AJLLLSE
GLOBAL RESEARCH NETWORK

AMERICAN Journal of Language, Literacy and Learning in STEM Education
Volume 3, Issue 5, 2025 ISSN (E): 2993-2769

Priority Directions for Ensuring Cybersecurity in Military Activities

Bakhtiyor Temirovich Turayev
Head of the cycle of the Academy of the Armed Forces of the Republic of Uzbekistan

Nisormatov Mukhubillo Lutfullayevich
Senior Lecturer at the Academy of the Armed Forces of the Republic of Uzbekistan

Abstract. *This article discusses the issues of ensuring cybersecurity in military activities. The increasing complexity of cyber threats and the increasing number of attacks on military infrastructure pose new challenges for the modern army. The authors point to the combination of a strategic approach, technical means, legal and regulatory framework and human resources as the main factors in ensuring military cybersecurity.*

In the context of the increasing integration of modern military operations and information and communication technologies, the strategic importance of cyberspace is growing sharply. Information and communication technologies (ICT) have become integral components of military command, intelligence, communications, and combat coordination systems. At the same time, wars are now being waged not only in the traditional physical space, but also in the virtual environment - cyberspace [3, 7, 12] . This situation makes the information systems, control infrastructures, communication and navigation networks of national armies the main targets for cyberattacks.

Today, the stability and functional continuity of any military infrastructure is ensured not only by technical means of protection, but also by the scientifically based implementation of modern cybersecurity concepts. In this regard, the issue of military cybersecurity is considered not only as a topical sectoral direction, but also as a key structural element of strategic security and state defense policy [1, 4, 6] . This approach brings military cybersecurity to a central place in the system of comprehensive provision of national security of the state.

The concept and relevance of military cybersecurity

Military cybersecurity is a system of comprehensive protection measures for military-oriented information systems, digital infrastructures, and network architectures against external and internal cyber threats. This concept encompasses not only technical means, but also organizational, legal, and human-based security strategies. Military cybersecurity is increasingly receiving attention as an integral part of modern military management [4, 8, 11] .

The relevance of the field is directly related to the following factors:

the intensification of information-psychological and cyberwarfare forms, that is, the increase in large-scale attacks targeting military information, control signals, and communications in virtual space;

the militarization of artificial intelligence, drones, and networked systems, which is creating new security gaps and creating previously non-existent types of cyber threats [5, 9, 13] ;

the expansion of cyberintelligence and sabotage activities, that is, the systematic conduct of secret analysis and damage actions by the enemy against military information and networks;

an increase in internal threats (insider threats), i.e., intentional or unintentional threats that can be committed by individuals operating within the military infrastructure.

These factors create the need for a multifaceted, systematic, and proactive approach to military cybersecurity issues. This requires strategic planning and the development of integrated protection mechanisms for ensuring digital security in military systems.

Typology of cyber threats in the military sector and main threat sources

The digitalization of modern military infrastructure exposes military command, intelligence, communications, and logistics systems to complex threats from cyberspace. To ensure military cybersecurity, it is necessary to correctly identify and analyze the mechanisms of cyber threats. The most common and high-risk types of cyber threats in the military are systematized below:

1. APT-attacks (Advanced Persistent Threat)

These types of attacks, which are long-term and targeted, have a multi-stage strategy, and are carried out by the enemy with the aim of penetrating deep into military systems and covertly collecting, modifying, or destroying sensitive information. They are characterized by a high level of training and financial support.

2. Malware

Malware targeting military systems — ransomware (software that encrypts data and demands a ransom), spyware (software designed to spy), and rootkits (software that provides hidden access at the operating system level) — aims to disrupt system functionality, steal sensitive information, or weaken user control.

3. Information and psychological operations (Information Operations)

Spreading fake news in cyberspace, manipulating social media, influencing the morale of soldiers or the public's opinion - these types of threats are tools that bypass traditional methods of warfare but cause significant strategic damage [3, 7, 12] .

