growing doubts about the credibility of other information released by the authorities.

This operation clearly demonstrates how social media can enable the rapid and wide dissemination of unverified information, particularly when such content is supported by posts from verified accounts — including official government profiles on platforms like X (formerly Twitter), Telegram, Facebook, and Instagram — as well as from influential but unverified OSINT sources. The *Ghost of Kyiv* operation also shows how disinformation can be strategically used to manipulate public opinion and enhance the combat readiness of one's own forces in wartime. Additionally, spreading myths about a pilot allegedly shooting down modern enemy aircraft can have a serious psychological effect on the adversary,

especially on elements of their command-and-control (C2) systems, which might interpret such information as evidence of foreign military involvement. This may suggest the presence of sophisticated foreign aid in the form of advanced missiles, upgraded fighter jets, or previously unknown air defense systems (such as modern surface-to-air missiles – SAMs).

This case highlights the dual importance of psychological operations in modern warfare: on one hand, the need to protect the information space by combating disinformation; on the other, their immense power to shape perception and behavior—both among one's own population and armed forces, and among the enemy. The effectiveness of such operations becomes especially evident when they are carried out in a coordinated manner, across multiple platforms, and involve a wide range of actors—from state institutions and media to independent digital influencers and OSINT communities—ensuring local, regional, and global reach and impact.

2.2.4 Israeli Disinformation About Palestine

The Israeli invasion of Gaza, which began on October 27, 2023, represents an example of the coordination between kinetic and non-kinetic—psychological—activities across the physical, cyber, and cognitive domains. What stands out in this aggression and genocide is the **war on social media**, led by the **Jewish Internet Defense Forces (JIDF)** and other actors acting independently based on ideological conviction or, to some extent, in a centralized manner with clear leadership and organized operations. During this aggression, false stories and disinformation about Hamas brutality were disseminated in the media to reduce public sympathy for Palestinians and to enable the resolution of the "Palestinian question" through complete ethnic cleansing and genocide. These fabrications were especially targeted at Western audiences, who increasingly exposed and rejected them as unfounded.

As part of its psychological operation aimed at the West, Israel employed various narratives in both mainstream media and on social media platforms, promoted through **agents of influence**, including social media personalities and Western politicians. Two key examples from many others highlight the workings of Israel's propaganda and disinformation machinery:

- **Hamas beheaded 40 Jewish babies**

The story about beheaded babies originated from a report by Israeli news outlet i24News and journalist Nicole Zedeck, who interviewed Israeli reservist David Ben Zion. Max Blumenthal and Alexander Rubinstein reported on October 11 that Ben Zion is a notorious radical leader in the Israeli settler movement on the

West Bank. Earlier in the year, he had called on armed settlers to "wipe out" the Palestinian village of Harawa, which was attacked and set on fire multiple times (Khouri, 2023).
Israeli authorities and apologists such as Ben Shapiro never provided evidence of the claim and instead deflected by using **ad hominem** attacks against those demanding proof. On several occasions, even the **IDF itself denied** the claim (Solmaz & Call, 2023), but the story continued to circulate as truth on many pro-Zionist accounts on social media.

- **Palestinian Islamic Jihad bombed the Al-Ahli Arab Hospital / their rocket misfired**

One of Israel's unofficial spokespeople, @HananyaNaftali, tweeted in celebration of the Israeli Air Force bombing the Al-Ahli hospital. After public outrage, the tweet was deleted[19], and an official narrative emerged blaming the blast on a misfired rocket from **Palestinian Islamic Jihad**. However, live footage from **Al Jazeera** on October 18, 2023, around 7 PM local time, showed a bright flash in the sky that changed direction before impact—followed by two explosions, one of which occurred much closer to the camera (Al Jazeera Staff, 2023). Shortly afterward, the official Israeli account on X (formerly Twitter) posted a video claiming to prove that the explosion was caused by Islamic Jihad. But just minutes later, **Aric Toler**, a former Bellingcat researcher now with **The New York Times**, pointed out that the timestamp on the video read **8 PM**, a full hour after the actual explosion (Gilbert, 2023). The @Israel account deleted the post after this fact-check.

Western media outlets, such as **CNN** and **Fox News**, often support Israeli narratives and publish contradictory or misleading information, sometimes justifying attacks on civilians and civilian infrastructure. The basic journalistic principles of **objectivity and accuracy** are frequently missing, turning these outlets into propaganda tools that shape or reinforce public opinion. While some media are labeled as "free," they show strong political and ideological loyalty to specific actors and often construct tailored narratives. This is reflected in the affiliations and beliefs of employees and management, as well as the interests of financial backers. For example, **CNN's** reporting showed clear bias, using semantic distinctions where **Palestinians were "dead"** and **Israelis were "killed."** This kind of subliminal framing aimed to create a narrative of **who is the victim**, subtly reversing the roles of victim and aggressor to generate sympathy. What undermines the official media narrative most powerfully is the existence of social media platforms like **X**, where **"the other side"**—Palestinian

[19] See more on Naftali's X account.

voices—can share footage and reports about ongoing bombardments and killings, increasingly recognized as signs of **genocide**, amplified through online dehumanization.

Various pro-Zionist influencers on social media act offensively, openly calling for **genocide against Palestinians**. These actors sometimes cite religious texts to justify the complete destruction of groups, such as the biblical command to destroy Amalek. Influencers like **Ben Shapiro, Gad Saad**, and others are losing public support, while pro-Palestinian influencers are gaining visibility. What is specific and unique to psychological operations on social media is the power that certain actors have to **shape the views and beliefs** of others. In psychological warfare, **influencers are the tip of the spear**, supported by other elements such as **troll and bot farms, fake opposition, and false flag narratives**. Influencers and agents of influence like Ben Shapiro have large follower bases who **willingly spread or create falsehoods,** or conduct **false flag operations** (such as the earlier *Blacktivist* case), either to gather information, solicit donations, or generate internal conflict. Such operations are executed through **coordinated attacks and role-playing**, creating the illusion of legitimacy and truth around every influencer involved.

The **Israeli aggression against Palestine**, including **ethnic cleansing and genocide**, is pushed to the background due to the strength of Israel's psychological operations conducted by the government, military, and pro-Israeli influencers. The **attempt to control the narrative** is based on spreading lies and disinformation designed to provoke disgust and condemnation of Palestinians among Western audiences. However, because of social media platforms like **X**, which do not censor truth and allow each side to present evidence and facts, a growing number of people around the world are beginning to see the reality of Israel's actions and the **ongoing ethnic cleansing that is being conducted "online."** Today**, control over the population through traditional media is far less effective**, largely due to the rise of **citizen journalism**, which enables objectivity and factual accuracy to emerge outside of institutional narratives.

2.3 The Influence of Social Media on the Perception and Behavior of Target Audiences

Social media, as an inseparable part of modern society and individual life, has a significant impact on daily decision-making and the formation of attitudes and opinions. The internet and its associated communities, such as social networks, have transformed consumers, societies, and corporations by providing broader access to information, improved social networking, and enhanced communication capabilities. The connection of different individuals into a group oriented toward a specific idea is very similar to social bonds in real life. Developing a sense of social connection is an essential aspect of human life and one that improves

various dimensions of psychological well-being (Mauss et al., 2011), where establishing social bonds in the online space can be equivalent to those in the physical world.

The way social media operates is similar to how consumer product marketing works. However, in this case, what is sold is not a physical product, but an **ideological or mental product**—a psychological product. The method remains the same: a certain idea must be presented to a specific target group in order for them to become its primary consumers. The idea must be tailored to the demographics of the group being targeted, which requires a careful study of cultural, religious, social, and other relevant trends. For example, if a political campaign targets individuals of African descent (such as African Americans, Afro-British, or Afro-French), a completely different approach must be used compared to groups of Asian or Middle Eastern origin, which is based primarily on cultural elements. The group is then divided into smaller identity subgroups, and targeted messaging is developed accordingly—based on gender, sex, sexual orientation, religion, culture, prior political affiliation, and more. In addition to racial identity, other categories may include health status. For example, individuals with diabetes or cancer may be targeted as a strong voter base if a political candidate supports health reforms addressing those specific conditions.

Treating different racial, ethnic, religious, or other groups in the same way will not yield adequate results in psychological campaigns or in efforts to control narratives. Therefore, the idea being promoted in the context of a psychological operation must adopt the characteristics of a **brand**, and be adapted and modified for each demographic (and other) category and subcategory—based on gender, age, sexual orientation, political preferences, and other factors. This enables the creation of a perceived sense of importance—that the target groups matter to the decision-maker (whether a president, candidate, ruling party, opposition, or NGO), and that the decision-maker supports and fights for them, even building a kind of emotional connection with them.

In addition to their role in election processes and presidential campaigns, social media also plays a role in large-scale **national tensions and preparations for war**. In such cases, social media platforms are used to spread propaganda—by state actors such as the Ministry of Defense and armed forces, who create their own video or photo content aimed at attracting certain groups, typically men[20]. However, these campaigns are sometimes directed at non-traditional groups as

[20]See recruiting video: First Jump | Be All You Can Be | U.S. Army; https://www.youtube.com/watch?v=luc9saxt_YQ (07.11.2023.)

well—such as women and LGBTQ+ individuals[21]. The reasoning behind these tailored recruitment ads lies in state policy in times of peace and war. What is noticeable is that during peacetime or in politically sensitive periods, recruitment campaigns are more inclusive and targeted at sexual and other minorities. In contrast, during wartime or in periods of immediate conflict, the focus shifts to men and **traditional models of masculinity**—such as strength, power, fatherhood, brotherhood, and similar values. The current global geopolitical situation, including the potential for a new conflict in the Middle East, has highlighted a **recruitment crisis in the U.S. military** (Putterman, 2023). This is largely due to previous recruitment campaigns that focused on LGBTQ+ and BIPOC minorities, who traditionally show less interest in national defense. This type of favoritism has alienated heterosexual white men, who were often victims of discrimination in promotions and benefits—despite meeting all criteria in terms of completed missions, education, and tasks. The focus on and favoring of sexual and racial minorities can be interpreted as part of political strategies aimed at gaining votes. However, this approach **harms the military structure**, where there is no room for inclusivity or liberal civilian ideals. In the military, everything is based on **merit**, not privilege or tolerance. This socio-political phenomenon of **inclusivity, tolerance, and general apathy** is commonly referred to as *"woke"*, and is widely blamed for **weakening the United States** and reducing its military strength and global dominance.

3. Development and Strategies on Social Media

3.1. How Psychological Operations Are Developed and Implemented on Social Media

The development and implementation of psychological operations on social media—as their main vehicle—represents a highly complex and sophisticated process. This process is based on the recognition of several key factors necessary for the success of the operation itself, as well as the consequences that may follow its successful execution.

The foundation of every psychological operation is the identification of the target that will be addressed and against which certain activities will be undertaken. This identification forms the basis of the entire process, generating the initial assumptions for the operation's success. The process can include various elements and phases depending on creativity and the effectiveness of implementation.

An example of a successful psychological operation may include the following cycle and its elements:

[21]See recruiting video: EMMA |THE CALLING| GOARMY; https://www.youtube.com/watch?v=MIYGFSONKbk (04.05.2021)

Identification of the target audience

Identifying the target audience is the foundation of any propaganda, psychological, or related campaign aiming to produce an effect at the socio-political level. Without identifying the group to be targeted, it is impossible to deliver the right message. Therefore, the primary task of any campaign is selecting the audience to be treated. This may include racial, ethnic, national, or religious groups—focusing first on general categories, followed by profiling and targeted actions toward subgroups.

Strategy development

Strategy development is closely tied to the identification of the target audience. It correlates directly with the cultural trends, traditions, habits, and thought patterns of the audience. Based on demographic elements such as gender, race, religion, and others, approaches must be developed to influence the audience consciously and subconsciously. Strategies may be built on identities (nationality, sexual orientation), dogmas (religion), or cultural and societal trends. Each strategy must include: a) clearly defined goals, b) selection of key messages and topics, and c) planning and development of tactics for each platform and message carrier individually. This can be seen as a top-down process: strategy – operations – tactics.

Segmentation and audience division

Due to the general nature and diversity of mass audiences and identities, all actions must be specified. While identification provides the basis, deeper understanding is needed through analysis of which groups, subgroups, cultures, subcultures, and countercultures constitute the audience. Each group must receive tailored messages that depend on the strategic goal—be it calming, mobilization, or action. Each group should be addressed through the most suitable medium for them: videos (short clips, podcasts, photos), print (books, journals, academic papers), text (news articles, social media posts), or music (songs, performances). Every subgroup has its preferred medium, and it must be identified and utilized.

Psychological profiling

This is based on monitoring identified groups and subgroups. Each has different reactions to certain events and news, so it is essential to record, classify, and analyze these. Profiling is easiest via comment and reaction analysis on social media discussions. For example, by analyzing comments on a military recruitment ad, one can gauge group attitudes. Furthermore, one should consider how other users react to those comments—agreement, disagreement, or neutrality. Reaction systems such as like/dislike, repost, upvote/downvote help in this process. Users are then classified by demographics (gender, race, ethnicity, religion) and interest spheres or cultural trends.

Creating targeted content

Depending on the culture, trends, and interests of the group being addressed, content is created to attract attention, provoke thought, and subtly introduce ideas. In the early phases, propaganda must be subtle and ambiguous, gradually becoming more direct and open. The content should provoke emotions—often anger—yet without causing demoralization that could lead to apathy. The goal is to inspire the group toward action while maintaining a positive or determined outlook.

Optimizing for virality

For content to be adopted, it must go viral and reach a broad segment of the target group. This can happen in two ways: a) artificially via bots and technical methods, or b) organically through high-quality content. Initially, a combination of both is optimal—creating compelling content supported by bot engagement. Given that algorithms can detect bot activity, it is crucial to invest in creating resonant, relatable content.

Use of bots and trolls

To sustain the narrative and perception of widespread acceptance, it is often necessary to artificially amplify agreement through bots (AI-simulated users) and trolls (real people operating fake accounts). These actors spread ideas, initiate discussions, or engage in false flag activities[22] to compromise the opposition. Larger operations may use troll and bot farms—paid groups acting across social media, forums, and news sites.

Content implementation

Content implementation, meaning the launch of psychological-propaganda material and actions, must occur at precise times. This timeframe—lasting from weeks to months—should align with political or social events such as an election or the buildup to war. The implementation is typically divided into three phases: a) before the event, b) during the event, and c) after the event. The intensity and scope of activities will vary to ensure maximum effect. A psychological operation does not end with the event itself; it continues and adapts regardless of outcomes. For example, the victory or defeat of a presidential candidate does not end the operation, which is adjusted accordingly.

Measuring impact and consequences

Measurement can be quantitative or qualitative. Quantitative methods include tracking reactions (likes/dislikes, reposts, comments), which can be assigned values representing full support or rejection. Targeted surveys may be used,

[22] The actor presents themselves as their ideological opponent and disseminates radical and extremist content. This tactic is used to deter neutral and moderate activists, and to dehumanize and demonize the adversary.

though care must be taken to hide the sponsor's identity and intent. Qualitative analysis includes examining comment tone, emotional reactions, depth of engagement, content relevance, and changes in user opinions (based on historical behavior and posts).

Content adaptation

This final phase involves analyzing all previous steps to refine approaches. Adjustments are made in methods, content delivery, and target selection. Hypotheses about what works and what does not are verified, identifying which actions yield the highest impact. It is also an opportunity to test new strategies prompted by observations or changing political and social dynamics. Adapting content is essential for long-term psychological operations, allowing for the extraction of insights and lessons for future use.

3.2. Analysis of Strategies and Tactics with Examples

When analyzing the strategies and tactics used for the successful implementation of psychological operations on social media, it is important to understand that they are numerous, adaptable, and dependent on specific moments and societal developments. They are closely linked to the previously described cycle of action and draw their foundation from it.

The strategies and tactics commonly employed in psychological operations include:

- False flag narratives
- Doxxing
- Use of fake identities
- Use of memes as carriers of information
- Spreading conspiracy theories
- Disinformation

3.2.1. False flag narratives

These narratives represent a strategy essential for dividing the public and target groups. This disruption of unity and ideological coherence enables the creation of a narrative centered around internal conflict and the struggle for dominance. False flag narratives are implemented by creating fake accounts that present themselves as members of a particular group, gain their trust, and at a critical moment begin spreading false information and narratives. The primary objective is to present a false narrative as originating from the group itself, where it is not crucial whether the falsehood is eventually exposed. The goal is to discredit and compromise the target group to reduce its public influence and support.

Example: A malicious actor seeking to damage the reputation of a civil rights group may create a social media account that appears to belong to a genuine

activist. Through high engagement, the account builds a large follower base, often supported by bots and trolls to boost its credibility. Once trust is established, the account begins disseminating ambiguous content—partially true, distorted, or framed negatively. Initially, the disinformation is subtle and hard to detect. Later, the account may escalate to more extreme messages involving radicalism or calls for violence against the state or other communities. This tactic creates polarization and ultimately discredits the legitimate efforts of the target group to gain broader support and bring about change. In such cases, provocateurs may completely derail the activities of those fighting for human rights, spark violence, and provoke a heavy-handed response from the state, effectively eliminating any form of organized civil action. The general public, in turn, distances itself from the group, withdraws support, and abandons all efforts to defend its rights.

3.2.2. Doxxing

Doxxing represents an effective strategy for silencing, intimidating, and physically endangering individuals who do not align with certain narratives or who become a threat due to their political and social influence on social media and other platforms. It is an OSINT-based process involving the collection of private information about a person or group, such as residential address, number of family members and their personal details (workplace, school attendance, health status), IP address[23], private photos, and more. By publishing this private data on social networks or other public platforms, the goal is to intimidate the target by demonstrating that their personal life is vulnerable to outside infiltration. Revealing sensitive aspects such as financial or health conditions or family issues serves to discredit the individual (via ad hominem tactics), potentially leading to a loss of public support and diminishing the impact of their messages regarding civil rights or national security threats.

Example: A human rights activist becomes the target of doxxers who, through surveillance of the activist's social media accounts and the use of OSINT tools, obtain information such as IP address[24], residential location (via data mining[25]), or daily habits if the individual is active on platforms like Instagram, Twitter, or TikTok. Once collected, this data is disseminated across social media, usually in a coordinated effort by multiple fake accounts with the intention of intimidation.

[23] An **IP address (Internet Protocol)** is a unique number that identifies a device on the Internet or a local network. In essence, IP addresses are identifiers that allow the transfer of information between devices on a network: they contain location data and make devices accessible for communication.

[24] Obtaining an IP address is not a significant obstacle for members of intelligence services or parallel—para-state security systems.

[25] Data mining is the process of sorting through large datasets to identify patterns and relationships that can help solve business problems through data analysis.

If any "dirty secrets" are found—such as personal fetishes, family problems, etc.—they are exaggerated or entirely fabricated and built upon existing facts.

3.2.3. Use of Fake Identities

Fake identities are commonly used in everyday online activity, particularly to create polarization in online discussions or to support agitators and aggressive actors by making their views seem widely accepted. They can also be used for various purposes such as disinformation, espionage, data gathering within interest groups, spreading propaganda, building bot networks, committing fraud, and more. The possible applications of fake identities are endless and often interwoven.

Example: A social media account presenting as an attractive woman can quickly gain popularity, which is then used to spread disinformation, propaganda, or carry out scams (e.g., through donation services like CashApp, Apple Cash, or Xbon). Fake identities can also be used in false flag narratives to track, monitor, and gather data on supporters of certain ideas, movements, or narratives.

3.2.4. Use of Memes as Idea Carriers

With the rise of the internet and the spread of information through social media, it has become possible to create specific types of information carriers—memes. A meme is both simple and complex to define. Most people describe memes as "funny pictures with text," but their role goes far beyond just making people laugh. In *Evolutionary Psychology, Memes and the Origin of War* (2006), Keith Henson defines a meme as "a replicating pattern of information: a way of doing things, learned cultural elements, beliefs, or ideas." Memes are also considered by military experts such as Lieutenant Colonel Prosser (2005), who sees them as powerful tools for the U.S. military in psychological operations (PSYOP), information operations (IO), and strategic communication in nonlinear warfare. Through memes, it is possible to influence the attitudes of enemies, allies, and neutral actors. Although often humorous, memes carry specific messages and can set trends using irony, sarcasm, or cynicism. They can be used to promote or oppose a political candidate or movement, support nationalism, spread hate, or push certain ideologies. What makes memes unique is that effective memes cannot be created artificially by government officials who are assigned the task but do not understand online culture and trends. These cultures and trends cannot be learned through presentations, briefings, or intelligence reports. They are something naturally absorbed and created by users through their daily activity online. There is evidence that many state-led meme campaigns have failed because their creators were quickly recognized as "feds"[26] in the comment

[26] A colloquial internet term for the police – an abbreviation of Federal police, sometimes also used to refer to FBI agents and members of other intelligence agencies. The term spooks is also occasionally used – meaning "ghosts" or "phantoms" – to describe agents of the CIA, NSA, FBI,

sections due to memes that looked bureaucratic or fake. This often comes from a generational gap between "boomers"[27] and younger users like millennials[28] and Gen Z[29], who grew up with internet culture. For a meme to be successful and go viral, it must be "organic," meaning it must be created by someone deeply familiar with online humor, norms, and visual language. Viral memes usually include short, strong messages that resonate with emotions or beliefs. Interestingly, political groups on the right have been more successful at creating memes, while those on the left often over-explain their ideas using too much text, which weakens the message. Today, a teenager using a smartphone can make a powerful, viral meme-based campaign—whether for army recruitment or supporting a politician—more effectively than trained professionals. Videos with suffixes like *-wave*[30], *-core*[31], and others can seem friendly and familiar to users who relate to the subject or message in the content.

Example: If a political figure is being promoted, traditional propaganda posters with slogans may have the opposite effect. A stronger impact can be made through satire and irony that highlight certain traits of the candidate, making them look more relatable or even superhuman (e.g., comparing them to superheroes). Memes can also be used to mock opponents, which sometimes has a greater effect than promoting one's own side. For a meme to succeed, research must first be done on the trends that are currently popular and usable for delivering the intended message.

3.2.5. Creation and Dissemination of Conspiracy Theories

Conspiracy theories are a specific concept used to send certain messages and trigger emotions in a broader audience. These theories cannot be effective unless they are combined with other online activities such as disinformation, narrative control, meme creation, and more. What makes conspiracy theories particularly

---

and similar agencies who are active on social media. See examples on the Twitter account: Posts By Feds (@SuspectFed).

[27] A boomer (baby boomer) refers to a demographic cohort born between 1946 and 1964, but in internet culture, the term is often used cynically or ironically to describe anyone who does not understand online culture or technology – typically anyone born before the 1990s.

[28] A millennial is someone born between 1981 and 1996. However, members of Generation Z often refer to millennials as boomers as well – usually due to their age. Online culture, not dictionaries, defines who is considered a boomer or millennial

[29] According to the Collins Dictionary, Generation Z includes people born between the mid-1990s and the mid-2010s.

[30] The suffix -wave refers to a microgenre of ironic pop culture, usually based on unique and niche trends.

[31] Similar to the -wave suffix, -core refers to a specific activity or lifestyle around which an individual's personality is shaped. For example: techcore, militarycore, pilotcore, techbrocore, financialbrocore, and so on.

useful is their viral potential to mobilize passive audiences and spread panic or hatred.

The effectiveness of conspiracy theories in narrative control comes from their dual purpose. The first use is to create and spread fear and panic, either to scare the opponent or control the population. Throughout history, there have been examples of this use, although many were eventually exposed as false. The second use involves a more complex psychological operation: damaging the credibility of individuals or groups with insider knowledge about illegal, immoral, or unethical actions by a government, company, or organization. This is done by creating a real or fake social media account supported by bots, which begins to share both real and obviously false information related to the whistleblower's topic. Over time, other similar accounts appear with modified but similar content. The general audience starts seeing these accounts as delusional or unreliable, and eventually, even true whistleblowers are placed in the same category. The more accounts spreading similar ideas, the more unrealistic the original truth appears, leading people to ignore or reject it.

3.2.6. Disinformation

Disinformation is one of the most common and well-known strategies used in media and information warfare. It dates back to World War I and II, and continued through the Cold War. Disinformation can be seen as a milder form of fake news, and in some cases, it results from incorrect or incomplete reporting, which changes the meaning of a message and leads to false conclusions (Raskrinkavanje, 2019). The goal of a malicious actor is not to spread completely false information that can easily be disproven, as this would damage the credibility of the campaign. Instead, disinformation usually contains a small part of the truth. The message is designed to influence the reader subtly, using emotionally charged words and clever sentence structure. The reader may then interpret the message as truth and share it with others. This process of unintentionally spreading false information is often referred to in the literature as *misinformation*.

The manipulation of information in the media is now more widespread and accessible than ever before. Social media has allowed unverified and misleading content to spread quickly, often supported by actors with specific political or ideological goals. The purpose of these campaigns is to create division, encourage radicalization or hatred, and even cause fear and panic.

The use of disinformation on social media is a critical part of psychological operations. It can be used against the enemy to weaken their morale, or against one's own population to shape public opinion. This opinion is formed through subtle manipulation of facts in the media. Claire Wardle (2016) identifies six

types of false information that can be used in psychological operations: genuine content used in the wrong context, fake news websites designed to look like trusted brands, completely fake news, false information, manipulated content, and parody or satire. Disinformation actors often work with existing materials, changing headlines or twisting the context to deliver hidden messages and influence how people think.

3.3. Cooperation Between State Actors and Malicious Groups

The implementation of psychological operations on social media, aimed at changing narratives or creating new socio-political trends, requires strong support—material, financial, ideological, organizational, and counterintelligence-security. For the operations of non-state malicious actors and groups in the online space to be successful and effective, there must be, ideally in secret, a connection with state institutions, organizations, or high-ranking government officials. The success of such psychological operations largely depends on the strength of this connection, as malicious groups often act as "contractors," while state actors give orders and fund the operations.

When speaking about state actors, their goals usually involve threatening, weakening, or taking control of a target audience or enemy. In this context, psychological operations are a tool of unconventional warfare. In order to influence others—enemies, neutral actors, allies, or their own population—states must invest significant amounts of money and resources. These resources are used to acquire technical equipment, professional personnel, and "manpower," meaning activists and operational agents. State actors (such as institutions, organizations, political parties, or individual politicians) are typically the ones who create the key ideas and narratives. They then pass these tasks down to malicious groups to execute. For the operation to succeed, ideological indoctrination and compatibility between the state and the group are crucial. At the same time, these malicious groups must include trained personnel capable of understanding the assigned tasks and independently finding effective ways to carry them out. Creativity is a critical "resource" that cannot be bought, and the ability to adapt daily to changing social and political events plays a key role in producing strong results.

