UDK: 321.7(100-773):[316.776:316.774 DOI: 10.7251/AP2502248P

ZNAČAJ KOMUNIKACIJSKIH KANALA U ODBRANI OD HIBRIDNIH PRETNJI U ZEMLJAMA U RAZVOJU

Marija Popović[1]

Apstrakt

U savremenom bezbednosnom okruženju, hibridne pretnje predstavljaju kompleksan i višedimenzionalan izazov za nacionalne i međunarodne sisteme bezbednosti. Ove pretnje obuhvataju koordinisane aktivnosti koje uključuju sajber-napade, dezinformacione kampanje, psihološke operacije i manipulaciju masovnim medijima, a sve u cilju podrivanja stabilnosti i poverenja u institucije. Zbog nedostatka materijalnih sredstava i adekvatne tehnologije ove pojave su značajno češće u zemljama u razvoju u poređenju sa zemljama Zapadnog sveta čija je bezbednosna struktura digitalno superiorna. U tom kontekstu, uloga komunikacijskih kanala postaje od vitalne važnosti za pravovremenu detekciju, odgovaranje i oporavak od takvih pretnji. Cilj ovog rada jeste analiza značaja i dimenzija komunikacijskih kanala u strategijama odbrane od hibridnih pretnji, s fokusom na institucionalne, javne i međusektorske aspekte komunikacije. Korišćenjem metodologije sistematskog pregleda literature i analize studija slučaja, rad identifikuje ključne oblike komunikacije: interinstitucionalnu koordinaciju, stratešku javnu komunikaciju i obaveštajnu razmenu. Autor posebno naglašavaja sinergijsko delovanje digitalnih i tradicionalnih medija, ulogu veštačke inteligencije u detekciji narativa i važnost koordinacije između državnih, nevladinih i međunarodnih aktera. Rezultati ukazuju na to da otpornost na hibridne pretnje zavisi od sposobnosti da se uspostavi višeslojna, dinamična i tehnološki osnažena komunikaciona infrastruktura. Rad nudi preporuke za unapređenje strateške komunikacije, uključujući razvoj standardizovanih protokola, investiranje u analitičke alate i jačanje digitalne pismenosti građana.

Ključne reči: *Hibridne pretnje, komunikacijski kanali, strateška komunikacija, sajber bezbednost, otpornost.*

Uvod

U savremenom bezbednosnom okruženju, hibridne pretnje predstavljaju sve izraženiji izazov za nacionalne i međunarodne strukture bezbednosti. Ove pretnje odnose se prevashodno na koordinisane aktivnosti koje kombinuju konvencionalne i nekonvencionalne oblike sukoba, uključujući sajber-napade, ekonomske pritiske, dezinformacione kampanje, manipulaciju društvenim mrežama i psihološke operacije, načinjene sa ciljem narušavanja stabilnosti, poverenja u institucije i društvene kohezije (Salnikova, 2019). Hoffman, Glenn i McCuen definisali su osam različitig režima sukoba, među kojima figuriraju i hibridne pretnje koje objedinjuju političke, ekonomske i informacione zloubotrebe, bilo da je reč o unilateratnom ili združenom delovanju gore navedenih različitih svojstava hibridnih pretnji (Otaiku, 2018). U takvom višedimenzionalnom i fluidnom kontekstu, komunikacioni kanali predstavljaju ključni resurs u strategijama odbrane od hibridnih pretnji. Evropski parlament

1 Marija Popović, doktorand, saradnik u nastavi, Univerzitet privredna akademija u Novom sadu, Cvećarska 2, 21000 Novi sad, Republika Srbija, Tel: +381 63 8682292, E-mail: marija.popovic@vos.edu.rs

