Rexhep Mustafovski
Marko Radovanović
Aleksandar Petrovski

DOI: 10.2478/cmc-2026-0011

OD PODPORE ZA KOMUNIKACIJE DO VARNIH MULTIDOMENSKIH OMREŽIJ: MODERNIZACIJA OKVIROV VOJAŠKE KOMUNIKACIJE

FROM SIGNAL SUPPORT TO SECURE MULTI-DOMAIN NETWORKS: MODERNIZING MILITARY COMMUNICATIONS FRAMEWORKS

Povzetek Članek preučuje spreminjajočo se vlogo komunikacijskih platform v vojaških operacijah in prikazuje njihov prehod od podpornih instrumentov do ključnih dejavnikov za hitro sprejemanje odločitev ter uspeh misij. Analizira omrežno komunikacijo, podporo signalov, kibernetsko varnost ter integracijo združenih in večnacionalnih sil, s posebnim poudarkom na preobremenjenosti elektromagnetnega spektra, kibernetskih grožnjah in varnem prenosu v spornih okoljih. Rezultati poudarjajo njeno izrazito neizmenljivost s širšimi modeli, kot sta strateška komunikacija in internet stvari na bojišču, kar zagotavlja operativno odpornost, povečuje učinkovitost ter ponuja prilagodljivost prihodnjim inovacijam, vključno z umetno inteligenco, kvantnim šifriranjem in naprednimi satelitskimi sistemi.

Ključne besede ***Okviri obrambne komunikacije, šifrirana taktična omrežja, koalicijska omrežja, zagotavljanje informacij, odpornost poveljevanja in nadzora.***

Abstract This paper examines the evolving role of communication platforms in military operations, showing their shift from supportive instruments to critical enablers of rapid decision-making and mission success. It analyzes networked communication, signal support, cybersecurity, and the integration of joint and multinational forces, with particular focus on electromagnetic spectrum congestion, cyber threats, and secure transmission in contested environments. The results highlight its distinct non-interchangeability with broader models such as Strategic Communications (StratCom) and Internet of Battlefield Things (IoBT), ensuring operational resilience, enhancing effectiveness, and offering adaptability to future innovations, including Artificial Intelligence (AI), quantum encryption, and advanced satellite systems.

Key words ***Defense communication frameworks, encrypted tactical networks, coalition networks, information assurance, command-and-control resilience.***

Introduction

The success of military operations relies on communication platforms which are dependable, protected, and able to adapt to changing conditions. With warfare becoming increasingly focused on networks, the capacity to share real-time data across land, air, sea, space, and cyberspace has turned into a core requirement for strategy. Military communication systems now include advanced radio technologies, satellite links, and encrypted data exchange, all designed to maintain coordination between deployed units and command elements (Wigness et al., 2022; Alkanjr and Mahgoub, 2023; Butun and Mahgoub, 2024). The growing complexity of multinational missions, combined task forces, and irregular conflicts has underlined the demand for secure and interoperable infrastructures capable of functioning in hostile environments (Farooq and Zhu, 2018; Doku, 2020; Feng et al., 2020).

Signal support stands at the center of modern communication, providing reliable connectivity and sustaining information flow in the face of cyber intrusions, electronic warfare (EW), and environmental obstacles. Military doctrine highlights flexibility, redundancy, and survivability as vital elements, ensuring that forces can remain connected even when main channels are lost (Heidari and Jabraeil Jamali, 2022; Karim and Rawat, 2023). The U.S. Army's Field Manual 6-02 (FM 6-02) presents the main principles of signal support, stressing the interoperability, resilience, and strong cybersecurity practices which are essential to achieving mission goals (Singh and Mishra, 2024). These principles become decisive in large-scale combat operations, where maintaining command and control (C2) often determines whether missions succeed or fail (Liu et al., 2023; Kufakunesu, 2024, Radovanovic et al., 2026).

The move from analog systems to digital platforms has brought significant improvements, including faster transfer of information, automated network control, and embedded encryption methods (Masuduzzaman et al., 2024; Rutravigneshwaran et al., 2024; Singh and Mishra, 2024). New technologies such as software-defined radios (SDRs), wideband satellite systems, and intelligent cyber defense tools have improved battlefield connectivity, making it possible to achieve immediate situational awareness and quicker command decisions (Azar et al., 2019; Joshi et al., 2023). Yet these advances do not remove long-standing problems, particularly overcrowding in the electromagnetic spectrum, the risk of jamming, and cyberattacks launched by hostile actors (Heidari et al., 2022).

Cybersecurity remains a central concern for all military communication systems. Digital warfare, espionage, and sabotage continue to endanger sensitive networks, requiring advanced encryption standards, quantum-resistant methods, and intrusion detection systems which respond quickly to vulnerabilities (Doku et al., 2020). The U.S. Department of Defense Information Network (DODIN) is critical in protecting military communication and applying multi-layer encryption, blockchain-based authentication, and adaptive firewalls to secure the data (Kunatsa et al., 2024). The use of artificial intelligence and machine learning to manage responses and detect intrusions is expected to transform the way military networks are protected in the

coming years (Liu et al., 2023; Masuduzzaman et al., 2024; Rutravigneshwaran et al., 2024).

