The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness

Rexhep MUSTAFOVSKI
Ss. Cyril and Methodius University
Faculty of Electrical Engineering and Information Technologies
Skopje, Republic of North Macedonia
rexhepmustafovski@gmail.com

Abstract: *The way communication platforms are used in military operations has changed a lot over the years. They're now essential for mission success, quick decision-making, and maintaining strategic advantages. This paper dives into the modern communication tools that are making waves in military settings, with a spotlight on networked communication, signal support, cybersecurity strategies, and how different forces work together in joint and multinational missions. It also tackles some of the major hurdles, like congestion in the electromagnetic spectrum, cyber threats, and the need for secure data transmission in challenging environments. By pulling insights from FM 6-02: Signal Support to Operations and the latest scientific research, this paper highlights recent advancements in military communication tech and how they boost operational effectiveness. Additionally, the research looks ahead at future possibilities, such as AI-driven communication platforms, quantum encryption, and cutting-edge satellite networks for defense purposes. This paper's primary contribution is the development of a structured, AI-enabled communication workflow that integrates quantum-safe encryption, blockchain authentication, and satellite-based coordination to improve decision-making and resilience in multi-domain operations.*
Keywords: *Military communication, secure networks, battlefield connectivity, radio systems, cybersecurity, signal support, tactical communications, AI in defense*

1 Introduction

The effectiveness of military operations depends heavily on reliable, secure, and adaptable communication platforms. As modern warfare becomes increasingly network-centric, the ability to transmit real-time information across multiple operational domains—land, air, sea, space, and cyberspace—has become a strategic necessity. Military communication systems have evolved to integrate advanced radio networks, satellite-based communication, and encrypted data transmission, ensuring seamless coordination between deployed forces and command centers [1], [3], [5]. The increasing complexity of multinational operations, joint task forces, and asymmetric warfare has further emphasized the need for highly secure and interoperable communication infrastructures that can operate even in contested environments [6]–[8].

A key aspect of modern military communication is signal support, which provides robust network connectivity and ensures continuous information flow despite cyber threats, electronic warfare (EW) attacks, and environmental disruptions. Military doctrines emphasize the importance of agility, redundancy, and survivability in communication networks, ensuring that forces remain operational even when primary channels are compromised [9], [11]. The U.S. Army's Field Manual 6-02 (FM 6-02) outlines fundamental principles of signal support, including interoperability, network resilience, and cybersecurity strategies essential for mission success [17]. These principles are crucial in large-scale combat operations, where the ability to maintain command and control (C2) can determine operational success or failure [12], [14].

The transition from analog to digital military communication platforms has introduced a range of advantages, such as higher data

transfer rates, AI-assisted network management, and automated encryption protocols [15]–[17]. The introduction of software-defined radios (SDRs), wideband satellite networks, and AI-driven cyber defense mechanisms has further enhanced battlefield communication, allowing for real-time situational awareness and faster decision-making [4], [10]. However, despite these advancements, challenges remain, particularly regarding electromagnetic spectrum congestion, jamming threats, and cyberattacks from adversarial forces [7], [9].

Cybersecurity remains one of the most critical concerns in military communication platforms. Cyber warfare, espionage, and digital sabotage pose a significant risk to military networks, requiring advanced encryption techniques, quantum-safe cryptographic methods, and AI-based intrusion detection systems to mitigate vulnerabilities [6], [8]. The Department of Defense Information Network (DODIN) plays a crucial role in securing data transmission, integrating multi-layer encryption protocols, blockchain-based authentication, and adaptive firewall mechanisms [13], [16]. The role of artificial intelligence and machine learning in automating cybersecurity responses and threat detection is expected to further revolutionize military communication strategies [14]–[17].

This paper explores the current state of military communication platforms, their integration with modern defense technologies, and the challenges posed by electronic warfare and cybersecurity threats. The study also discusses future trends in military communication, including quantum encryption, AI-assisted battlefield networking, and low-Earth orbit (LEO) satellite communication systems [2], [5], [12]. By analyzing these technological advancements and their impact on military operations, this research aims to provide valuable insights into the future of secure and resilient communication platforms in defense applications [1], [4], [8].

The main scientific contribution of this study lies in its proposal of an adaptive workflow for next-generation military communication platforms. By integrating AI-driven automation, blockchain security, and low-latency satellite connectivity, the paper introduces a novel architecture that significantly enhances tactical coordination, cyber resilience, and real-time situational awareness in hostile environments.