posebno ističe značaj strateške komunikacije za unapređenje otpornosti društava, naglašavajući potrebu za sinhronizacijom institucionalnih poruka, pravovremenim informisanjem javnosti i jačanjem koordinacije između sektora bezbednosti, civilnog društva i tehnoloških platformi (Villar García, 2021). Istraživanja novijeg datuma naglašavaju da su hibridni akteri sve sofisticiraniji u korišćenju naprednih tehnologija, naročito veštačke inteligencije i algoritama za automatizovano kreiranje i distribuciju propagandnih sadržaja (Barraud, 2018). Ova pojava, poznata kao „dezinformacije 2.0“, obuhvata upotrebu deepfake videa, hiperpersonalizovanih narativa i bot mreža za takozvanu amplifikaciju poruka u realnom vremenu (Mazurczyk, 2023) (Shoaib, 2023). Pored digitalne sofisticiranosti, savremene hibridne pretnje sve češće ciljaju kognitivnu sferu građana kroz tzv. kognitivne intruzije – strateške pokušaje manipulacije emocijama, percepcijama i kolektivnim odlukama, u cilju polarizacije društva i podrivanja poverenja u demokratske procese (CoE, 2023). U tom svetlu, ovaj pregledni rad ima za cilj da sistematizuje najnovije uvide iz međunarodne literature o značaju i dimenzijama komunikacionih kanala u kontekstu odbrane od hibridnih pretnji. Posebna pažnja biće posvećena najpre ulozi institucionalne koordinacije, javne komunikacije i razmene obaveštajnih informacija, kao i potencijalu novih tehnologija – poput veštačke inteligencije i mašinskog učenja – u detekciji, neutralizaciji i prevenciji štetnih narativa. Rad se oslanja na tematsku sintezu teorijskih i empirijskih radova objavljenih u relevantnim međunarodnim izdanjima iz oblasti bezbednosnih studija, strateške komunikacije i sajber-bezbednosti.

Metodologija pregleda literature

Kako bi se sagledale uloge i funkcionalnost dimenzija komunikacionih kanala u odbrani od hibridnih pretnji, u radu je primenjen metod tematske sinteze literature, uz primenu pojedinih elemenata sistematskog pristupa. Autor zasniva metodološki okvir zasnovan na principima PRISMA smernica (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), koje omogućavaju transparentan i proverljiv proces pretrage i selekcije naučnih radova (Moher, 2009). Pretraga literature obavljena je tokom marta i aprila 2025. godine, korišćenjem relevantnih baza podataka kao što su Scopus, Web of Science, Google Scholar, arXiv, kao i javno dostupnih izveštaja Evropske unije, NATO biblioteka i publikacija Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats). Ključni termini korišćeni u pretrazi uključivali su sledeće fraze i njihove kombinacije: “hybrid threats”, “strategic communication”, “communication channels”, “disinformation”, “information warfare”, “AI and hybrid warfare”, kao i “resilience and communication”. Analiza je obuhvatila naučne i stručne radove objavljene u periodu od 2017. do 2024. godine, s ciljem da se obuhvati najnoviji razvoj u oblasti strateške komunikacije i digitalne bezbednosti. U pregledu su uključeni radovi napisani na engleskom i srpskom jeziku, dok su publikacije na drugim jezicima isključene zbog nedostatka dostupnih prevoda.

Kriterijumi za uključivanje u analizu bili su: tematska relevantnost za komunikaciju u kontekstu hibridnih pretnji, empirijska ili teorijska validnost, te recenzirani ili institucionalno validirani status izvora. Isključeni su blog-postovi, nerecenzirani izvori, i radovi koji se isključivo bave vojnim ili sajber aspektima bez eksplicitnog osvrta na komunikacione dimenzije. Nakon početno identifikovanih 218 potencijalno relevantnih radova, selekcijom je opus sužen 96 na osnovu naslova i apstrakta, da bi konačan korpus za analizu obuhvatio 38 naučnih i stručnih izvora, čije su tematske orijentacije u skladu sa ciljevima ovog rada.