4. Network outages (DDoS attacks)

Distributed Denial of Service (DDoS) attacks are aimed at temporarily disrupting the operation of military information resources, command and control centers, and servers. These types of attacks are usually used to mask other attacks or to create operational isolation.

These threats require not only technical, but also organizational and strategic measures in the military sphere. Their identification, modeling and prediction must be carried out on the basis of a comprehensive approach to cybersecurity.

Cybersecurity priorities

Organizational and technical measures : to ensure cybersecurity in modern military information systems, it is not enough to use only individual technological means. In this regard, it is necessary to develop and implement a coordinated system of measures based on a comprehensive organizational and technical approach. The main priorities in this area are outlined below:

- ➢ Formation of cybersecurity management centers. Establishment of Cybersecurity Operations Centers (SOC) in military structures, which will allow for a rapid and coordinated response to information threats . These centers will monitor information flows, analyze attacks, develop incident response measures, and provide ongoing control;
- ➢ Network segmentation and isolation . Military network infrastructure increases the level of protection by separating components operating in high-risk areas and regulating traffic based on limited access rights. Segmentation and isolation serve to localize any potential attack and prevent its spread throughout the system;

- real-time monitoring of information flows . Implementation of SIEM (Security Information and Event Management) systems is essential for early detection and neutralization of cyber threats. SIEM systems allow for effective threat management by collecting, analyzing, and detecting unexpected activity in real-time log data;
- Conduct regular security audits and stress tests . To determine and strengthen the level of cybersecurity, military systems should undergo regular audits, penetration testing, and scenario-based simulated attacks (red/blue team exercises). These measures serve to identify vulnerabilities in the system, assess the resilience of defense mechanisms, and continuously improve them.

Capacity building and human resource development : One of the key factors in ensuring military cybersecurity is human capital, that is, a resource of highly qualified military personnel and technical specialists with knowledge and skills in modern information security [4, 6, 10, 11] . To reliably protect military infrastructure, it is necessary to form, develop and continuously update a competent personnel system in the field of cybersecurity. Priority measures in this direction include:

- Systematically implement cyber literacy and advanced training courses . The peculiarity of modern cyber threats is that they are often carried out through the influence of the human factor. Therefore, cyber literacy programs specifically designed for military personnel should cover areas such as immunity to phishing attacks, password policies, mobile security, and incident response protocols. It is advisable to strengthen the advanced training processes with practical exercises and scenario-based simulations;
- formation of special cyber troops . The creation of separate military units for operations in cyberspace has become a strategic necessity. The cyber troops should include technical specialists, intelligence officers, information analysts and the necessary technopark infrastructure. This structure should have the capacity to carry out not only defensive, but also offensive cyber operations;
- Recruitment and adaptation of IT specialists to military service . Regional and international experience shows that the cybersecurity potential is significantly increased by recruiting IT specialists to military service and retraining them on the basis of special programs. In this process, it is important to ensure the coordinated integration of military-administrative discipline and technical skills. It is also recommended to establish a platform for internships, scientific research and innovative projects in cooperation with the civilian sector.

Improving the legal and regulatory framework : effective management of cybersecurity and legal protection of information infrastructure in the military sphere is a pressing issue that requires the formation of not only technological, but also regulatory and normative foundations. The stability, continuity and legitimacy of military cybersecurity policy depend on the perfection of the legal and regulatory framework. The following are the areas that are considered priority in this area:

- develop and update legislation in line with national and international cybersecurity standards . To ensure the security of military information systems, it is necessary to develop a unified cybersecurity policy at the national level. In this regard, special regulatory documents related to national military sectors should be developed on the basis of legislation adapted to international legal and regulatory systems, such as ISO/IEC 27001, NIST Cybersecurity Framework, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). Such an approach will prevent legal gaps and strengthen international cooperation against cross-border cyber threats [1, 2, 3];
- legal regulation of the activities of specialists working in military information systems . The powers, responsibilities, confidentiality plans, contractual obligations and service discipline of personnel working in military cyber infrastructures should be regulated at the legislative level. At the same time, internal regulations on information security, service protocols and practical procedures based on security standards should be developed;
- clearly define liability and judicial mechanisms for cyberattacks . If cyberattacks are directed at military facilities, control systems or communication channels, these actions are considered a

war crime or a threat to national security. Therefore, the classification of cybercrimes, measures of administrative and criminal liability for those who commit them, as well as the criteria for legal assessment of damage, should be established on the basis of clear legislation;