An especially important element is counterintelligence, meaning the protection of the individuals or groups carrying out the psychological operations. This includes stopping or obstructing any investigations that may be launched against them. It is also necessary to ensure that these actors are not being monitored by intelligence agencies or cyber units of criminal police. Since psychological activities may become visible and attract attention, having control over security

and intelligence bodies (such as intelligence services, police, cyber police, etc.) reduces the risk of exposure and increases the overall effectiveness of the operation. For this reason, fighting against psychological operations becomes extremely difficult—and nearly impossible—if methods, tools, and actors are not clearly identified. The only way to counter them is by launching one's own counter-psychological operations.

4. The Impact of Psychological Operations on National Security and the Fight Against Them

Protecting national security in the modern era is no longer limited to physical threats but also includes those that exist in the non-material world. Fighting against unconventional threats, such as hostile psychological operations on social media, requires the engagement of the entire security sector or the creation of specialized units focused on this issue.

The consequences of hostile actions can be numerous. They essentially destroy society and the nation, weaken state policy, and can lead to major negative or even catastrophic outcomes, such as uprisings or civil wars. When discussing the risks and consequences of unchecked actions by malicious actors, democratic processes are usually the first to suffer. Influence over public opinion through long-term psychological operations and campaigns that shape new narratives can greatly affect citizens' decisions and make them more vulnerable to foreign, politically aggressive actors.

As a result of continuous, decentralized, and multi-sectoral malicious activity—as well as natural developments such as the emergence of opposition and new political movements—social instability and divisions re-emerge.

Effectively combating psychological operations on social media requires a large-scale effort by state security services, as well as collaboration with non-governmental organizations focused on human and civil rights. The state sector—especially intelligence and counterintelligence agencies, and cybercrime units[32]—must continuously monitor social networks and identify certain actors as possible foreign agents. Because of the sensitivity of infringing on human rights and limiting freedom of speech, such activities must be well-documented, transparent, and subject to change and review by ethical ad hoc or permanent committees. In addition to monitoring suspicious behavior, it is necessary to keep records of individuals or groups spreading the same or similar ideas, follow their content,

[32] Depending on the political and social system of a given country. The concept is not limited to Bosnia and Herzegovina.

and conduct risk assessments regarding the potential spread of harmful narratives that could provoke internal conflicts and divisions.

Creating specialized state bodies that work together with NGOs is crucial in the fight against psychological operations and aggressive campaigns on social media. These bodies should function as an intelligence-investigative service that monitors user activities, collects data, establishes facts, and tracks suspicious behavior such as the activity of bots and trolls controlled by foreign actors. In cooperation with NGOs, it is also possible to carry out counter-psychological campaigns and operations aimed at discrediting malicious actors and increasing citizens' resilience to hostile influence. This can be achieved through coordinated awareness campaigns, the publication of materials providing evidence and facts about such operations, and active participation on social media—especially through podcasts and expert-led broadcasts that aim to demystify and expose harmful operations. The key to effectively resisting psychological operations on social media is their exposure and the implementation of our own counter-psychological and counter-propaganda strategies.

Conclusions and Recommendations

Modern technologically advanced times have completely changed the paradigm of modern warfare. Wars can no longer be won solely through military means; it is now necessary to fully subjugate the targeted nation and society. This is achieved with the help of social media and psychological operations conducted on these platforms. The human mind has become the new battlefield, where battles and operations are fought, opening a Pandora's box of new threats and methods of disruption. This evolution in the understanding of war and military operations requires specific measures to prevent hostile actions aimed at influencing the minds of citizens, who are now more exposed than ever to malicious and aggressive influence. The key element in this is the use of modern technology and social trends, particularly social media. Through the creation and dissemination of video, audio, and text content, it is possible to insert information aimed at creating internal divisions, fear, hatred, and more. Today, information has a much greater influence on human life, especially because of its viral nature and the perception of those who are the primary targets and consumers. Information—especially manipulated content and broader influence operations—can create social unrest and allow hostile actors to destabilize a country or nation without using conventional means such as military, political, diplomatic, or economic tools. However, psychological operations can also be used in coordination with conventional destabilization strategies, making their impact even greater.

An attack on the human mind and the entire society today represents an effective tool for achieving aggressive goals. Therefore, it is essential to take significant action to prevent such activities. Social media represents a suitable tool for hostile and malicious influence on the human mind. Because of this, it is necessary to study both social networks and their application in psychological operations conducted by foreign state and non-state actors that pose ongoing threats. In addition to studying these threats, it is necessary to implement counter-PSYOP activities to prevent malicious actors from creating and maintaining narratives that are later transferred from online platforms into real life. Based on the above, the following recommendations are essential for effectively fighting this threat:

- Establish specialized units within Ministries of Security, Defense, or their equivalents to combat hostile psychological and information operations;
- Create research centers focused on the study of psychological operations and information warfare;
- Conduct counter-PSYOP operations;
- Record, classify, and monitor aggressive and malicious actors operating in the online space;
- Continuously monitor malicious and aggressive actors in cyberspace;
- Develop a database of aggressive actors and their PSYOP operations to enable identification and classification;
- Study strategies, operations, and tactics of psychological operations on social media;
- Ensure cyber control over social media platforms;
- Cooperate with non-governmental organizations that work to protect civil and human rights;
- Educate broader social groups, especially children and adolescents;
- Actively engage on social media through various formats;
- Publish materials that expose aggressive and malicious actors and their psychological operations on social media;
- Regularly inform the public through the media;
- Provide open communication channels for citizens to report specific disinformation trends;
- Monitor and control cyberspace for malicious activities.

These activities, undertaken by state agencies, will enable the reduction or complete elimination of aggressive and malicious influence from hostile actors who base their operations on unconventional tools and methods. By limiting their activity in cyberspace, the spread of propaganda, indoctrination, and disinformation can be significantly reduced, and society will be less vulnerable to subjugation by hostile actors.

Literature

Al Jazeera Staff. (20. 10 2023). *Investigations reveal discrepancies in Israel's Gaza hospital attack claims.* Preuzeto od Al Jazeera: https://www.aljazeera.com/news/2023/10/20/what-have-open-source-videos-revealed-about-the-gaza-hospital-explosion

Andrew, C., & Mitrokhin, V. (2000). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of KGB.* Basic Books.

BBC News. (09. 10 2019). *Russian trolls' chief target was 'black US voters' in 2016*. Preuzeto od BBC News: https://www.bbc.com/news/technology-49987657

Bubola, E. (01. 05 2022). *Ukraine acknowledges that the 'Ghost of Kyiv' is a myth*. Preuzeto od The New York Times: https://www.nytimes.com/2022/05/01/world/europe/ghost-kyiv-ukraine-myth.html

Cadwalladr, C., & Graham-Harrison, E. (17. 03 2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* Preuzeto od The Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cambridge Dictionary. (2023). *Propaganda*. Preuzeto od Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/propaganda

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact",. *MIS Quarterly*, 1165-1188.

Culliford, E. (12. 10 2020). *How political campaigns use your data*. Preuzeto od Reuters: https://www.reuters.com/graphics/USA-ELECTION/DATA-VISUAL/yxmvjjgojvr/

Cusick, S. G. (2006). Music as torture / Music as weapon. *Sociodad de Etnomusicologia TRANS 10*.

European External Action Service (EEAS). (2020). *EUMC Glossary of acronyms and definitions - Revision 2019.* Brussels: European Union Military Committee (EUMC).

Fridman, O., Kabernik, V., & Granelli, F. (2022). *Info Ops - From World War I to the Twitter Era.* London: Lyne Reinner.

Gilbert, D. (18. 10 2023). *Who's Responsible for the Gaza Hospital Explosion? Here's Why It's Hard to Know What's Real*. Preuzeto od Wired:

https://www.wired.com/story/al-ahli-baptist-hospital-explosion-disinformation-osint/

Giles, K. (2016). *Handbook of Russian Information Warfare.* Rome, Italy: NATO Defense College.

Goulart, K. (2024). *Social network*. Preuzeto 07. 11 2023 iz TechTarget: https://www.techtarget.com/searchcio/definition/social-network

Henson, K. (2006). Evolutionary psychology, memes and the origin of war. *Mankind Quarterly*, 443-459.

Hern, A. (06. 05 2018). *Cambridge Analytica: how did it turn clicks into votes?* Preuzeto od The Guardian: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Humphrey, C. (16. 09 2023). *The Ghostly Legacies of America's War in Vietnam*. Preuzeto od The Foreign Policy: https://foreignpolicy.com/2023/09/16/vietnam-war-psyops-ghosts/

Joint Chiefs of Staff (JCS). (2010). *Joint Publication 3-13.2 - Psychological Operations.* Washington DC: Joint Chiefs of Staff (JCS).

Khouri, R. G. (13. 10 2023). *Watching the watchdogs: Babies and truth die together in Israel-Palestine.* Preuzeto od Al-Jazeera: https://www.aljazeera.com/opinions/2023/10/13/watching-the-watchdogs-babies-and-truth-die-together-in-israel-palestine

Kramer, M. (26. 05 2020). *Lessons From Operation "Denver," the KGB's Massive AIDS Disinformation Campaign*. Preuzeto od The MIT Press Reader: https://thereader.mitpress.mit.edu/operation-denver-kgb-aids-disinformation-campaign/

Lakić, Z., Kovačević, Z., & Kovačević, I. (2024). Terorizam - bezjednosna prijetnja Zapadnom Balkanu. *Zaštita i sigurnost, godina 4., broj 2.*, 191-201.

Lasswell, H. D. (1995). Propaganda. U R. Jackall, *Propaganda* (str. 13). New York : New York University Press.

Levin, S. (30. 09 2017). *Did Russia fake black activism on Facebook to sow division in the US?* Preuzeto od The Guardian: https://www.theguardian.com/technology/2017/sep/30/blacktivist-facebook-account-russia-us-election

Levin, S., Solon, O., & Walker, S. (21. 10 2017). *'Our pain for their gain': the American activists manipulated by Russian trolls*. Preuzeto od The guardian: https://www.theguardian.com/world/2017/oct/21/russia-social-media-activism-blacktivist

Mauss, I. B., Shallcross, A. J., Troy, A. S., John, O. P., Ferrer, E., Wilhelm, F. H., & Gross, J. J. (2011). Don't hide your happiness! Positive emotion dissociation, social connectedness, and psychological functioning. *Journal of Personality and Social Psychology*, 738–748.

Merriam - Webster. (2019). *Disinformation*. Preuzeto od Merriam - Webster: https://www.merriam-webster.com/dictionary/disinformation

Mshvidobadze, K. (21. 03 2011). *The Battlefield On Your Laptop*. Preuzeto od Radio Free Europe: https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, godina 4., broj 2.*, 314-339.

NATO Standardization Agency . (2013). *NATO Glossary of Terms and Definitions.* Brussels, Belgium: NATO Standardization Agency .

Newton, K. (08. 08 2019). *Aspidistra: The wartime breakthrough you've never heard of.* Preuzeto od History of government: https://history.blog.gov.uk/2019/08/08/aspidistra-the-wartime-breakthrough-youve-never-heard-of/

Noor, A. S., Hosen, N., Hassan, N., Ismail, A. S., Rahim, F. N., & Tarmidi, Z. (2022). Active learning: Game-changer to short attention span in Gen Z. *New Academia Learning Innovation 2022*, (str. 369-371). Johor Bahru, Malaysia.

Prosser, M. (2005). *Memetics: A Growth Industry in US Military operations.* Quantico, Virginia: USMC, School of Advanced Warfighting, Marine Corps University.

Putterman, S. (25. 09 2023). *Politicians blame 'wokeism' for low military recruitment. The problem is more complex.* Preuzeto od PolitiFact: https://www.politifact.com/article/2023/sep/25/politicians-blame-wokeism-for-low-military-recruit/

RAF Upwood. (02 2002). *Radar and Radio*. Preuzeto od R.A.F. UPWOOD: http://www.rafupwood.co.uk/radarandradio.html

Raskrinkavanje. (2019). *Dezinformacija*. Preuzeto od Medijska pismenost: https://medijskapismenost.raskrinkavanje.ba/oblici-manipulacija-i-kome-se-obratiti-ako-ih-uocite/koji-sve-oblici-medijskih-manipulacija-postoje/dezinformacija/

Selhorst, A. (2016). Russia's Perception Warfare - The development of Gerasimov's doctrine in Estonia and Georgia and it's application in Ukraine. *Militaire Spectator*, 148-164.

Solmaz, M., & Call, E. (11. 10 2023). *Despite refutations from Israeli military, headlines that Hamas 'beheaded babies' persist*. Preuzeto od Anadolu Agency: https://www.aa.com.tr/en/middle-east/despite-refutations-from-israeli-military-headlines-that-hamas-beheaded-babies-persist/3016167

Solon, O. (19. 03 2018). *Facebook's value falls $37bn amid backlash from Cambridge Analytica data scandal*. Preuzeto od The Guardian: The Guardian. https://www.theguardian.com/news/2018/mar/19/facebook-value-declines-data-scandal

Thomas, T. L. (1997). Russian Information-Psychological Actions: Implications for U.S. PSYOP. *Special Warfare*, 12-19.

U.S. Department of Defense. (2014). *Joint Publication 3-13.3, Psychological Operations.* Washington DC: U.S. Department of Defense.

US Army Special Operations Recruiting. (2023). *Psychological operations.* Preuzeto 07. 11 2023 iz https://www.goarmysof.army.mil/PO/

Wardle, C. (18. 11 2016). *6 types of misinformation circulated this election season*. Preuzeto od Columbia Journalism Review: https://www.cjr.org/tow_center/6_types_election_fake_news.php

UREĐENJE SISTEMA VJEŠTAČANJA U KRIVIČNOM POSTUPKU U MEĐUNARODNOM I KOMPARATIVNOM PRAVU I PRIJEDLOZI ZA UNAPREĐENJE U FEDERACIJI BOSNE I HERCEGOVINE

DOI: *10.70329/2744-2403.2025.5.9.8*

Stručni rad

Nermin Kadribašić, MA[1]

Sažetak:

Vještaci predstavljaju jednu od ključnih dokaznih radnju u krivičnim postupcima u Bosni i Hercegovini. Otkrivanje i dokazivanje krivičnih djela, posebno kompleksnih krivičnih djela u pravilu zahtjeva korištenja vještaka različitih specijalnosti. Međutim praksom u sudskim postupcima u Bosni i Hercegovini je uočen značajni izazovi prilikom angažovanja i korištenja vještaka u krivičnim postupcima. Analizom međunarodnih dokumenata i usporednog zakonodavstva koji regulišu pitanja statusa i uloge vještaka ukazuju na činjenicu da normativni okvir treba da bude adekvatan u svim svojim dijelovima kako bi se osiguralo adekvatan mehanizam izbora i korištenja vještaka. Rad je identificirao niz različitosti u normativnom okviru koji uređuju status vještaka i ponudio niz preporuka u unapređenju normativnog okvira Federacije Bosne i Hercegovine, prvenstveno Zakona o vještacima Federacije Bosne i Hercegovine.

Ključne riječi: *ekspertno vještačenje, ekspertni vještaci, uloga i značaj vještačenja, status vještaka*

[1] Stručnjak za vladavinu prava i doktorant, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.

Uvod

Vještačenje u krivičnom postupku predstavlja jednu od čestih dokaznu radnji koje se poduzimaju i nerijetko imaju odlučujući uticaj na ishod sudskog postupka. U praksi su rijetki slučajevi gdje se, bez obzira na to koje je krivično djelo u pitanju, postupak vodi bez učešća vještaka (USAID Projekat pravosuđa u BiH, 2017). Vještačenje u Bosni i Hercegovini su uređeni nizom pravnih propisa, od kojih su osnovni zakoni o vještacima i zakoni o krivičnim postupcima. U Bosni i Hercegovini, ali i generalno u zemljama zapadnog balkana još uvijek se javljaju različiti izazovi u različitim fazama sistema vještačenja (Svjetska Banka, 2019). Pravosudni sistem u Bosni i Hercegovini, a posebno tužilački sistem se susreće sa mnogobrojnim poteškoćama u provođenju i osiguranje efikasnog i kvalitetnog vještačenja koje je od presudnog značaja u otkrivanju i dokazivanju krivičnih djela, posebno krivičnih djela privrednog kriminala i korupcije. Mnogi su razlozi koji utiču na poteškoće u provođenju efikasnih i kvalitetnih vještačenja. Neki od razloga su svakako normativne i institucionalne prirode, te je s tim u vezi u ponuđen komparativni prikaz sistema vještačenja u zemljama u regionu. Namjera komparativnog prikaza je da posluži kao okvir za razmatranje mogućnosti unapređenja sistema vještačenja u krivičnom postupku kroz pregled relevantnih i dobrih praksi u kompariranim pravnim sistema, posebno u dijelu koji se odnosi na normativni okvir u Federaciji Bosne i Hercegovine. Važno je napomenuti da je duži niz godina uočena potreba za izmjenom Zakona o vještacima FBIH, ali da je Vlada Federacije BiH utvrdila Nacrt zakona o vještacima u Federaciji BiH u novembru 2020. godine.[2] S tim u vezi će se pored trenutnog važećeg zakonskog rješenja tokom ovog rada će se ponuditi i osvrt na utvrđeni nacrt Zakona.

1. Kriteriji i faktori za odabir komparativnih primjera

Za komparativni prikaz normativnog i institucionalnog sistema vještačenja odabrani su primjeri Srbije, Hrvatske, Slovenije i Federacije Bosne i Hercegovine. Kriteriji koji su primijenjeni kod odabira se odnose na regionalni kriterij, moguće sličnosti i razlike u obavezama koje proizilaze iz procesa o pridruživanju Evropskoj Uniji[3] ali i kriterij sličnosti i uporedivosti pravnih tradicije. Slovenija je zemlja članica Evropske unije od 01. maja 2004. godine i

[2] Nacrt zakonskog rješenja dostupan na https://www.javnarasprava.ba/fbih/Zakon/1604

[3] Zemlje regije su potpisale tzv. Sporazum o stabilizaciji i pridruživanju (SSP) koji nova, treća generacija sporazuma o pridruživanju ponuđena isključivo državama zapadnog Balkana, u sklopu Procesa stabilizacije i pridruživanjakoji je važi za zemlje koje nisu postale članicom Evropske unije od 01. Juna 2004. godine. Od promatranih zemlja Slovenija nije bila dijelom Sporazum o stabilizaciji i pridruživanja zato što je već 17 godina zemlja članica Evropske unije, odnosno postala je zemljom članicom .

odavno je ispunila obaveze u procesu pridruživanja Evropskoj uniji, dok je Hrvatska zemlja članica od 01. jula 2013. godine kada je i prestao da važi Sporazum o pridruživanju i stabilizaciji. Crna Gora i Srbija su države kandidatkinje, dok je Bosna i Hercegovina potencijalni kandidat za zemlju članicu Evropske unije.
Također prilikom početnog istraživanja za potrebe odabira komparativnih primjera uočeno je da zemlje regije imaju slična rješenja koja se tiču krivičnoprocesnih zakonodavstava koja tretiraju pitanja vještaka i vještačenja, a što je i logično zbog činjenice da su nekada ove zemlje bile dijelovi iste jurisdikcije i pravnog sistema. Ipak posebni propisi koji regulišu pitanje sudskih vještaka sadrže određene razlike koja mogu ponuditi praktična rješenja i za unapređenje sistema korištenja vještaka u Bosni i Hercegovini.

Faktori, koji su analizirani kroz više podfaktora, a koji će se posebno analizirati između promatranih zemalja regije prikazani su u priloženoj tabeli:

Faktori koji su analizirani u promatranim zemljama	**Podfaktori unutar svakog analiziranog faktora**
Uloga vještačenja i stalnih (sudskih) vještaka u krivičnom postupku	• Razlozi za određivanje vještačenja • Pravo određivanja vještačenja • Angažovanje privatnih vještaka i stručnih lica
Kriteriji za odabir određenog (stalnog) sudskog vještaka	• Lista (stalnih) sudskih vještaka • Stručna ustanova ili državni organ
Izbor i imenovanja lica za (stalnog) sudskog vještaka	• Uslovi koje mora posjedovati fizičko lice da bi bilo imenovano za vještaka • Odgovorna institucije za imenovanje (stalnih) sudskih vještaka • Procedura izbora (stalnih) sudskih vještaka
Dužnosti i prava (stalnog) sudskog vještaka u procesu izrade nalaza i mišljenja	• Dužnosti (stalnog) sudskog vještaka u procesu izrade nalaza i mišljenja • Prava (stalnog) sudskog vještaka u procesu izrade nalaza i mišljenja
Nadzor nad radom vještaka, sankcionisanje i razrješenje (stalnih) sudskih vještaka	• Nadzor nad radom (stalnih) sudskih vještaka • Sankcionisanje sudskih vještaka • Postupak razrješenja (stalnih) sudskih

	vještaka
Uloga stručnih tijela/udruženja (stalnih) sudskih vještaka	• Institucionalizacija stručnih tijela/udruženja • Sastav stručnih tijela/udruženja
Zaključna razmatranja	• Zaključna razmatranja; • Preporuke;

.

1.1. Normativni okvir za korištenju vještaka u krivičnom postupku u uporednim zakonodavstvima

a) Zakoni o krivičnim postupcima u zemljama regiona

U promatranim jurisdikcijama pravni osnov za upotrebu i određivanje dokazne radnje vještačenja, a samim time i statusa i uloga vještaka u krivičnom postupku je, kao i u Federaciji BiH, regulisano prvenstveno važećim zakonima o krivičnim postupcima. Tako je Zakonom o krivičnom postupku Srbije (u daljnjem tekstu ZKP Srbije) u glavi VII tačka V. u čl. 112.-132. normirana upotreba dokazne radnje vještačenja i određivanje vještaka.[4] U Hrvatskoj u Glavi XVII. tačka 8. u čl. 308.- 328. Zakona o krivičnom postupku (u daljnjem tekstu ZKP Hrvatske) određeno je kada i na koji način se određuje dokazna radnja vještačenja i određivanje vještaka.[5] Zakon o krivičnom postupku Slovenije[6] (ZKP Slovenije) u poglavlju XVIII, tačka 7. u čl. 248.-267. uređuje dokaznu radnju vještačenje i status i ulogu vještaka u krivičnim postupcima.

b) Propisi o stalnim sudskim vještacima

U promatranim zemljama regiona normativno su uspostavljeni posebni propisi koji određuju uslove koji se odnose generalno na status vještaka koji postupaju ne u samo krivičnim postupcima, već i u drugim sudskim postupcima, kao i upravnim i prekršajnim postupcima. Međutim, u nekim zemljama ti propisi nisu regulisani posebnim (*lex specialis)* zakonima o vještacima kao što je to slučaj u Bosni i Hercegovini. Tako je u Hrvatskoj, status vještaka regulisan Zakonom o sudovima.[7] Dalje je Pravilnikom o stalnim sudskim vještacima[8] donesenim od

---

4 Zakon o krivičnom postupku Republike Srbije "Službeni glasnik RS" br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014)

5 Zakon o kaznenome postupku Republike Hrvatske "Narodne novine HR" br. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14

6 Zakon o krivičnom postupku Slovenije dostupno na http://pisrs.si/Pis.web/pravniRedRSSearch?search=the+criminal+procedure+act

7 Zakon o sudovima "Narodne novine HR" br. 28/13, 33/15, 82/15

8 Pravilnik o stalnim sudskim vještacima "Narodne novine HR" br. 28/13

strane Ministarstva pravosuđa Hrvatske detaljnije normirana, odnosno razrađena pitanja od značaja za vještake. Slična su normativna rješenja i u Sloveniji gdje su Zakonom o redovnim sudovima Slovenije[9] regulisana opća statusa stalnih vještaka, dok je Pravilnikom o sudskim vještacima i procjeniteljima[10] detaljno normirano imenovanje, položaj, obaveze i prava sudskih vještaka.

U Srbiji, pitanja vještaka koji se angažuju u svim sudskim i drugim postupcima, kao i u Bosni i Hercegovini, normirana su posebnim (*lex specialis)* zakonima. Tako je je u Srbiji status vještaka normiran Zakonom o sudskim vještacima.[11]

2. Uloga vještačenja i vještaka u krivičnom postupku

a) Razlozi za određivanje vještačenja

Potreba za određivanjem vještaka u krivičnom postupku se javlja u situacijama u kojima organ koji vodi postupak ne posjeduje posebna stručna znanja za utvrđivanje ili ocjenjivanje određenih relevantnih činjenica i donošenja konačne odluke, zbog čega se određuje vještačenje i imenuje lice koje raspolaže potrebnim stručnim znanjima da ocijeni ill utvrdi takvu činjenicu. Ovo je posebno bitno kod složenih krivičnih djela i oblasti, poput oblasti kriminala u sektoru obnovljivih izvora energije je veoma kompleksna oblast jer podrazumijeva interdisciplinarno polje koje zahtjeva kadar specifičnog obrazovanja (Kreso, 2025). Gore navedeni razlozi za određivanje vještaka su jednako riješeni u zakonima o krivičnim postupcima upoređivanih zemalja iz regije, i one se odnose na pružanje „pomoći“ u utvrđivanju ili ocjenjivanu neke vanpravne činjenice za koje organ koji vodi određenu fazu krivičnog postupka ne posjeduje stručna znanja. Pored toga, iako krivičnoprocesnim zakonskim rješenjima u promatranim zemljama nije posebno propisana zabrana određivanja vještačenja iz oblasti koje se tiču pravnih pitanja, podrazumijeva se da se stručna znanja odnose na oblasti koje nisu pravne prirode koje logički posjeduje organ koji vodi krivični postupak. Izuzetak postoji u ZKP-u Srbije gdje je u članu 113. stav 2. izričito navedeno da se vještačenje kao dokazna radnja ne može odrediti radi ocjene ili utvrđivanja pravnog pitanja .

Kao što je ranije navedeno, vještačenje i vještaka u promatranim zemljama regiona određuje organ koji vodi postupak, i to u pravilu pisanom naredbom.

---

[9] Zakon o redovnim sudovima slovenije „Službeni list SLO“ br. 10/77, 4/82, 37/82, 7/86, 41/87, 24/88, 8/90, 19/94 in 19/94

[10] Pravila o sudskim vještacima i procjenjiteljima „Službeni list SLO“ br. 7/02, 75/03, 72/05, 71/07, 84/08 in 88/10)

[11] Zakon o sudskim veštacima "Službeni glasnik RS“, br. 44/10

b) Pravo određivanja vještačenja

U promatranim zemljama organ koji vodi postupak određuje vještačenje i imenuje vještaka po službenoj dužnosti ili na prijedlog stranaka, te organ koji vodi postupak ima diskrecijsko pravo u odluci da li će odrediti vještačenje. To zapravo znači da je diskrecijsko pravo u odlučivanju da li u svakom konkretnom slučaju postoji potreba za određivanjem vještačenja u rukama organa koji vodi postupak. Organ koji vodi postupak može prihvatiti prijedlog stranke u postupku za samo vještačenje, ali i prijedlog koje specifično pravno ili fizičko lice odrediti za vještaka. Međutim važno je napomenuti da sam prijedlog stranke ili branioca u krivičnom postupku ničime ne obavezuje sud, odnosno organ koji vodi postupak da ne odbije takav prijedlog i ne donese naredbu o vještačenju. Ovakva rješenja su prihvaćena u svim zemljama regije i vrlo su slična rješenjima koja postoje u Federaciji Bosne i Hercegovine, gdje pismenu naredbu za vještačenje izdaje tužilac ili sud.

U Srbiji, organ koji vodi postupak po službenoj dužnosti ili na prijedlog stranke ili branioca određuje vještačenje pismenom naredbom,[12] Hrvatskoj se također navodi da vještačenje određuje organ pisanim nalogom tijelo koje vodi postupak[13] dok su ista ili slična rješenja uređena i u Sloveniji.

Kao neki od razloga zbog kojeg se diskreciono pravo određivanja vještačenja dodjeljuje organu koji vodi postupak su i to da vještačenje može dosta uticati na sam krivični postupak (Svjetska Banka, 2010). Uticaj vještačenje se može odraziti na efikasnost samog postupka iz razloga da izrada nalaza i mišljenja iziskuje određeno vrijeme. Duža izrada nalaza i mišljenja vještaka se posebno mogu očekivati u predmetima gdje je neophodno provesti složenija vještačena koji mogu znatno usporiti sam postupak, te ukoliko se neosnovano određuju mogu uticati na načelo efikasnosti krivičnog postupka. Također vještačenje iziskuje i određena finansijska sredstva bez obzira što iste snosi- organ koji vodi postupak ili neka od stranaka u postupku, uslijed čega se utiče i na načelo ekonomičnosti krivičnog postupka. Upravo zbog toga, kako u promatranim zemljama, tako i u zemljama evropsko-kontinentalnog prava, odluka o određivanju vještačenja dodijeljena je organu koji vodi postupak da odredi da li je u konkretnom slučaju potrebno sprovesti vještačenje.

[12] Član 113. ZKP-a Srbije
[13]Član 309 ZKP-a Hrvatske

c) Angažovanje privatnih vještaka i stručnih lica

Iako u evropsko-kontinentalnom pravu isključivo diskrecijsko pravo za određivanje vještačenja ima organ koji vodi postupak, često se razmatra pitanje mogućnosti angažovanja vještaka odnosno stručnog lica od strane stranaka u krivičnom postupku, kao i sama dokazna vrijednost angažmana takvih lica i njihovih eventualnih nalaza i mišljenja. Dokazna radnja i postupak vještačenje, koje je kao takvo propisano u krivičnim postupcima u promatranim zemljama regije, u krivičnom postupku nije *kontradiktorno* u tom smislu da bi svaka stranka imala "svog" vještaka koji daje iskaz pred sudom ili daje sudu pisani nalaz i mišljenje, te postojanje istih nije prihvatljivo, jer vještak na sudu mora dati svoj iskaz objektivno.[14] U evropsko- kontinentalnom pristupu vještačenju podrazumijeva se da je vještak osoba koja je objektivna i nepristrasna i pruža pomoć organu koji vodi krivični postupak. Međutim, često se u praksi dešava da stranke u postupku, najčešće osumnjičeni ili optuženi odnosno njihovi branioci angažuju lice koje je vještak ili stručnjak iz određene oblasti kako bi pomogao u pripremi odbrane, ali i podržao njene argumente, te također izradio svoj "nalaz" i "mišljenje" o određenoj stvari. Ovo je posebno izraženo kod procesuiranja organiziranih kriminalnih grupa što je je oduvijek predstavljalo značajan izazov i problematiku za državne agencije i službe za provedbu zakona (Muhić, 2024). Takva eventualna pomoć, kao i nalazi i mišljenje "privatnih" vještaka ne mogu se smatrati dokaznom radnjom vještačenja, nego se ona po pravilu nazivaju *stručna pomoć odbrane* te nemaju značaj dokazne radnje vještačenja. Stranke takve osobe („privatne vještake") mogu predložiti za svjedoka na glavnoj raspravi, te sud često i odobrava da takve osobe stručnog znanja iznesu svoje mišljenje o prethodno provedenom vještačenju koje je ranije odredio organ koji vodi postupak. Međutim u Bosni i Hercegovini i većini zemalja promatranih radi komparativne analize, krivičnoprocesnim zakonodavstvima nisu posebno propisana pitanja koja regulišu ulogu i status stručnih savjetnika stranaka u postupku koji bi eventualno bili u mogućnosti da kritički ocijene nalaz, mišljenje i iskaz vještaka i vještačenje.
Od promatranih zemalja jedino je u Srbiji u ZKP-u regulisano pitanje stručnog savjetnika, a u vezi sa naređenim vještačenjem koje mogu angažovati stranke u postupku.[15] Naime pitanje regulisanja pozicije stručnog savjetnika predstavljaju novitet u Zakonu o krivičnom postupku Srbije koji je stupio na snagu u 2011. godini. Tako je regulisano da pored prava da predlažu vještačenje i vještake, stranke imaju i pravo da izaberu sebi stručnog savjetnika uvijek kada organ

[14] Bayer V., Kazneno procesno pravo-odabrana poglavlja, Knjiga I, - Uvod u teoriju kazneno procesnog prava (priredio D.Krapac) u Hrvatska pravna revija Zorislav Kaleb "Privatno vještačenje dostavljeno od stranke u sudu u kaznenom postupku

[15] Ovakvo riješenje je specifično za Italijansko krivično procesno zakonodavstvo gdje također stranke imaju pravo angažovanja tehničkog savjetnika odbrane

postupka odredi vještačenje[16]. To pravo pripada strankama bez obzira na to da li je vještak određen po službenoj dužnosti ili od strane organa koji vodi postupak po prijedlogu suprotne stranke. Javni tužilac je do podizanja optužnice organ postupka, pa stručnog savjetnika može da ima samo poslije podizanja optužnice, ali malo je vjerovatno da će ga i tada angažovati[17]. Stručni savjetnik stranke mora da ima iste kvalifikacije kao i vještak. Slobodno izabrani savjetnik ne mora bit nužno izabran sa liste stalnih sudskih vještaka. Stručnog savjetnika na teret budžetskih sredstava (član 125. stav 3 ZKP Srbije) može dobiti samo okrivljeni i oštećeni kao tužilac. O postavljanju stručnog savjetnika odlučuje organ koji vodi postupak, odnosno odlučuje sud. Stručnom savjetniku je omogućeno da prisustvuje vještačenju kojem imaju pravo da prisustvuju okrivljeni i njegov branilac (član 126. stav 1 ZKP Srbije).

Osnovna razlika između vještaka i stručnog savjetnika je u tome što stručni savjetnik organima postupka ne podnosi nalaz i mišljenje, već samo ukazuje na nedostake u nalazu i mišljenju vještaka koga je odredio sud. Stručni savjetnik se ispituje o predmetu vještačenja i tada ima priliku da izloži svoj nalaz i svoje mišljenje, ali njegov iskaz ni tada nema procesnu formu nalaza i mišljenja veštaka. Taj iskaz ima dokaznu snagu i sudija se u obrazloženju presude na njega može pozvati. Prema zakonskim odredbama stručnom savjetniku je zabranjeno da radi na štetu postupka, ali to ne znači nužno da je dužan da sarađuje sa organima postupka.

2.1. Kriteriji za odabir određenih vještaka

Zahtjev da vještak posjeduje određena stručna znanja predstavlja neophodan uslov svakog vještačenja bez obzira na to kako je normativno regulisan[18], te kao takav treba da bude jedan od faktora koji preovladavaju za izbor određenog vještaka. Zakoni o krivičnom postupku u regiji najčešće samo generalno normiraju koji su to uslovi koje treba posjedovati lice da bi bilo imenovano za vještaka.
Krivično procesnim zakonodavstvima je određeno da se vještačenje određuje kad za utvrđivanje ili ocjenu neke važne činjenice treba pribaviti nalaz i mišljenje od lica koje raspolaže potrebnim stručnim znanjem, te se o vještaku govori kao o licu koje raspolaže stručnim znanjem. Samo pitanje procjene

[16] Član 125. ZKP-a
[17] KOMENTAR ZAKONIKA O KRIVIČNOM POSTUPKUXIII izdanje – 1032 strane (prema novom Zakoniku o krivičnom postupku iz 2011.godine) autori: prof dr Momčilo Grubač i prof dr Tihomir Vasiljević izdavač PROJURIS, 2013.
[18] Vještačenje u krivičnom postupku: nova praksa u starim normativnim okvirima i drugi problem str 29-54 Snežana Čolaković

postojanja stručnosti i adekvatnog specijalističkog profila vještaka prepušta se organima koji vode krivični postupak, što je donekle problematično uzimajući u obzir da predstavnici organa koji vode postupak nemaju ta specifična znanja da procijene stručnost određenog vještaka. Ipak, takvo diskrecijsko pravo određivanja vještaka je donekle ograničeno krivično-procesnim zakonodavstvom promatranih zemalja u smislu postojanja lista stalnih sudskih vještaka, ili je prepušteno drugim stručnim ustanovama da odrede stručno lice ili lica koja će sprovesti konkretno naređeno vještačenje.

a) **Lista stalnih sudskih vještaka**

Postojanje liste stalnih sudskih vještaka, koja je po pravilu obavezna za sud, odnosno organ koji vodi postupak, je najrasprostranjeniji način kontrole stručnih referenci i znanja vještaka u krivičnom postupku posmatranih sistema. Svrha liste stalnih sudskih vještaka je potvrda kompetencije onih osoba koje su određene da vrše različita vještačenja kako u krivičnom, tako i u drugim sudskim postupcima. Takva ograničenja su određena zakonima o krivičnim postupcima. Tako je primjera radi u Hrvatskoj, ukoliko za koju vrstu vještačenja kod suda postoje stalno određeni vještaci, drugi vještaci koji nisu kod suda određeni se mogu samo odrediti ako su stalni sudski vještaci spriječeni, ili ako to zahtijevaju druge okolnosti[19]. Slično je rješenje i u Sloveniji gdje je navedeno da kada sud određuje vještaka, može samo odrediti stalnog sudskog vještaka sa liste stalnih sudskih vještaka, osim u slučaju spriječenosti ili drugih relevantnih okolnosti.
U Crnoj Gori je navedeno da vještačenje određuje organ koji vodi postupak pisanom naredbom koja mora da sadrži: zadatak i obim vještačenja, rok za podnošenje pisanog nalaza i mišljenja i određivanje lica koje će izvršiti vještačenje a koje je upisano u Registar sudskih vještaka ili Registar pravnih lica za vršenje vještačenja[20]. Samo izuzetno se može odrediti za vještaka lice koje nije upisano Registar sudskih vještaka ili Registar pravnih lica za vršenje vještačenja, i to onda kada za takvu vrsta vještačenja nema postavljenih sudskih vještaka[21]. Pored odredbi ZKP-a Crne Gore, Zakon o sudskim vještacima Crne Gore određuje i da je nadležni sud prilikom izbora dužan da u pojedinom predmetu, po pravilu, određuje vještaka koji ima prebivalište na području tog suda, a posebno vodeći računa da vještaci iz iste oblasti budu ravnomjerno angažovani. Ovakvom zakonskom odredbom se ograničava mogućnost kontinuiranog određivanja istih i samo određenih vještaka, a ukoliko na listi stalnih sudskih vještaka postoji više njih[22].

[19] Član 309. St.4 ZKP Hrvatske
[20] Član 137. st.1 ZKP Crna Gora
[21] Član 137. St.4 ZKP Crna Gora
[22] Član 26. Zakona o sudskim vještacima Crna Gore

U Srbiji je uvedena situacija da organ koji vodi postupak određuje vještačenje pisanom naredbom, te se navodi da ako za određenu vrstu vještačenja postoje vještaci sa spiska stalnih vještaka, drugi vještaci se mogu odrediti samo ako postoji opasnost od odlaganja, ako su stalni vještaci spriječeni, ili ako to zahtijevaju druge okolnosti[23]. Zakon o sudskim vještacima Srbije[24] također naglašava da je Sud, odnosno organ koji vodi postupak, dužan da prati rad vještaka i da za vještačenje u pojedinom predmetu određuje vještaka koji ima prebivalište na području tog suda, vodeći računa da vještaci iz iste oblasti budu ravnomjerno angažovani.

Iz ovakvih zakonskih odredbi proizlazi zaključak da listu stalnih sudskih vještaka zakonodavac uzima kao dovoljno sredstvo za kontrolu vještakovih stručnih kompetencija, koje također omogućava brz i uspješan izbor vještaka, pa procesnu radnju imenovanja vještaka svodi na izbor imena lica odgovarajuće struke sa postojeće liste[25].

Ipak od promatranih zemalja regije, važno je istaći da samo zakoni o krivičnom postupku u Bosni i Hercegovini ne propisuju obavezu da je organ koji vodi postupak dužan odrediti vještaka sa liste stalnih sudskih vještaka, odnosno zakoni o krivičnom postupku uopće ne poznaju pojam stalnog sudskog vještaka. To znači da u Bosni i Hercegovini postojeće liste stalnih sudskih vještaka ne obavezuju organ koji vodi krivični postupak da odredi vještaka sa liste stalnih sudskih vještaka. Zakon o vještacima Federacije BiH čak eksciplitno navodi da lista stalnih sudskih vještaka nije obavezujuća za sud ili drugi organ koji vodi postupak, odnosno druge učesnike u postupku, osim ako je drugačije predviđeno propisima kojima se uređuju pravila postupka[26]. Zakonskim odredbama nije regulisano na koji način će organ koji vodi postupak ocijeniti stručnost i kompetenciju određenog lica koje će imenovati za provođenje određenog vještačenja.

b) **Stručna ustanova ili državni organ**

Zemlje čiji su sistemi odabrani za komparativnu analizu, kao i Federacija Bosne i Hercegovine, u svojim krivično procesnim zakonodavstvima predviđaju da ako za određenu vrstu vještačenja postoji stručna ustanova ili se vještačenje može obaviti u okviru državnog organa, takva vještačenja, a naročito složenija, povjeriti će se, po pravilu, takvoj ustanovi, odnosno organu. Ustanova, odnosno

[23] Član 114. ZKP Srbija
[24] Član 18. Zakona o sudskim vještacima Srbije.
[25] Snježana Čolaković "Veštačenje kao dokaz u krivičnom postupku" str.31
[26] Član 11 zakona o vještacima Republike Srpske i član 14 Zakona o vještacima Federacije BiH

organ određuje jednog ili više stručnjaka odgovarajuće specijalnosti koji će izvršiti vještačenje.[27] Ovime se određivanje osobe/a koja/a posjeduje/u dovoljno stručnog i specijalitičkog znanja daje stručnoj ustanovi specijaliziranoj za provođenje određenih vještačenja.

Standard je da u pravilu jedno ili više fizičkih lica može biti određeno za vještake u krivičnom postupku, što predstavlja princip da vještačenje predstavlja individualni i lični doprinos stručnog mišljenja određenog stručnjaka, ali i da odgovornost za eventualne propuste i istinitost nalaza i mišljenja jeste na pojedincu vještaku (CEPEJ, 2012). S tim u vezi je navedeno da ukoliko organ koji vodi postupak odredi, da se vještačene povjeri stručnoj ustanovi ili državnom organu takav organ će odrediti koja fizička lica će provesti vještačenja, te će o imenima tih lica obavijestiti organ koji vodi postupak. Ovakva zakonska rješenja prepoznaju svi zakoni o krivičnim postupcima promatranih zemalja. Potrebno je da ukoliko se vještačenje povjeri takvom pravnom licu, da onda to pravno lice odredi jednog ili više stručnjaka koji će sprovesti vještačenje (CEPEJ,2012).

2.2. Izbor i imenovanje stalnih sudskih vještaka

a) Uslovi koje mora posjedovati fizičko lice da bi bilo imenovano za vještaka

Proces izbora i imenovanja vještaka je u promatranim zemljama regije uređeno, ili kao što je već ranije navedeno, posebnim zakonima o vještacima kao što je slučaj u Srbiji i Federaciji BiH, ili kao što je slučaj u Sloveniji i Hrvatskoj gdje je to općenito uređeno zakonima o sudovima i specifičnije pravilnicima o sudskim vještacima i procjeniteljima.
Propisi u svim promatranim zemljama regulišu uslove koje trebaju ispunjavati fizička i pravna lica da bili imenovana za stalne sudske vještake. Promatranim zemljama uslovi i kriteriji da fizičko lice bude izabrano su na različiti način regulisani, u određenim zemljama su kriteriji i uslovi uopćeni i niži dok su u pojedinim zemljama dosta konkretnije određeni i kriteriji za izbor su dosta viši. Tako naprimjer, uslovi da bi osoba bila imenovana za vještaka u Srbiji treba da ima odgovarajuće stečeno visoko obrazovanje na studijama drugog stepena (završene diplomske akademske studije – master, specijalističke akademske studije, specijalističke strukovne studije), odnosno na osnovnim studijama, za određenu oblast vještačenja.[28] Važeći zakoni o sudskim vještacima u Srbiji određuju kao uslove i da fizičko lice ima najmanje pet godina radnog iskustva u

[27] Član 137 st.2 ZKP-a Crne Gore
[28] Član 6 Zakona o sudskim vještacima Crne Gore i član 6 Zakona o sudskim vještacima Srbije.

struci, te da posjeduje stručno znanje i praktična iskustva za određenu oblast vještačenja. Kao izuzetak se propisuje da se za sudskog vještaka može imenovati i lice koje ima završenu srednju školu ukoliko ne postoji dovoljan broj vještaka za određenu oblast.

Pored gore navedenih stručnih uslova, Zakon o sudskim vještacima Srbije navodi da osoba mora biti dostojna za obavljanje vještačenja. Na ovaj način se pokušava dodatno uticati na preduslov da kandidat za sudskog vještaka posjeduje određeni nivo integriteta.

Pravilnik o sudskim vještacima i procjeniteljima Slovenije propisuje vrlo slične uslove za imenovanje određene osobe kao vještaka kao i zakoni o sudskim vještacima Srbije, s tim da kao uslov nije naveden stepen školske spreme, i da radno iskustvo u struci osobe koja se želi kandidovati za listu treba da bude u trajanju najmanje od 6 godina. [29]

U Hrvatskoj uslovi za imenovanje za stalnog sudskog vještaka su određeni konkretnije nego u ostalim zemljama regije, te su sami uslovi i kriteriji znatno zahtjevniji. Zakon o sudovima Hrvatske uopćeno propisuje da vještak može biti osoba sa završenim odgovarajućim stručnim studijem, preddiplomskim ili diplomskim univerzitetskim studijem.[30] Za stalnog sudskog vještaka se iznimno može imenovati i osoba sa završenom srednjom školskom spremom odgovarajuće struke.

Pravilnikom o stalnim sudskim vještacima se propisuju detaljniji uslovi koje treba da posjeduje određena osoba da bi se imenovala za sudskog vještaka. Pravilnikom se prvenstveno propisuje da vještak može biti osoba koja je državljanin Republike Hrvatske, državljanin države članice Europske unije ili državljanin države potpisnice Sporazuma o Europskom gospodarskom prostoru. Također se Pravilnikom zahtijeva da je osoba zdravstveno sposobna za obavljanje poslova stalnog sudskog vještaka, a što nije određeno propisima drugih posmatranih sistema.

Što se tiče stručnog i akademskog znanja Pravilnikom o stalnim sudskim vještacima se navodi i sljedeći uslovi:

1. Da je nakon završenog odgovarajućeg studija odnosno odgovarajuće škole radila na poslovima u struci i to:
   a) najmanje 8 godina – ako je završila diplomski sveučilišni studij ili specijalistički diplomski stručni studij;
   b) najmanje 10 godina – ako je završila odgovarajući preddiplomski sveučilišni studij ili preddiplomski stručni studij;
   c) najmanje 12 godina – ako je završila odgovarajuću srednju školu, a za pojedinu struku nema odgovarajućeg preddiplomskog sveučilišnog studija ili preddiplomskog stručnog studija odnosno

[29] Član 5 Pravilnika o sudskim vještacima i procijeniteljima
[30] Član 126. Stav 2. Zakona o sudovima Hrvatske

diplomskog sveučilišnog studija ili specijalističkog diplomskog stručnog studija.

Pravilnik kao obavezu definiše i sklopljen ugovor o osiguranju od odgovornosti za obavljanje poslova stalnog sudskog vještaka. Kao poseban uslov kojima se tretira pitanje integriteta vještaka Pravilnikom je propisano da se za stalnog sudskog vještaka ne može imenovati osoba za koju postoje smetnje za prijem u državnu službu.

Pored gore navedenih akademskih, stručnih i ostalih uslova za imenovanje određene osobe za vještaka u Hrvatskoj se kao poseban uslov određuje i da je lice prethodno uspješno završilo stručnu obuku. U odnosu na ostale sisteme korištenja vještaka, **o**buka kao poseban uslov da bi se lice uopće imenovalo za stalnog sudskog vještaka je kao takva jedino propisana u Pravilniku o stalnim sudskim vještacima Hrvatske. Pa tako npr. Zakoni o sudskim vještacima Srbije i Slovenije ne normiraju posebno obavezu pohađanje obuke kao uslov za imenovanje ili provođenje vještačenja. Zakon o vještacima FBiH obuku ne propisuju kao uslov za imenovanje na listu sudskih vještaka, već je normirano da je nakon imenovanja vještak dužan završiti obuku o obavljanju poslova vještačenja prema pravilniku koji donosi nadležni entitetski ministar pravde.

b) Odgovorne institucije za imenovanje sudskih vještaka, njen sastav i proces imenovanja

Srbija
Postupak imenovanja stalnih sudskih vještaka prema Zakonu o sudskim vještacima sprovodi jedino Ministarstvo pravde Srbije, te pozitivno zakonodavstvo ne prepoznaje posebnu stručnu komisiju koju imenuje ministarstvo.

Slovenija
Ministarstvo pravde Slovenije provodi postupak imenovanja stalnih sudskih vještaka. Ministarstvo također može , da ukoliko procijeni potrebnim , zahtijevati poseban stručni ispit koji provodi Komisija koju za takve potrebe imenuje Ministar pravde. Komisija se sastoji od predsjednika i najmanje dva člana i zapisničara. Predsjednik Komisije se imenuje iz jednog od ministarstava iz Vlade Slovenije sa najmanje završenim drugim stepenom pravnog fakulteta. Druga dva člana Komisije su imenovani iz reda stručnjaka i oni moraju imati najmanje stručne kvalifikacije kao što ih posjeduje i kandidat za sudskog vještaka. Zapisničar Komisije je uposlenik Ministarstva pravde.

Hrvatska
Nadležna institucija za postupak imenovanja stalnog sudskog vještaka u Hrvatskoj je Županijski ili trgovački sud, odnosno predsjednici županijskih i trgovačkih sudova u Hrvatskoj, kojima lice koje smatra da posjeduje kvalifikacije podnosi zahtjev za imenovanje za stalnog sudskog vještaka. Ukoliko predsjednik županijskog ili trgovačkog suda ocijeni da kandidat ispunjava uslove on prije imenovanja upućuje kandidata na stručnu obuku u nadležno udruženje sudskih vještaka koje imenuje mentora koji je član Udruženja stalnih sudskih vještaka.

Federacija BiH
Zakon o vještacima FBiH utvrđuje obavezu federalnog ministra pravde da objavi javni poziv za imenovanje vještaka i imenuje Komisiju sastavljenu od stalnih članova, i to u FBiH od predsjednika Vrhovnog suda FBiH ili sudije kojeg on ovlasti, predsjednika entitetske Advokatske komore ili advokata kojeg on ovlasti, glavnog federalnog tužioca ili tužioca kojeg on ovlasti, predstavnika entitetskog ministarstva pravde, te tri privremena člana koje iz reda vodećih stručnjaka u oblastima u kojima se vještačenja obavljaju imenuju stalni članovi većinom glasova

c) Procedura izbora stalnih sudskih vještaka

Srbija
Ministar pravde objavljuje javni poziv za imenovanje vještaka u „Službenom glasniku Republike Srbije" i na internet stranici Ministarstva pravde, kada utvrdi da postoji nedovoljan broj vještaka za određenu oblast vještačenja. Zahtjev za imenovanje sa prilozima kojima se dokazuje ispunjenost uslova za obavljanje vještačenja kandidat za vještaka podnosi ministarstvu. Rješenje o imenovanju vještaka donosi ministar pravde. Protiv rješenja kojim se odbija zahtjev za imenovanje, kandidat za vještaka može pokrenuti upravni spor. Rješenje o imenovanju vještaka sadrži prezime, ime jednog roditelja i ime vještaka, njegovo prebivalište i adresu, zvanje, oblast vještačenja i užu specijalnost vještaka. Rješenje se objavljuje u „Službenom glasniku Republike Srbije" i na internet stranici Ministarstva pravde. Zakon o sudskim vještacima Srbije ne propisuje obavezu izrade dodatnih podzakonskih akata koji regulišu postupak imenovanja vještaka, kao ni uspostavljanje posebnih tijela koja će provjeravati stručnost kandidata u postupku imenovanja novih sudskih vještaka. Ministarstvo vodi Registar vještaka koji se vodi i u elektronskom obliku i javno je dostupan preko internet stranice ministarstva.
Pored Registra vještaka, ministarstvo vodi i zbirku isprava za svakog vještaka. U zbirci isprava čuvaju se dokumenta na osnovu kojih je izvršen upis u Registar

vještaka, kao i prijave podnijete protiv vještaka, rješenja o izrečenim novčanim kaznama i prijedlozi za razrješenje vještaka.

Slovenija

Ministarstvo pravde Slovenije, dva puta u kalendarskoj godini, objavljuje poziv za podnošenje prijava za imenovanje sudskih vještaka, sudskih procjenitelja i tumača. Poziv se objavljuju u skladu sa potrebama u određenom području stručnosti koji je identifikovan na osnovu obrazloženih mišljenja predsjednika sudova. Za potrebe utvrđivanja posjedovanja odgovarajućih uslova Ministarstvo pravde može tražiti mišljenje o kandidatu i njegovim uslovima od određene javne institucije, profesionalne institucije ili profesionalnog udruženja ili neke druge odgovarajuće institucije. Ministarstvo pravde imenuje Komisiju ukoliko procijeni da je neophodno da kandidat za vještaka treba da izađe na stručni ispit. Komisija provodi specifične ili stručne ispite. Rok za provođenje testiranja mora biti objavljen najranije 30 dana prije polaganja testa. Test se sastoji od općih pravnih pitanja koji su isti za sve kandidate i specifičnih pitanja za različite oblasti. Program testova po specifičnim oblastima priprema Centar za edukaciju nosilaca pravosudne funkcije u Sloveniji. Centar ima mandat i da vrši pripremne seminare i obuke za potencijalne kandidate za sudske vještake.
Sudski vještaci se imenuju na dan polaganja zakletve pred ministrom pravde. Ministarstvo pravde vodi registar imenovanih vještaka koje dostavlja nadležnim sudovima i drugim relevantnim institucijama.