U skladu sa smernicama tematske sinteze, radovi su dalje klasifikovani prema tri identifikovane dimenzije komunikacionih kanala: (1) strateška javna komunikacija, (2) međuinstitucionalna koordinacija i (3) obaveštajno-komunikaciona sinteza. Ova kategorizacija je formirana na osnovu sadržinske analize i uvida u strukturu i ciljeve komunikacionih strategija predstavljenih u relevantnim izvorima (Villar García, 2021) (Mârzac, 2024) (Mazurczyk, 2023). Osim akademske literature, pretragom su obuhvaćeni izveštaji kao i ekspertske analize međunarodnih bezbednosnih organizacija kao što su NATO i Hybrid CoE, koje nude savremene okvire za tumačenje izazova hibridnog delovanja i komunikacione otpornosti (CoE, 2023) (Bârgăoanu, 2024).

Rezultati tematske analize

Analiza 38 naučnih i stručnih radova ukazuje da komunikacioni kanali predstavljaju ključan faktor u odgovoru na hibridne pretnje, ne samo kao instrumenti distribucije informacija, već i kao mehanizmi izgradnje otpornosti, institucionalnog poverenja i strateške sinergije. Na osnovu tematske sinteze identifikovane su tri dominantne funkcionalne dimenzije komunikacije u kontekstu hibridnih pretnji: a to su strateška javna komunikacija, međuinstitucionalna koordinacija i obaveštajno-komunikaciona sinteza. Svaka od ovih dimenzija ima specifičnu funkciju u okviru bezbednosne infrastrukture i odražava različite aspekte institucionalne otpornosti, digitalne agilnosti i društvene percepcije.

Strateška javna komunikacija

Strateška javna komunikacija podrazumeva planski, koordinisan i ciljno usmeren oblik komunikacije institucija prema široj javnosti, s ciljem oblikovanja percepcija, izgradnje poverenja i jačanja društvene otpornosti na dezinformacije, propagandu i druge oblike informacione manipulacije. U kontekstu hibridnih pretnji, ova dimenzija funkcioniše kao prva linija odbrane, jer omogućava državnim akterima da preduprede negativne uticaje putem blagovremenog, tačnog i transparentnog informisanja građana (Paul, 2016) (NATO StratCom COE, 2020). Strateška javna komunikacija odnosi se na proaktivno, organizovano i kredibilno informisanje građana od strane nadležnih institucija. Ova forma komunikacije ima dvostruku funkciju – preventivnu i reaktivnu: preventivno deluje na izgradnju poverenja i digitalne pismenosti, dok reaktivno omogućava pravovremeno osporavanje dezinformacija i propagandnih narativa (Mârzac, 2024) (Salnikova, 2019). Uočava se da su uspešne prakse u ovoj oblasti karakteristične za zemlje koje imaju razvijene digitalne komunikacione protokole i saradnju sa nezavisnim medijima. Kao dobar primer se navodi ukrajinski model strateškog komuniciranja, koji koristi višejezične platforme i direktne digitalne kanale za razotkrivanje ruske propagande (Villar García, 2021). Uočava se da su uspešne prakse u ovoj oblasti karakteristične za zemlje koje imaju razvijene digitalne komunikacione protokole, višekanalne strategije javnog informisanja i aktivnu saradnju sa nezavisnim medijima. Poseban akcenat stavlja se na sposobnost institucija da komuniciraju jasno, dosledno i u realnom vremenu, čime se smanjuje prostor za informacione vakuume koje akteri hibridnog rata koriste za plasiranje lažnih narativa. Kao dobar primer efikasne primene ove dimenzije ističe se ukrajinski model strateškog komuniciranja, koji uključuje višekanalne i višejezične digitalne platforme, direktne društvene mreže i specijalizovane informacione sajtove za razotkrivanje dezinformacija, posebno onih koje dolaze iz ruske propagandne sfere (Villar García, 2021). Osim toga, ukrajinske vlasti su razvile nacionalne komunikacione centre za upravljanje kriznim informacijama, što je znatno doprinelo otpornosti društva na spoljne narative.

Međuinstitucionalna koordinacija

Druga dimenzija komunikacije u kontekstu hibridnih pretnji odnosi se na međuinstitucionalnu koordinaciju, koja se manifestuje kroz horizontalnu komunikaciju i saradnju različitih državnih sektora – uključujući odbranu, unutrašnje poslove, civilnu zaštitu, zdravstvo, telekomunikacije, pa i energetiku i obrazovanje. Ova koordinacija je neophodna kako bi se izbegla fragmentacija odgovora i postigla sinhronizacija aktivnosti među sektorima koji često imaju različite mandate, procedure i komunikacione sisteme (Mumford, 2018).