Introduction of technological innovations : The expansion of the scope of threats in the field of cybersecurity and their complexity makes the introduction of advanced technological solutions in military infrastructures a strategic necessity. In the context of digital transformation, the use of innovative technologies that allow not only to respond to existing risks, but also to predict, detect and automatically neutralize them is of urgent importance. Priority technological approaches in this direction include:

- AI-based threat prediction systems . AI and machine learning algorithms enable early detection of threats and automatic analysis of anomalies in cybersecurity. AI-based platforms analyze log files, network activity, and user behavior in real time, allowing for early detection of potential threats. This approach serves to form a proactive rather than reactive defense model [9, 13].
- Quantum cryptography : In the face of the weaknesses of traditional cryptographic methods, cryptography based on quantum technologies (e.g. Quantum Key Distribution – QKD) provides an absolute level of security for the encryption and transmission of military data. This technology, based on quantum mechanics, makes it almost impossible for a third party to intercept the keys. This creates a strategic advantage for military communication, intelligence and control systems [2, 5].
- Autonomous defense systems and automatic countermeasures (Counter-Cyber Operations) . Autonomous cyber defense systems are capable of detecting, isolating, and neutralizing threats without user intervention. These systems operate based on the "detect-respond-mitigate" cycle. Automatic countermeasures (counter-cyber ops) can also be developed against enemy attack sources, such as blocking malicious traffic, tracing attacks, and temporarily isolating source servers [3, 7, 12].

Conclusion and suggestions

In modern military activities, cybersecurity is considered not only as a tool aimed at solving technical problems, but also as one of the supporting factors for the functional stability of military management and the strategic security of the state. Against the background of the digitization of military infrastructure, the rapid development of artificial intelligence and network technologies, the scale of threats is becoming more complex. In such conditions, relying only on technological solutions is not enough - a comprehensive approach is required, based on the combination of human resources, institutional and legal frameworks and advanced technological strategies.

An effective military policy on cybersecurity should be based on the following: infrastructures that allow for the early prediction, rapid identification, neutralization, and analysis of threats; a pool of highly qualified personnel; strict regulatory procedures, and international cooperation platforms.

Suggestions:

Introducing the "Cybersecurity" major as a separate specialty in military higher education institutions. This major will serve as a new foundation for military technical education. The curriculum should include practical simulations, cyber laboratories, and analytical modules based on real threats;

development of a national military cybersecurity doctrine. This doctrine serves as the primary document defining the goals, principles, threat classification, response strategies, and international positions of military policy in cyberspace.

deepening international cooperation and developing joint initiatives. It is necessary to conduct coordinated cybersecurity expertise exchange, joint research, and counter-cyberattack operations within military cooperation platforms such as NATO, SCO, and CSTO.

Ensuring military cybersecurity serves as a strategic guarantee for the state's information sovereignty and digital protection. Its systematic development is formed at the intersection of science, technology, education, and diplomatic policy.

List of used literature

1. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018.
2. ISO/IEC 27001:2022. Information Security Management Systems — Requirements. International Organization for Standardization, Geneva.
3. NATO Cooperative Cyber Defense Center of Excellence. Cybersecurity Strategic Outlook, Tallinn, 2021.
4. Turaev BX Principles of organizing cybersecurity in military information systems. – Tashkent: Military Publishing House, 2022.
5. CSEC.uz – Reports of the Center for Information Security in Cyberspace of the Republic of Uzbekistan, 2022–2023. https://www.csec.uz
6. