UDC 621.396:355.4:004.056

V. Ushakov

INTEGRATION OF 5G NETWORKS INTO MILITARY COMMUNICATION SYSTEMS: PROSPECTS AND CHALLENGES

The article examines the technical capabilities of 5G that are critical for military use, including high bandwidth, ultra-low latency, increased reliability, support for massive device connectivity, and mechanisms of network segmentation (network slicing). The potential of 5G is shown for building distributed sensor networks, supporting swarms of unmanned and autonomous combat platforms, integrating artificial intelligence systems into command and weapon-control loops, as well as automating logistics processes. The international experience of NATO, the United States, EU member states, and China in implementing defense-oriented corporate 5G networks and integrating them with existing communication systems is summarized. It is substantiated that the widespread use of virtualized components, open interfaces, and multivendor solutions in 5G leads to a significant increase in the attack surface and forms a new spectrum of cyber threats, compatibility issues with other communication systems, and risks of technological dependence on foreign suppliers. The main approaches to the phased integration of 5G into the military communication systems of Ukraine's Defense Forces are formulated, including requirements for corporate network architecture, cybersecurity organization, and supplier risk management.

Keywords: *5G, military communications, tactical networks, cybersecurity, autonomous combat platforms, C4ISR systems, Internet of Military Things (IoMT), corporate 5G networks, artificial intelligence.*

Statement of the problem. The experience of the large-scale armed aggression against Ukraine has demonstrated a sharp increase in the requirements for military communication systems: the need to simultaneously support a large number of distributed command posts, reconnaissance and strike assets, unmanned and autonomous platforms, as well as real-time automated command-and-control systems. The existing communication infrastructure of the Defense Forces is formed mainly on the basis of previous-generation technologies and is designed for significantly smaller traffic volumes, different latency profiles, and a lower level of cyber threats. This leads to channel overload, instability of command-and-control services, and limits the full implementation of network-centric approaches to planning and conducting operations.

At the same time, a number of NATO member states, the United States, EU countries, and China have already developed long-term strategies for employing fifth-generation mobile communication technologies for defense purposes, are deploying experimental corporate 5G networks at training ranges and military bases, and are testing scenarios for their use in tactical networks, logistics, and intelligence systems [2, 3, 6, 8, 9, 14, 15]. However, the results of these programs cannot be directly transferred to the Ukrainian context due to differences in the structure of the Defense Forces, the condition of existing infrastructure, resource constraints, and the specific nature of threats posed by the adversary. The situation is further complicated by a high level of uncertainty regarding the cybersecurity of 5G networks, their compatibility with existing communication assets, and the risks of technological dependence on foreign suppliers.

Thus, the relevance of this topic is determined by:

– the established scientific and practical problem of substantiating approaches to the integration of 5G technologies into the communication and command system of the Defense Forces of Ukraine;

– the need to define the requirements for the architecture of such solutions, assess their impact on the resilience and cybersecurity of networks, establish limitations related to interaction with existing

systems, and develop the foundations for the phased implementation of 5G technologies under ongoing combat operations and strict resource constraints.

Analysis of recent research and publications. In international practice, the issue of employing 5G technologies in the military domain is considered primarily in strategic and doctrinal documents. The strategies of the U.S. Department of Defense define 5G as a key element in modernizing communication infrastructure, focusing on corporate networks for military bases, training ranges, and experimental zones, as well as on supporting new C4ISR and logistics services [2, 3]. NATO STO documents shape the vision of the role of 5G in future operations, describe the potential of network slicing, support for tactical units, and integration with existing communication systems, but mostly remain limited to framework architectural approaches and individual demonstrational projects [9]. At the same time, the specifics of high-intensity combat operations, which are characteristic of Ukraine, are practically not detailed in these documents.

A significant contribution to the formation of the scientific and analytical foundation is made by studies devoted to scenarios of military application of 5G. Works by NATO C2COE (the NATO Command and Control Centre of Excellence), European authors, and analytical centers examine the capabilities of 5G for tactical networks, platform interaction, and maritime and ground applications, emphasizing the importance of corporate networks and integration with command-and-control systems [7, 10, 15]. Certain publications demonstrate the prospects of using 5G to support land-force operations and form a *digital battlefield*; however, they mostly operate with scenarios involving limited use of electronic warfare assets and cyberattacks [6]. Analytical reviews concerning China show that this state views 5G as a platform for building integrated military–civilian networks, supporting autonomous systems, and conducting information confrontation [14], yet issues of countering such solutions, as well as the possibilities of asymmetric responses by other states, remain insufficiently explored.

The issues of 5G cybersecurity and its application in IoT/IoMT are reflected in a number of international recommendations and systematic reviews. EU and ENISA (European Union Agency for Cybersecurity) documents propose a set of *tools for managing* risks associated with suppliers, virtualization, open interfaces, and supply chains [4, 5], while ITU (International Telecommunication Union) and NIST NCCoE (National Cybersecurity Center of Excellence of the U.S. National Institute of Standards and Technology) focus on general threat models and technical protection measures for operator networks [12]. Scientific reviews on 5G-IoT emphasize the complexity of ensuring confidentiality, integrity, and availability of data in large-scale sensor networks and mobile devices, drawing attention to vulnerabilities related to access protocols, key management, and equipment heterogeneity [11, 13]. At the same time, most works are oriented toward civilian operators and do not take into account the specifics of the combat environment, in which the adversary simultaneously employs electronic warfare, cyber means, and kinetic effects against infrastructure elements.

A separate area is constituted by research on the integration of artificial intelligence into tactical networks and communication systems, where 5G is viewed as one of the key transport layers. Contemporary reviews demonstrate significant potential for using AI in adaptive network resource management, dynamic routing and radio planning, as well as for supporting real-time decision-making [8]. However, issues of compatibility of such solutions with existing communication systems, their resilience to targeted attacks on AI models, and the practical aspects of implementation under limited computational resources at field nodes are addressed only fragmentarily.

In summary, the reviewed studies provide an extensive understanding of the potential of 5G in military communications, outlining basic corporate network architectures, threat models, and general approaches to cybersecurity [2–7, 9, 10–13]. At the same time, the issues of adapting these solutions to the conditions of prolonged high-intensity combat operations, integrating 5G with the existing communication infrastructure of the Defense Forces, assessing the resilience of 5G networks to combined electronic and cyber effects, as well as defining safe models of interaction with foreign suppliers of equipment and software remain insufficiently developed. The subsequent sections of the article are dedicated to addressing these gaps in the context of the needs and constraints of Ukraine's defense sector.

The purpose of the article is to substantiate approaches to integrating 5G technologies into the communication and command system of the Defense Forces of Ukraine by analyzing the capabilities of 5G, cyber threats, compatibility issues, and by formulating recommendations for their phased implementation.

Summary of the main material.

1. Key characteristics of 5G relevant to military communications.

Fifth-generation mobile communication technology combines three main classes of services: eMBB (enhanced Mobile Broadband), URLLC (Ultra-Reliable Low-Latency Communications), and mMTC (massive Machine-Type Communications) [1]. For military applications, URLLC and mMTC are of greatest interest, as they provide ultra-low latency (on the order of milliseconds) with high channel reliability, as well as the capability to simultaneously connect a large number of sensors, platforms, and command nodes [1, 2]. An additional advantage is network slicing, which enables the creation of logically isolated segments of the network for critical and non-critical services with guaranteed quality-of-service parameters [9].

A distinctive feature of 5G is the extensive use of network function virtualization, software-defined networking, and open interfaces, which makes it possible to flexibly reallocate resources among services, rapidly deploy new functions, and adapt network configurations to changing conditions [2]. For military communication systems, this opens the possibility of creating adaptive tactical networks in which resources are automatically redistributed to directions with the most critical load, for example, in areas of mass employment of unmanned systems or during intensive fire engagements.

2. 5G capabilities for IoMT and autonomous platforms.

Studies by NATO C2COE, RAND (the U.S. “Research ANd Development” analytical center), and a number of European authors demonstrate that 5G is a well-suited transport foundation for the concept of the Internet of Military Things, which encompasses reconnaissance sensor networks, surveillance systems, unmanned aerial vehicles, and ground and maritime autonomous platforms [6, 7, 15]. The high connection density combined with URLLC enables the formation of distributed surveillance and strike networks in which data from numerous sensors and platforms are aggregated and transmitted to processing centers almost in real time.

In the maritime and coastal domain, 5G is viewed as a supplement to satellite and traditional radio systems to provide high-speed channels between ships, shore infrastructure, and unmanned maritime platforms [15]. For land forces, the key capability is supporting swarms of UAVs and ground robotic platforms, where a 5G network provides the exchange of telemetry, video, and control commands, as well as machine-to-machine interaction among platforms [6, 14].

3. Integration of 5G and artificial intelligence in tactical networks.

Contemporary research focuses on how the use of artificial intelligence in combination with 5G can enhance the effectiveness of tactical communication networks. In particular, the prospects of applying AI algorithms for dynamic radio-resource planning, adaptive routing, traffic anomaly detection, and decision-support for command elements have been demonstrated [8]. In this case, 5G serves as a high-speed and low-latency transport layer that enables placing part of the intelligent functions closer to the network edge (edge computing) and reducing system response time, which is especially important for systems sensitive to reaction latency, such as the Internet of Military Things.

For Ukraine’s security and defense forces, this creates prerequisites for building distributed command-and-control systems in which individual AI-based analytic modules can be placed directly at tactical-level nodes, analyzing data streams from sensors, UAVs, and reconnaissance systems and automatically generating recommendations for commanders. At the same time, integrating such solutions requires clearly defined requirements for computational resources, protection of AI models from compromise, and ensuring their resilience to targeted attacks [8].

4. Cybersecurity aspects of 5G use in military networks.

The European 5G cybersecurity *toolbox*, along with ENISA, ITU, and NIST NCCoE recommendations, shows that the deployment of 5G is accompanied by a significant expansion of the attack surface due to virtualization, cloud infrastructure, open interfaces, and the use of components from multiple vendors [4, 5, 12]. Scientific reviews dedicated to 5G-IoT security emphasize vulnerabilities in access protocols, key-management issues, firmware-update challenges for large numbers of devices, and the risks of endpoint compromise [11, 13].

For military networks, this implies the need to apply *zero-trust* principles, strict segmentation and microsegmentation, multi-level access control, and continuous monitoring of traffic anomalies. Additionally, it is necessary to account for the possibility of combining cyberattacks with electronic warfare measures and physical destruction of individual nodes, which requires designing the network

with redundancy of key elements, the use of several independent routes, and degraded-mode operation scenarios [5, 12].

5. Compatibility with existing infrastructure and supplier risks.

Documents from the United States, NATO, and the EU emphasize the importance of integrating 5G with existing communication systems, including tactical radio networks, satellite channels, and legacy wired systems [2, 3, 7, 9]. Various options for gateways and intermediate layers are proposed to ensure interoperability between IP-based 5G networks and systems that use other protocols and standards. At the same time, considerable attention is given to the issue of supplier selection, assessment of supply-chain risks, the presence of hazardous dependencies on specific states, and the possibility of hidden influence on network infrastructure [4, 5, 14].

For Ukraine, both the technical and the political-economic aspects of this issue are relevant. A significant part of the existing military communications infrastructure is based on equipment of different generations and standards, which complicates the creation of a unified information space. The selection of 5G solutions must be carried out with regard to the requirement for full control over software, transparency of supply chains, and the possibility of local production or at least the deployment of network elements by domestic enterprises of the defense-industrial complex [3, 5, 14].

6. International experience in integrating 5G into military communication systems.

The U.S. experience demonstrates a predominantly experimental and demonstrational approach to integrating 5G into military infrastructure. The strategy and implementation plans include the creation of a number of pilot sites at bases and training ranges, where scenarios for employing corporate 5G networks to support logistics, tactical operations, manufacturing processes of defense enterprises, and interaction with existing communication systems are tested [2–4]. At the same time, primary attention is devoted to building isolated networks controlled by the defense department's operator, with clearly defined cybersecurity requirements, supply-chain control, and the ability to scale solutions in the future.

Within NATO, a number of research programs and experiments have been conducted dedicated to the use of 5G in supporting Alliance operations, including the development of corporate network architectures, the application of network slicing mechanisms, and ensuring interoperability with existing C4ISR systems [7, 9]. Publications and technical reports emphasize the importance of standardized interfaces, the capability to deploy 5G in both stationary and mobile configurations, and the need for close coordination among member states in selecting suppliers and defining cybersecurity requirements [4, 5]. The experience of European countries is further complemented by projects involving the use of 5G in the maritime domain, where the technology is applied to provide communication between ships, port infrastructure, and unmanned maritime platforms [15].

The Chinese approach is characterized by deep integration of the civilian and military spheres, high-density deployment of 5G networks, and the implementation of the "military–civil fusion" concept in the telecommunications sector [14]. 5G is viewed as a foundational platform for building integrated reconnaissance, surveillance, and command networks, supporting autonomous systems, and enabling high-speed data exchange between heterogeneous platforms. At the same time, there are substantial differences in the regulatory framework, governance structure, and resource capabilities, which complicate the direct transfer of the Chinese model to the Ukrainian context.

A comparison of these examples makes it possible to distinguish common features of international experience: a predominantly phased nature of 5G integration (from experimental test ranges to critical facilities), a focus on defense-oriented corporate networks, strict requirements for cybersecurity and supplier control, as well as an emphasis on integration with existing infrastructure rather than its complete replacement [2–7, 9, 14, 15]. At the same time, almost all of the cited solutions were developed in conditions without prolonged high-intensity combat operations, which necessitates their adaptation to the specifics of the Ukrainian theater of war and the resource constraints of Ukraine's defense sector.

7. Proposed model for the phased integration of 5G into Ukraine's military communication system.

Based on the analysis of international experience and scientific research, a model for the phased implementation of 5G in the military communication system of the Defense Forces of Ukraine is proposed.

The first stage is experimental corporate networks. The deployment of isolated corporate 5G networks at training ranges, training centers, and selected stationary rear facilities for testing typical application scenarios: support for UAVs, sensor networks, logistics processes, and C4ISR elements [2,

3, 6, 7]. At this stage, the national regulatory framework, threat models, and requirements for the architecture of secure 5G solutions are formed.

The second stage is the deployment in critical rear nodes. Integration of corporate 5G networks into logistics hubs, operational-strategic-level command posts, and facilities with increased requirements for bandwidth and reliability. Interaction with existing fiber-optic and radio-relay systems is envisaged, along with the implementation of advanced network-slicing mechanisms and cybersecurity-monitoring tools [3, 5, 7, 9].

The third stage is integration with tactical networks and combat platforms. Deployment of mobile or transportable 5G solutions in areas of combat operations to support tactical units, UAV *swarms*, distributed sensor networks, and real-time decision-support systems [6, 7, 14, 15]. At this stage, issues of resilience to electronic warfare, the ability to rapidly deploy and dismantle the network, and integration with AI algorithms for automated resource management become critical [8].

The fourth stage is the long-term perspective of integration with next-generation networks. Taking global trends into account, a gradual transition to integrated 5G/6G architectures is envisaged, in which the core network and data-processing services combine terrestrial, aerial, and space segments, providing a stable information environment for the Defense Forces [9, 10].

The proposed model can be used as a basis for developing departmental concepts for the evolution of military communication systems, infrastructure modernization programs, and research and development plans in the field of defense-oriented 5G solutions.

Conclusions

The study has shown that fifth-generation mobile communication technology is one of the key factors in transforming the military communication and command systems of the Defense Forces. The high bandwidth, ultra-low latency, support for massive device connectivity, and advanced network-slicing mechanisms characteristic of 5G create the prerequisites for building distributed sensor networks, supporting *swarms* of unmanned and autonomous platforms, integrating artificial intelligence systems into command-and-control loops, and automating logistics processes.

At the same time, it has been established that the extensive use of virtualization, cloud technologies, open interfaces, and multivendor infrastructure significantly expands the attack surface and generates a new spectrum of cyber threats, compatibility issues with existing communication assets, and risks of technological dependence on foreign suppliers. The international experience of the United States, NATO, EU countries, and China confirms the feasibility of a phased transition to defense-oriented corporate 5G networks; however, it does not provide ready-made solutions for the conditions of prolonged high-intensity combat operations in which Ukraine currently finds itself.