2 Literature Review

The study of military communication platforms has evolved significantly in recent years, with various technological advancements, operational challenges, and security concerns shaping the field. Several scholarly works and military doctrines have explored the integration of digital communication networks, cybersecurity measures, and tactical communication strategies in modern warfare [1]–[3]. The transition from analog to digital systems, the emergence of AI-driven networking, and the adoption of secure satellite communications have played a crucial role in improving the efficiency of military communication platforms [4], [5].

One of the key components of military communication is interoperability, which ensures seamless information exchange between different branches of the armed forces and multinational coalitions [6], [7]. The U.S. Army's Field Manual FM 6-02 emphasizes the importance of joint operations, where different communication networks must operate efficiently under a unified system [17]. Research highlights the role of secure radio networks, software-defined radios (SDRs), and advanced satellite communication systems in achieving this goal [8], [9]. Table 1 provides an overview of traditional vs. modern military communication platforms, showing their differences in terms of data transmission, security, and adaptability.

Table 1. Comparison of Traditional and Modern Military Communication Platforms

Feature	Traditional Communication	Modern Digital Communication
Transmission Medium	Analog radio signals	Encrypted digital networks
Data Rate	Low	High-speed broadband
Security	Vulnerable to interception	End-to-end encryption & AI-based security
Interoperability	Limited	Fully integrated with joint/multinational operations
Adaptability	Fixed-frequency systems	Software-defined, frequency-agile systems
Reliability in Combat	Prone to jamming	Resistant to EW & cyber threats

While prior studies have discussed individual elements such as AI, SDRs, or satellite systems, this paper uniquely proposes an integrated framework combining these technologies with blockchain and quantum encryption. The proposed workflow advances beyond existing architecture by offering real-time threat adaptation, predictive decision support, and unified cross-domain operations, which are not concurrently addressed in existing literature.

2.1 Advancements in Military Communication Platforms

The integration of AI and machine learning (ML) in military communication networks has allowed automated threat detection, real-time data processing, and network self-healing capabilities [10], [11]. AI-based systems can predict cyber threats, manage bandwidth distribution, and optimize data transmission in congested environments, significantly enhancing operational efficiency [12], [13].

Satellite communication (SATCOM) plays a pivotal role in long-range military operations, providing beyond-line-of-sight (BLOS) connectivity, global reconnaissance, and secure battlefield networking [14], [15]. Low-Earth Orbit (LEO) satellites have gained popularity due to their low latency, high-speed data transmission, and enhanced resilience against jamming [16], [17]. These systems complement traditional geostationary satellites (GEO), ensuring continuous coverage in remote and contested environments. Table 2 highlights the differences between various satellite communication technologies used in military operations.

Table 2. Comparison of Military Satellite Communication Technologies

Feature	Geostationary Satellites (GEO)	Medium Earth Orbit (MEO)	Low Earth Orbit (LEO)
Altitude	~35,786 km	~5,000–20,000 km	~500–1,500 km
Latency	High (~500ms)	Moderate (~200ms)	Low (~50ms)
Coverage	Global but with delay	Regional	High-speed global coverage
Jamming Resistance	Moderate	High	Very High
Data Transfer Speed	Limited	Moderate	High-speed broadband
Deployment Cost	High	Moderate	Lower than GEO/MEO

2.2 Cybersecurity Challenges in Military Communication

As digital transformation continues in military operations, cybersecurity remains a critical challenge. Hostile actors, state-sponsored cyber units, and non-state entities are continuously attempting to exploit vulnerabilities in military networks [5], [6]. Recent cyber-attacks on defense infrastructures highlight the necessity for multi-layered encryption, real-time intrusion detection, and AI-driven anomaly detection systems [7]–[9].

Cyber threats can disrupt battlefield communications, intercept classified intelligence, or manipulate strategic data, leading to severe consequences on national security. The FM 6-02 doctrine outlines cyber protection measures, including encryption protocols, threat monitoring, and secure data transmission techniques to mitigate these risks [17].

To address these cybersecurity concerns, military forces are investing in post-quantum encryption, blockchain authentication, and AI-driven cybersecurity tools [10], [11]. Automated network defense mechanisms, combined with zero-trust security models, are expected to play a crucial role in securing military communication networks [12], [13].