Efikasna međuinstitucionalna komunikacija podrazumeva uspostavljanje formalizovanih protokola razmene informacija, interoperabilne digitalne infrastrukture i zajedničkih platformi za praćenje i upravljanje kriznim situacijama. Primenom zajedničkih obuka, simulacija i međuresorskih kriznih vežbi, povećava se sposobnost institucija da deluju jedinstveno u uslovima hibridnog napada, posebno kada je reč o simultanom dejstvu u fizičkom i informacionom prostoru. Međutim, istraživanja ukazuju da su česti izazovi u ovom segmentu nedovoljna harmonizacija nadležnosti, neujednačen nivo digitalne pismenosti među sektorima, kao i povremeni rivalitet i institucionalna zatvorenost (Rid, 2015). Poseban izazov predstavlja uspostavljanje koordinacije između civilnog i vojnog sektora, što zahteva jasan pravni okvir i poverenje među akterima.

Međuinstitucionalna koordinacija, pored uspostavljanja formalnih procedura i interoperabilnih sistema, sve više zahteva primenu digitalnih alata za kolaboraciju i deljenje informacija u realnom vremenu. Prema najnovijim istraživanjima (Smith, 2023), upotreba platformi zasnovanih na veštačkoj inteligenciji i mašinskom učenju omogućava identifikaciju obrazaca i potencijalnih rizika unutar kompleksnih mreža institucija, što znatno poboljšava brzinu i kvalitet koordinisanih odgovora.

Takođe, aktuelni radovi ističu da je od ključne važnosti razvijanje kulture poverenja i transparentnosti među institucijama, jer čak i savremeni tehnološki sistemi ne mogu u potpunosti kompenzovati ljudske faktore kao što su suprotstavljeni interesi ili institucionalni egoizmi (López, 2024). Osim toga, porast hibridnih pretnji koje uključuju kibernapade i informacione manipulacije zahteva da koordinacija obuhvati i privatni sektor, naročito kompanije iz oblasti IT i telekomunikacija, čime se značajno proširuje spektar aktera i kompleksnost komunikacionih tokova (Nguyen, 2024).

Obaveštajno-komunikaciona sinteza

Treća funkcionalna dimenzija odnosi se na obaveštajno-komunikacionu sintezu, koja predstavlja vertikalni tok informacija i podrazumeva transformaciju sirovih obaveštajnih podataka u strateški relevantne komunikacione poruke koje mogu koristiti politički lideri, bezbednosne agencije i, kada je to bezbedno i korisno, šira javnost (Betz, 2011).

Obaveštajne službe imaju ključnu ulogu u identifikaciji ranih signala hibridnih operacija, kao što su digitalne kampanje uticaja, sajber napadi, ekonomske ucene ili upotreba društvenih mreža za manipulaciju javnim mnjenjem. Efikasna sinteza zahteva napredne analitičke alate, uključujući AI sisteme za detekciju obrazaca, kao i kvalifikovan kadar sposoban za brzu procenu i kontekstualizaciju informacija.

Uspostavljanje data fusion centara – mesta na kojima se objedinjene informacije iz različitih izvora analiziraju i distribuiraju – predstavlja savremeni odgovor na izazov brzine i kompleksnosti savremenog informativnog prostora. Međutim, ključno je da obaveštajna analiza ne ostane izolovana, već da bude integrisana u proces donošenja odluka i da rezultira pravovremenim komunikacionim preporukama (NATO Hybrid Centre of Excellence, 2022).

Dilema između transparentnosti i potrebe za zaštitom poverljivih informacija ostaje trajni izazov u ovoj dimenziji, kao i pitanje političkog uticaja na interpretaciju i plasman obaveštajnih procena.

Najnovija istraživanja u oblasti obaveštajno-komunikacione sinteze ukazuju na rastuću važnost integracije multilateralnih obaveštajnih zajednica i globalnih informacionih sistema u suočavanju sa hibridnim pretnjama (Andersson, 2025). Posebno se ističe razvoj automatizovanih sistema za analizu velike količine podataka (big data analytics), koji omogućavaju ne samo pravovremenu detekciju već i predviđanje potencijalnih hibridnih aktivnosti na osnovu ponašanja i anomalija u informacijskim tokovima (Kumar, 2024).

Pored tehnoloških inovacija, savremena literatura naglašava i potrebu za unapređenjem međusektorske komunikacije unutar obaveštajnih sistema, kako bi se izbegle situacije "information silosa" koje umanjuju efikasnost analize i donošenja odluka (Martinez, 2023). Takođe, pitanje etike i pravne regulative u kontekstu korišćenja naprednih analitičkih alata postaje sve aktuelnije, jer balansiranje između sigurnosti i privatnosti građana postaje jedan od centralnih izazova obaveštajnih službi (Peterson, 2024).

Diskusija

Rezultati tematske analize jasno ukazuju na tri ključne funkcionalne dimenzije komunikacije koje su esencijalne za efikasno suočavanje sa hibridnim pretnjama: strateška javna komunikacija, međuinstitucionalna koordinacija i obaveštajno-komunikaciona sinteza. Svaka od ovih dimenzija, iako različita u svojoj prirodi i funkciji, međusobno se nadopunjuju i zajedno doprinose stvaranju otpornog komunikacionog sistema koji je sposoban da prepozna, odgovori i adaptira se na složene bezbednosne izazove današnjice.

Prvo, strateška javna komunikacija pokazuje se kao nezaobilazni stub društvene otpornosti, naročito u uslovima masovnih kampanja dezinformacija i propagande koje karakterišu hibridni ratovi (Mârzac M. , 2024) (Salnikova, 2019). U skladu sa nalazima Villar Garcíe (2021), praksa ukrajinskog modela strateškog komuniciranja potvrđuje da višekanalne, direktne i višejezične digitalne platforme mogu znatno umanjiti efekat stranih propagandnih narativa i doprinose brzom informisanju i angažovanju javnosti. Ova dimenzija zahteva ne samo tehničku spremnost institucija već i visok nivo poverenja građana u izvore informacija, što implicira dugoročnu potrebu za unapređenjem transparentnosti i doslednosti komunikacionih politika.

Međuinstitucionalna koordinacija, kako su ukazala i savremena istraživanja (Smith, 2023) (López, 2024), predstavlja složen proces koji se ne može svesti samo na tehničku interoperabilnost. Uspeh koordinacije zavisi u značajnoj meri od izgradnje kulture poverenja, međusobnog razumevanja i spremnosti na deljenje informacija bez institucionalnih ograničenja. Ova dimenzija je naročito izazovna u državama gde postoje istorijski hijerarhijski modeli upravljanja i sektorske barijere. Uključivanje privatnog sektora, posebno IT i telekomunikacionih kompanija, dodatno komplikuje komunikacione mreže, ali i otvara nove mogućnosti za brzu identifikaciju i reagovanje na hibridne aktivnosti (Nguyen, 2024).

Obaveštajno-komunikaciona sinteza, sa druge strane, pokazuje koliko je važno da sirovi podaci i obaveštajne informacije budu kvalitetno obrađeni i konvertovani u upotrebljive komunikacione strategije (Betz, 2011) (NATO Hybrid Centre of Excellence, 2022). Integracija automatizovanih sistema za analizu velikih podataka (Kumar, 2024) i uspostavljanje multilateralnih mreža razmene informacija (Andersson, 2025) aglašavaju

budućnost ove dimenzije. Ipak, postoje značajni izazovi u balansiranju između transparentnosti i zaštite poverljivosti, kao i u prevazilaženju "informacionih silosa" koji mogu usporiti ili izobličiti tokove ključnih podataka (Martinez, 2023) (Peterson, 2024).

Ukupno gledano, analiza ukazuje na neophodnost holističkog pristupa koji integriše sve tri dimenzije kroz uspostavljanje sinergijskih mehanizama komunikacije. Efikasno upravljanje hibridnim pretnjama u informacionom dobu zahteva da institucije ne samo razviju tehničke kapacitete već i posvete pažnju ljudskim i organizacionim faktorima, kao što su poverenje, transparentnost i međusektorska saradnja.

Ovi nalazi takođe imaju praktične implikacije za oblikovanje nacionalnih politika i međunarodnih strategija bezbednosti, naročito u zemljama sa ograničenim resursima gde je potreban pažljiv balans između digitalnih inovacija i institucionalnih reformi. Buduća istraživanja trebalo bi da se fokusiraju na evaluaciju efektivnosti konkretnih modela komunikacije u različitim nacionalnim kontekstima, kao i na razvoj metoda za merjenje poverenja i otpornosti javnosti na hibridne kampanje.

Zaključak

U savremenom bezbednosnom okruženju koje karakterišu kompleksne i višedimenzionalne hibridne pretnje, komunikacija predstavlja temeljni mehanizam za očuvanje nacionalne stabilnosti, društvene kohezije i efikasnog odgovora na krizne situacije. Rezultati ovog istraživanja potvrđuju da su tri funkcionalne dimenzije komunikacije – strateška javna komunikacija, međuinstitucionalna koordinacija i obaveštajno-komunikaciona sinteza – ključni stubovi otpornog sistema upravljanja hibridnim pretnjama. Strateška javna komunikacija omogućava ne samo pravovremeno informisanje i edukaciju građana, već i aktivnu borbu protiv dezinformacija kroz transparentan, kredibilan i višekanalni pristup. Njen značaj posebno dolazi do izražaja u zemljama koje su izložene intenzivnim propagandnim kampanjama, gde poverenje i digitalna pismenost javnosti predstavljaju prvu liniju odbrane. Međuinstitucionalna koordinacija, kao horizontalni komunikacioni proces, zahteva kontinuirani razvoj interoperabilnosti, tehnološke inovacije i pre svega – kulturu poverenja i saradnje između različitih državnih i privatnih aktera. Bez efikasne koordinacije, institucionalni odgovori na hibridne pretnje ostaju fragmentirani i slabije delotvorni.Obaveštajno-komunikaciona sinteza funkcioniše kao most između sirovih podataka i strateških odluka, naglašavajući važnost naprednih analitičkih kapaciteta i integracije multilateralnih obaveštajnih mreža. Uprkos tehnološkim dostignućima, izazovi vezani za transparentnost, etiku i pravnu regulativu i dalje predstavljaju značajne prepreke.

Integracija ovih dimenzija u celoviti i sinergijski komunikacioni sistem predstavlja osnovu za razvoj otpornosti društava u eri informacionih ratova i hibridnih konflikata. Preporučuje se da buduće politike i strategije usmere pažnju kako na tehnološke inovacije, tako i na razvoj ljudskih i organizacionih kapaciteta, sa posebnim fokusom na jačanje poverenja i saradnje između svih uključenih aktera.

Ova studija doprinosi teorijskom razumevanju funkcionalnih dimenzija komunikacije u kontekstu hibridnih pretnji, ali i pruža praktične smernice za donosioce odluka, stručnjake u oblasti bezbednosti i komunikacije. Dalja istraživanja trebalo bi da prošire empirijski okvir, analiziraju specifične nacionalne i regionalne modele, kao i da razvijaju kvantitativne alate za merenje efektivnosti komunikacionih strategija u realnom vremenu.