The scientific novelty of the work lies in the comprehensive combination of analyzing the technical potential of 5G, cybersecurity, organizational, and supplier risks with the development of a structured model for the phased integration of 5G into the military communication system of Ukraine's security and defense forces. A coherent sequence of stages is proposed — from experimental corporate networks to integration with tactical systems and prospective 5G/6G architectures — taking into account requirements for resilience, compatibility, and cybersecurity. The practical significance of the results lies in the possibility of using the proposed approaches when forming departmental communication-development concepts, infrastructure modernization plans, and specialist training programs.

Prospects for further research are associated with an in-depth quantitative assessment of the resilience of corporate 5G networks to combined electronic and cyber effects, the development of testing methodologies under range conditions, the creation of trust models for elements of supply chains, and the integration of 5G solutions with national command-and-control and weapon systems. A separate area involves the development of applied scenarios for employing 5G for specific units and branches of the armed forces, taking into account the experience of ongoing combat operations.

References

1. New services & applications with 5G ultra-reliable low latency communications (2018). 5G Americas. Retrieved from: https://www.5gamericas.org/new-services-applications-with-5g-ultra-reliable-low-latency-communications/ (accessed 18 June 2025) [in English].

2. Department of Defense 5G strategy (2020). U.S. Department of Defense. Retrieved from: https://www.cto.mil/wp-content/ uploads/2020/05/ DoD_5G_Strategy_May_2020.pdf (accessed 18 June 2025) [in English].

3. Department of Defense Chief Information Officer (2024). DoD private 5G deployment strategy. U.S. Department of Defense. Retrieved from: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD_Private5GDeploymentStrategy_508.pdf (accessed 18 June 2025) [in English].

4. 5G cybersecurity standards (2022). ENISA. *European Union Agency for Cybersecurity.* Retrieved from: https://www.enisa.europa.eu/publications/ 5g-cybersecurity-standards (accessed 18 June 2025) [in English].

5. Cybersecurity of 5G networks – EU toolbox of risk-mitigating measures (2020). *European Union. European Commission.* Retrieved from: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (accessed 18 June 2025) [in English].

6. Gopal V. (2021*).* Militarisation of 5G: A necessity for the forces (CLAWS Issue Brief No. 291). *Centre for Land Warfare Studies*. Retrieved from: https://www.researchgate.net/publication/351903860_Militarisation_of_5G_A_Necessity_for_the_Forces (accessed 18 June 2025) [in English].

7. Lee M., Dimarogonas J., Geist E., Manuel S., Schwankhart R., & Downing B. (2023). Opportunities and risks of 5G military use in Europe (Research Report RR-A1351-2). *RAND Corporation*. Retrieved from: https://www.rand.org/ pubs/research_reports/ RRA1351-2.html (accessed 18 June 2025) [in English].

8. Monzon Baeza V., Parada R., Concha Salor L., & Monzo C. (2025). AI integration in tactical communication systems and networks: A survey and future research directions. *Systems, 13*(9), p. 752. Retrieved from: https://doi.org/ 10.3390/systems13090752 (accessed 18 June 2025) [in English].

9. NATO Science and Technology Organization (2024). 5th generation international mobile telecommunications (5G) technologies application to NATO operations. Volume I (STO Technical Report TR IST-187). *NATO STO*. Retrieved from: https://www.sto.nato.int/document/5th-generation-international-mobile-telecommunications-5g-technologies-application-to-nato-operations-vol-i/ (accessed 18 June 2025) [in English].

10. Van Sambeek M. (2019). 5G technologies in military communications. *In C2COE Symposium "Get Connected"*, Brussels, Belgium, 26–27 June 2019. Retrieved from: https://c2coe.org/wp-content/uploads/2019/10/PDF-5G-Technologies-in-Military-Communications-Mr.-Marcel-van-Sambeek.pdf (accessed 18 June 2025) [in English].

11. Sousa A., & Reis M. J. C. S. (2024). 5G security features, vulnerabilities, threats, and data protection in IoT and mobile devices: A systematic review. *Evolutionary Studies in Imaginative Culture, 8*(S2), pp. 414–427. Retrieved from: https://doi.org/ 10.70082/esiculture.vi.1054 (accessed 18 June 2025) [in English].

12. ITU-D Study Group 2, Question 3/2 (2024). 5G cybersecurity. *International Telecommunication Union*. Retrieved from: https://www.itu.int/pub/D-STG-SG02.03.2-2024 (accessed 18 June 2025) [in English].

13. Valadares D. C. G., Will N. C., Sobrinho Á., Lima A., Morais I., & Santos D. F. de S. (2023). Systematic literature review on 5G-IoT security aspects. *Preprints*. Retrieved from: https://doi.org/10.20944/preprints202311.0565.v1 [in English].

14. Wu H. (2023). China's approach to military 5G networks and related military applications. *NATO Cooperative Cyber Defence Centre of Excellence.* Retrieved from: https://ccdcoe.org/library/publications/chinas-approach-to-military-5g-networks-and-related-military-applications/ (accessed 18 June 2025) [in English].

15. Zmysłowski D., Skokowski P., Malon K., Maślanka K., & Kelner J. (2023). Naval use cases of 5G technology. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation,* 17*(*3), pp. 595–603. Retrieved from: https://doi.org/10.12716/1001.17.03.11(accessed 18 June 2025) [in English].

The article was submitted to the editorial office on 19 November 2025

УДК 621.396:355.4:004.056

В. А. Ушаков

ІНТЕГРАЦІЯ 5G-МЕРЕЖ У СИСТЕМИ ВІЙСЬКОВОГО ЗВ'ЯЗКУ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

Сучасні операції сил оборони України потребують високошвидкісних, захищених і гнучких систем військового зв'язку, здатних підтримувати масове підключення сенсорів, безпілотних та автономних платформ, систем підтримки прийняття рішень і логістичних сервісів у реальному часі. Традиційні мережі тактичного рівня, засновані на технологіях попередніх поколінь, не забезпечують необхідної пропускної здатності, затримки та стійкості до кіберзагроз в умовах інтенсивного застосування противником засобів радіоелектронної боротьби й кібероперацій. Технологія п'ятого покоління мобільного зв'язку (5G) розглядається провідними арміями світу як ключовий елемент трансформації C4ISR-систем, тактичних мереж і інфраструктури Internet of Military Things (IoMT).

У статті розглянуто технічні можливості 5G, що є критичними для військового застосування, зокрема високу пропускну здатність, наднизьку затримку, підвищену надійність, підтримку масового підключення пристроїв та механізми мережевої сегментації (network slicing). Показано потенціал 5G для побудови розподілених сенсорних мереж, підтримки роїв безпілотних та автономних бойових платформ, інтеграції систем штучного інтелекту в контури управління військами й зброєю, а також автоматизації логістичних процесів. Узагальнено міжнародний досвід НАТО, США, держав ЄС і Китаю щодо впровадження корпоративних 5G-мереж оборонного призначення та їх інтеграції з наявними системами зв'язку. Обґрунтовано, що масове використання віртуалізованих компонентів, відкритих інтерфейсів та багатовендорних рішень у 5G призводить до суттєвого зростання площі атаки й формує новий спектр кіберзагроз, проблем сумісності з нинішніми системами зв'язку та ризиків технологічної залежності від іноземних постачальників. Сформульовано основні підходи до поетапної інтеграції 5G у системи військового зв'язку сил оборони України, включно з вимогами до архітектури корпоративних мереж, організації кіберзахисту та управління постачальницькими ризиками.

Ключові слова: *5G, військовий зв'язок, тактичні мережі, кібербезпека, автономні бойові платформи, C4ISR-системи, Internet of Military Things (IoMT), корпоративні 5G-мережі, штучний інтелект.*

Ushakov Volodymyr – Lecturer at the Department of Military Communications and Informatization, National Academy of the National Guard of Ukraine
https://orcid.org/0009-0002-9543-4882