2.3 Future Trends in Military Communication Platforms

The future of military communication is being shaped by AI-driven automation, quantum-safe encryption, and next-generation tactical communication platforms. Some of the emerging trends include:

- AI-Powered Autonomous Networks: AI-driven systems will automate network management, optimize signal transmission, and predict potential threats [14].
- Quantum Communication: The adoption of quantum key distribution (QKD) and quantum-safe encryption will enhance data security in military operations [15], [16].
- Integrated IoT-based Defense Systems: The Internet of Battlefield Things (IoBT) will enable real-time sensory integration, predictive analytics, and automated reconnaissance [17].
- Augmented Reality (AR) Communication: The use of AR and holographic battlefield interfaces will improve situational awareness and mission coordination [9], [10].

3 A New Workflow for the Next Generation of Military Communication Systems

The proposed workflow consists of six key stages, ensuring secure, adaptive, and mission-driven communication that enhances interoperability among military branches, joint task forces, and multinational coalitions.

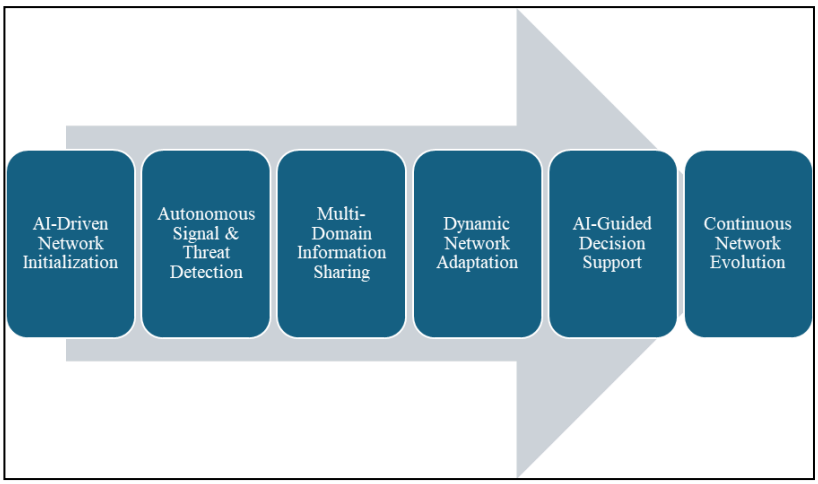

Fig. 1. Workflow for the Next Generation of Military Communication Systems

- **Workflow Steps and Explanation:**

1. **AI-Driven Network Initialization & Configuration**
   - The network automatically establishes a secure and encrypted connection across all deployed units.
   - AI-based network optimization identifies the best communication pathways to minimize latency and bandwidth congestion.
   - Quantum encryption secures data transmission from the start to prevent cyberattacks.

2. **Autonomous Tactical Signal Management & Threat Detection**
   - AI-powered systems continuously monitor radio frequency (RF) environments for jamming attempts or cyber threats.
   - Smart spectrum management automatically adjusts frequency usage, ensuring optimal connectivity in contested environments.
   - Blockchain-based authentication ensures that only authorized personnel can access sensitive communications.

3. **Real-Time Multi-Domain Information Sharing**
   - Edge computing and IoT sensors collect, analyze, and distribute battlefield intelligence instantly.
   - AI-based speech recognition converts voice commands into encrypted digital messages for secure, instant dissemination.
   - Unified Command Network (UCN) ensures seamless communication between land, air, sea, space, and cyber forces.

4. **Dynamic Network Adaptation in Combat Environments**
   - Low-Earth Orbit (LEO) satellite networks provide real-time battlefield coverage, reducing reliance on vulnerable ground infrastructure.
   - SDR-based radio networks dynamically switch frequencies to avoid electronic warfare (EW) interference.
   - Cloud-based situational awareness platforms allow commanders to access real-time intelligence anywhere.

5. **AI-Guided Decision Support & Predictive Analytics**
   - AI-powered battlefield assistants analyze incoming data and recommend the best tactical responses based on real-time intelligence.
   - Predictive cybersecurity models anticipate cyber threats and apply preemptive countermeasures.
   - Automated logistical coordination ensures supply chains remain intact and uninterrupted.

6. **Continuous Network Evolution & Learning**
   - Self-healing networks use machine learning (ML) to identify weak points and automatically reinforce connectivity.
   - AI-based after-action reviews (AARs) analyze communication effectiveness and optimize future missions.
   - Secure post-mission data storage ensures historical operational records remain classified and protected.