Hrvatska

Nadležna institucija za postupak imenovanja stalnog sudskog vještaka u Hrvatskoj je Županijski ili trgovački sud, odnosno predsjednici županijskih i trgovačkih sudova u Hrvatskoj. Ukoliko predsjednik županijskog ili trgovačkog suda ocijeni da kandidat koji je poslao zahtjev za imenovanje ispunjava uslove za imenovanje za stalnog sudskog vještaka, predsjednik nadležnog suda prije imenovanja upućuje kandidata na stručnu obuku u Hrvatsko društvo sudskih vještaka i procjenitelja (HDSV), koja je nadležna institucija za provođenje obuke u Hrvatskoj.

Stručna obuka se obavlja prema programu što ga za svaku posebnu djelatnost izrađuje i utvrđuje odgovarajuće strukovno udruženje. HDSV, nakon što od određenog predsjednika suda primi zahtjev, imenuje mentora koji će biti zadužen za provođenje stručne obuke kandidata za stalnog sudskog vještaka. Pravilnik o stalnim sudskim vještacima propisuje da se za mentora može imenovati stalni sudski vještak koji ima najmanje pet godina iskustava u

obavljanju poslova sudskog vještačenja[31]. Ipak Pravilnik o provođenju obuke za poslove stalnog sudskog vještaka utvrđuje nešto specifičnije i rigoroznije uslove koje mentor mora posjedovati. Tako se u članu 12. Pravilnika navodi da mentor može biti član HDSV-a koji ima visoku stručnu spremu, položen stručni ispit s područja struke istovjetnog sa kandidatovom, za struke gdje je to prema zakonu obavezno, te najmanje deset godina staža u sudskom vještačenju. Također mentor mora imati isti ili više naučni stepen zvanja od samog kandidata. Voditelj podružnice i Vijeće podružnice HDSV-a odlučuje o imenovanju mentora i o tome obavještava Upravni odbor HDSV-a. Mentor organizira i provodi osposobljavanje kandidata prema programu obuke koji sadrži teorijski i praktični dio. U teorijskom dijelu mentor upoznaje kandidata s najnovijim znanstvenim saznanjima, stručnim skupovima, stručnom literaturom, zakonskim i podzakonskim aktima, koji uređuju područje vještačenja za koje se kandidat osposobljava. Mentor upoznaje kandidata sa Etičkim kodeksom sudskih vještaka i Statutom HDSV-a. Praktični dio obuke podrazumijeva prikupljanje podataka na terenu, izradbu nacrta, skica, izračuna, analiza, izradu nalaza i mišljenja i pristup na raspravu.

Osposobljavanje kandidata za sudskog vještaka utvrđuje se u trajanju 6-12-mjeseci. Nakon obavljene obuke kandidata za osposobljavanje kandidata za sudskog vještaka, mentor sastavlja izvještaj o postupku obuke i konačnim mišljenjem i dostavlja ga nadležnom organu HDSV-a. HDSV u roku od trideset dana po prijemu izvještaja mentora, upućuje izvještaj o uspješnom osposobljavanju kandidata, sudu koji je kandidata uputio na osposobljavanje, s preporukom za imenovanje stalnog sudskog vještaka.

HDSV je dužan županijske i trgovačke sudove izvještavati o programima stručne obuke i godišnjem rasporedu održavanja stručne obuke.

Nadzor nad provođenjem stručne obuke stalnih sudskih vještaka u HDSV-u obavljaju Ministarstvo pravosuđa i nadležni županijski odnosno trgovački sud prema rasporedu kojeg donosi ministar pravosuđa. O provedenom nadzoru sastavlja se pisani izvještaj.

Prije imenovanja za stalnog sudskog vještaka kandidat je dužan predsjedniku županijskog odnosno trgovačkog suda koji je nadležan za njegovo imenovanje dostaviti dokaz o sklopljenom ugovoru o obveznom osiguranju od odgovornosti za obavljanje poslova stalnog sudskog vještaka. Nakon završene stručne obuke i prikupljenih dokaza o ispunjavanju uvjeta za imenovanje stalnim sudskim vještakom, predsjednik odgovarajućeg županijskog odnosno trgovačkog suda odlučit će o zahtjevu. Stalni sudski vještak imenuje se na vrijeme od četiri godine. Popisi stalnih sudskih vještaka vode županijski i trgovački sudovi.

Federacija Bosne i Hercegovine

[31] Član 6 Pravilnika o stalnim sudskim vještacima Hrvatske

Vještaci se imenuju putem javnog poziva koji objavljuju entitetski ministar pravde. Ministar pravde imenuju komisiju koja provjerava da li su kandidati stručni za obavljanje poslova vještaka kao i njihovu nepristrasnost i integritet.
Zakon o vještacima Federacije BiH utvrđuju obavezu ministra pravde da objavi javni poziv za imenovanje vještaka i imenuje Komisiju sastavljenu od stalnih članova, i to u FBiH od predsjednika Vrhovnog suda FBiH ili sudije kojeg on ovlasti, predsjednika entitetske Advokatske komore ili advokata kojeg on ovlasti, glavnog federalnog tužioca ili tužioca kojeg on ovlasti, predstavnika ministarstva pravde, te tri privremena člana koje iz reda vodećih stručnjaka u oblastima u kojima se vještačenja obavljaju imenuju stalni članovi većinom glasova.

3. Dužnosti i prava (stalnog) sudskog vještaka u procesu izrade nalaza i mišljenja

Zakon o krivičnom postupku Srbije uređuje da je vještak dužan da se odazove pozivu i da da svoj pisani nalaz i mišljenje u roku određenom u naredbi. Rok određen naredbom, iz opravdanih razloga, na zahtjev vještaka, može se produžiti. Vještak je dužan da predmet vještačenja brižljivo razmotri, da tačno navede sve što zapazi i nađe i da svoje mišljenje iznese nepristrasno i u skladu sa pravilima nauke ili vještine. Vještak je dužan odgovoriti i na sva dodatna pitanja koja, kao i da razjasni sve ostale eventualne nedoumice organu koji vodi postupak.
Vještak je dužan sve svoje nalaze i mišljenja da unosi u zapisnik. U zapisniku o vještačenju ili u pisanom nalazu i mišljenju naznačiće se ko je izvršio vještačenje, kao i zanimanje, stručna sprema i specijalnost vještaka

Zakonom o vještacima Srbije je uređeno da su stalni sudski su skladu za važećim zakonskim propisima su dužni da se pridržava rokova određenih aktom suda kojim mu je vještačenje povjereno. Ako vještak iz objektivnih razloga ne može završiti vještačenje u određenom roku, dužan je da podnese sudu, najkasnije osam dana prije isteka roka, obavještenje o razlozima zbog kojih nije u mogućnosti da završi vještačenje i kratak prikaz rezultata do tada obavljenih radnji. Nakon prijema obavještenja, sud će odrediti novi rok u kojem vještačenje mora biti završeno ili vještačenje povjeriti drugom vještaku. U složenijim vještačenjima, u kojima je određen duži rok za vještačenje, vještak je dužan da podnosi sudu svakih trideset dana kratak izvještaj o rezultatima do tada obavljenih radnji. Ako vještak ne postupa u skladu sa ovim članom smatraće se da neuredno vrši vještačenje. U zakonu o sudskim vještacima je posebno

naznačeno da je vještak obavezan na čuvanje tajnosti podataka do kojih je došao u vršenju vještačenja.

Prava vještaka

Zakon o krivičnom postupku Srbije generalno naznačava da prilikom izrade nalaza i mišljenja vještak ima pravo da mu se daju dodatna razrješnjenja same naredbe i da pregleda spise. Vještak također ima pravo da predlaže da se prikupe dokazi ili pribave dodatna mišljenja i podaci koji mu mogu biti od pomoći u radu. Vještak ima pravo pristupa svim dokumentima, dokazima i drugim materijalima neophodnih za izradu nalaza i mišljenja.
Zakon o krivičnom postupku prpoznaje, kao što je već ranije navedeno stručnog savjetnika u vezi sa poslovima vještačenja u krivičnom postupku. Dužnosti i prava stručnih savjetnika su također propisana ZKP-om Srbije. Tako je propisano da je stručni savjetnik dužan da punomoć bez odlaganja podnese organu postupka, da stranci pruži pomoć stručno, savjesno i blagovremeno, da ne zloupotrebljava svoja prava i da ne odugovlači postupak. Stručni savjetnik ima pravo da bude obaviješten o danu, satu i mjestu vještačenja i da prisustvuje vještačenju kojem imaju pravo da prisustvuju okrivljeni i njegov branilac, da u toku vještačenja pregleda spise i predmet vještačenja i predlaže vještaku preduzimanje određenih radnji, da daje primedbe na nalaz i mišljenje vještaka, da na glavnom pretresu postavlja pitanja vještaku i da bude ispitan o predmetu veštačenja. Pre ispitivanja od stručnog savetnika će se zahtijevati da položi zakletvu.

Zakonom o stalnim sudskim vještacima Srbije je uređeno da je Vještake dužan da se pridržava rokova određenih rješenjem suda i da vještačenje obavlja savjesno, stučno i nepristrasno.Pored toga je propisano i da je vještak dužan da čuva tajnost podataka koje je saznao obavljajući tokom provođenja vještačenja. Zakonom o sudskim vještacima je dalje naznačeno da vještak za poslove vještačenja ima pravo na odgovarajuću naknadu.

Slovenija

Zakon o krivičnom postupku Slovenije na vrlo sličan način reguliše dužnosti i obaveze sudskih vještaka kao i zakoni o krivičnom postupcima Crne Gore i Srbije. Pravilnikom o sudskim vještacima i procijeniteljima u Sloveniji je utvrđeno da sudski vještaci su dužni izraditi nalaz i mišljenje na zakonit i odgovoran način u skladu sa pravilima struke i nauke. Također vještaci su dužni poštovati rokove koje su propisani od strane organa koji vodi postupak. Općenito takvi rokovi ne mogu biti kraći od trideset niti dužio od šezdeset dana. Ukoliko vještak nije u

mogućnosti da izradi nalaz i miljenje u datom roku dužan je o istom obavijestiti nadležni organ najkasnije petnaest dana prije isteka roka. Pravilnikom je još i regulisano da će sudski vještaci povjerene materijale i dokaze čuvati pažljivo i odgovorno, te da će se voditi zakonom o zaštiti ličnih podataka prema informacijama do kojih dođe prilikom izrade nalaza i mišljenja.

Hrvatska

Obaveze i dužnosti sudskih vještaka prema Pravilniku o stalnim sudskim vještacima Hrvatske u procesu vještačenja prvenstveno propisuju obavezu stalnog sudskog vještaka da se pridržavaju rokova na izradi vještačenja koje mu je određeno od strane organa koji vodi postupak. Ukoliko stalni sudski vještak kojem je povjereno vještačenje ne može završiti u predviđenom roku dužan je o tome obavijestiti organ koji vodi postupak najkasnije u roku od osam dana izvjestiti sud. Također sudski vještak je dužan o istome podnjeti izvještaj o razlozima zbog kojih nije moguće da završi određeno vještačenje, kao i da da kratki prikaz rada na vještačenju koje je poduzeo do dana podnošenja izvještaja. U složenijim vještačenjima za koja je određen dužii rok za izradu nalaza i mišljenja vještak je dužan jednom mjesečno podnijeti sudu kratki izvještaj o rezultatima do tada obavljenih radnji. Stalni sudski vještak također je dužan čuvati kao tajnu sve ono što je saznao u obavljanju poslova stalnog sudskog vještaka.

Prava stalnih sudskih vještaka se prvenstveno ogledaju u smislu da oni imaju pravo na pripadajuću nagradu za svoj rad na poslovima vještačenja kao i pravo na naknadu eventualnih putnih troškova.

4. Nadzor nad radom vještaka, sankcionisanje i razrješenje vještaka

Srbija

Nadzor nad sudskim vještacima je uređen na način da je sud, odnosno organ koji vodi postupak dužan da nadzire rad vještaka te da je na sjednicama prvostepenih sudova uspostavljena obaveza da se najmanje jedanput godišnje razmatraju pitanja od značaja za rad vještaka. Na osnovu zaključaka sjednice predsjednik suda može utvrditi potrebu za podnođenjem prijedloga za razrješenje vještaka. Obrazloženi prijedlog za razrješenje vještaka zbog nestručnog, neurednog ili nesavjesnog vještačenja može podnijeti sud, organ koji vodi postupak, odnosno stranke ili drugi učesnici u sudskom ili drugom postupku. Tako je nadzor nad vještakom Zakonom o sudskim vještacima omogućen i drugim učesncima u postupku. Nadzor nad vještakom vrši i Ministarstvo pravde na način da vrši

pregled pristiglih prijedloga za razrješenje sudskih vještaka i o takvim prijedlozima donosi odluku. Zakon o sudskim vještacima je kao jedinu sankciju predvidio razrješenje. Zakon o krivičnom postupku Srbije na sličan način određuje sankcije kao i odgovarajući zakon Crne Gore. Tako je određeno da ako vještak koji je uredno pozvan ne dođe, a izostanak ne opravda, ili se bez odobrenja udalji sa mjesta gdje treba da bude ispitan, organ postupka može narediti da se prinudno dovede, a sud ga može i kazniti novčano do 100.000 dinara, a stručnu ustanovu do 300.000 dinara. Ako vještak, nakon upozorenja na posljedice uskraćivanja vještačenja, bez opravdanog razloga neće da vještači, ili ne da nalaz i mišljenje u roku koji mu je određen, sud ga može kazniti novčano do 150.000 dinara, a stručnu ustanovu do 500.000 dinara. Ministarstvo pravde Srbije će razriještiti vještaka ukoliko se ispune uslovi koji su propisani Zakonom o sudskim vještacima Srbije. Uslovi koji su propisani da bi se vještak razrješio su istovjetni uslovima koji su propisani i kao takvi ranije navedeni u Crnoj Gori.

Kako Zakon o sudskim vještacima Srbije ne prepoznaje formiranje Komisije koja vrši imenovanje vještaka, u postupku koji se vodi po prijedlogu za razrješenje vještaka Ministar pravde može formirati stručnu komisiju od tri člana iz reda vodećih stručnjaka u oblasti u kojoj vještak vještači, radi ocijene stručnosti rada vještaka, i može omogućiti vještaku da se izjasni o činjenicama i okolnostima na kojima se zasniva prijedlog za razrješenje.

Hrvatska

Nadzor nad radom stalnih sudskih vještaka dužni su provoditi prvenstveno predsjednici županijskih odnosno trgovačkih sudova tj. institucije koje su ih imenovale. Pored toga i predsjednici sudova i državni odvjetnici prate rad stalnih sudskih vještaka te su dužni o svojim zapažanjima obavještavati predsjednike nadležnih županijskih odnosno trgovačkih sudova. Posredni nadzor vrše i stranke odnosno njihovi punomoćnici te strukovne udruge na način da mogu podnijeti primjedbe na ponašanje stalnog sudskog vještaka. Primjedbe se podnose predsjedniku suda koji je imenovao vještaka.

ZKP Hrvatske također propisuje da će se odrediti sankcije u slučaju da vještak koji je uredno pozvan ne dođe, a izostanak ne opravda, ili ako odbije vještačiti. Vještak se može kazniti novčano do 20.000,00 kuna, a u slučaju neopravdanog izostanka može se i prisilno dovesti. I Pravilnik o stalnim sudskim vještacima propisuje određene sankcije u slučaju nesavjesnog i neprofesionalnog rada stalnih sudskih vještaka. Propisano je da će se stalnom sudskom vještaku koji ne poštuje sud ili stranke, ne preuzima dodijeljene mu predmete, ne opravda zašto u roku nije dovršio povjereno mu vještačenje, ili iz drugih ozbiljnih razloga privremeno uskratiti obavljanje poslova stalnog sudskog vještaka najmanje tri

mjeseca, a najduže godinu dana. Rješenje o privremenoj uskrati obavljanja poslova stalnog sudskog vještaka donosi predsjednik suda koji je imenovao stalnog sudskog vještaka.

Imenovanog stalnog sudskog vještaka razriješit će predsjednik odgovarajućeg županijskog odnosno trgovačkog suda, kada se ispune uslovi za to. Uslovi za razrješenje su kada to lice koje je imenovano za stalnog sudskog vjštaka samo zatraži, kada se dokaže da nema uslove za stalnog sudskog vještaka ili u međuvremenu prestanu uslovi na osnovu kojih je postavljen za vještaka. Također uslovi za razrješenje su i činjenica da je osuđen za krivična djela koja su kao takva zapreka i za obavljanje dužnosti u državnoj službi i ako neodgovorno i nesavjesno obavlja dužnosti stalnog sudskog vještaka.

Slovenija

Nadzor nad radom sudskih vještaka u Sloveniji vrše neposredno nadležni sud, odnosno predsjednik suda i ministar pravde Slovenije. Tako ukoliko dođe do kršenja nekih do dužnosti sudskih vještaka ministar pravde na prijedlog predsjednika suda ili na svoju inicjativu može pokenuti proceduru za razrješenje. Posredno nadzor nad radom vještaka vrše i stranke u postupku koje o eventualnim kršenjima vještaka mogu obavijestiti nadležnog predsjedinka suda ili ministarstvo pravde.

Zakon o krivičnom postupku Slovenije na sličan način uređuju sankcionisanje vještaka kao i drugim promatranim zemljama regije. Propisano je da u slučaju da vještak koji je uredno pozvan ne dođe, a izostanak ne opravda, ili ako odbije vještačiti može mu se izreći novčana kazna. Minimalna novčana kazna je u iznosu od jedne petine prosječne plate (u Sloveniji?) koja je zadnja objavljena u Sloveniji, dok je maksimalna kazna koja se može izreći tri prosječne neto plate u Sloveniji. Zakonom o sudovima je propisano da će se donijeti i privremena zabrana obavljanja dužnosti ukoliko je protiv vještaka pokrenut krivični postupak po službenoj dužnosti.

Postupak razrješenja vještaka pokreće ministar pravde samoinicijativno ili na prijedlog predsjednika suda. Ministar pravde, razrješava vještaka: 1. ako on sam traži razrješenje; 2. više ne ispunjava uslove propisane za obavljanje poslova vještaka; 3, ako ne izvršava svoje dužnosti u zadanim rokovima;
4. ako nesavjesno obavljaju svoje dužnosti; 5. ako dvaput neopravdano odbije zahtjev suda, da napravi izvještaj, mišljenje, vrednovanje, usmeno i pismeno prevođenje; 6. ako se bave aktivnostima na kojima dodatno zarađuju, što bi moglo utjecati na objektivnost i nezavisnost od vanjskih utjecaja za obavljanje ove funkcije.

Ono što je posebno specifično za pokrenuti postupak razrješavanja vještaka u Sloveniji, jeste činjenica da ukoliko je postupak razrješavanja pokrenut zbog namjernog nesavjesnog obavljanja svoje dužnosti, ministar pravde može uspostaviti komisiju koja će analizirati izrađene nalaza i mišljenja sudskog vještaka. Ovaj postupak je kao takav propisan u Zakonu o sudovima Slovenije. Komisija koju imenuje ministar se sastoji od stručnjaka iz oblasti struke vještaka protiv kojeg je pokrenut postupak razrješavanja. Intencija zakonodavca Slovenije je da samo stručnjaci iz iste oblasti imenovanog vještaka mogu procijeniti da li su nalaz i mišljenje namjerno nesavjesno izrađeni.

5. Uloga stručnih tijela/udruženja vještaka

Uloga stručnih tijela/udruženja je različito uređeno u promatranim zemljama. U određenim zemljama već samim zakonskim i podzakonskim aktima se daje vrlo značajna uloga ovakvim tijelima kako u samom procesu imenovanja vještaka, obuka vještaka ali i u postupcima nadzora nad radom sudskih vještaka. Dok, nasuprot tome, određene promatrane zemlje regije daju vrlo malu ulogu ili skoro nikakvu ulogu ovakvim stručnim tijelima.
Zemlja koje prepoznaju vrlo značajnu ulogu stručnih tijela/udruženja vještaka je Hrvatska, dok Srbija i Slovenija znatno manje vrjednuju ulogu takvih stručnih tijela.

Pravilnik o stalnim sudskim vještacima u Hrvatskoj propisuje također značajnu ulogu stručnih udruženja. Prvenstvena uloga se promatra u osmišljavanju i provođenju obuke lica kao neophodnog uslova za imenovanje određene osobe za stalnog sudskog vještaka i imenovanju mentora koji će takvu obuku sprovesti. Takav propis *de facto* označava da se bez odobrenja stručnog udruženja lice ne može imenovati za stalnog sudskog vještaka. Naime Pravilnikom o stalnim sudskim vještacima je propisano da se sposobnost kandidata za obavljanje poslova stalnog sudskog vještaka utvrđuje na temelju izvještaja o provedenoj stručnoj obuci kod stalnog sudskog vještaka odgovarajuće struke pod čijim je nadzorom. Nakon obavljene stručne obuke odgovarajuće stručno udruženje dužno je na temelju izvještaja stalnog sudskog vještaka kod kojeg je kandidat bio na stručnoj obuci (mentora) u roku od mjesec dana izraditi mišljenje u pisanom obliku o uspješnosti obavljene obuke i osposobljenosti kandidata za obavljanje poslova sudskog vještačenja i dostaviti ga predsjedniku odgovarajućeg županijskog odnosno trgovačkog suda.

Pored ove uloge Pravilnikom je navedena da stručna udruženja mogu i podnijeti i primjedbe na rad sudskih vještaka predsjedniku nadležnog suda, čime je

dodatno ojačana uloga stručnih udruženja u smislu nadzora nad radom stalnih sudskih vještaka.

Srbija prepoznaje stručna tijela/udruženja samo u tome da prilikom postupka imenovanja kandidat za sudskog vještaka može kao jednu od referencu navesti preporuku ili učešće na seminarima ili savjetovanjima u organizaciji stručnih udruženja. U Sloveniji se na isti način tretiraju stručna udruženja kao i u Srbiji, s tim da se u Sloveniji stručna udruženja spominju kao i mogući suorganizatori Centru za edukaciju nosilaca pravosudne funkcije u organizaciji pripremnih obuka za polaganje pismenog stručnog ispita za izbor za stalnog sudskog vještaka.

Zaključci i preporuke

Kako bi se unaprijedio zakonski i normativni okvir vještačenja u Bosni i Hercegovini, neophodno je da isti sadrži jasno definisane kriterije, utemeljene na najboljim međunarodnim standardima i preporukama. Uvođenje transparentnijih, profesionalnijih i meritokratskih principa u sistem imenovanja i nadzora nad radom vještaka ključan je korak ka jačanju povjerenja u pravosudni sistem. U tom kontekstu, preporučuje se sljedeće**:**

1. **Iniciranje izmjena relevantnih propisa o vještacima**, uz oslanjanje na dokazane međunarodne i regionalne prakse koje garantuju efikasnost, nezavisnost i odgovornost vještaka u sudskim postupcima;
2. **Institucionalizacija uloge stručnih udruženja**, naročito u procesima imenovanja, kontinuiranog stručnog usavršavanja i eventualnog sankcionisanja vještaka, čime bi se osigurao dodatni nivo stručne kontrole i profesionalne etike;
3. **Usklađivanje nadležnih tijela za imenovanje vještaka s međunarodnim propisima i preporukama**, čime bi se osigurala nepristrasnost i objektivnost u procesu izbora kandidata;
4. **Razmatranje mogućnosti uključivanja predstavnika relevantnih profesionalnih udruženja kao privremenih članova komisija za imenovanje vještaka**, naročito u Federaciji Bosne i Hercegovine, radi postizanja šireg stručnog konsenzusa i povećanja kredibiliteta izbora;
5. **Utvrđivanje seta jasnih i mjerljivih kvalifikacija za angažovanje vještaka**, koji bi obuhvatao kriterije poput stručnih sposobnosti, formalnog obrazovanja, akademskih zvanja (npr. magistar ili doktor nauka), pohađanih relevantnih obuka, praktičnog iskustva u odgovarajućoj oblasti, te prethodnog iskustva u svojstvu vještaka.

Literatura

I. KNJIGE I ČLANCI

1. European judicial systems Edition 2012 (2010 data): Efficiency and quality of justice, dostupno na: http://www.coe.int/T/dghl/cooperation/cepej/default_en.asp
2. European judicial systems Edition 2014 (2012 data): Efficiency and quality of justice, dostupno na: http://www.coe.int/T/dghl/cooperation/cepej/default_en.asp
3. Emir Muhić „Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa" (2024); Časopis Zaštita i Sigurnost.
4. Guidelines on the role of court-appointed experts in judicial proceedings of Council of Europe's Member States, dostupno na: http://www.coe.int/T/dghl/cooperation/cepej/default_en.asp
5. Inda Kreso „Metode infiltracije organizovanih kriminalnih grupa u legalne tokove novca kroz ulaganja u projekte obnovljivih izvora energije" (2024); Časopis Zaštita i Sigurnost.
6. Snežana Soković: „Veštačenje u krivičnom postupku: nova praksa u starim normativnim okvirima i drugi problemi", str. 29–54, Zbornik Instituta za kriminološka i sociološka istraživanja, 2008, XXVII (1-2)
7. Study on the role of experts in judicial systems of the Council of Europe Member States, dostupno na: https://...RoleExperts_en.pdf
8. USAID-ov Projekat pravosuđa u BiH (2017, decembar). Analiza sistema angažovanja vještaka u predmetima korupcije i organizovanog i privrednog kriminala.

II. PRAVNI PROPISI

9. Zakon o krivičnom postupku Bosne i Hercegovine, "Službeni glasnik BiH" br. 3/03 … 72/13
10. Zakon o krivičnom postupku Federacije BiH, "Službene novine FBiH" br. 35/03 … 9/09
11. Zakon o krivičnom postupku Republike Srpske, "Službeni glasnik RS" br. 50/03 … 92/09
12. Zakon o krivičnom postupku Brčko distrikta BiH, "Službeni glasnik BD BiH" br. 10/03 … 9/13
13. Zakon o vještacima, FBiH – "Službene novine FBiH" br. 49/05, 38/08
14. Zakon o vještacima, RS – "Službeni glasnik RS" br. 74/17

15. Pravilnik o obuci vještaka (FBiH) – "Službene novine FBiH" br. 48/07, 29/17
16. Pravilnik o uslovima za obavljanje poslova vještačenja BD – "Službeni glasnik BD BiH" br. 38/16
17. ZKP – čl. 269 (BiH i BD), čl. 284 (RS i FBiH)
18. Kazneni zakon [Penal Code], Hrvatski sabor, "Narodne novine" br. 125/2011 (izmjene NN 84/21, 36/2024)
19. Krivični zakonik Crne Gore, "Službeni list RCG" br. 70/2003 … i "Službeni list CG" br. 3/2020, posljednja verzija objavljena 19.12.2023. (Ministarstvo pravde CG)
20. Krivični zakonik, Ministarstvo pravde Republike Srbije, "Službeni glasnik RS" br. 85/2005 … 35/2019

21. Kazenski zakonik (KZ-1), Republika Slovenija, Ministrstvo za pravosodje, "Uradni list RS"

REGULATION OF THE EXPERT WITNESS SYSTEM IN CRIMINAL PROCEEDINGS IN INTERNATIONAL AND COMPARATIVE LAW AND PROPOSALS FOR IMPROVEMENT IN THE FEDERATION OF BOSNIA AND HERZEGOVINA

DOI: *10.70329/2744-2403.2025.5.9.8*

Expert article

Nermin Kadribašić, MA[32]

Abstract:

Expert witnesses represent one of the key evidentiary mechanisms in criminal proceedings in Bosnia and Herzegovina. The detection and prosecution of criminal offenses—particularly complex ones—generally require the involvement of expert witnesses from various fields. However, judicial practice in Bosnia and Herzegovina has revealed significant challenges in the appointment and use of expert witnesses in criminal cases. An analysis of international instruments and comparative legislation regulating the status and role of expert witnesses points to the necessity of a coherent and comprehensive normative framework to ensure proper mechanisms for the selection and application of expertise. This paper identifies several inconsistencies and gaps in the legal framework governing expert witnesses and offers a set of recommendations aimed at improving the normative system in the Federation of Bosnia and Herzegovina, primarily focusing on the Law on Expert Witnesses of the Federation of Bosnia and Herzegovina.

Keywords*: expert examination, expert witnesses, role and significance of expert witnessing, status of expert witnesses*

[32] Rule of Law Expert and PhD Candidate at the Faculty of Criminal Justice, Criminology and Security Studies

Introduction

Expert witnessing in criminal proceedings represents one of the most frequently used evidentiary actions, often having a decisive influence on the outcome of a trial. In practice, it is rare to conduct proceedings—regardless of the type of criminal offence—without the involvement of expert witnesses (USAID Justice Project in BiH, 2017). In Bosnia and Herzegovina, expert witnessing is regulated by a set of legal provisions, primarily laws on expert witnesses and criminal procedure laws. In Bosnia and Herzegovina, as well as in the wider Western Balkans region, various challenges still arise at different stages of the expert witnessing system (World Bank, 2019). The judicial system in Bosnia and Herzegovina, particularly the prosecutorial system, faces numerous difficulties in implementing and ensuring efficient and high-quality expert witnessing. This is of crucial importance in detecting and proving criminal offences, especially those related to economic crime and corruption. Multiple factors contribute to these difficulties, some of which are normative and institutional in nature. In this regard, a comparative overview of expert witnessing systems in neighbouring countries is presented. The purpose of this comparative analysis is to serve as a framework for considering possible improvements to the expert witnessing system in criminal proceedings, by reviewing relevant and effective practices in comparable legal systems, with particular focus on the normative framework in the Federation of Bosnia and Herzegovina. It is important to note that the need to amend the Law on Expert Witnesses of the Federation of BiH has been recognised for many years. The Government of the Federation of BiH adopted the Draft Law on Expert Witnesses in the Federation of BiH in November 2020[33]. Accordingly, alongside the currently applicable legal provisions, this paper also offers a reflection on the content of the adopted draft law.

1. Criteria and Factors for the Selection of Comparative Examples

For the comparative analysis of the normative and institutional framework of expert witnessing, the selected examples include Serbia, Croatia, Slovenia, and the Federation of Bosnia and Herzegovina. The criteria applied in the selection process are based on regional proximity, potential similarities and differences in obligations arising from the European Union accession process, and the similarity and comparability of legal traditions[34]. Slovenia has been a member of

[33] Draft legal solution available at https://www.javnarasprava.ba/fbih/Zakon/1604

[34] The countries of the region have signed the so-called Stabilization and Association Agreement (SAA), a new, third generation association agreement offered exclusively to the countries of the Western Balkans, as part of the Stabilization and Association Process, which is valid for

the European Union since May 1, 2004, and has long fulfilled the obligations related to the accession process. Croatia became a member on July 1, 2013, at which point the Stabilisation and Association Agreement ceased to apply. Montenegro and Serbia are candidate countries, while Bosnia and Herzegovina holds the status of a potential candidate for EU membership. Furthermore, during the initial research aimed at selecting appropriate comparative examples, it was observed that countries in the region have similar solutions regarding criminal procedural legislation related to expert witnesses and expert witnessing. This is logical, given that these countries were once part of the same jurisdiction and legal system. Nevertheless, specific legal provisions regulating the role of court experts contain certain differences, which may offer practical solutions for improving the system of using expert witnesses in Bosnia and Herzegovina. The factors analysed—broken down into several sub-factors—and which will be examined in detail among the selected countries of the region are presented in the attached table.

Table 1 Analysed factors and subfactors for improving system of using expert witnesses

Factors that were analyzed in the observed countries	**Sub-factors within each analyzed factor**
The role of expert testimony and permanent (court) experts in criminal proceedings	• Reasons for ordering an expert opinion • The right to order an expert opinion • Hiring private experts and professionals
Criteria for selecting a specific (permanent) court expert	• List of (permanent) court experts • Professional institution or state body
Selection and appointment of persons	• Requirements that a natural person must

countries that have not become members of the European Union since June 1, 2004. Of the countries under consideration, Slovenia was not part of the Stabilization and Association Agreement because it has been a member of the European Union for 17 years, or rather, it has become a member state.

for (permanent) court expert	possess to be appointed as an expert • Institutions responsible for appointing (permanent) court experts • Procedure for selecting (permanent) court experts
Duties and rights of a (permanent) court expert in the process of drawing up findings and opinions	• Duties of a (permanent) court expert in the process of drawing up findings and opinions • The rights of a (permanent) court expert in the process of drawing up findings and opinions
Supervision of the work of experts, sanctioning and dismissal of (permanent) court experts	• Supervision of the work of (permanent) court experts • Sanctioning of court experts • Procedure for dismissal of (permanent) court experts
The role of professional bodies/associations of (permanent) court experts	• Institutionalization of professional bodies/associations • Composition of professional bodies/associations
Final considerations	• Concluding considerations; • Recommendations;

1.1. Normative Framework for the Use of Expert Witnesses in Criminal Proceedings in Comparative Legal Systems

a) Criminal Procedure Laws in the Countries of the Region
In the observed jurisdictions, the legal basis for the use and determination of expert witnessing as an evidentiary action—and consequently, the status and role of expert witnesses in criminal proceedings—is primarily regulated, as in the Federation of Bosnia and Herzegovina, by the applicable criminal procedure laws. In Serbia, the Criminal Procedure Code (hereinafter CPC of Serbia) regulates the use of expert witnessing and the appointment of expert witnesses in Title VII, Section V, Articles 112–132.[35] In Croatia, the Criminal Procedure Code (hereinafter CPC of Croatia) addresses the determination and execution of expert witnessing as an evidentiary action in Title XVII, Section 8, Articles 308–328.[36] In Slovenia, the Criminal Procedure Code (CPC of Slovenia) regulates expert witnessing and the status and role of expert witnesses in criminal proceedings in Chapter XVIII, Section 7, Articles 248–267.[37]

b) Provisions on Court-Appointed Permanent Expert Witnesses
In the countries of the region, specific normative acts have been adopted to define the general conditions for the status of expert witnesses who operate not only in criminal proceedings, but also in other judicial, administrative, and misdemeanor procedures. However, in some of these countries, such provisions are not regulated through separate (lex specialis) laws on expert witnesses, as is the case in Bosnia and Herzegovina. For instance, in Croatia, the status of expert witnesses is governed by the Law on Courts.[38] Furthermore, the Ministry of Justice of Croatia adopted the Rulebook on Permanent Court Expert Witnesses[39], which more precisely defines issues relevant to expert witnesses. Similar normative solutions exist in Slovenia, where the general status of court experts is regulated by the Law on Regular Courts of Slovenia[40], while the Rulebook on Court Experts and Appraisers[41] regulates in detail the appointment, duties, rights, and responsibilities of court experts. In Serbia, the issues related

[35] Criminal Procedure Code of the Republic of Serbia "Official Gazette of the Republic of Serbia" No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014)
[36] Law on Criminal Procedure of the Republic of Croatia "Narodne novine HR" no. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14
[37]Criminal Procedure Code of Slovenia available at http://pisrs.si/Pis.web/pravniRedRSSearch?search=the+criminal+procedure+act
[38] Law on Courts "Narodne novine HR" no. 28/13, 33/15, 82/15
[39] Rulebook on permanent court experts "Narodne novine HR" no. 28/13
[40] Law on Regular Courts of Slovenia "Official Gazette of SLO" no. 10/77, 4/82, 37/82, 7/86, 41/87, 24/88, 8/90, 19/94 and 19/94
[41] Rules on court experts and appraisers "Official Gazette of SLO" no. 7/02, 75/03, 72/05, 71/07, 84/08 and 88/10)

to expert witnesses engaged in all court and other proceedings are, as in Bosnia and Herzegovina, regulated by a special (lex specialis) law. The status of expert witnesses in Serbia is governed by the Law on Court Expert Witnesses[42].

2. The Role of Expert Witnessing and Expert Witnesses in Criminal Proceedings

a) Reasons for Ordering Expert Witnessing

The need to appoint an expert in criminal proceedings arises in situations where the authority conducting the procedure lacks the specialized knowledge required to establish or assess certain relevant facts and to make a final decision. For this reason, expert witnessing is ordered, and a person with the necessary expertise is appointed to evaluate or determine such facts. This is particularly important in the case of complex criminal offences and areas such as crime in the renewable energy sector, which is a highly complex field as it involves an interdisciplinary domain that requires personnel with specialized education (Kreso, 2024).The above-mentioned reasons for appointing expert witnesses are equally addressed in the criminal procedure laws of the countries under comparison, and they primarily relate to providing "assistance" in establishing or evaluating facts that are not legal in nature, and which the competent authority does not possess the expertise to assess. Although the criminal procedure laws in the countries considered do not explicitly prohibit expert witnessing in matters concerning legal questions, it is generally understood that expert knowledge refers to non- legal fields—since legal matters fall under the competence of the authority conducting the proceedings. An exception is found in the CPC of Serbia, where Article 113, Paragraph 2 explicitly states that expert witnessing as an evidentiary action cannot be ordered for the purpose of evaluating or establishing a legal issue.

b) The Right to Order Expert Witnessing

In the observed countries, the authority conducting the proceedings orders expert witnessing and appoints expert witnesses either ex officio or upon the proposal of the parties. This means that the authority has discretionary power to decide whether expert witnessing is necessary in each specific case. The authority may accept a proposal from a party to conduct expert witnessing, including a proposal to appoint a specific individual or institution as the expert. This is particularly evident in the prosecution of organized criminal groups, which has always posed a significant challenge and issue for state agencies and law enforcement services (Muhić, 2024). However, it is important to note that such a proposal from a party or a defence counsel is not binding on the court or

[42] Law on Court Experts "Official Gazette of the Republic of Serbia", No. 44/10

the authority in charge of the proceedings. The authority may reject the proposal and choose not to issue an order for expert witnessing. These solutions are accepted throughout the region and closely resemble the provisions in the Federation of Bosnia and Herzegovina, where a written order for expert witnessing is issued by the prosecutor or the court.

In Serbia, the authority conducting the procedure issues a written order[43] for expert witnessing either ex officio or upon a party's or defence counsel's request. Similarly, in Croatia, expert witnessing is ordered by the competent body via a written order[44], and the same or similar provisions are found in Slovenia.

Some of the reasons why discretionary authority to order expert witnessing is granted to the competent body include the fact that expert witnessing can significantly affect the criminal procedure (World Bank, 2010). The preparation of expert reports and opinions requires time, which can impact the efficiency of proceedings, particularly in complex cases requiring extensive expert analysis. If such expert witnessing is ordered without sufficient grounds, it may hinder the principle of procedural efficiency. Moreover, expert witnessing entails financial costs, regardless of whether they are borne by the authority or one of the parties, which may influence the principle of procedural economy. For these reasons, both in the observed countries and in other continental European legal systems, the decision on whether to conduct expert witnessing is entrusted to the competent authority leading the procedure.

c) Engagement of Private Experts and Specialist Advisors

Although in the continental European legal tradition the exclusive discretionary right to order expert witnessing lies with the authority conducting the proceedings, the possibility of parties to a criminal case engaging their own expert or specialist advisor is often considered, along with the evidentiary value of such engagements and their reports or opinions. Expert witnessing, as an evidentiary action formally regulated in the criminal procedures of the observed regional countries, is not adversarial in the sense that each party would have "their own" expert to testify before the court or submit a written report. Such an arrangement is not acceptable because the expert must provide an objective opinion before the court[45]. In the continental European approach, an expert is

[43] Article 113 of the Serbian Criminal Code
[44] Article 309 of the Croatian Criminal Code
[45] Bayer V., Criminal Procedural Law - Selected Chapters, Book I, - Introduction to the Theory of Criminal Procedural Law (edited by D. Krapac) in Croatian Law Review Zorislav Kaleb "Private Expert Opinion Submitted by a Party to the Court in Criminal Proceedings

presumed to be objective and impartial, and provides assistance to the authority conducting the criminal proceedings. Nevertheless, it is common practice for parties—most often suspects or defendants and their legal counsel—to engage individuals who are experts or specialists in a given field to assist in preparing the defence, support their arguments, or produce their own "report" and "opinion" on a specific matter. This kind of support, along with the reports and opinions of such "private" experts, cannot be considered formal expert witnessing. These are usually referred to as defence expert assistance and do not carry the same evidentiary weight as official expert witnessing. Such individuals (the so-called "private experts") may be proposed by the parties to appear as witnesses during the main hearing. Courts often allow such persons with expert knowledge to express their opinion on the expert report previously conducted by the officially appointed expert. However, in Bosnia and Herzegovina and in most of the countries included in the comparative analysis, criminal procedure laws do not explicitly regulate the role and status of party-appointed advisors who could critically evaluate the findings, opinions, and testimony of court- appointed experts.

Among the observed countries, only Serbia's Criminal Procedure Code explicitly addresses the issue of specialist advisors in relation to expert witnessing ordered during proceedings[46]. The introduction of specialist advisors was a novelty in Serbia's CPC, which came into force in 2011. The law stipulates that, in addition to the right to propose expert witnessing and nominate experts, the parties also have the right to appoint a specialist advisor whenever expert witnessing is ordered[47]. This right exists regardless of whether the expert was appointed ex officio or based on the proposal of the opposing party. The public prosecutor, who conducts the proceedings before the indictment is filed, may appoint a specialist advisor only after the indictment has been filed, although it is unlikely that they would do so[48]. The specialist advisor must have the same qualifications as the expert but does not necessarily have to be selected from the list of permanent court experts. Specialist advisors paid from public funds (Article 125, Paragraph 3 of the CPC of Serbia) may only be appointed for the defendant and the injured party acting as a private prosecutor. The appointment of a specialist advisor is decided by the authority conducting the proceedings, i.e. the court. The specialist advisor is permitted to attend the expert witnessing, just as the defendant and defence counsel have the right to be

[46] This solution is specific to Italian criminal procedure legislation, where parties also have the right to hire a technical defense advisor.
[47] Article 125 of the Criminal Procedure Code
[48] Commentary on the criminal procedure code, 13th edition – 1032 pages (according to the new Criminal Procedure Code from 2011) authors: Prof. Dr. Momčilo Grubač and Prof. Dr. Tihomir Vasiljević, publisher PROJURIS, 2013.

present (Article 126, Paragraph 1 of the CPC of Serbia). The key distinction between an expert and a specialist advisor lies in the fact that the specialist advisor does not submit findings and opinions to the authority conducting the proceedings. Instead, the advisor highlights deficiencies in the report and opinion of the court-appointed expert. The advisor may be examined on the subject of the expert analysis and has the opportunity to present their own findings and opinion, but their statement does not carry the procedural weight of an official expert report. Nonetheless, it holds evidentiary value, and the judge may refer to it in the reasoning of the verdict. By law, the specialist advisor is prohibited from acting to the detriment of the proceedings, although this does not mean they are required to cooperate with the authorities.

2.1. Criteria for the Selection of Specific Expert Witnesses

The requirement that an expert possess specific professional knowledge is a necessary condition for any expert witnessing process[49], regardless of how it is regulated in legal provisions. This should be a key factor in selecting a particular expert. Criminal procedure laws in the region generally provide only a broad framework regarding the qualifications a person must have to be appointed as an expert witness. These laws stipulate that expert witnessing is to be ordered when the assessment or determination of an important fact requires the findings and opinion of a person with the necessary expert knowledge. Experts are thus defined as individuals who possess such expertise. The assessment of whether the appointed individual truly possesses the required qualifications and appropriate specialization is typically left to the authority conducting the criminal proceedings. This can be problematic, considering that these authorities often do not have the specific knowledge needed to assess the expert's competence accurately.

Nonetheless, such discretionary powers are somewhat limited by the criminal procedure laws of the observed countries, which usually require the existence of lists of permanent court experts or delegate the selection of experts to specialized institutions that appoint competent professionals for a given expert task.

a) List of Permanent Court Experts

The existence of a list of permanent court experts—generally binding for the court or the authority leading the proceedings—is the most widespread mechanism for controlling the professional credentials and expertise of expert

[49] Expertise in criminal proceedings: new practice within the old normative framework and another problem pp. 29-54 Snežana Čolaković.

witnesses in criminal procedures in the observed legal systems. The purpose of such lists is to confirm the competence of individuals authorized to conduct expert analyses in criminal and other types of proceedings. This requirement is set out in the criminal procedure laws. For instance, in Croatia, if the court has permanent experts for a specific type of expert witnessing, other experts who are not designated by the court may be appointed only if the permanent court experts are unavailable or if there are other justified reasons[50]. Slovenia has a similar provision, stipulating that courts may appoint only permanent court experts from the official list, except in cases of unavailability or other valid circumstances.

In Montenegro, the procedure stipulates that expert witnessing is ordered by a written decision of the competent authority, which must include: the task and scope of the expertise, the deadline for submitting a written report and opinion, and the designation of the expert listed in the Register of Court Experts or the Register of Legal Entities for Expert Witnessing[51]. Exceptionally, a person not listed in these registers may be appointed only if no registered experts are available for the required area of expertise. In addition to the CPC, Montenegro's Law on Court Experts requires the competent court to primarily appoint an expert residing within its jurisdiction and to ensure balanced distribution of assignments among experts in the same field[52]. This limits the repeated appointment of the same individuals when multiple experts from the same field are available[53].

In Serbia, the competent authority issues a written order to appoint an expert witness. The law specifies that if there are experts from the list of permanent experts available for a particular type of expert witnessing, other experts may only be appointed in cases of risk of delay, unavailability of the listed experts, or other justified reasons[54]. The Law on Court Experts of Serbia further requires the court or other competent authority to monitor the performance of appointed experts and, when possible, to appoint experts residing within its jurisdiction, ensuring balanced engagement of experts in the same professional area[55].

These legal provisions indicate that the legislator considers the list of permanent court experts to be a sufficient mechanism for verifying professional

[50] Article 309, Paragraph 4, CPC of Croatia
[51] Article 137, Paragraph 1, CPC of Montenegro
[52] Article 137, Paragraph 4, CPC of Montenegro
[53] Article 26, Law on Court Experts of Montenegro
[54] Article 114, CPC of Serbia
[55] Article 18, Law on Court Experts of Serbia.

competence, facilitating a quick and effective selection process by reducing the appointment procedure to selecting a suitable name from an existing list[56].

However, among the countries observed in this regional comparison, it is important to emphasize that only the criminal procedure laws of Bosnia and Herzegovina do not require the authority conducting the proceedings to appoint an expert from a list of permanent court experts. In fact, these laws do not even recognize the concept of a "permanent court expert." Consequently, the existing lists of permanent court experts in Bosnia and Herzegovina are not binding on judicial or investigative authorities when selecting an expert witness. The Law on Expert Witnesses of the Federation of Bosnia and Herzegovina explicitly states that the list of permanent court experts is not binding for courts, authorities, or other participants in the proceedings, unless otherwise specified by procedural rules[57]. Moreover, the law does not define how the authority conducting the proceedings should evaluate the qualifications and competence of the individual they intend to appoint as an expert in a given case.

b) Expert Institutions or State Authorities

The countries selected for this comparative analysis, as well as the Federation of Bosnia and Herzegovina, include provisions in their criminal procedure laws stating that, if a specialized institution exists for a certain type of expert analysis—or if such analysis can be carried out within a state authority—then, as a rule, that institution or authority should be entrusted with the task, especially in complex cases. The institution or authority then appoints one or more professionals with the relevant specialization to conduct the expert analysis[58]. This approach delegates the responsibility for selecting the appropriate expert(s)—those with sufficient expertise and specialization—to a professional institution that is specifically equipped to perform expert analyses.

It is a general standard that one or more natural persons may be appointed as expert witnesses in criminal proceedings, following the principle that expert witnessing constitutes an individual and personal contribution of a professional opinion by a specific expert. Accordingly, responsibility for the accuracy and integrity of the report and opinion lies with the individual expert (CEPEJ, 2012). In line with this principle, when the authority conducting the proceedings entrusts expert witnessing to a specialized institution or state authority, that institution is required to designate the individuals who will carry out the analysis

[56] Snježana Čolaković "Expertise as evidence in criminal proceedings" p.31.
[57] Article 11 of the Law on Expert Witnesses of the Republika Srpska and Article 14 of the Law on Expert Witnesses of the Federation of BiH
[58] Article 137, paragraph 2, of the CPC of Montenegro.

and to inform the authority of their identities. This procedure is recognized in the criminal procedure laws of all the countries under comparison. It is important that, if expert analysis is delegated to such a legal entity, that entity must then appoint one or more experts who will actually perform the task (CEPEJ, 2012).

2.2. Selection and Appointment of Permanent Court Experts

a) Conditions a Natural Person Must Meet to Be Appointed as an Expert Witness

The process of selecting and appointing expert witnesses in the observed countries of the region is regulated either by specific laws on expert witnesses— as is the case in Serbia and the Federation of Bosnia and Herzegovina—or more generally by laws on the judiciary, with further specification provided through rulebooks on court experts and appraisers, as in Slovenia and Croatia. All the reviewed countries prescribe conditions that natural and legal persons must fulfill to be appointed as permanent court experts. However, the level of detail and stringency of these conditions varies: in some countries the criteria are more general and less demanding, while in others they are more specific and significantly stricter.

For example, in Serbia, a person wishing to be appointed as an expert must have completed a relevant higher education program at the second cycle level (Master's, specialist academic or vocational studies), or a relevant undergraduate degree, in the specific area of expertise[59]. The current Law on Court Experts in Serbia further requires that the candidate have at least five years of professional experience and possess both theoretical knowledge and practical experience in the relevant field. Exceptionally, a person with a secondary school diploma may be appointed as an expert if there are not enough experts in a given area.

In addition to professional qualifications, the Serbian law requires that a person be "worthy" of performing expert witness duties, thus introducing an element of integrity as a condition for appointment.

Slovenia's Rulebook on Court Experts and Appraisers prescribes similar conditions to those found in Serbian legislation, but without specifying the

[59] Article 6 of the Law on Court Experts of Montenegro and Article 6 of the Law on Court Experts of Serbia.

required educational level. It does, however, require a minimum of six years of professional experience in the relevant field[60].

In Croatia, the conditions for appointment are more detailed and demanding than in other regional systems. The Law on Courts generally provides that a court expert must hold a completed relevant professional, undergraduate, or graduate university degree. Exceptionally, a person with only secondary education may be appointed if there is no higher education program in the relevant field[61]. The Rulebook on Permanent Court Experts in Croatia defines the conditions in greater detail. It requires that the candidate be a citizen of the Republic of Croatia, a citizen of an EU member state, or a citizen of a country that is a signatory to the European Economic Area Agreement. It also introduces a requirement not found in other systems—that the candidate be medically fit to perform the duties of a permanent court expert. Regarding educational and professional background, the Rulebook states the following requirements:

1. After completing the relevant educational program, the candidate must have worked in the field for:

a) At least 8 years if they completed a graduate university or specialist graduate professional study program;
b) At least 10 years if they completed a relevant undergraduate university or professional study program;
c) At least 12 years if they completed a relevant secondary school, and no appropriate higher education programs exist for that specific field.

The Rulebook also mandates that a candidate must have a professional liability insurance policy for performing court expert duties. Regarding integrity, it specifies that a person cannot be appointed as a court expert if they are ineligible for employment in public service.

In addition to academic, professional, and other general conditions, Croatia stands out by requiring successful completion of a professional training program as a condition for appointment. This is a unique requirement among the observed systems. Serbia and Slovenia do not explicitly require training prior to appointment or during expert witness service. In the Federation of Bosnia and

[60] Article 5 of the Rulebook on court experts and appraisers.
[61] Article 126 Paragraph 2 of the Law on Courts of Croatia

Herzegovina, the Law on Expert Witnesses does not require training as a precondition for being placed on the expert list, but it does stipulate that, after appointment, the expert must complete training in accordance with a rulebook issued by the competent entity-level Ministry of Justice.

b) Competent Institutions for the Appointment of Court Experts, Their Composition and Appointment Process

Serbia
According to the Law on Court Experts, the appointment procedure for permanent court experts in Serbia is carried out exclusively by the Ministry of Justice. The current legislation does not recognise the existence of a specialised expert commission appointed by the ministry.

Slovenia
The Ministry of Justice of Slovenia is responsible for conducting the procedure of appointing permanent court experts. The Ministry may also, if it considers it necessary, require a special professional examination, which is conducted by a Commission appointed for that purpose by the Minister of Justice. The Commission consists of a president, at least two members, and a recording secretary. The president of the Commission is selected from one of the ministries within the Government of Slovenia and must have completed at least a second cycle law degree. The two other members of the Commission are appointed from among professionals and must have at least the same level of qualification as the candidate for court expert. The recording secretary is an employee of the Ministry of Justice.