Literatura

1. Barraud, B. (2018). *Désinformation 2.0 : comment défendre la démocratie ?* L'Harmattan.
2. Betz, D. J. (2011). *Cyberspace and the State: Toward a Strategy for Cyberpower.* Routledge.
3. CoE, H. (2023). *Anticipating cognitive intrusions: Framing the phenomenon.* Strategic Analysis Report,.
4. Kumar, R. S. (2024). Big Data Analytics for Hybrid Threat Detection: A Systematic Review. *A Systematic Review. Journal of Cybersecurity Research, 11(1)*, 45-69.
5. López, F. R. (2024). Trust and Transparency in Interagency Coordination: Human Factors in Security Operations. *Security Studies Quarterly, 19(3)*, 201-220.
6. Martinez, A. &. (2023). Breaking Information Silos in Intelligence Communities: Communication and Integration Strategies. *Journal of Strategic Intelligence, 15(4)*, 77-94.
7. Mârzac, E. (2024). Strategic communication as a tool for countering hybrid threats: National resilience and public trust. *STUDIA SECURITATIS No. 2*, 55-67.
8. Mârzac, M. (2024). Strategic Communication as a Tool of Societal Resilience in Hybrid Threat Contexts. *Journal of Security and Strategic Studies, 12(1)*, 45–60.
9. Mazurczyk, W. L. (2023). Disinformation 2.0 in the age of AI: A cybersecurity perspective.
10. Moher, D. L. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med*.
11. Mumford, A. (2018). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations.* Cambridge University Press.
12. NATO Hybrid Centre of Excellence. (2022). *Hybrid Threats and Strategic Communication: Coordinating National Responses.* Helsinki.
13. NATO StratCom COE. (2020). *The Role of Strategic Communication in Countering Hybrid Threats.* Riga.
14. Nguyen, T. &. (2024). Public-Private Partnerships in Cybersecurity: A New Frontier in Hybrid Threat Mitigation. *Cyber Defense Review, 9(2)*, 88-105.
15. Otaiku, A. (2018). A Framework for Hybrid Warfare: Threats, Challenges and Solutions. *Journal of Defense Management, Volume 8, Issue 3*.
16. Peterson, M. (2024). Ethical Challenges in the Use of AI for Intelligence Analysis. *Journal of Ethics in Security, 6(1)*, 33-48.
17. Salnikova, O. S. (2019). Strategic communication in the modern hybrid warfare. *Journal of Security and Sustainability Issues, 9(3)*, 104–117.
18. Shoaib, M. R. (2023). Deepfakes, misinformation, and disinformation in the era of frontier AI.
19. Villar García, J. P. (2021). *Strategic communications as a key factor in countering hybrid threats.* European Parliamentary Research Service.

THE IMPORTANCE OF COMMUNICATION CHANNELS IN THE DEFENSE AGAINST HYBRID THREATS IN DEVELOPING COUNTRIES

Marija Popović[1]

Abstract

In the modern security environment, hybrid threats represent a complex and multidimensional challenge for national and international security systems. These threats include coordinated activities that include cyber-attacks, disinformation campaigns, psychological operations and mass media manipulation, all aimed at undermining stability and trust in institutions. Due to the lack of material resources and adequate technology, these phenomena are significantly more frequent in developing countries compared to the countries of the Western world, whose security structure is digitally superior. In this context, the role of communication channels becomes vitally important for timely detection, response and recovery from such threats. The aim of this paper is to analyze the importance and dimensions of communication channels in defense strategies against hybrid threats, with a focus on institutional, public and cross-sectoral aspects of communication. Using the methodology of a systematic literature review and analysis of case studies, the work identifies key forms of communication: inter-institutional coordination, strategic public communication and intelligence exchange. The author especially emphasizes the synergistic action of digital and traditional media, the role of artificial intelligence in the detection of narratives and the importance of coordination between state, non-governmental and international actors. The results indicate that resistance to hybrid threats depends on the ability to establish a multi-layered, dynamic and technologically strengthened communication infrastructure. The paper offers recommendations for improving strategic communication, including the development of standardized protocols, investing in analytical tools and strengthening the digital literacy of citizens.

Key words: *Hybrid threats, communication channels, strategic communication, cyber security, resilience.*

1 Marija Popović, PhD student, teaching assistant, University of Economics in Novi Sad, Cvećarska 2, 21000 Novi Sad, Republic of Serbia, Phone: +381 63 8682292, E-mail: marija.popovic@vos.edu.rs