Table 3. Workflow for Next-Generation Military Communication

Step	Process	Technology Used	Impact on Military Operations
1. AI-Driven Network Initialization	Automatic secure connections & encrypted channels	AI-driven routing, quantum encryption	Faster & safer mission readiness
2. Autonomous Signal & Threat Detection	Real-time RF scanning & adaptive spectrum use	AI-assisted EW defense, blockchain security	Enhanced jamming resistance & secure access control
3. Multi-Domain Information Sharing	Seamless cross-platform communication	IoT-based intelligence, AI speech recognition	Faster battlefield awareness
4. Dynamic Network Adaptation	Resilient satellite & SDR-based networks	LEO satellites, cloud-based ops centers	Reliable comms in contested environments
5. AI-Guided Decision Support	AI-driven battlefield analysis & predictive logistics	AI-powered analytics threat modeling	Improved decision-making speed
6. Continuous Network Evolution	Self-healing networks & adaptive AI	ML-based security, after-action data analysis	Long-term resilience & future optimization

The proposed next-generation military communication workflow will revolutionize military operations by providing:

1. **Uninterrupted Communication in High-Risk Environments**
   - AI-powered adaptive frequency shifting and SDR ensure continuous connectivity even under electronic warfare conditions.
   - Decentralized blockchain authentication prevents data spoofing or interference.
   - LEO satellites ensure resilient BLOS (Beyond-Line-of-Sight) communication in remote areas.

2. **Improved Decision-Making & Tactical Coordination**
   - AI-driven command assistants analyze real-time battlefield data and offer rapid, informed decision recommendations.
   - Enhanced situational awareness allows commanders to adapt quickly based on automated intelligence reports.
   - Interoperable networks enable seamless collaboration among land, air, sea, and cyber units.

3. **Faster Deployment & Readiness**
   - AI-driven network automation reduces deployment times by instantly configuring communication systems.
   - Autonomous security systems ensure data protection from cyberattacks before missions begin.
   - Predictive analytics assist in early detection of potential threats, ensuring forces are prepared.

4. **Advanced Cybersecurity Protection Against Digital Threats**
   - AI-driven cybersecurity models predict malware, phishing, and cyber-intrusion attempts before they happen.
   - Quantum-safe encryption ensures that classified military data remains unbreakable.
   - Dynamic firewall systems prevent adversaries from exploiting communication vulnerabilities.

5. **Greater Interoperability Between Allied Forces**
   - The Unified Command Network (UCN) ensures that all allied forces, regardless of branch or nation, can

communicate without compatibility issues.
- Standardized AI-assisted voice translation systems allow seamless communication between different military forces in multinational operations.
- The integration of cloud-based command centers enables real-time data access from global military installations.

Table 4. Impact of Next-Generation Military Communication on Operational Success

Key Advantage	Traditional Communication	Next-Generation Communication	Impact on Operations
Speed of Deployment	Manual setup & configuration	AI-automated network setup	Reduced setup time & faster mission readiness
Reliability in Combat	Prone to jamming	Adaptive SDRs & LEO satellites	Continuous connection in high-risk areas
Cybersecurity	Encryption only	AI-driven security & quantum-safe encryption	Stronger data protection & cyber resilience
Interoperability	Limited to branch-specific networks	Unified Command Network (UCN)	Seamless allied coordination
Threat Response	Manual security checks	AI-assisted real-time anomaly detection	Preemptive cyber defense measures

4 Challenges in Implementing the Proposed Next-Generation Military Communication Platform

While the proposed AI-driven, quantum-encrypted, and multi-domain military communication platform offers significant advantages in security, interoperability, and efficiency, its implementation presents several challenges. Military environments demand high resilience, rapid adaptability, and uncompromising security, making the integration of advanced technologies a complex and resource-intensive endeavour. Below are the key challenges that must be addressed for successful deployment.

a. Cybersecurity Threats and Quantum-Resistant Encryption

One of the most significant challenges in implementing this next-generation communication platform is ensuring robust cybersecurity. Military networks are prime targets for cyber warfare, espionage, and digital sabotage by state-sponsored actors and sophisticated adversaries. The adoption of quantum encryption enhances security, but the transition from traditional encryption methods poses integration challenges, high computational costs, and compatibility issues with legacy systems. Additionally, AI-powered cybersecurity tools must be rigorously tested to avoid vulnerabilities that adversaries could exploit.

b. Electromagnetic Spectrum Management and Jamming Resistance

Modern warfare relies heavily on the electromagnetic spectrum for secure radio, satellite, and networked communication. However, spectrum congestion, frequency interference, and electronic warfare (EW) attacks pose severe threats. Adaptive frequency hopping, AI-driven spectrum allocation, and SDR (Software-Defined Radios) help mitigate these risks, but their deployment requires extensive testing in real-world combat scenarios. Additionally, adversaries constantly develop advanced jamming and spoofing techniques, making continuous adaptation and countermeasure development essential.

c. Interoperability with Legacy and Allied Systems

Military forces operate with a mix of old and new communication technologies, making interoperability a major concern. Many allied forces and joint coalitions use different encryption standards, radio frequencies, and data-sharing protocols, requiring a universal framework to ensure seamless communication. The proposed Unified Command Network (UCN) can enhance cross-force connectivity, but integrating diverse national defense systems into a single secure framework is a technically and politically complex challenge.

d. AI and Automation Risks in Battlefield Decision-Making

The integration of AI-driven decision support systems and automated battlefield analytics enhances efficiency but also introduces risks related to machine bias, decision latency, and potential adversarial manipulation. AI must interpret real-time battlefield data with high accuracy, but errors in object classification, speech recognition, or enemy movement prediction can lead to tactical failures. Additionally, AI's reliance on massive data sets raises concerns about data security, ethical considerations, and the risk of enemy AI-based countermeasures.

e. Infrastructure Deployment in Remote and Hostile Environments

Deploying a resilient, battlefield-ready communication infrastructure requires secure, mobile, and easily maintainable networking equipment. Remote operations—such as desert, jungle, or arctic warfare—face logistical challenges in establishing LEO satellite links, maintaining power sources, and protecting hardware from environmental stressors. Military-grade energy-efficient, solar-powered, and autonomous relay nodes can help mitigate these issues, but ensuring long-term network uptime remains a challenge.

f. High Costs and Budget Constraints

The development, testing, and large-scale implementation of next-generation military communication networks require substantial investment. Quantum-safe encryption, AI-driven cybersecurity, and satellite-based networking involve expensive research, hardware procurement, and system training costs. Many military organizations face budget constraints, long procurement cycles, and policy debates that could delay adoption and full-scale deployment.

g. Resistance to Change and Human Adaptation

The shift to AI-enhanced, real-time, and automated communication platforms may face resistance from military personnel accustomed to traditional systems. Soldiers and commanders require extensive training to operate new encrypted networks, AI-driven interfaces, and cloud-based data-sharing platforms. Without proper user adaptation, trust, and operational readiness, even the most advanced system could fail under real-world combat pressure.

5 Conclusion

The rapid advancement of military communication platforms has redefined modern warfare, enabling faster decision-making, improved battlefield coordination, and enhanced cybersecurity. As conflicts become more technologically driven, military forces must adopt AI-driven automation, quantum-safe encryption, and real-time satellite-based connectivity to maintain operational superiority. The transition from traditional analog and single-frequency radio systems to adaptive, software-defined networks and AI-enhanced communication infrastructures ensures that military units remain connected even in contested, high-risk environments. Interoperability remains a cornerstone of future military communication, enabling seamless integration among different

branches, joint forces, and multinational coalitions. The Unified Command Network (UCN), enhanced by AI-assisted real-time speech translation and blockchain authentication, will allow allied forces to share intelligence, coordinate logistics, and execute joint operations without compatibility issues. Additionally, the deployment of LEO satellite networks will significantly reduce reliance on vulnerable ground-based infrastructure, ensuring uninterrupted connectivity and beyond-line-of-sight (BLOS) communication in remote battlefields. Cybersecurity is another crucial factor in military communication, as digital threats continue to evolve. AI-powered threat detection, self-healing networks, and quantum-resistant encryption will provide unparalleled protection against cyber espionage, electronic warfare, and digital sabotage. The integration of predictive analytics and automated cyber-defense mechanisms ensures preemptive threat mitigation before hostile actors can exploit vulnerabilities.

The next generation of military communication will be more adaptive, intelligent, and secure, offering greater operational flexibility and resilience. By integrating AI, autonomous network management, and multi-domain interoperability, military forces can achieve superior situational awareness, faster response times, and enhanced combat effectiveness. These advancements will not only strengthen battlefield capabilities but also ensure long-term strategic dominance in modern and future conflicts. Military success will increasingly depend on who can communicate faster, more securely, and more efficiently in the evolving digital battlespace.

References

[1] Abdelzaher, Tarek / Wigness, Mike / Russell, Sean / Swami, Ananthram: *Internet of Battlefield Things: Challenges, Opportunities, and Emerging Directions.* IoT for Defense and National Security, 2023, pp. 5–22.

[2] Akbar, Ridho S / Kholid, Fadhil / Kasiyanto, Kharis / Widiatmoko, Donny / Achmad, Agus: *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), 2024, pp. 19–32.

[3] Alkanjr, Bilal / Mahgoub, Ibrahim: *A Novel Deception-Based Scheme to Secure the Location Information for IoBT Entities.* IEEE Access, 2023, pp. 15–554.

[4] Azar, Jad / Makhoul, Amal / Barhamgi, Mounira / Couturier, Raphael: *An Energy Efficient IoT Data Compression Approach for Edge Machine Learning.* Future Generation Computer Systems, 2023, pp. 168–175.

[5] Butun, Ismail / Mahgoub, Ibrahim: *Expandable Mix-Zones as a Deception Technique for Providing Location Privacy on Internet-of-Battlefield Things (IoBT) Deployments.* IEEE Access, 2024.

[6] Doku, Reginald / Rawat, Danda B / Garuba, Muritala / Njilla, Laurent: *Fusion of Named Data Networking and Blockchain for Resilient Internet-of-Battlefield-Things.* IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2023, pp. 1–6.

[7] Farooq, M. Junaid / Zhu, Quanyan: *Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT).* IEEE Transactions on Wireless Communications, 2023, pp. 2618–2632.

[8] Feng, Yujie / Li, Ming / Zeng, Chen / Liu, Hu: *Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective.* Entropy, 2023, pp. 1166.

[9] Heidari, Alireza / Jamali, Jabraeil: *Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions.* Cluster Computing, 2023, pp. 3753–3780.

[10] Joshi, Suraj / Thakar, Anshuman / Patel, Chirag: *Applications of Machine Learning and Deep Learning in Securing Internet of Battlefield Things: A Futuristic Perspective.* 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2023, pp. 333–338.

[11] Karim, Hossain / Rawat, Danda B: *Evaluating Machine Learning Classifiers for Data Sharing in Internet of Battlefield Things.* IEEE Symposium Series on Computational Intelligence (SSCI), 2023, pp. 1–7.

[12] Kufakunesu, Rachel / Myburgh, Herman / De Freitas, Allan: *The Internet of Battle Things: A Survey on Communication Challenges and Recent Solutions.* Discover Internet of Things, 2024, pp. 3–19.

[13] Kunatsa, Tendai / Myburgh, Herman C / De Freitas, Allan: *Optimal Power Flow Management for a Solar PV-Powered Soldier-Level Pico-Grid.* Energies, 2024, pp. 459.

[14] Liu, Dandan / Abdelzaher, Tarek / Wang, Tianyu / Hu, Yibo / Li, Jian / Liu, Shiyang / Caesar, Matthew / Kalasapura, Deepak / Bhattacharyya, Jay / Srour, Nabil: *IoBT-OS: Optimizing the Sensing-to-Decision Loop for the Internet of Battlefield Things.* IEEE International Conference on Computer Communications and Networks (ICCCN), 2023, pp. 1–10.

[15] Masuduzzaman, Mohammad / Rahim, Tariqul / Islam, Asif / Shin, Sun Yoon: *UAV-Employed Intelligent Approach to Identify Injured Soldier on Blockchain-Integrated Internet of Battlefield Things.* IEEE Transactions on Network and Service Management, 2024.

[16] Rutravigneshwaran, Prabu / Anitha, Gunasekaran / Prathapchandran, Krishnakumar: *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, 2024, pp. 287–299.

[17] Singh, Rakesh Kumar / Mishra, Satyendra: *TinyML Meets IoBT Against Sensor Hacking.* The Network and Distributed System Security (NDSS) Symposium, Workshop on Security and Privacy in Standardized IoT (SDIoTSec), 2024, pp. 1–9.

Rexhep Mustafovski, MSc, is a Teaching and Research Assistant at the Military Academy "General Mihailo Apostolski" - Skopje, Department for Cybersecurity and Digital Forensics. He holds a Master's degree from the Faculty of Electrical Engineering and Information Technologies, University "Ss. Cyril and Methodius" - Skopje. His research interests include radar systems, IoT security, object detection technologies, and integrated control and monitoring systems. He has authored and co-authored more than 20 scientific and professional papers published in international conferences and journals, including several indexed in high-impact factor journals. His work contributes to advancements in next-generation radar systems, cybersecurity, and military applications of digital technologies.