Croatia
The competent institution for the appointment of permanent court experts in Croatia is the County or Commercial Court. The presidents of these courts are the authorities to whom individuals who believe they meet the necessary qualifications submit their applications for appointment. If the court president assesses that the candidate meets the prescribed conditions, the candidate is referred to professional training organised by the relevant association of court experts. This association appoints a mentor who is a member of the Association of Permanent Court Experts.

Federation of Bosnia and Herzegovina
The Law on Expert Witnesses of the Federation of Bosnia and Herzegovina obliges the Federal Minister of Justice to publish a public call for the

appointment of expert witnesses and to appoint a Commission composed of permanent members. These include the President of the Supreme Court of FBiH or a judge authorised by them, the President of the Bar Association of the Federation or a lawyer appointed by them, the Chief Federal Prosecutor or a prosecutor authorised by them, a representative of the Federal Ministry of Justice, and three temporary members. These temporary members are appointed by majority vote of the permanent members from among leading experts in the fields in which expert witnessing is conducted.

c) Procedure for the Selection of Permanent Court Experts

Serbia

The Minister of Justice publishes a public call for the appointment of court experts in the Official Gazette of the Republic of Serbia and on the website of the Ministry of Justice, when it is determined that there is an insufficient number of experts in a specific field. The candidate submits an application to the ministry along with the necessary documents proving that they meet the legal requirements. The decision on appointment is made by the Minister of Justice. If the application is rejected, the candidate has the right to initiate an administrative dispute. The appointment decision includes the expert's surname, parent's name, first name, residence and address, title, field of expertise, and area of specialisation. The decision is published in the Official Gazette and on the ministry's website. The Law on Court Experts in Serbia does not require the adoption of additional by-laws governing the appointment procedure, nor the establishment of special bodies to evaluate the expertise of candidates. The Ministry maintains a Register of Experts, available online and in electronic form. It also keeps an individual file for each expert, containing documentation used for registration, as well as any complaints, fines, or proposals for dismissal.

Slovenia

The Ministry of Justice of Slovenia publishes a call for applications for the appointment of court experts, appraisers, and interpreters twice a year. The call is based on identified needs in specific areas of expertise, according to the justified opinions of court presidents. To verify qualifications, the ministry may request an opinion on the candidate from a public institution, professional organisation, or other relevant body. If the ministry determines that the candidate must take a professional exam, it appoints a commission to organise it. The exam consists of general legal knowledge (the same for all candidates) and specific questions related to each area of expertise. The exam must be announced at least 30 days before the scheduled date. The content is prepared by the Judicial Training Centre, which is also responsible for preparatory seminars and training. Experts are appointed on the day they take an oath before the

Minister of Justice. The Ministry maintains a register of appointed experts, which is shared with competent courts and other relevant institutions.

Croatia

The competent institutions for appointing permanent court experts in Croatia are the County and Commercial Courts. Individuals submit applications to the president of the competent court. If the president determines that the applicant meets the necessary conditions, the candidate is referred to professional training at the Croatian Association of Court Experts and Appraisers (CACEA), which appoints a mentor from among its experienced members. The training programme is defined by the relevant professional association for each field. According to the Rulebook, the mentor must be a court expert with at least five years of experience[62]. However, the Rulebook on the training process introduces stricter criteria. Article 12 states that the mentor must be an CACEA member with a higher education degree, passed a professional exam in the same field as the candidate (if required by law), at least ten years of experience in expert work, and a scientific or academic title equal to or higher than that of the candidate. The mentor organises and implements the training, which includes both theoretical and practical elements. Theoretical training covers relevant legal, professional, and scientific knowledge, literature, and ethical standards. The practical part includes field data collection, drafting sketches and calculations, and participating in court hearings. Training lasts between 6 and 12 months. After completion, the mentor submits a report to CACEA, which within 30 days forwards the report and a recommendation for appointment to the court. CACEA is responsible for informing courts about training programmes and annual training schedules. Oversight of training is conducted by the Ministry of Justice and the competent courts, based on a schedule set by the Minister. A written report is produced after inspections. Before being appointed, the candidate must submit proof of liability insurance. Once training is complete and all conditions are met, the court president makes a final decision. Experts are appointed for a period of four years. The County and Commercial Courts maintain lists of appointed experts.

Federation of Bosnia and Herzegovina

Experts are appointed through a public call issued by the entity Minister of Justice. The minister appoints a commission that evaluates the candidates' expertise, impartiality, and integrity. The Law on Expert Witnesses in FBiH requires the Minister of Justice to establish a commission composed of permanent members: the President of the Supreme Court of FBiH (or a delegated judge), the President of the Bar Association (or a delegated lawyer),

[62] Article 6 of the Rulebook on Permanent Court Experts of Croatia

the Chief Federal Prosecutor (or a delegated prosecutor), and a representative of the Ministry of Justice. Additionally, three temporary members are appointed by majority vote from among leading experts in the fields in which expert witnessing is performed.

3. Duties and Rights of Permanent Court Experts During the Preparation of Expert Reports and Opinions

Serbia

The Criminal Procedure Code of Serbia stipulates that an expert is obliged to respond to the court's summons and to deliver a written report and opinion within the deadline specified in the court order. This deadline may be extended, upon the expert's request, for justified reasons. The expert is required to carefully examine the subject of the analysis, to accurately report all findings and observations, and to express their opinion impartially and in accordance with scientific principles or professional standards. The expert must also respond to additional questions and clarify any issues raised by the authority conducting the proceedings. All findings and opinions must be documented in the official record. This record, or the written expert report and opinion, must include the name of the person who performed the analysis, their profession, level of education, and area of specialisation. According to the Law on Court Experts of Serbia, experts are obliged to comply with the deadlines set by the court decision assigning the analysis. If the expert cannot complete the task within the deadline for objective reasons, they must notify the court no later than eight days before the deadline expires and provide a brief overview of the actions completed up to that point. Upon receiving this notification, the court will either set a new deadline or assign another expert. For more complex cases with longer deadlines, the expert must submit a short progress report every thirty days. Failure to comply with these provisions is considered improper conduct. The law also clearly states that experts must maintain confidentiality regarding any information obtained during their work.

Rights of Experts in Serbia

The Criminal Procedure Code of Serbia provides that during the preparation of their report and opinion, the expert has the right to request clarification of the order and to examine case files. They may also request that additional evidence or opinions be collected if necessary for their work. The expert has access to all relevant documents and materials required for their analysis. The law also

recognises the role of the specialist advisor in relation to expert analysis. The duties and rights of these advisors are also defined. A specialist advisor must promptly submit their authorisation to the court, provide the party with professional and timely assistance, refrain from abusing their rights, and avoid unnecessary delays in the procedure. Advisors have the right to be informed of the date, time, and location of the expert analysis, to be present at the analysis, review the files and materials, suggest actions to the expert, raise objections to the report and opinion, and ask questions during the main hearing. Before testifying, the advisor must take an oath. According to the Law on Court Experts, experts must carry out their tasks conscientiously, professionally, and impartially. They are also obligated to protect any confidential information obtained during the expert procedure. The law further specifies that experts are entitled to appropriate compensation for their work.

Slovenia

The Criminal Procedure Code of Slovenia regulates the duties and obligations of court experts in a similar manner as the criminal procedure laws of Serbia and Montenegro. The Rulebook on Court Experts and Appraisers requires experts to perform their duties lawfully and responsibly, in line with professional and scientific standards. Experts must adhere to the deadlines set by the court or other competent authority. These deadlines generally cannot be shorter than thirty or longer than sixty days. If the expert is unable to complete the work within the specified time, they must notify the authority no later than fifteen days before the deadline expires. The rulebook also requires experts to handle all entrusted materials and evidence with care and to respect the provisions of data protection laws when processing personal information obtained during the preparation of their report and opinion.

Croatia

The obligations of court experts in Croatia, as defined by the Rulebook on Permanent Court Experts, primarily relate to adhering to deadlines set by the competent authority. If an expert cannot complete the analysis on time, they are required to notify the court at least eight days before the deadline and to submit a report explaining the reasons and summarising the work done up to that point. In complex cases where longer deadlines are allowed, the expert must submit a brief progress report to the court every month. Experts are also obliged to maintain confidentiality regarding all information acquired during the performance of their duties. The rights of permanent court experts mainly include the right to be fairly compensated for their work, as well as the right to reimbursement for any travel expenses incurred during the course of their duties.

4. Supervision, Sanctioning, and Dismissal of Court Experts

Serbia

Supervision over the work of court experts is defined so that the court or the authority conducting the proceedings is obligated to monitor the expert's work. At least once a year, first-instance courts are required to review matters related to the work of court experts. Based on the conclusions of such sessions, the president of the court may determine the need to submit a proposal for dismissal. A reasoned proposal for dismissal, based on unprofessional, negligent, or irresponsible performance, may be submitted by the court, the authority leading the proceedings, parties, or other participants in judicial or administrative proceedings. This means that oversight of experts is also open to other actors in the process. The Ministry of Justice supervises experts by reviewing submitted proposals for dismissal and issuing decisions on them. The Law on Court Experts in Serbia prescribes dismissal as the only formal sanction. The Criminal Procedure Code also includes financial sanctions: if an expert who was duly summoned fails to appear without justification, or leaves the examination location without permission, the authority may order forced appearance and impose a fine of up to 100,000 dinars, or up to 300,000 dinars for an expert institution. If the expert refuses to conduct the analysis or fails to deliver a report within the deadline, a fine of up to 150,000 dinars may be imposed, or up to 500,000 dinars for institutions. The Ministry of Justice will dismiss an expert if the legal conditions set by the Law on Court Experts are met. These conditions are similar to those prescribed in Montenegro. Since the Serbian law does not foresee a permanent commission for expert appointments, in dismissal proceedings the Minister of Justice may establish an ad hoc commission of three experts from the relevant field to assess the expert's competence. The expert also has the right to respond to the facts and circumstances on which the dismissal proposal is based.

Croatia

Supervision of permanent court experts is primarily conducted by the presidents of the County or Commercial Courts that appointed them. In addition, court presidents and state attorneys monitor their work and are obliged to report their findings to the competent court presidents. Indirect oversight is exercised by parties, their legal representatives, and professional associations through the submission of complaints regarding the expert's conduct. Complaints are submitted to the court that appointed the expert. The Criminal Procedure Code provides for sanctions if the expert fails to appear without justification or refuses to testify. The expert may be fined up to 20,000 kuna and may be brought in by force if absent without justification. The Rulebook on Permanent Court Experts also provides sanctions for unprofessional or negligent conduct, including

temporary suspension from duties for a period ranging from three months to one year. The suspension is decided by the court that appointed the expert. Permanent experts may be dismissed by the president of the appointing court if any of the following conditions are met: at the expert's own request, if the expert no longer meets the legal requirements, if those conditions have ceased to exist, if the expert is convicted of criminal offences that disqualify them from public service, or if the expert performs duties irresponsibly.

Slovenia

In Slovenia, supervision is carried out by the competent court, the court president, and the Minister of Justice. If an expert violates their professional obligations, the Minister may initiate dismissal proceedings either at the court's proposal or ex officio. Parties in the proceedings may also inform the court or the ministry about potential violations. The Criminal Procedure Code allows for financial sanctions if the expert fails to appear, refuses to testify, or delays the submission of a report. The minimum fine is one-fifth of the average monthly salary in Slovenia, while the maximum is three times the average net salary. The Law on the Courts also provides for temporary suspension from duties if criminal proceedings are initiated against the expert. The dismissal procedure may be initiated by the Minister of Justice, either independently or at the proposal of a court president. Grounds for dismissal include the expert's own request, loss of required qualifications, repeated failure to meet deadlines, negligent conduct, repeated refusal to prepare reports or attend proceedings, or conflicts of interest affecting objectivity. What is specific to Slovenia is that in cases of alleged intentional misconduct, the Minister may establish a commission to assess the expert's past reports and opinions. This commission must consist of professionals from the same field of expertise, as only peers are considered capable of assessing whether the expert's work was deliberately negligent. This procedure is regulated by the Law on the Courts.

5. The Role of Professional Bodies/Associations of Court Experts

The role of professional bodies and associations of court experts is regulated differently across the countries under observation. In some legal systems, national laws and by-laws assign these organisations a significant role not only in the appointment process but also in the training of experts and in monitoring their work. In contrast, other countries in the region assign little to no formal role to such professional bodies.

Among the countries observed, Croatia gives the most prominent role to professional associations of court experts, while Serbia and Slovenia assign them only a marginal function.

In Croatia, the Rulebook on Permanent Court Experts clearly defines a substantial role for professional associations. Their primary responsibility lies in designing and implementing training programmes, which are mandatory for an individual to be appointed as a permanent court expert. Additionally, these associations are responsible for appointing mentors who supervise and guide candidates during their training. This effectively means that without the approval and assessment of the professional association, an individual cannot be appointed as a permanent court expert. According to the Rulebook, the suitability of a candidate for expert duties is established based on the report prepared after the completed training under the supervision of an experienced court expert from the relevant field. After the training, the association must, within one month, issue a written opinion on the quality and outcome of the training and the candidate's preparedness. This opinion is then submitted to the president of the relevant County or Commercial Court for final decision-making. Furthermore, the Rulebook states that professional associations may also submit formal complaints about the work of court experts to the president of the competent court. This provision strengthens the supervisory role of such associations in the functioning and accountability of court experts.

In Serbia, professional associations are acknowledged only in a limited sense. During the appointment process, a candidate may cite their participation in seminars or training events organised by such associations as part of their professional references. However, there is no formal or institutional role for professional associations in the appointment, training, or oversight of court experts.

In Slovenia, the role of professional associations is similarly limited. They may participate as co-organisers of preparatory training for the written examination required for the appointment of court experts, in collaboration with the Judicial Training Centre. However, their role remains supportive and optional, rather than formally integrated into the institutional framework of appointment and supervision.

In summary, while Croatia embeds professional bodies into the core procedures of expert training, certification, and oversight, Serbia and Slovenia view them more as auxiliary actors whose involvement is largely informal and consultative.

Conclusions and Recommendations

In order to improve the legal and normative framework for expert witnessing in Bosnia and Herzegovina, it is essential that the system includes clearly defined criteria based on the best international standards and recommendations. Introducing more transparent, professional, and merit-based principles in the appointment and oversight of expert witnesses is a key step toward strengthening trust in the judiciary. In this context, the following recommendations are proposed:

1. Initiate amendments to relevant legislation on expert witnesses, drawing on proven international and regional practices that ensure the efficiency, independence, and accountability of experts in judicial proceedings.
2. Institutionalise the role of professional associations, particularly in the processes of appointment, continuous professional development, and, where necessary, sanctioning of expert witnesses, thereby ensuring an additional level of professional oversight and ethical standards.
3. Align the competent bodies responsible for the appointment of experts with international legal frameworks and recommendations, in order to guarantee impartiality and objectivity in the selection process.
4. Consider the inclusion of representatives of relevant professional associations as temporary members of appointment commissions, particularly in the Federation of Bosnia and Herzegovina, to encourage broader professional consensus and increase the credibility of the selection process.
5. Establish a set of clear and measurable qualifications for the engagement of expert witnesses, including criteria such as professional competence, formal education, academic titles (e.g. Master's or Doctoral degrees), relevant completed training programmes, practical experience in the field of expertise, and previous experience as a court expert.

References

I. BOOKS AND ARTICLES

1. *European Judicial Systems Edition 2012 (2010 data): Efficiency and Quality of Justice,* available at: http://www.coe.int/T/dghl/cooperation/cepej/default_en.asp
2. *European Judicial Systems Edition 2014 (2012 data): Efficiency and Quality of Justice,* available at: http://www.coe.int/T/dghl/cooperation/cepej/default_en.asp
3. Emir Muhić, "Operational Use of OSINT in the Investigation of Organized Criminal Groups" (2024); Journal of Protection and Security.
4. *Guidelines on the Role of Court-Appointed Experts in Judicial Proceedings of Council of Europe's Member States*, available at: http://www.coe.int/T/dghl/cooperation/cepej/default_en.asp
5. Inda Kreso, "Methods of Infiltration by Organized Criminal Groups into Legal Financial Flows through Investments in Renewable Energy Projects" (2024); Journal of Protection and Security.
6. Snežana Soković, "Expert Witnessing in Criminal Proceedings: New Practices in Old Normative Frameworks and Other Issues," *Journal of the Institute for Criminological and Sociological Research*, 2008, XXVII (1–2), pp. 29–54
7. *Study on the Role of Experts in Judicial Systems of the Council of Europe Member States*, available at: https://...RoleExperts_en.pdf
8. USAID Justice Project in Bosnia and Herzegovina (December 2017), *Analysis of the System of Engaging Experts in Cases of Corruption, Organized and Economic Crime*

II. LEGAL DOCUMENTS

7. Criminal Procedure Code of Bosnia and Herzegovina, "Official Gazette of BiH" nos. 3/03 … 72/13
8. Criminal Procedure Code of the Federation of BiH, "Official Gazette of FBiH" nos. 35/03 … 9/09
9. Criminal Procedure Code of Republika Srpska, "Official Gazette of RS" nos. 50/03 … 92/09
10. Criminal Procedure Code of Brčko District of BiH, "Official Gazette of BD BiH" nos. 10/03 … 9/13
11. Law on Expert Witnesses (Federation of BiH), "Official Gazette of FBiH" nos. 49/05, 38/08
12. Law on Expert Witnesses (Republika Srpska), "Official Gazette of RS" no. 74/17
13. Rulebook on Expert Training (FBiH), "Official Gazette of FBiH" nos. 48/07, 29/17
14. Rulebook on Conditions for Expert Work (Brčko District), "Official Gazette of BD BiH" no. 38/16
15. CPC – Art. 269 (BiH and BD), Art. 284 (RS and FBiH)
16. Criminal Code, Croatian Parliament, "Narodne novine" no. 125/2011 (amended NN 84/21, 36/2024)
17. Criminal Code of Montenegro, "Official Gazette of the Republic of Montenegro" no. 70/2003 … and "Official Gazette of Montenegro" no. 3/2020, latest version published 19 December 2023 (Ministry of Justice of Montenegro)
18. Criminal Code, Ministry of Justice of the Republic of Serbia, "Official Gazette of RS" nos. 85/2005 … 35/2019
19. Criminal Code (KZ-1), Republic of Slovenia, Ministry of Justice, "Official Gazette of RS"

ZAKONSKA REGULATIVA DIGITALNE IMOVINE – PRIMJER ZAKONA O DIGITALNOJ IMOVINI REPUBLIKE SRBIJE

DOI: *10.70329/2744-2403.2025.5.9.9*

Pregledni naučni rad

Čuljević Ilda, MA iur., Općina Ilidža
Gurda Ena, MA iur., Advokatska kancelarija Amra Gurda

Sažetak:

Predmet ovog istraživanja je zakonska regulativa digitalne imovine – primjer Zakona o digitalnoj imovini Republike Srbije. [1]. Republika Srbija je jedna od prvih država koja je usvojila zakon o digitalnoj imovini i samim tim se izvukla iz "sive zone", za razliku od mnogih drugih država, među kojima je i Bosna i Hercegovina. Ona je kao savremena država opredjeljena za integraciju u savremene međunarodne tokove.[2] Međutim, specifičnost uređenja države Bosne i Hercegovine je direktno implicirala donošenje i provođenje zakona u različitim pravnim oblastima.[3]

[1] Koju čine virtuelne valute (vrsta digitalne imovine koju nije izdala i za čiju vrednost ne garantuje centralna banka, niti drugi organ javne vlasti, koja nije nužno vezana za zakonsko sredstvo plaćanja i nema pravni status novca ili valute, ali je fizička ili pravna lica prihvataju kao sredstvo razmene i može se kupovati, prodavati, razmenjivati, prenositi i čuvati elektronski) i digitalni tokeni (vrsta digitalne imovine i označava bilo koje nematerijalno imovinsko pravo koje u digitalnoj formi predstavlja jedno ili više drugih imovinskih prava, što može uključivati i pravo korisnika digitalnog tokena da mu budu pružene određene usluge).

[2] Petrović Ž. (2022). Ujedinjeni narodi i NATO u ratnoj i postratnoj Bosni i Hercegovini - stručni rad. U Časopisu: Zaštita i sigurnost za 2022. godinu, Godina 2, br. 2, str. 103. Dostupno na: https://zisjournal.com/wp-content/uploads/2024/06/Godina_2.Broj_1.pdf. Datum pristupa: 01.07.2025. godine.

[3] Delić H. (2021). Uloga sistema sigurnosti Bosne i Hercegovine u migrantskoj krizi, u svijetlu kompleksnog uređenja države Bosne i Hercegovine - stručni članak. U Časopisu: Zaštita i sigurnost za 2021. godinu, Godina 1, br. 1, str. 53. Dostupno na: https://zisjournal.com/wp-content/uploads/2024/06/Godina_1.Broj_1.pdf. Datum pristupa: 01.07.2025. godine

Zakon je stupio na snagu 2021. godine i sadrži 146 članova podijeljenih u IX glava. Zakonska definicija digitalne imovine podrazumijeva digitalni zapis vrijednosti koji se može digitalno kupovati, prodavati, razmjenjivati ili prenositi, i koji se može koristiti kao sredstvo razmjene ili u svrhu ulaganja, pri čemu digitalna imovina ne uključuje digitalne zapise valuta koje su zakonsko sredstvo plaćanja i drugu finansijsku imovinu koja je uređena drugim zakonima[4]*. U pravnom smislu, digitalna imovina se smatra novim institutom, pa samim tim i posebnom imovinom i jednom od najvećih izazova savremenog imovinskog prava, pa su gotovo neograničeni potencijali primjene digitalnih sredstava u budućnosti, te ekonomičnost i efikasnost glavni su razlozi povećanog interesa zakonodavaca širom svijeta i brojnih međunarodnih finansijskih organizacija za ovu vrstu imovine (Mirković, 2023, 20). Zakon poznaje dvije vrste digitalne imovine i to : virtuelne valute i digitalne tokene. Najznačajnija virtuelna valuta je bitcoin.*

Rad se sastoji od dva dijela. U prvom dijelu rada se obrađuje pojam digitalne imovine kao pravnog istituta, kao i najznačanija EU uredba o tržištima kriptoimovine koja je usvojena 2023. godine. U drugom dijelu rada se obrađuje zakonska regulativa digitalne imovine u Republici Srbiji, kao centralna tema ovog rada, sa osvrtom na status digitalne imovine u Bosni i Hercegovini.

***Ključne riječi**: zakonska regulativa, digitalna imovina*

[4] Zakon o digitalnoj imovini. "Sl. glasnik RS", broj : 153/2020.

1. POJAM DIGITALNE IMOVINE KAO PRAVNOG INSTITUTA

Digitalna imovina je novi pravni institut, koji je u rječnike prava ušao zahvaljujući razvoju interneta i digitalne komunikacije (Čolaković, 2023, 166). Smatra se posebnom imovinom i jednom od najvećih izazova savremenog imovinskog prava, pa su gotovo neograničeni potencijali primjene digitalnih sredstava u budućnosti, te ekonomičnost i efikasnost glavni su razlozi povećanog interesa zakonodavaca širom svijeta i brojnih međunarodnih finansijskih organizacija za ovu vrstu imovine (Mirković, 2023, 20). Na osnovu toga se stvara novi imovinskopravni institut, digitalna svojina, a pitanje njegove standardizacije postavlja se kao pitanje neophodnosti zakonske regulative, kako na nacionalnom tako i na međunarodnom nivou (Mirković, 2023, 20).

Međutim, u pogledu definiranja digitalnog sadržaja, postoji niz različitih definicija prema legislativi Europske unije, pa tako Direktiva 2019/770 o određenim aspektima ugovora o isporuci digitalnog sadržaja i digitalnih usluga[5] i Direktiva 2011/83/EU o pravima potrošača[6] određuju pojam digitalnog sadržaja kao podatke koji su proizvedeni i isporučeni u digitalnom obliku navodeći kao primjere: računalne programe, aplikacije, igre, glazbe, videozapise ili tekstove bez obzira na to pristupa li im se preuzimanjem ili strujanjem, s opipljivog medija ili na bilo koji drugi način[7]. Digitalni sadržaj definiran je i u Direktivi (EU) 2015/2366 o platnim uslugama[8] kao roba ili usluge koje se proizvode i isporučuju u digitalnom obliku te čija je uporaba ili potrošnja ograničena na tehnički uređaj koji ni na koji način ne uključuje upotrebu ili potrošnju fizičkih dobara ili usluga.

[5] Direktiva (EU) 2019/770 Europskog parlamenta i Vijeća od 20. maja 2019. godine o određenim aspektima ugovora o isporuci digitalnog sadržaja i digitalnih usluga, SL L 136, pristupljeno 08.01.2025. godine

[6] Direktiva 2011/83/EU Europskog parlamenta i Vijeća od 25. oktobra 2011. godine o pravima potrošača, izmjeni Direktive Vijeća 93/13/ EEZ i Direktive 1999/44/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive Vijeća 85/577/EEZ i Direktive 97/7/EZ Europskog parlamenta i Vijeća, Tekst značajan za EGP, Sl. L. 304, 22.11.2011. posebno izdanje za Hrvatsku, Chapter 15 Volume 008 P. 260–284.

[7] Preambula 19, čl. 2. tačka. 11. Direktive 2011/83 o pravima potrošača.

[8] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/ EZ (Tekst značajan za EGP) SL L 337, 23.12.2015, p. 35–127.

1.1. UREDBA (EU) 2023/1114 EUROPSKOG PARLAMENTA I VIJEĆA OD 31. MAJA 2023. GODINE O TRŽIŠTIMA KRIPTOIMOVINE I IZMJENI UREDABA (EU) BR. 1093/2010 I (EU) BR. 1095/2010 TE DIREKTIVA 2013/36/EU I (EU) 2019/1937

Europsko Vijeće[9] je Uredbu (EU) 2023/1114 formalno odobrilo 16.05.2023. godine, te se Uredbom o tržištima kriptoimovine (MiCA) prvi put kriptoimovina, izdavatelji kriptoimovine i pružatelji usluga povezanih s kriptoimovinom stavljaju pod jedan usklađeni zakonodavni okvir. Na prvom mjestu se treba definirati kriptoimovina. Kriptoimovina je digitalni prikaz vrijednosti ili prava, a može se prenositi ili pohranjivati elektroničkim putem, s pomoću tehnologije distribuiranog zapisa (DLT)[10] ili slične tehnologije. Kriptoimovina je jedna od glavnih primjena DLT-a u financijama. Uredbom su obuhvaćene tri vrste kriptoimovine : **tokeni vezani uz imovinu** (održavaju stabilnu vrijednost vezivanjem uz nekoliko valuta koje su zakonsko sredstvo plaćanja („fiducijarne valute"), pojedinačnu robu ili više vrsta robe, pojedinačnu kriptoimovinu ili skup kriptoimovine ili košaricu takve imovine, te se koriste se kao sredstvo plaćanja za kupnju robe i usluga te kao sredstvo čuvanja vrijednosti, **tokeni e-novca** (održavaju stabilnu vrijednost vezivanjem uz vrijednosti samo jedne fiducijarne valute i elektronička su zamjena za kovanice i novčanice, te služe prije svega kao sredstvo plaćanja), te **druga kriptoimovina kao što su korisnički tokeni.** Bitno je napomenuti da se kriptoimovina upotrebljava: kao sredstvo plaćanja/razmjene, za potrebe ulaganja, za pristup robi ili uslugama, za kombinaciju naprijed navedenih znački. Novim pravilima uvode se zahtjevi za izdavatelje kriptoimovine i pružatelje usluga povezanih s kriptoimovinom kad je posrijedi : nadzor i odobravanje transakcije, transparentnost i otkrivanje utjecaja kriptoimovine na okoliš.

Nadalje je bitno istaći da je pružateljima usluga povezanih s kriptoimovinom potrebno odobrenje za rad u EU-u, te moraju ispunjavati stroge zahtjeve za zaštitu lisnica potrošača i odgovarat će ako izgube kriptoimovinu ulagatelja, a Europsko nadzorno tijelo za bankarstvo (EBA) vodit će javni registar pružatelja usluga povezanih s kriptoimovinom koji ne ispunjavaju obaveze[11]. Svakako će kriptoimovina koja je već uređena zakonodavstvom EU-a i dalje će podlijegati postojećim pravilima[12].

---

[9] Preuzeto sa : https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32023R1114 dana 08.01.2025. godine.

[10] Vrsta tehnologije koja omogućava decentralizirano pohranjivanje, ažuriranje i validaciju šifriranih podataka.

[11] Preuzeto sa : https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32023R1114 dana 08.01.2025. godine.

[12] Ibid.

U pogledu koristi pravila EU-a o kriptoimovini[13], ističu se : pravna sigurnost za kriptoimovinu koja nije obuhvaćena postojećim zakonodavstvom EU-a, bolja zaštita potrošača i ulagača, zaštitne mjere protiv finansijskog kriminala i manipuliranja tržištem, inovacije i pošteno tržišno natjecanje, finansijska stabilnost i smanjenje visokog ugljičnog otiska kriptoimovine.

Na koncu je bitno naglasiti da se pravilima EU-a o tržištima kriptoimovine bolje štite prije svega potrošači i ulagači, te se reguliraju rizici od financijskog kriminala, a sa druge strane se potiču inovacije.

2. ZAKONSKA REGULATIVA DIGITALNE IMOVINE U REPUBLICI SRBIJI

Zakon o digitalnoj imovini u Republici Srbiji je usvojen od strane Narodne skupštine Republike Srbije, na snagu je stupio dana 21.12.2020. godine, a počeo je da se primjenjuje dana 29.06.2021. godine[14]. Početak primjene Zakona o digitalnoj imovini se vezuje za uobičajeni period od 6 mjeseci od usvajanja Zakona (koja odredba je sastavni dio svakog Zakona u prijelaznim i završnim odredbama[15]), a koji period ima za cilj da omogući dovoljno vremena za stvaranje uslova za njegovu primjenu (npr. donošenje podzakonskih akata), kao i mogućnost da se svi zainteresovani učesnici na tržištu digitalne imovine upoznaju sa odredbama Zakona (npr. uspostavljanje pravne izvjesnosti, kao i oporezivanje ove vrste imovine). Republika Srbija je jedna od prvih država koja je podržala donošenje naprijed navedenog Zakona, te je samim tim odskočila iz "sive zone" i dokazala da ide u korak sa suvremenim svijetom, za razliku od Bosne i Hercegovine i mnogih drugih država.

Zakon o digitalnoj imovini u Republici Srbiji koji je u konačnici i stupio na snagu sadrži 146 članova koji su inkorporirani u IX glava, dok je nacrt pomenutog Zakona sadržavao samo 70 članova. Nakon usmene rasprave je dodano čak više duplo više članova, međutim naprijed navedeno nije ni iznenađujuće s obzirom da se radi o reguliranju ere digitalizacije koja iz dana u dan napreduje na svjetskom planu.

Donošenje Zakona o digitalnoj imovini u Republici Srbiji je ujedno prouzrokovalo i izmjene i dopune glavnih poreskih zakona u Republici Srbiji, koji

[13] Ibid.
[14] "Sl. glasnik RS", broj : 153/2020.
[15] Čl. 146.

uvode kao oporezivu kategoriju digitalnu imovinu[16], što je svakako bio uzročno-posljednični korak.

U ovom radu ćemo se baviti najznačajnijim odredbama pomenutog Zakona i ukratko ih izložiti uz analizu.

U širem smislu zakonodavac je donošenjem naprijed navedenog Zakona dozvolio posjedovanje i trgovanje digitalnom imovinom[17]. Zakonska definicija digitalne imovine podrazumijeva digitalni zapis vrijednosti koji se može digitalno kupovati, prodavati, razmjenjivati ili prenositi, i koji se može koristiti kao sredstvo razmjene ili u svrhu ulaganja, pri čemu digitalna imovina ne ukjljučuje digitalne zapise valuta koje su zakonsko sredstvo plaćanja i drugu finansijsku imovinu koja je uređena drugim zakonima[18].

Zakonom[19] su regulirane dvije vrste digitalne imovine i to : virtuelne valute i digitalni tokeni, a podjela je značajna s obzirom na primjenjivanje različitog pravnog režima. V*irtuelna valuta* je vrsta digitalne imovine koju nije izdala i za čiju vrijednost ne garantuje centralna banka, niti drugi organ javne vlasti, koja nije nužno vezana za zakonsko sredstvo plaćanja i nema pravni status novca ili valute, ali je fizička ili pravna lica prihvataju kao sredstvo razmjene i može se kupovati, prodavati, razmenjivati, prenositi i čuvati elektronski; a *digitalni token* je vrsta digitalne imovine i označava bilo koje nematerijalno imovinsko pravo koje u digitalnoj formi predstavlja jedno ili više drugih imovinskih prava,

---

[16] Npr. Zakon o porezu na dodatu vrijednost. ("Sl. glasnik RS", br. 84/2004, 86/2004 - ispr., 61/2005, 61/2007, 93/2012, 108/2013, 6/2014 - usklađeni din. izn., 68/2014 - dr. zakon, 142/2014, 5/2015 - usklađeni din. izn., 83/2015, 5/2016 - usklađeni din. izn., 108/2016, 7/2017 - usklađeni din. izn., 113/2017, 13/2018 - usklađeni din. izn., 30/2018, 4/2019 - usklađeni din. izn., 72/2019, 8/2020 - usklađeni din. izn., 153/2020, 138/2022 i 94/2024) i Zakon o porezu na dohodak građana. ("Sl. glasnik RS", br. 24/2001, 80/2002, 80/2002 - dr. zakon, 135/2004, 62/2006, 65/2006 - ispr., 31/2009, 44/2009, 18/2010, 50/2011, 91/2011 - odluka US, 7/2012 - usklađeni din. izn., 93/2012, 114/2012 - odluka US, 8/2013 - usklađeni din. izn., 47/2013, 48/2013 - ispr., 108/2013, 6/2014 - usklađeni din. izn., 57/2014, 68/2014 - dr. zakon, 5/2015 - usklađeni din. izn., 112/2015, 5/2016 - usklađeni din. izn., 7/2017 - usklađeni din. izn., 113/2017, 7/2018 - usklađeni din. izn., 95/2018, 4/2019 - usklađeni din. izn., 86/2019, 5/2020 - usklađeni din. izn., 153/2020, 156/2020 - usklađeni din. izn., 6/2021 - usklađeni din. izn., 44/2021, 118/2021, 132/2021 - usklađeni din. izn., 10/2022 - usklađeni din. izn., 138/2022, 144/2022 - usklađeni din. izn., 6/2023 - usklađeni din. izn., 92/2023, 116/2023 - usklađeni din. izn., 6/2024 - usklađeni din. izn. i 94/2024).

[17] Koju čine virtuelne valute (vrsta digitalne imovine koju nije izdala i za čiju vrednost ne garantuje centralna banka, niti drugi organ javne vlasti, koja nije nužno vezana za zakonsko sredstvo plaćanja i nema pravni status novca ili valute, ali je fizička ili pravna lica prihvataju kao sredstvo razmene i može se kupovati, prodavati, razmenjivati, prenositi i čuvati elektronski) i digitalni tokeni (vrsta digitalne imovine i označava bilo koje nematerijalno imovinsko pravo koje u digitalnoj formi predstavlja jedno ili više drugih imovinskih prava, što može uključivati i pravo korisnika digitalnog tokena da mu budu pružene određene usluge).

[18] Zakon o digitalnoj imovini. "Sl. glasnik RS", broj : 153/2020.

[19] Ibid.

što može uključivati i pravo korisnika digitalnog tokena da mu budu pružene određene usluge[20].

Članom 3. su regulisane usluge koje su povezane sa digitalnom imovinom i obuhvataju :

1. prijem, prenos i izvršenje naloga koji se odnose na kupovinu i prodaju digitalne imovine za račun trećih lica;
2. usluge kupovine i prodaje digitalne imovine za gotov novac i/ili sredstva na računu i/ili elektronski novac;
3. usluge zamjene digitalne imovine za drugu digitalnu imovinu;
4. čuvanje i administriranje digitalne imovine za račun korisnika digitalne imovine i sa tim povezane usluge;
5. usluge u vezi sa izdavanjem, ponudom i prodajom digitalne imovine, sa obavezom njenog otkupa (pokroviteljstvo) ili bez te obaveze (agentura);
6. vođenje registra založnog prava na digitalnoj imovini;
7. usluge prihvatanja/prenosa digitalne imovine;
8. upravljanje portfoliom digitalne imovine;
9. organizovanje platforme za trgovanje digitalnom imovinom.

Nadalje je propisana i djelatnost koja se tiče davanja savjetodavnih usluga[21] povezanih s digitalnom imovinom (investiciono savjetovanje, davanje investicionih preporuka, savjetovanje u vezi sa strukturom kapitala, poslovnom strategijom, izdavanje digitalne imovine, kao i druge savjetodavne usluge povezane s digitalnom imovinom). Bitno je naglasiti da pružalac savjetodavnih usluga nije dužan da za pružanje tih usluga pribavi dozvolu nadzornog organa, već samo o tome obavijesti korisnika njegove usluge[22].

Zakonodavac je nadalje u članu 6. predvidio rudarenje kriptovaluta, a isto se definira kao sticanje digitalne imovine učestvovanjem u pružanju usluge računarskog potvrđivanja transakcija u informacionim sistemima koji se odnose na određenu digitalnu imovinu, te je bitno istaći da se na ove sticaoce digitalne imovine ne primijenjuju zakonske odredbe, ali za slučaj da se isti odluče da sa tako stečenom digitalnom imovinom trguju putem davaoca usluga povezanih sa digitalnom imovinom, onda se i na njih jednako primjenjuju zakonske odredbe,

[20] Član 2.
[21] Član 5.
[22] Pa se može pojaviti kao fizičko ili pravno lice.

te je nesporno da mogu trgovati po OTC pravilima[23], kao i sva druga lica (iz čega proizilazi da je OTC trgovanje dozvoljeno Zakonom).

Zakonodavac je predvidio osnovna načela u članu 8. i 9. i to : načelo neutralnosti, efikasnosti, ekonomičnosti i digitalizacije postupka.

Prema načelu neutralnosti, odredbe zakona se ravnopravno odnose na svu digitalnu imovinu bez obzira na tehnologiju na kojoj je ta digitalna imovina zasnovana, uključujući stabilnu digitalnu imovinu. Prema načelima efikasnosti, ekonomičnosti i digitalizacije postupka, svako lice (pravno i fizičko) koje pokreće upravni postupak (zahtjev za odobrenje objavljivanja bijelog papira, zahtjev za izdavanje dozvole za pružanje usluga povezanih s digitalnom imovinom) podnosi odgovarajući zahtjev putem posebnog web portala kojim upravlja služba Vlade Republike Srbije koja je nadležna za projektovanje, usklađivanje, razvoj i funkcionisanje sistema elektronske uprave, i uz taj zahtjev dostavlja cjelokupnu dokumentaciju utvrđenu zakonom i propisima donijetim na osnovu zakona kojom dokazuje ispunjenost uslova za usvajanje tog zahtjeva, čime se gasi birokracija i ulazi se u eru digitalizacije svijeta.

Nadalje je zakonodavac isključivo naglasio da bilo koja vrsta digitalne imovine nije zvanično sredstvo plaćanja[24], te da finansijske institucije (banke, osiguravajuće kuće), pod nadzorom Narodne banke, ne mogu posjedovati digitalnu imovinu[25]. Međutim, kada je riječ o poslovanju pravnih lica i preduzetnika u vezi s digitalnom imovinom, zakonodavac predviđa da nenovčani ulozi u privredno društvo mogu biti u digitalnim tokenima koji se ne odnose na pružanje usluga i rada; prihvatanje digitalne imovine u zamjenu za prodatu robu i/ili pružene usluge u trgovini na malo, preko pružaoca usluga povezanih s digitalnom imovinom – ali on onda mijenja digitalnu imovinu u zvanično sredstvo plaćanja i takvo isplaćuje klijentu; dozvoljena je uspostava založnog prava na digitalnoj imovini, koje se stiče upisom u registar založnog prava koji vodi pružalac usluga[26]; dozvoljena je i fiducija[27]

Kada je riječ o prinudnom izvršenju na digitalnoj imovini, zakonodavac je to također predvidio, pa kada izvršenik u sudskom izvršnom postupku posjeduje digitalnu imovinu, povjerilac se može naplatiti iz vrijednosti iste.

[23] "Over the counter" trgovanje (neposredno trgovanje između dva lica).
[24] Član 12.
[25] Član 13.
[26] Dužnik može založiti svoju digitalnu imovinu kao sredstvo obezbjeđenja.
[27] Kojom dužnik prenese pravo svojine na digitalnoj imovini na povjerioca kao obezbjeđenje neke obaveze, a ovaj se obavezuje da mu je vrati ako obaveza bude ispunjena.

Međutim, postavlja se pitanje provođenja naprijed navedenog u praksi, a što će svakako vrijeme pokazati.

Budući da je zakonom reguliran postupak kreiranja i izdavanja digitalne imovine u Republici Srbiji, prije svega se sačinjava Bijeli papir (White paper) koji se šalje nadležnom organu na odobrenje[28], te se nakon toga pristupa inicijalnim ponudama digitalne imovine[29].

Kada je riječ o sekundarnom trgovanju digitalnom imovinom, isto je zakonodavac predvidio, pa čak i onom izdatom izvan Republike, za koju nije izdat bijeli papir u skladu sa Zakonom, ako se radi o digitalnoj imovini kojom se u značajnoj mjeri trguje na globalnom tržištu preko licenciranih, odnosno registrovanih platformi u skladu s propisima Evropske unije[30].

Članom 37. je propisano trgovanje i upotreba pametnih ugovora. Szabo (1996, 18) navodi da je pametni ugovor digitalni transakcijski protokol koji izvršava odredbe ugovora, a ciljevi dizajna pametnog ugovora su zadovoljavanje uobičajenih zahtjeva u ugovorima (načine plaćanja, anonimnost) i minimiziranje potrebe za povjerljivom trećom osobom[31].

Posljednično naprijed navedenom, zakonodavac je radi zaštite obavezao pružaoca usluga da se priklone propisima o sprječavanju pranja novca i finansiranja terorizma, te su izvršene izmjene i dopune naprijed navedenog Zakona u pogledu definiranja i uvrštavanja digitalne imovine u isti[32].

2.1. STATUS DIGITALNE IMOVINE U BOSNI I HERCEGOVINI

Kada je riječ o zakonskoj regulativi digitalne imovine u Bosni i Hercegovini, ista još uvijek nije implementirala u bosansko-hercegovačko zakonodavstvo. Međutim, na tragu naprijed navedenog, u Republici Srpskoj su u 2022. godini

[28] Član 19.

[29] Postupak je kompatibilan američkom sistemu ICO (Initial Coin Offering) u kojem izdavač digitalne imovine nudi istu za tačno utvrđenu cijenu, prije nego što ista bude puštena na javno tržište.

[30] Član 31.

[31] Koristi pametne ugovore za izvršavanje kompleksnih načina plaćanja uz malu naknadu i jednostavnu izvedbu.

[32] „Sl. glasnik RS“, broj : 113/17, 91/19, 153/20, 92/23 i 94/24.

usvojene izmjene i dopune Zakona o tržištu hartija od vrijednosti[33] u članu 2. poslije alineje 24. dodaju se nove alineje 25, 26. i 27. koje glase :

- **'**Virtuelna valuta' je digitalni zapis vrijednosti koji nije emitovala i za čiju vrijednost ne garantuje centralna banka, niti drugi organ javnog sektora, koja nije nužno vezana za zakonsko sredstvo plaćanja i nema pravni status novca ili valute, ali je fizička i pravna lica prihvataju kao sredstvo razmjene i može se kupovati, prodavati, razmjenjivati, prenositi i čuvati elektronskim putem.
- 'Pružalac usluga povezanih sa virtuelnim valutama' je pravno ili fizičko lice koje pruža jednu ili više slijedećih usluga : čuvanje i upravljanje virtuelnih valuta u ime trećih lica (pružalac depozitarnih usluga novčanika), organizovanje platforme za trgovanje virtuelnim valutama, razmjena virtuelnih valuta za valutu koja je zakonsko sredstvo plaćanja, razmjena virtuelnih valuta za drugu virtuelnu valutu, prenos virtuelne valute, tj. zaprimanje i izvršavanje naloga za virtuelnu valutu u ime trećih strana, sprovođenje ponude, odnosno prodaje virtuelnih valuta.
- 'Pružalac depozitarnih usluga novčanika' je pravno ili fizičko lice koje pruža uslugu čuvanja privatnih kriptografskih ključeva u ime drugog lica radi držanja, čuvanja i prenosa virtuelnih valuta."

Iz naprijed navedenog proizilazi da iako u našem bosansko-hercegovačkom pravu ne postoji zakonsko uporište za digitalnu imovinu kako je prethodno i navedeno, Republika Srpska je napravila korak naprijed i u pomenuti zakon involvirala odredbe o digitalnoj imovini, iz čega se može zaključiti da će u budućnosti raditi na donošenju pozitivnog propisa u pogledu digitalne imovine, a zakonska rješenja će vjerovatno biti slična, ako ne i ista kao u susjednoj Republici Srbiji.

Što se tiče Federacije Bosne i Hercegovine, u istoj ne postoji još uvijek interes ni za izmjene i dopune Zakona o tržištu hartija od vrijednosti, kao u Republici Srpskoj, iz čega proizilazi da se Federacija Bosne i Hercegovine nalazi u dubokoj „sivoj zoni", s obzirom da za naprijed navedenim izmjenama i dopunama kasni za Republikom Srpskom duže od dvije godine, pa se postavlja pitanje da li će i kada doći na red razmatranje donošenja Zakona o digitalnoj imovini?

U svemu naprijed izloženom, jedino je pozitivno što je na nivou države Bosne i Hercegovine usvojen Zakon o sprječavanju pranja novca i finansiranja

[33] „Službeni glasnik Republike Srpske", br. 92/06, 34/09, 30/12, 59/13, 108/13, 4/17, 63/21 i 11/22).

terorističkih aktivnosti 2024. godine[34], u kojem je definirana virtuelna valuta[35] kao digitalni zapis vrijednosti koji nije emitovala i za čiju vrijednost ne garantuje centralna banka, niti drugi organ javnog sektora, koja nije nužno vezana za zakonsko sredstvo plaćanja i nema pravni status novca ili valute, ali je fizička i pravna lica prihvataju kao sredstvo razmjene i može se prenositi, čuvati, kupovati, prodavati, razmjenjivati elektronskim putem. Naprijed navedeno je svakako preduslov za donošenje Zakona o digitalnoj imovini u nekoj skorijoj ili daljoj budućnosti.

Međutim, ono što je trenutno sporno jeste da je u Bosni i Hercegovini, tačnije enitetu Republike Srpske registrirano nekoliko privrednih društava koje pružaju usluge koje su povezane sa digitalnom imovinom, a nadležna Komisija za hartije od vrijednosti RS izdaje dozvole subjektima koji ispune uvjete za obavljanje poslova u vezi sa virtuelnim valutama. Dakle, na polju digitalne imovine sve su veća interesovanja subjekata, a nadležni organi očito nemaju problema što ne postoji zakonski okvir za uređenje naprijed pomenute materije, što dodatno stvara konfuziju i pravnu nesigurnost, te sve veću mogućnost za malverzacije.

ZAKLJUČAK

Digitalizacija svijeta je u punom jeku, te je pitanje reguliranja digitalne imovine prepoznao znatno mali krug zemalja, među kojima je i Republika Srbija. Republika Srbija još 2021. godine usvaja zakon koji stupa na snagu šest mjeseci poslije i koji se počinje primjenjivati, dok Bosna i Hercegovina na početku 2025. godine još uvijek nema ni naznaku kada bi Zakon o digitalnoj imovini mogao doći na red za predlaganje od strane nadležnih tijela. Upravo iz naprijed navedenog se može zaključiti da je Bosna i Hercegovina i dalje u „sivoj zoni“ za razliku od Republike Srbije. Zakonodavac u Republici Srbiji detaljno regulira područje digitalne imovine, a što se kroz najznačajnije odredbe Zakona i obradilo kroz ovaj rad.

Što se tiče Bosne i Hercegovine, dolazi do neznatnih izmjena i to u jednom entitetu, Republici Srpskoj, u Zakonu o tržištu hartija od vrijednosti, u kojem zakonodavac definira pojam digitalne imovine, što je svakako jedan korak naprijed, dok Federacija Bosne i Hercegovine čak ni to nije učinila. Postavlja se pitanje pravne nesigurnosti neregulisanog područja, budući da u Bosni i Hercegovini postoji nekoliko registriranih pravnih lica koje pružaju usluge koje su povezane sa digitalnom imovinom, a nadležna Komisija za hartije od

[34] „Sl. glasnik BiH“, broj : 13/2024.
[35] Član 4.

vrijednosti RS izdaje dozvole subjektima koji ispune uvjete za obavljanje poslova u vezi sa virtuelnim valutama.

Zaključak je da Republika Srbija treba da prati Europske standarde i shodno tome, vrši izmjene i dopune, ukoliko bude potrebe za istim, dok Bosna i Hercegovina treba podhitno poduzeti korake koji vode do zakonske regulacije digitalne imovine, što će svakako doprinijeti efikasnosti i ekonomičnosti, kao i pravnoj sigurnosti svih zainteresiranih lica koji žele pružati usluge koje su povezane sa digitalnom imovinom.

LITERATURA

1. Čolaković, M. (2023). Nasljeđivanje digitalne imovine : ima li digitalnog života nakon smrti? *U Zborniku radova „Aktualnosti Građanskog i Trgovačkog Zakonodavstva i Pravne Prakse“, br. 20, 162-181.*
2. Direktiva 2011/83/EU Europskog parlamenta i Vijeća od 25. oktobra 2011. godine o pravima potrošača, izmjeni Direktive Vijeća 93/13/ EEZ i Direktive 1999/44/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive Vijeća 85/577/EEZ i Direktive 97/7/EZ Europskog parlamenta i Vijeća, Tekst značajan za EGP, Sl. L. 304, 22.11.2011. posebno izdanje za Hrvatsku, Chapter 15 Volume 008 P. 260–284.
3. Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/ EZ (Tekst značajan za EGP) SL L 337, 23.12.2015, p. 35–127.
4. Direktiva (EU) 2019/770 Europskog parlamenta i Vijeća od 20. maja 2019. godine o određenim aspektima ugovora o isporuci digitalnog sadržaja i digitalnih usluga, SL L 136, pristupljeno 08.01.2025. godine.
5. Mirković, P. (2023). Digitalna imovina – legislativni pristup regulisanju novog imovinskopravnog instituta. *U Pravo – teorija i praksa, vol. 40, 17-31.*
6. Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16), 18(2).*
7. Kritpoimovina : Kako EU regulira tržište. *Vijeće Europske unije*. Preuzeto sa : https://www.consilium.europa.eu/hr/policies/crypto-assets-how-the-eu-is-regulating-markets/ dana 08.01.2025. godine.
8. Zakon o digitalnoj imovini. (Sl. glasnik RS, broj : 153/2020).
9. Zakon o porezu na dodatu vrijednost. ("Sl. glasnik RS", br. 84/2004, 86/2004 - ispr., 61/2005, 61/2007, 93/2012, 108/2013, 6/2014 - usklađeni din. izn., 68/2014 - dr. zakon, 142/2014, 5/2015 - usklađeni din. izn., 83/2015, 5/2016 - usklađeni din. izn., 108/2016, 7/2017 - usklađeni din. izn., 113/2017, 13/2018 - usklađeni din. izn., 30/2018, 4/2019 - usklađeni din. izn., 72/2019, 8/2020 - usklađeni din. izn., 153/2020, 138/2022 i 94/2024).
10. Zakon o porezu na dohodak građana. ("Sl. glasnik RS", br. 24/2001, 80/2002, 80/2002 - dr. zakon, 135/2004, 62/2006, 65/2006 - ispr., 31/2009, 44/2009, 18/2010, 50/2011, 91/2011 - odluka US, 7/2012 - usklađeni din. izn., 93/2012, 114/2012 - odluka US, 8/2013 - usklađeni

din. izn., 47/2013, 48/2013 - ispr., 108/2013, 6/2014 - usklađeni din. izn., 57/2014, 68/2014 - dr. zakon, 5/2015 - usklađeni din. izn., 112/2015, 5/2016 - usklađeni din. izn., 7/2017 - usklađeni din. izn., 113/2017, 7/2018 - usklađeni din. izn., 95/2018, 4/2019 - usklađeni din. izn., 86/2019, 5/2020 - usklađeni din. izn., 153/2020, 156/2020 - usklađeni din. izn., 6/2021 - usklađeni din. izn., 44/2021, 118/2021, 132/2021 - usklađeni din. izn., 10/2022 - usklađeni din. izn., 138/2022, 144/2022 - usklađeni din. izn., 6/2023 - usklađeni din. izn., 92/2023, 116/2023 - usklađeni din. izn., 6/2024 - usklađeni din. izn. i 94/2024).