This paper examines the present state of communication platforms in defense, their links with modern military technologies, and the challenges created by electronic warfare and hostile cyber activity. It also considers the emerging directions in the field, including quantum-based encryption, AI-supported battlefield networks, and the use of low-Earth orbit (LEO) satellites for defense communication (Akbar et al., 2024; Kufakunesu et al., 2024). By assessing these innovations and their role in ongoing operations, the research aims to outline the future path toward secure and resilient military communication platforms (Azar et al., 2019).

1 RESEARCH METHODOLOGY AND PURPOSE OF THE STUDY

This research follows a qualitative and doctrinal analytical methodology which examines military communication frameworks through official doctrine, scientific literature, and emerging technological concepts. The study synthesizes information from U.S. Army FM 6-02, NATO AJP-6.0 communications doctrine, and recent academic work to assess how communication platforms are evolving toward greater resilience, interoperability, and security. The methodology relies on a comparative analysis of existing doctrinal guidance, technological developments, and operational requirements relevant to secure communication in contested environments.

Based on this methodology, the study addresses the following research questions:

1. How do existing U.S. and NATO doctrinal frameworks define the principles of resilient military communication in modern operations?
2. What technological advances most significantly influence communication security, interoperability, and continuity in contested environments?
3. How can a layered communication framework enhance operational effectiveness in UAV-to-TOC mission profiles?

A layered communication framework enhances operational effectiveness in UAV-to-TOC mission profiles by structuring communication processes into distinct yet interdependent functional levels, each responsible for a specific aspect of secure and reliable exchange of information. In such mission environments, where unmanned aerial vehicles operate as forward sensing and data acquisition platforms while the Tactical Operations Center serves as the decision-making hub, the continuity and integrity of communication become critical for mission success.

The layered approach enables the systematic separation of concerns, allowing encryption, signal control, data transmission, adaptive connectivity, decision support, and network reinforcement to operate as coordinated components rather than isolated functions. This structural organization reduces system vulnerability by

ensuring that disruption in one layer does not lead to total communication failure. For example, even in the presence of electronic warfare activities such as jamming or spectrum interference, adaptive connectivity mechanisms can maintain alternative communication paths, while higher layers continue to process and validate incoming data.

Furthermore, the framework improves interoperability between heterogeneous systems deployed across air and ground segments. UAV platforms often rely on diverse communication technologies, including line-of-sight radio links, satellite communication, and data relay nodes. A layered structure harmonizes these technologies by providing standardized interfaces and protocols across layers, ensuring seamless integration with command systems at the TOC level. This directly contributes to faster data fusion, improved situational awareness, and more accurate decision-making.

Another important contribution of the layered framework lies in its support for real-time data prioritization and secure transmission. UAV-generated data, such as imagery, telemetry, and sensor intelligence, must be transmitted with minimal delay while preserving confidentiality and integrity. By embedding security mechanisms within each layer, including authentication, encryption, and intrusion detection, the framework ensures that sensitive information remains protected throughout the transmission process. At the same time, decision-support layers enable the filtering and analysis of incoming data, allowing commanders to focus on actionable intelligence rather than raw information streams.

The layered design supports scalability and adaptability in dynamic operational environments. UAV-to-TOC missions often evolve rapidly, requiring the communication system to adjust to changing network conditions, mission objectives, and threat levels. A modular layered framework allows for the integration of emerging technologies such as artificial intelligence, quantum-resistant encryption, and autonomous network management without disrupting the overall system architecture. This adaptability strengthens long-term operational resilience and ensures that communication capabilities remain aligned with future multi-domain operational requirements.

The contribution of this paper is threefold. First, it integrates doctrinal, technological, and operational perspectives into a unified conceptual model for resilient communication. Second, it introduces a structured six-layer framework tailored for multi-domain environments and coalition operations. Third, it identifies capability gaps and highlights future directions for enhancing military communication systems through AI-driven defense, quantum-secure methods, and multi-layer network protection mechanisms.

2 RELATED WORK

Research on military communication platforms has developed considerably in recent years, with technological progress, operational demands, and security risks guiding its direction. A number of academic studies and military doctrines have examined how digital networks, protection strategies, and tactical communication methods are being used in today's defense operations (Radovanovic et al., 2024). The replacement of analog systems with digital ones, the rise of intelligent network management, and the secure use of satellite communication have each been central in improving the performance of military communication systems (Mustafovski et al., 2025).

Interoperability has been identified as a central requirement for effective military communication, as it allows information to flow smoothly across different service branches and between allied forces (Doku et al., 2020, Radovanovic et al., 2023). Field Manual FM 6-02 of the U.S. Army highlights that success in joint missions relies on communication networks working together as one coordinated system. Studies underline that secure radio systems, software-defined radios (SDRs), and advanced satellite technologies provide the foundation for reaching this level of connectivity (Heidari et al., 2022). Table 1 presents a comparison between older and newer communication platforms, outlining how they differ in their data handling, protective measures, and flexibility (Mustafovski, 2025).

Table 1: Comparison of Traditional and Modern Military Communication Platforms

Feature	Conventional Frameworks	Proposed Secure Framework
Transmission Medium	Basic radio and satellite channels	Encrypted multi-layer digital networks with adaptive routing
Data Rate	Limited throughput	High-capacity, mission-optimized transfer speeds
Security	Susceptible to interception and disruption	Integrated end-to-end encryption with quantum-ready algorithms
Interoperability	Partial integration across services	Tailored joint and multinational compatibility
Adaptability	Static frequency and rigid protocols	Dynamic spectrum allocation with software-defined controls
Reliability in combat	Easily degraded by jamming and EW attacks	Maintains continuity under EW and cyber-contested environments

2.1 Doctrinal Foundation for Modern Military Communication

Modern military communication is guided by a combination of national and multinational doctrinal frameworks which define how forces establish, protect, and manage information exchange in complex operational environments. The U.S. Army's Field Manual 6-02 (FM 6-02) outlines the principles of signal support, emphasizing interoperability, resilience, network survivability, and secure information flow during all phases of operations. FM 6-02 provides the foundation for land force

communication, but its scope is limited to the Army and joint operations in which Army signal formations participate. For multinational and coalition contexts, additional doctrinal layers are required.

NATO doctrine AJP-6.0, which focuses on Communications and Information Systems (CIS), provides standardized guidance for planning, deploying, and protecting communication capabilities in Alliance operations. AJP-6.0 defines the roles of CIS nodes, COMSEC and EMSEC requirements, accreditation procedures, and the operational responsibilities necessary to maintain secure and interoperable networks between NATO partners. Closely related is AJP-3.20, which addresses cyber and electromagnetic activities (CEMA), and outlines how forces must coordinate electronic warfare, cyber defense, and spectrum management during operations. These doctrines stress the importance of layered protection, common standards, and coordinated procedures across allied forces.

Additionally, Joint Publication JP 6-0 offers complementary guidance for joint U.S. operations, detailing communication responsibilities at the strategic, operational, and tactical levels. JP 6-0 differentiates between service-specific communication support and multi-domain requirements, highlighting the need for unified network control and redundant pathways in contested environments. Another important doctrinal concept is Multi-Domain Operations (MDO), which requires communication architectures capable of supporting simultaneous activities across the land, air, sea, space, and cyber domains. MDO shifts the focus toward resilient networks which enable the rapid convergence of forces, synchronized actions, and continuous situational awareness.

Together, FM 6-02, NATO AJP-6.0, AJP-3.20, JP 6-0, and the MDO concept create a comprehensive doctrinal framework which informs the development of resilient communication systems. By aligning technical advancements with doctrinal principles, military organizations can better ensure that communication platforms remain interoperable, mission-driven, and able to withstand the combined pressure of electronic warfare, cyber threats, and physical disruption.

2.2 Advancements in Military Communication Platforms

The use of artificial intelligence (AI) and machine learning (ML) within defense communication networks has introduced the automated detection of intrusions, immediate data handling, and self-repairing network functions. Such systems are able to forecast cyber risks, allocate bandwidth effectively, and improve the flow of data in crowded networks, which leads to higher levels of efficiency in operations (Kufakunesu et al., 2024; Kunatsa et al., 2024; Radovanovic et al., 2025).

Satellite communication (SATCOM) remains a core element of extended-range missions, offering beyond-line-of-sight (BLOS) coverage, worldwide surveillance, and secure links for forces in the field (Liu, et al., 2023). Low-Earth Orbit (LEO)

satellites are increasingly used because of their shorter delay, faster transfer of information, and stronger protection against interference. They serve as a complement to geostationary satellites (GEO), creating a more reliable coverage system for distant and contested regions (Mustafovski, 2025).

2.3 Operational Resilience in Military Communication

As armed forces integrate digital systems into their operations, the ability to keep networks stable under pressure has become a decisive factor. Hostile states, organized cyber units, and irregular groups are persistently seeking to undermine the reliability of military communication infrastructure. Documented incidents targeting defense systems confirm the urgent requirement for strong layers of protection, continuous monitoring, and rapid-response detection mechanisms (Heidari et al., 2022).

Disruptions to operational communication can delay orders, expose sensitive data, or distort information needed for mission planning, creating serious risks for national defense (Mustafovski et al., 2025). The FM 6-02 doctrine stresses resilience measures such as encryption standards, traffic surveillance, and trusted transmission procedures to counter these challenges.

To strengthen resilience, armed forces are adopting new approaches including post-quantum protective methods, blockchain-based validation, and automated monitoring platforms. Defensive mechanisms which react instantly to network anomalies, combined with strict verification models, are now seen as essential components for safeguarding communication in contested environments.

2.4 CIS and CEMA Security Architecture

Secure military communication relies on well-defined security architecture which integrates communications and information systems (CIS) with cyber and electromagnetic activities (CEMA). CIS doctrine establishes the principles for protecting communication infrastructures, ensuring confidentiality, integrity, and the availability of information across all operational levels. Core elements of CIS security include communication security (COMSEC), emission security (EMSEC), and procedural controls which safeguard classified exchanges from interception, manipulation, or unauthorized disclosure.

COMSEC governs the encryption standards, key management, authentication processes, and protective measures used to secure voice and data transmission. These measures ensure that hostile actors cannot access sensitive information during operations. EMSEC addresses the protection of equipment and facilities from unintentional electromagnetic emissions which may reveal operational details or enable adversaries to reconstruct transmitted information. Together, COMSEC and EMSEC form essential components of any accredited military communication

system, particularly when operating within coalition environments where shared interoperability standards must be observed.

CEMA doctrine adds an additional layer of protection by coordinating cyber defense, electronic warfare, and spectrum management under a unified operational structure. Cyber defense focuses on intrusion detection, vulnerability assessment, and rapid response mechanisms which secure networks from malicious activities. Electronic warfare principles guide the mitigation of jamming, spoofing, and hostile control of the electromagnetic spectrum, ensuring that forces maintain access to critical frequencies during combat. Spectrum management ensures the organized allocation and safeguarding of frequencies required by joint and multinational units.

Modern architecture increasingly adopts zero trust principles, which require continuous verification of user identities, device integrity, and network access privileges. This approach eliminates reliance on perimeter-based defenses and introduces strict controls across all layers of communication. Accreditation frameworks define the procedures for validating that systems comply with the required security standards before deployment. These accreditation processes are especially important in coalition operations, where different nations must trust shared communication systems and adhere to NATO interoperability and security requirements.

By integrating CIS protection measures with CEMA responsibilities, armed forces create a comprehensive security architecture capable of withstanding cyber-attacks, electronic interference, and technical failures. This integrated approach reinforces the survivability of communication networks, enhances operational reliability, and supports the execution of complex missions in contested and hostile environments.

2.5 Strengthening Military Communication Frameworks

The development of future military communication frameworks is moving toward greater resilience, advanced protection, and integration with emerging technologies. Key areas of improvement include:

- Autonomous Network Defense: Intelligent systems will manage traffic loads, adjust connections in real time, and detect vulnerabilities before they can be exploited. Research conducted under the DARPA Cyber Hunting at Scale and Network Defense programs demonstrates how autonomous defensive agents can detect, classify, and mitigate network threats in real time (DARPA, 2023).
- Quantum-Secure Methods: The use of quantum key distribution (QKD) and encryption resistant to quantum computing will protect critical data exchanges. The National Institute of Standards and Technology has released post-quantum cryptography standards which outline requirements for

quantum-resilient key exchange and authentication mechanisms essential for future military networks (NIST, 2022).

- IoBT-Enabled Operations: The Internet of Battlefield Things (IoBT) will link sensors, vehicles, and wearables, creating predictive awareness and automated decision support. The U.S. Army Research Laboratory's Internet of Battlefield Things (IoBT) program provides empirical evidence on how distributed sensing, edge analytics, and adaptive mesh networks enhance connectivity in contested environments (U.S. Army ARL, 2021).
- Immersive Command Interfaces: Augmented reality and holographic displays will give commanders clearer control of missions and enhance coordination across units. NATO's Science and Technology Organization identifies augmented reality systems, cognitive decision-support tools, and resilient edge computing as priority areas for future command-and-control architecture (NATO STO, 2023). The U.S. Army's Integrated Visual Augmentation System (IVAS) program demonstrates how mixed-reality displays can integrate tactical data, navigation pathways, and communication overlays to improve situational awareness in dispersed formations (U.S. Army, 2021).

3 A LAYERED FRAMEWORK FOR RESILIENT MILITARY COMMUNICATION

The proposed framework introduces six structured layers that guarantee secure, adaptive, and mission-focused communication while reinforcing interoperability across services, combined task forces, and coalition partners.

Framework Layers and Functions:

1. Secure Initialization and Encryption Setup
    - Networks are established with multi-layer encryption across all operational units.
    - Optimization tools identify reliable links to reduce delay and congestion.
    - Quantum-resistant protocols safeguard transmissions from the outset.
2. Tactical Signal Control and Intrusion Monitoring
    - Systems monitor radio frequencies to detect jamming or hostile interference.
    - Adaptive spectrum control reallocates frequencies to sustain connections.
    - Authentication methods using distributed ledgers verify user access securely.
3. Integrated Multi-Domain Data Exchange
    - Edge devices and field sensors gather and share operational intelligence in real time.

- Voice instructions are converted into encrypted digital signals for instant relay.
- A unified command backbone enables coordination across land, air, sea, space, and cyber assets.

4. Adaptive Connectivity in Hostile Conditions
   - LEO satellites deliver responsive coverage, reducing dependency on ground stations.
   - Software-defined radios shift channels dynamically to counter electronic warfare.
   - Cloud-supported awareness platforms give leaders direct access to updated data.
5. Decision Support and Predictive Protection
   - Analytical tools evaluate live information to recommend tactical actions.
   - Forecast models identify cyber risks and deploy preventive defenses.
   - Automated resource tracking maintains operational logistics without disruption.
6. Ongoing Network Development and Reinforcement
   - Self-correcting systems strengthen weak points to ensure continuity.
   - Structured after-action assessments refine future communication effectiveness.
   - Encrypted archives protect mission data for long-term operational security (Mustafovski, 2025).

Table 2: Framework for Resilient Military Communication

Layer	Process	Technology Applied	Impact on Military Operations
1. Secure Initialization	Establishes multi-layer encryption and optimized links	Quantum-resistant protocols, adaptive routing	Reliable and protected mission startup
2. Signal Control & Monitoring	Detects jamming and reallocates spectrum securely	Distributed authentication, EW monitoring tools	Stronger defense against hostile interference
3. Multi-Domain Data Exchange	Shares intelligence across all operational domains	IoBT sensors, encrypted voice-to-data conversion	Seamless cooperation between land, air, sea, space, and cyber units
4. Adaptive Connectivity	Maintains links in contested environments	LEO satellite systems, SDR-based frequency agility	Sustained communications under electronic warfare
5. Decision Support Layer	Analyzes live data and forecasts threats	Predictive analytics, cyber risk modeling	Faster and more accurate command decisions

Layer	Process	Technology Applied	Impact on Military Operations
6. Network Reinforcement	Strengthens weak points and stores mission data securely	Self-healing networks, encrypted archival systems	Long-term resilience and secure mission continuity

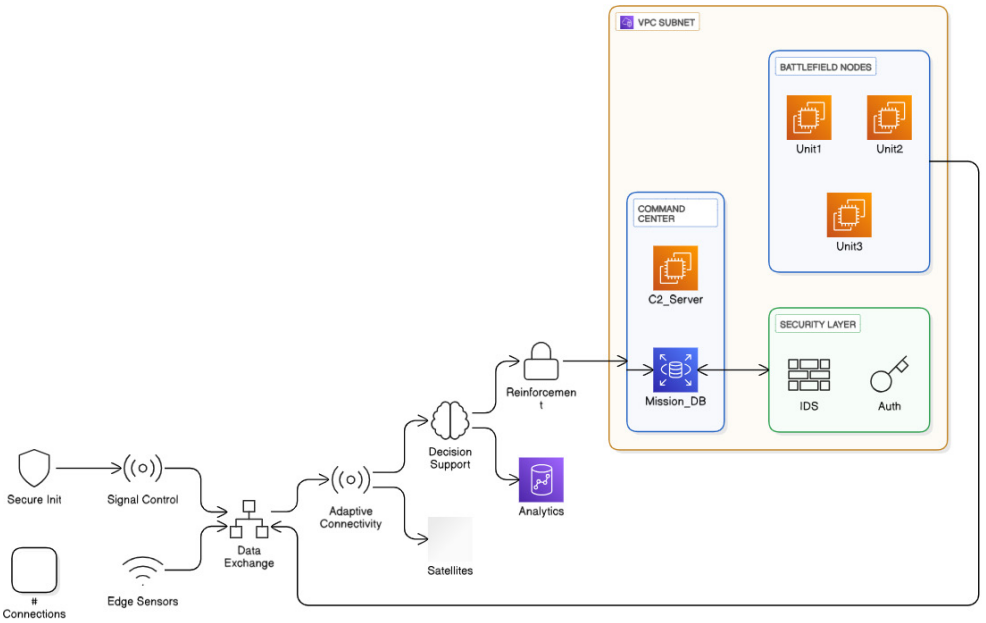

Figure 1: Layered Framework for Resilient Military Communication

Figure 1 illustrates the proposed layered framework, designed to ensure secure, adaptive, and mission-focused communication in modern military operations. The framework is composed of six interconnected layers:

1. Secure Initialization – establishes encrypted channels and ensures protected connectivity at the start of missions.

2. Signal Control – monitors the radio frequency environment, detects jamming attempts, and reallocates the spectrum dynamically to maintain communication.

3. Data Exchange – integrates information from edge sensors and field units, enabling real-time intelligence sharing across operational domains.

4. Adaptive Connectivity – employs Low Earth Orbit (LEO) satellites and software-defined radios (SDRs) to sustain resilient communication even in contested or degraded environments.

5. Decision Support – processes battlefield data through analytics to provide commanders with actionable insights and predictive threat modeling for faster and more accurate decision-making.

6. Reinforcement – secures mission data in protected databases, supported by intrusion detection systems (IDS) and authentication services, ensuring both long-term resilience and operational continuity.

The architecture emphasizes interoperability between command centers, battlefield nodes, and security layers, while incorporating external assets such as satellites and edge sensors. By integrating these components, the framework provides a communication infrastructure that resists electronic warfare, supports multi-domain operations, and preserves mission effectiveness under cyber and physical threats (Mustafovski, 2025).

Table 3: Impact of Resilient Communication Framework on Operational Effectiveness

Key Advantage	Conventional communication	Resilient Framework	Impact on Operations
Speed of Deployment	Manual configuration and delayed setup	Automated initialization with secure protocols	Faster preparation and improved mission readiness
Reliability in Combat	Susceptible to disruption and jamming	LEO satellite coverage with SDR-based flexibility	Sustained connectivity in contested environments
Cybersecurity	Basic encryption with limited protection	Multi-layer security with quantum-safe methods	Stronger defense of classified data and networks
Interoperability	Restricted to branch-specific systems	Unified backbone for joint and coalition forces	Smooth coordination across Allied operations
Threat Response	Manual monitoring and delayed reaction	Predictive detection with automated countermeasures	Preemptive defense against cyber and EW threats

The adoption of this resilient communication framework provides clear benefits for modern military operations. By automating deployment and securing initialization through advanced protocols, forces can achieve faster mission readiness with reduced delays. The integration of LEO satellites and software-defined radios ensures that communication remains stable even in contested or degraded environments, strengthening operational reliability in high-risk areas. Multi-layered security, supported by quantum-safe encryption, protects sensitive information from interception and manipulation, thereby reinforcing cyber defense. Interoperability across joint and coalition partners enables seamless coordination between different branches and allied nations, eliminating compatibility barriers. Finally, predictive detection and automated countermeasures allow proactive responses to cyber and electronic warfare threats, ensuring that forces maintain an information advantage throughout operations.

4 LIMITATIONS AND SCOPE

This study presents a conceptual analysis of resilient military communication frameworks, grounded in selected doctrinal sources and recent technological developments. The scope of the paper is limited to publicly available information from U.S. and NATO doctrinal publications, as well as open scientific literature on communication security and emerging technologies. Classified operational procedures, nation-specific implementation details, and system-level performance data are outside the boundaries of this research. The proposed framework does not aim to replace formal doctrinal guidance but to offer an integrated perspective which connects doctrinal principles with technological trends relevant to UAV-to-TOC communication contexts. Further, the analysis does not include empirical field testing or simulation-based validation, which would be required to evaluate performance under real operational conditions. The focus remains on outlining structural elements, identifying capability gaps, and highlighting areas where doctrinal and technological development converge.

Conclusion

The steady progress of military communication systems has reshaped the way modern conflicts are conducted, making it possible to reach decisions more quickly, coordinate forces more effectively, and secure information against outside threats. As technology becomes a decisive factor in warfare, armed forces need to rely on automated network tools, quantum-protected encryption, and real-time satellite links to preserve their advantage. The move from older analog radios and fixed-frequency systems to flexible, software-defined solutions supported by intelligent management now guarantees that units stay connected in dangerous and contested areas. Interoperability continues to be essential, allowing land, air, sea, space, and cyber elements to operate together under one integrated structure. The Unified Command Network (UCN), with added real-time language translation and secure blockchain-based access, gives coalition partners the ability to share intelligence, plan logistics, and carry out missions without technical barriers. The expansion of Low Earth Orbit (LEO) satellites further reduces reliance on ground installations, making uninterrupted beyond-line-of-sight communication possible in remote regions. Protecting these networks remains critical, since digital attacks are evolving quickly. Intrusion detection, resilient self-healing systems, and encryption designed to resist quantum computing will shield operations against espionage, electronic warfare, and cyber disruption. Forecasting tools and automated defenses also strengthen early warning capabilities, ensuring that vulnerabilities are contained before they can be exploited.

The future of military communication will be marked by flexibility, intelligence, and security, offering armed forces a foundation for more reliable coordination and battlefield resilience. By combining autonomous management, predictive defense, and cross-domain connectivity, commanders will benefit from broader situational awareness, quicker reactions, and more decisive action. These developments will not only improve combat effectiveness in the short term, but also secure long-term

dominance in complex operational environments. The ability to maintain secure, rapid, and dependable communication will be the factor that defines military success in the digital age of conflict.

Future research should include empirical validation of the proposed framework through field experiments, controlled simulations, or operational case studies designed to observe communication performance in contested environments. Additional work is needed to analyze the impact of emerging technologies, such as quantum-resilient encryption, low Earth orbit satellite networks, and AI-supported defensive tools, on the resilience of coalition communication systems. Examining the interoperability of national and multinational communication architecture, particularly within NATO structures, would further strengthen the practical relevance of the model. Expanding the analysis to include mission-specific requirements for air, land, maritime, and cyber forces may also provide a broader operational foundation for future developments.

References

1. *Akbar, R. S., Kholid, F., Kasiyanto, K., Widiatmoko, D., Achmad, A., 2024. Design of Fuel Monitoring Application for Reservoir Tanks in Army Fuel Supply Point on Military Logistics Corps Based on Internet of Things. International Journal of Engineering and Computer Science Applications (IJECSA), 3(1): pp 19–32. DOI: 10.30812/ijecsa.v3i1.3737.*
2. *Alkanjr, B., Mahgoub, I., 2023. A novel deception-based scheme to secure the location information for IoBT entities. IEEE Access, 11: pp 15540–15554. DOI: 10.1109/ACCESS.2023.3244138.*
3. *Azar, J., Makhoul, A., Barhamgi, M., Couturier, R., 2019. An energy efficient IOT data compression approach for Edge Machine Learning. Future Generation Computer Systems, 96: pp 168–175. DOI: 10.1016/j.future.2019.02.005.*
4. *Butun, I., Mahgoub, I., 2024. Expandable mix-zones as a deception technique for providing location privacy on internet-of-battlefield things (IoBT) deployments. IEEE Access, 12: pp 149647–149661. DOI: 10.1109/ACCESS.2024.3461609.*
5. *DARPA, 2023. Cyber Hunting at Scale and Network Defense Program Report. Defense Advanced Research Projects Agency, Arlington, USA.*
6. *Doku, R., Rawat, D. B., Garuba, M., Njilla, L., 2020. Fusion of named data networking and blockchain for resilient internet-of-battlefield-things. 2020 IEEE 17th Annual Consumer Communications and Networking Conference (CCNC). DOI: 10.1109/CCNC46108.2020.9045395.*
7. *Farooq, M. J., Zhu, Q., 2018. On the secure and reconfigurable multi-layer network design for critical information dissemination in the internet of battlefield things (IoBT). IEEE Transactions on Wireless Communications, 17(4): pp 2618–2632. DOI: 10.1109/TWC.2018.2799860.*
8. *Feng, Y., Li, M., Zeng, C., Liu, H., 2020. Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective. Entropy, 22(10), 1166. DOI: 10.3390/e22101166.*
9. *Heidari, A., Jabraeil Jamali, M. A., 2022. Internet of things intrusion detection systems: A comprehensive review and Future Directions. Cluster Computing, 26(6): pp 3753–3780. DOI: 10.1007/s10586-022-03776-z.*

10. *Joshi, S., Thakar, A., Patel, C., 2023. Applications of Machine Learning and Deep Learning in Securing Internet of Battlefield Things: A Futuristic Perspective. 10th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, pp 333–338.*
11. *Karim, H., Rawat, D. B., 2023. Evaluating Machine Learning Classifiers for Data Sharing in Internet of Battlefield Things. IEEE Symposium Series on Computational Intelligence (SSCI): pp 1–7.*
12. *Kufakunesu, R., Myburgh, H., De Freitas, A., 2024. The Internet of Battle Things: A Survey on Communication Challenges and Recent Solutions. Discover Internet of Things, pp 3–19.*
13. *Kunatsa, T., Myburgh, H., De Freitas, A., 2024. Optimal Power Flow Management for a Solar PV-Powered Soldier-Level Pico-Grid. Energies, 459.*
14. *Liu, D., Abdelzaher, T., Wang, T., Hu, Y., Li, J., Liu, S., Caesar, M., Kalasapura, D., Bhattacharyya, J., Srour, N., 2023. IoBT-OS: Optimizing the Sensing-to-Decision Loop for the Internet of Battlefield Things. IEEE International Conference on Computer Communications and Networks (ICCCN): pp 1–10.*
15. *Masuduzzaman, M., Rahim, T., Islam, A., Shin, S. Y., 2024. UAV-Employed Intelligent Approach to Identify Injured Soldier on Blockchain-Integrated Internet of Battlefield Things. IEEE Transactions on Network and Service Management.*
16. *Mustafovski, R., 2025. The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness, Database Systems Journal Vol. XVI/2025: pp 1–11.*
17. *Mustafovski, R., Petrovski, A., Radovanovic, M., 2025. Integrating Quantum Technologies into Mobile Military Systems and Toc Frameworks. Land Forces Academy Review, 30(3): pp 466–478. DOI: 10.2478/raft-2025-0045.*
18. *Mustafovski, R., Petrovski, A., Radovanovic, M., 2025. Leveraging Satellite Technologies for Enhanced Humanitarian Aid and Crisis Management: A Scenario-Based Analysis. The Crisis Management and Disaster Response Centre of Excellence (CMDR COE), Sofia, Bulgaria, pp 127–140.*
19. *NATO STO, 2023. Emerging and Disruptive Technologies for Command and Control. NATO Science and Technology Organization, Brussels, Belgium.*
20. *NIST, 2022. Post-Quantum Cryptography Standards: Finalized Algorithms and Guidelines. National Institute of Standards and Technology, Gaithersburg, USA.*
21. *Radovanović, M., Akhundov, R. G., Hashimov, E. G., 2026. Artificial intelligence for decision support in multidomain military command and control. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. шістнадцятої міжнар. наук.-техн. конф., pp 48–51. https://repository.kpi.kharkov.ua/handle/KhPI-Press/101682 (Accessed 10 February 2026).*
22. *Radovanovic, M., Jokić, Ž., Petrovski, A., Mustafovski, R., 2025. Smart Modular Platforms for the Next Generation of Shooting Range Training. Scientific Technical Review, 75(1): pp 41–51. DOI: 10.5937/str00006R.*
23. *Radovanović, M., Petrovski, A., Behlić, A., Zied Chaari, M., Hashimov, E. G., Fellner, R., Agbeyangi, A. O., 2024. Unleashing Autonomous Forces: Integrating AI-Driven Drones in Modern Military Strategy. Control, Navigation and Communication Systems, 77(3): pp 55–69, DOI: 10.26906/SUNZ.2024.3.055.*
24. *Radovanović, M., Petrovski, A., Žnidaršič, V., Behlic, A., 2023. The C5ISR System Integrated with Unmanned Aircraft in the Large-Scale Combat Operations. Vojenské rozhledy, 32(2): 98–118. DOI: 10.3849/2336-2995.32.2023.02.098-118.*
25. *Rutravigneshwaran, P., Anitha, G., Prathapchandran, K., 2024. Trust-Based Support Vector Regressive (TSVR) Security Mechanism to Identify Malicious Nodes in the Internet of Battlefield Things (IoBT). International Journal of System Assurance Engineering and Management, pp 287–299.*

26. *Singh, R. K., Mishra, S., 2024. TinyML Meets IoBT Against Sensor Hacking. The Network and Distributed System Security (NDSS) Symposium, Workshop on Security and Privacy in Standardized IoT (SDIoTSec): pp 1–9.*
27. *U.S. Army ARL, 2021. Internet of Battlefield Things (IoBT) Research Program Overview. Army Research Laboratory, Adelphi, USA.*
28. *U.S. Army, 2021. Integrated Visual Augmentation System (IVAS) Soldier Lethality Program Summary. Department of the Army, Washington, D.C., USA.*
29. *Wigness, M., Abdelzaher, T., Russell, S., Swami, A., 2022. Internet of battlefield things: Challenges, opportunities, and emerging directions. IoT for Defense and National Security, pp 5–22. DOI: 10.1002/9781119892199.ch1.*

Email: rexhep.mustafovski@ugd.edu.mk

ORCID: 0009-0000-3257-0989

Email: markoradovanovicgdb@yahoo.com

ORCID: 0000-0002-9866-9639

Email: aleksandar.petrovski@ugd.edu.mk

ORCID: 0000-0002-5265-5813

Mag. Rexhep Mustafovski je pedagoški in raziskovalni asistent na Vojaški akademiji »General Mihailo Apostolski« v Skopju na Oddelku za kibernetično varnost in digitalno forenziko. Habilitiran je tudi na Univerzi Goce Delčev v Štipu v Severni Makedoniji. Raziskovalno se ukvarja s področjem kibernetske varnosti, varnih vojaških komunikacij, komunikacijskih sistemov brezpilotnikov itn.

Rexhep Mustafovski, MSc, is a Teaching and Research Assistant at the Military Academy General Mihailo Apostolski – Skopje, Department for Cybersecurity and Digital Forensics. He is also affiliated with Goce Delcev University – Stip, North Macedonia. His research work is focused on cybersecurity, secure military communications, UAV communication systems etc.

Email: rexhep.mustafovski@ugd.edu.mk

ORCID: 0009-0000-3257-0989

Mag. Marko Radovanović je dokončal magistrski študij na Univerzi v Beogradu in je trenutno inštruktor vojaških veščin na Vojaški akademiji v Beogradu, kjer uči taktiko z oborožitvenimi sistemi. Je avtor več znanstvenih in strokovnih člankov s področja vojaške znanosti, taktike, oborožitvenih sistemov itn.

Marko Radovanović, MSc, has graduated his master study at the University of Belgrade and he is currently an instructor of military skills at the Military Academy in Belgrade, where he teaches tactics with weapon systems. He has authored several dozen scientific and professional papers in the fields of military sciences, tactics, weapon systems, etc.

Email: markoradovanovicgdb@yahoo.com

ORCID: 0000-0002-9866-9639

Izr. prof. dr. Aleksandar Petrovski je od leta 2022 izredni profesor na Oddelku za vojaške znanosti in veščine in vodja Laboratorija za geografske informacijske sisteme na Vojaški akademiji General Mihailo Apostolski v Skopju. Je avtor več znanstvenih in strokovnih člankov, sodeloval je v več raziskovalnih in znanstvenih projektih.

Assoc. Prof. Aleksandar Petrovski, PhD, has held since 2022 the position of Associate Professor in the Department of Military Sciences and Skills and has also been appointed Head of the GIS Laboratory at the Military Academy "General Mihailo Apostolski" in Skopje. He has authored numerous scientific and professional papers and has participated in several research and scientific projects.

Email: aleksandar.petrovski@ugd.edu.mk

ORCID: 0000-0002-5265-5813