11. Zakon o sprječavanju pranja novca i finansiranja terorističkih aktivnosti. „Sl. glasnik BiH“, broj : 13/2024.
12. Zakon o sprječavanju pranja novca i finansiranja terorizma. „Sl. glasnik RS“, broj : 113/17, 91/19, 153/20, 92/23 i 94/24.
13. Zakon o tržištu hartija od vrijednosti. „Službeni glasnik Republike Srpske“, br. 92/06, 34/09, 30/12, 59/13, 108/13, 4/17, 63/21 i 11/22).
14. Petrović Ž. “Ujedinjeni narodi i NATO u ratnoj i postratnoj Bosni i Hercegovini” (2022). Časopis: Zaštita i sigurnost, str. 103. Dostupno na: https://zisjournal.com/wp-content/uploads/2024/06/Godina_2.Broj_1.pdf.
15. Delić H. “Uloga sistema sigurnosti Bosne i Hercegovine u migrantskoj krizi, u svijetlu kompleksnog uređenja države Bosne i Hercegovine” (2021). Časopis: Zaštita i sigurnost str. 53.

LEGAL REGULATION OF DIGITAL PROPERTY – EXAMPLE OF THE DIGITAL PROPERTY LAW OF THE REPUBLIC OF SERBIA

DOI: *10.70329/2744-2403.2025.5.9.9*

Scientific review article

Čuljević Ilda, MA iur ., Municipality Ilidza
Gurda Ena, MA iur ., Law office of Amra Gurda

Abstract:

Subject this one research is legal regulation digital property – example Digital Law property Republics Republic [36]of Serbia Serbia is one of the first country which adopted digital law property and by themselves the team got away with it from the " gray zone", unlike many others other country , among which is also Bosnia and Herzegovina. As a modern state, it is committed to integration into contemporary international trends.[37] However, the specificity of the organization of the state of Bosnia and Herzegovina directly implied the adoption and enforcement of laws in different legal areas.[38]

[36] Which consists of virtual currency (type digital property which not issued and for whose value does not guarantee central bank , nor another body of public authority, which not necessarily related to law means payments and no legal status of money or currency , but it is physical or legal faces accept as means exchanges and can be bought , sold , exchanged , transferred and to keep electronic) and digital tokens (type digital property and indicates either which intangible property right which in digital form represents one or more other property rights , what can include and right user digital tokens to be his provided certain services) .

[37] Petrović Ž. (2022). The United Nations and NATO in war and post-war Bosnia and Herzegovina - expert work. In the Journal: Protection and Security for 2022, Year 2, no. 2, p. 103.
Available at: https://zisjournal.com/wp-content/uploads/2024/06/Godina_2.Broj_1.pdf. Date of access: 01.07.2025. year.

[38] Delić H. (2021). The role of the security system of Bosnia and Herzegovina in the migrant crisis, in the light of the complex organization of the state of Bosnia and Herzegovina - professional article. In the Journal: Protection and Security for 2021, Year 1, no. 1, p. 53.

The law has entered on strength in 2021 and contains 146 members divided into IX chapters. Legal definition digital property implies digital record value that can be digitally buy , sell , exchange or to be transmitted , and which can be use as means exchanges or for the purpose of investments , at why digital property does not include digital currency notes that are legally means payments and another financial property which is arranged other laws [39]. In legal sense, digital property is considered new the institute , and then itself team and special property and one of the biggest challenges contemporary property rights , so they are finished unlimited potentials applications digital funds in the future , and economy and efficiency main are reasons increased interest legislators widely world and numerous international financial organization for this type property (Mirković, 2023, 20). He knows the law two types digital property and that: virtual currencies and digital tokens . The most important The virtual currency is bitcoin.

The work consists of two parts. In the first part part of the work is being processed concept digital property as legal institute , as and the most significant EU regulation on markets cryptoassets which was adopted in 2023 . In the second part of the work is being processed legal regulation digital property in the Republic Serbia , as central topic of this work, with in retrospect to digital status property in Bosnia and Herzegovina .

***Keywords**: legal regulation, digital property*

Available at: https://zisjournal.com/wp-content/uploads/2024/06/Godina_1.Broj_1.pdf. Date of access: 01.07.2025. year

[39] Digital Law property . " Official Gazette of RS" , number: 153/2020.

1. THE CONCEPT OF DIGITAL PROPERTY AS A LEGAL INSTITUTE

Digital property is a new legal institute , which is in dictionaries rights entered thanks to development internet and digital communication (Čolaković , 2023, 166). It is considered special property and one of the biggest challenges contemporary property rights , so they are finished unlimited potentials applications digital funds in the future , and economy and efficiency main are reasons increased interest legislators widely world and numerous international financial organization for this type property (Mirković, 2023, 20). Based on this , a new property law is created institute , digital property , and the question his/her standardization is set as question necessities legal regulations, how on national so and on international level (Mirković, 2023, 20).

However , in terms of defining digital content , there is series different definition according to legislative European union , and so on Directive 2019/770 on certain aspects delivery contract digital content and digital service[40] and Directive 2011/83/EU on rights consumer[41] determine concept digital content as data that is produced and delivered in digital in shape stating as examples : computer programs , applications , games , music , videos or texts regardless whether they are accessed by downloading or by flow , from the tangible media or on any other Digital mode[42] content is also defined in Directive (EU) 2015/2366 on payment instruments services[43] as goods or services which are produced and delivered in digital in shape and whose use is or consumption limited on technically device that neither in what way does it not include use or consumption physical goods or service .

[40] Directive (EU) 2019/770 of the European parliament and of the Council of May 20, 2019 on certain aspects delivery contract digital content and digital service , Official Journal L 136, accessed 08.01.2025. year

[41] Directive 2011/83/EU of the European parliament and Council of October 25 , 2011 on rights consumer , change Directives Council Directive 93/13/EEC and European Directive 1999/44/EC parliament and Councils and about putting outside strength Directives Council Directive 85/577/EEC and Directive 97/7/EC of the European parliament and Councils , Text significant for EGP, Sl. L. 304, 22.11.2011. in particular edition for Croatia , Chapter 15 Volume 008 P. 260–284.

[42] Preamble 19, Article 2 , point 11 of Directive 2011/83 on the rights consumer .

[43] Directive (EU) 2015/2366 of the European parliament and of the Council of November 25 , 2015 on salaries services on internal market , about the change Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010 and on the placing outside strength Directive 2007/64/EC (Text significant for EEA) OJ L 337, 23.12.2015, p. 35–127.

1.2. REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND COUNCIL OF MAY 31, 2023 ON CRYPTOASSETS MARKETS AND AMENDING REGULATION (EU) NO. 1093/2010 I (EU) NO. 1095/2010 AND DIRECTIVE 2013/36/EU AND (EU) 2019/1937

European The Council [44]formalized Regulation (EU) 2023/1114 approved on 16.05.2023. year , and the Regulation on markets cryptoassets (MiCA) for the first time cryptoassets , issuers cryptoassets and providers service crypto -asset related they put under one coordinated legislative frame . On the first the place needs define crypto assets . Crypto assets are digital display values or rights , and can be transferred or to store electronically by means of , with the help of technologies distributed records (DLT)[45] or similar technologies . Crypto assets are one of the main ones application of DLT in finance . By regulation are three types included cryptoassets : **tokens tied with property** (maintain) stable value by tying with several currencies that are legally means payments (" fiduciary" currency "), individual goods or more type of goods, individual cryptoasset or set cryptoassets or basket such property , and are used as means payments for purchase of goods and service and as means storage values , **e- money tokens** (maintain stable value by tying with values only one fiduciary currencies and electronic are exchange for coins and banknotes , and serve before everything as means payment) , and **other cryptoasset as what are user tokens** **.** It is important to note that cryptoassets uses : as means payments / exchanges , for needs investments , for access slave or services , for a combination forward the above-mentioned badges . New rules requirements for issuers are introduced cryptoassets and providers service crypto -asset related when it comes to : supervision and approval transactions , transparency and discovery influence cryptoassets on environment .

Furthermore, it is important point out that providers service crypto -asset related necessary work permit in the EU, and must to fulfill strict protection requests wallet consumer and to answer will if lose cryptoasset investors , and the European supervisory banking authority (EBA) lead will public register provider service related to cryptoassets that do not meet obligations [46]. Certainly will

[44] Retrieved from: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32023R1114 on 08.01.2025. year.

[45] A type of technology that enables decentralized storage, updating and validation of encrypted data.

[46] Retrieved from: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32023R1114 on 08.01.2025. year.

cryptoasset which is already arranged EU legislation and further will to be subject to existing rules [47].

In view of benefits EU rules on cryptoassets [48], they point out is : legal crypto asset security which not included existing EU legislation , better protection consumer and investors , protective measures against financial crime and manipulation market , innovation and honestly market competition , financial stability and reduction high carbon footprint cryptoassets .

In the end, it matters. emphasize that EU rules on markets cryptoassets better protect before everything consumers and investors , and are regulated risks from financial crime , and with others the parties are encouraged innovations .

3. LEGAL REGULATION OF DIGITAL PROPERTY IN THE REPUBLIC OF SERBIA

Digital Law they are in the Republic Serbia was adopted by Folk assemblies Republics of Serbia , on entered into force on 21.12.2020. year , and it began to be applied on June 29, 2021. year [49]. The beginning applications Digital Law property is attached to the usual period of 6 months from adoption Law (which the provision is integral part each Law in Transition and final provisions [50]) , and which period aims to enable enough time to create conditions for his application (eg , adoption) by-laws acts), as and the possibility for everyone interested participants on market digital property meet with provisions Law (eg establishment of legal certainty , as and taxation these types property). Republic Serbia is one of the first country which supported adoption forward of the above of the Law , and it is team bounced from the " gray zone" and proved to keep up with contemporary the world , unlike Bosnia and Herzegovina and many other country .

Digital Law property in the Republic Serbia which is ultimately and entered on strength contains 146 members who are incorporated in chapter IX , while the draft the aforementioned Law contained only 70 members . After oral discussions added even more double more members , however forward stated not neither surprising considering that it is about regulating the era of digitization which is progressing day by day on world plan .

[47] Ibid.
[48] Ibid.
[49] " Official Gazette of RS" , number: 153/2020.
[50] Art. 146.

Adoption of the Digital Law property in the Republic Serbia is also caused and changes and additions main tax law in the Republic Serbia , which introduce as taxable category digital property [51], which was certainly cause -and-effect step .

In this work we will deal with the most important provisions the aforementioned Law and in short them to expose with analysis .

In the wider sense the legislator , by adopting forward of the above Law allowed possession and trading digital property [52]. Legal definition digital property implies digital record value that can be digitally buy , sell , exchange or to be transmitted , and which can be use as means exchanges or for the purpose of investments , at why digital property does not include digital currency notes that are legally means payments and another financial property which is arranged other laws [53].

By law[54] are regulated two types digital property and that : virtual currencies and digital tokens , and the division is significant considering on application different legal regime . Virtual *currency* is *a* species digital property which not issued and for whose value does not guarantee central bank , nor another body of public authority, which not necessarily related to law means payments and no legal status of money or currency , but it is physical or legal faces accept as means exchanges and can be bought , sold , exchanged , transferred and to keep electronic ; and a

[51] For example, the Value Added Tax Act. ("Official Gazette of the RS", no. 84/2004, 86/2004 - corr ., 61/2005, 61/2007, 93/2012, 108/2013, 6/2014 - aligned with internal law , 68/2014 - other laws , 142/2014, 5/2015 - harmonized din. , 5/2016 - harmonized din . , 7/2017 - harmonized din . , 30/2019 - harmonized din . , 72/2019, 8/2020 - harmonized din. ed ., 153/2020, 138/2022 and 94/2024) and the Tax Law on income citizens . ("Official Gazette of RS", no. 24/2001, 80/2002, 80/2002 - other laws , 135/2004, 62/2006, 65/2006 - amended , 31/2009, 44/2009, 18/2010, 50/2011, 91/2011 - harmonized din . , 93/2012 - harmonized din . , 47/2013 , 48/2013 - corrected 57/2014, 68/2014 - Ph.D. law , 5/2015 - harmonized din. izn ., 112/2015, 5/2016 - harmonized din. izn ., 7/2017 - harmonized din. izn ., 113/2017, 7/2018 - harmonized din. izn ., 95/2018, 4/2019 - harmonized din. izn ., 86/2019, 5/2020 - harmonized din. izn ., 153/2020, 156/2020 - harmonized din. izn ., 6/2021 - harmonized din. izn ., 44/2021, 118/2021, 132/2021 - harmonized din. izn ., 10/2022 - harmonized din. exc ., 138/2022, 144/2022 - harmonized Din. izn ., 6/2023 - harmonized din. izn ., 92/2023, 116/2023 - harmonized din. izn ., 6/2024 - harmonized din. izn . and 94/2024).

[52] Which consists of virtual currency (type digital property which not issued and for whose value does not guarantee central bank , nor another body of public authority, which not necessarily related to law means payments and no legal status of money or currency , but it is physical or legal faces accept as means exchanges and can be bought , sold , exchanged , transferred and to keep electronic) and digital tokens (type digital property and indicates either which intangible property right which in digital form represents one or more other property rights , what can include and right user digital tokens to be his provided certain services) .

[53] Digital Property Law. " Official Gazette of RS" , number: 153/2020.

[54] Ibid.

digital token is a species digital property and indicates either which intangible property right which in digital form represents one or more other property rights , what can include and right user digital tokens to be his provided certain services [55].

Article 3 states: regulated services which are related with digital property and include :

10. reception , transmission and execution orders related to on shopping and sale digital assets for the account third faces ;
11. services purchases and sales digital assets for cash money and / or funds on account and / or electronically money ;
12. services replacements digital property for another digital property ;
13. keeping and administration digital assets for the account user digital property and with team related services ;
14. related services with by issuing , offering and by sale digital property , with obligation her/his purchase (patronage) or without it obligations (agency);
15. guidance registry pawn shop rights on digital property ;
16. services acceptance / transfer digital property ;
17. management portfolio digital property ;
18. organizing trading platforms digital property .

It is further prescribed and activity concerning benefits advisory service[56] connected to digital assets (investment) counseling , giving investment recommendation , counseling in connection with structure capital , business strategy , publishing digital property , as and others advisory services connected to digital property). It is important to emphasize that the provider advisory service not obliged to provide quiet service obtain permission supervisory authority, but just let me know user his/her services [57].

The legislator further provided in Article 6 mining cryptocurrency , and the same is defined as acquisition digital property by participating in providing services computer confirmations transaction in information systems related to on certain digital property , and it is important to point out that on these acquirers digital assets do not apply legal provisions , but just in case the same decide to so

[55] Article 2.
[56] Article 5.
[57] So it can appear as a natural or legal person.

acquired digital property they trade by way of giver service related with digital property , then and on them equally apply legal provisions , and it is indisputable that they can trade according to OTC rules [58], as and all other faces (from of which it follows that OTC trading allowed Law).

The legislator has foreseen basic the principles in Articles 8 and 9 and that : principle neutrality , efficiency , economy and digitalization procedure .

According to the principle neutrality , provisions the law is equal relationships on all digital property regardless on technology on Whose digital is this? property based , including stable digital property . According to the principles efficiency , economy and digitalization procedure , every person (legal and physical) which starts administrative procedure (application for approval publishing white paper , request for issuance permissions to provide service connected to digital property) submits appropriate request by way of special web portal by which manages service of the Government of the Republic Serbia which is responsible for the design , coordination , development and functioning system electronic administration , and with that request delivers the whole documentation established by law and regulations I bring on basis law with which proves fulfillment conditions for adoption that one request , which turns off bureaucracy and we are entering an era digitalization world .

Furthermore, the legislator exclusively emphasized that either which type digital property not officially means payments [59], and that financial institutions (banks , insurance companies) houses), under supervision Folk banks , I can't to own digital property [60]. However , when it comes to business legal faces and entrepreneurs related to digital property , legislator provides that non-monetary investment in the economy society I can to be in digital tokens that are not related on providing service and work; acceptance digital property in exchange for the sold goods and / or provided in- store services on a little , over provider service connected to digital property – but then he changes digital property in official means payments and such pays out to the client ; establishment is allowed pawn shop rights on digital property , which is acquired by registration pawn shop law that governs provider service [61]; it is also allowed fiduciary[62]

[58] "Over the counter" trading (immediate trading between two faces).

[59] Article 12.

[60] Article 13.

[61] Debtor can to pledge yours digital property as means security .

[62] Which debtor transfer right properties on digital property on creditor as security some obligations , and the latter undertakes to return it to him if obligation wake up fulfilled .

When it comes to forced execution on digital property , the legislator is also that predicted , so when executor in court executive procedure owns digital property , the creditor may to charge from values the same . However , a question arises implementation forward stated in practice , and what will certainly time show .

Since the law regulated procedure creation and publishing digital property in the Republic Serbia , before everything is made up of White paper (White paper) that is sent competent organ on approval [63], and then it is accessed initial offers digital property [64].

When it comes to secondary trading digital property , the same is the legislator predicted , and even and that one issued outside Republic , for which not issued white paper in accordance with By law , if it is digital property which in a significant way measure trades on global market over licensed , or registered platform in accordance with regulations European Union [65].

Article 37 stipulates trading and use smart of the contract . Szabo (1996, 18) states that he is smart contract digital transactional protocol that executes provisions contract , and the goals design smart contract are satisfaction usual requirements in contracts (ways payments , anonymity) and minimization need for confidentiality third person [66].

Consequently forward above , the legislator works protection obliged provider service to bow regulations on prevention washing money and financing terrorism , and are executed changes and additions forward of the above Law regarding defining and inclusions digital property in the same [67].

[63] Article 19.

[64] The procedure is compatible American to the ICO (Initial Coin Offering) system in which publisher digital property offers the same for exactly established price , before than what the same wake up released on public market .

[65] Article 31.

[66] Use smart contracts for execution complex way payments with small compensation and simple performance .

[67] "Official Gazette of RS", number: 113/17, 91/19, 153/20, 92/23 and 94/24.

3.1. STATUS OF DIGITAL ASSETS IN BOSNIA AND HERZEGOVINA

When it comes to the legal regulation of digital assets in Bosnia and Herzegovina, it has not yet been implemented in Bosnia and Herzegovina's legislation. However, following the above, amendments to the Law on the Securities Market were adopted in the Republika Srpska in 2022.[68] in Article 2, after paragraph 24, new paragraphs 25, 26 and 27 are added, which read:

- ' Virtual currency' is a digital record of value that has not been issued and whose value is not guaranteed by a central bank or other public sector body, which is not necessarily tied to a legal tender and does not have the legal status of money or currency, but is accepted by natural and legal persons as a means of exchange and can be bought, sold, exchanged, transferred and stored electronically.
- 'Virtual currency service provider' is a legal or natural person that provides one or more of the following services: safekeeping and management of virtual currencies on behalf of third parties (wallet depository service provider), organization of a platform for trading virtual currencies, exchange of virtual currencies for legal tender, exchange of virtual currencies for another virtual currency, transfer of virtual currency, i.e. reception and execution of orders for virtual currency on behalf of third parties, implementation of the offer, i.e. sale of virtual currencies.
- "A 'wallet custodian service provider' is a legal or natural person that provides the service of storing private cryptographic keys on behalf of another person for the purpose of holding, storing and transferring virtual currencies."

From the above, it follows that although there is no legal basis for digital property in our Bosnian and Herzegovina law, as previously stated, the Republika Srpska has taken a step forward and included provisions on digital property in the aforementioned law, from which it can be concluded that in the future it will work on adopting positive legislation regarding digital property, and the legal solutions will likely be similar, if not the same, as in the neighboring Republic of Serbia.

As for the Federation of Bosnia and Herzegovina, there is still no interest in amendments to the Law on the Securities Market, as in the Republic of Srpska, from which it follows that the Federation of Bosnia and Herzegovina is in a deep "gray zone", given that the aforementioned amendments are more than two years

[68] " Official Gazette of the Republic of Srpska", no. 92/06, 34/09, 30/12, 59/13, 108/13, 4/17, 63/21 and 11/22).

behind the Republika Srpska, so the question arises whether and when it will be time to consider the adoption of the Law on Digital Assets?

In all of the above, the only positive thing is that the Law on the Prevention of Money Laundering and Financing of Terrorist Activities of 2024 was adopted at the state level of Bosnia and Herzegovina [69], which defines virtual currency [70]as a digital record value that is not broadcast and for whose value does not guarantee central bank , nor other public authority sector , which not necessarily related to law means payments and no legal status of money or currency , but it is physical and legal faces accept as means exchanges and it can be transferred , stored , bought , sold , exchanged electronically via . Forward it is certainly stated prerequisite for adoption Digital Law property in some more recent or further future .

However , what is currently controversial is that in Bosnia and Herzegovina , more precisely entity Republika Srpska registered a few economic societies which provide services which are related with digital property , and the competent The RS Securities Commission issues permits to entities that fulfill conditions for performing related jobs with virtual currencies . So, on field digital property all are larger interests subjects , and the competent organs obviously they don't have problems which does not exist legally decoration frame forward mentioned matter , which additionally creates confusion and legal uncertainty , and all larger possibility of fraud .

CONCLUSION

The digitization of the world is in full swing, and the issue of regulating digital assets has been recognized by a considerably small circle of countries, among which is the Republic of Serbia. As early as 2021, the Republic of Serbia will adopt a law that will enter into force six months later and will begin to be implemented, while Bosnia and Herzegovina at the beginning of 2025 still has no indication when the Law on Digital Property could be proposed by the competent authorities. Precisely from the above, it can be concluded that Bosnia and Herzegovina is still in the "grey zone", unlike the Republic of Serbia. The legislator in the Republic of Serbia regulates the area of digital property in detail, and this work has dealt with the most important provisions of the Law.

As for Bosnia and Herzegovina, there are minor changes in one entity, the Republika Srpska, in the Law on the Securities Market, in which the legislator

[69] "Official Gazette of BiH", number: 13/2024.
[70] Article 4.

defines the concept of digital assets, which is certainly a step forward, while the Federation of Bosnia and Herzegovina has not even done so. The question of legal uncertainty in an unregulated area arises, since there are several registered legal entities in Bosnia and Herzegovina that provide services which are related with digital property , and the competent The RS Securities Commission issues permits to entities that fulfill conditions for performing related jobs with virtual currencies .

The conclusion is that the Republic Serbia should follow European standards and accordingly , performs changes and additions , if wake up needs for the same , while Bosnia and Herzegovina needs urgently undertake steps leading to legal regulations digital property , which will certainly contribute efficiency and economy , as and legal security all interested persons who want to provide services which are related with digital property .

LITERATURE

2. Čolaković, M. (2023). Inheritance of digital assets : is there digital life after death? *In the collection of works "Current Affairs of Civil and Commercial Legislation and Legal Practice", no. 20, 162-181.*
3. Delić H. (2021). The role of the security system of Bosnia and Herzegovina in the migrant crisis, in the light of the complex organization of the state of Bosnia and Herzegovina - professional article. In the Journal: Protection and Security for 2021, Year 1, no. 1, p. 53.
4. Directive 2011/83/EU of the European parliament and Council of October 25 , 2011 on rights consumer , change Directives Council Directive 93/13/EEC and European Directive 1999/44/EC parliament and Councils and about putting outside strength Directives Council Directive 85/577/EEC and Directive 97/7/EC of the European parliament and Councils , Text significant for EGP, Sl. L. 304, 22.11.2011. in particular edition for Croatia , Chapter 15 Volume 008 P. 260–284.
5. Directive (EU) 2015/2366 of the European parliament and of the Council of November 25 , 2015 on salaries services on internal market , about the change Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010 and on the placing outside strength Directive 2007/64/EC (Text significant for EEA) OJ L 337, 23.12.2015, p. 35–127.
6. Directive (EU) 2019/770 of the European parliament and of the Council of May 20, 2019 on certain aspects delivery contract digital content and digital service , Official Journal L 136, accessed 08.01.2025. year .
7. Mirković, P. (2023). Digital property – legislative approach to regulating a new property law institute. *In Law – theory and practice, vol. 40, 17-31.*
8. Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16), 18(2).*
9. Keyword: How the EU regulates the market. *Council of the European Union* . Retrieved from: https://www.consilium.europa.eu/hr/policies/crypto-assets-how-the-eu-is-regulating-markets/ on 08.01.2025. year.
10. Digital Property Law. (Official Gazette of RS, number: 153/2020).
11. Value Added Tax Law. ("Official Gazette of the RS", no. 84/2004, 86/2004 - corr ., 61/2005, 61/2007, 93/2012, 108/2013, 6/2014 - aligned with internal law , 68/2014 - other laws , 142/2014, 5/2015 - harmonized din. , 5/2016 - harmonized din . , 7/2017 - harmonized din . , 30/2019 -

harmonized din . , 72/2019, 8/2020 - harmonized din. izn ., 153/2020, 138/2022 and 94/2024).

12. Tax law on income citizens . ("Official Gazette of RS", no. 24/2001, 80/2002, 80/2002 - other laws , 135/2004, 62/2006, 65/2006 - amended , 31/2009, 44/2009, 18/2010, 50/2011, 91/2011 - harmonized din . , 93/2012 - harmonized din . , 47/2013 , 48/2013 - corrected 57/2014, 68/2014 - Ph.D. law , 5/2015 - harmonized din. izn ., 112/2015, 5/2016 - harmonized din. izn ., 7/2017 - harmonized din. izn ., 113/2017, 7/2018 - harmonized din. izn ., 95/2018, 4/2019 - harmonized din. izn ., 86/2019, 5/2020 - harmonized din. izn ., 153/2020, 156/2020 - harmonized din. izn ., 6/2021 - harmonized din. izn ., 44/2021, 118/2021, 132/2021 - harmonized din. izn ., 10/2022 - harmonized din. exc ., 138/2022, 144/2022 - harmonized Din. izn ., 6/2023 - harmonized din. izn ., 92/2023, 116/2023 - harmonized din. izn ., 6/2024 - harmonized din. izn . and 94/2024).
13. Petrović Ž. (2022). The United Nations and NATO in war and post-war Bosnia and Herzegovina - expert work. In the Journal: Protection and Security for 2022, Year 2, no. 2, p. 103. Available at: https://zisjournal.com/wp-content/uploads/2024/06/Godina_2.Broj_1.pdf. Date of access: 01.07.2025. year.
14. Prevention Act washing money and financing terrorist activities . "Official Gazette of BiH", number: 13/2024.
15. Law on the Prevention of Money Laundering and Financing of Terrorism. "Official Gazette of the Republic of Serbia", No.: 113/17, 91/19, 153/20, 92/23 and 94/24.
16. Securities Market Law. " Official Gazette of the Republic of Srpska", no. 92/06, 34/09, 30/12, 59/13, 108/13, 4/17, 63/21 and 11/22).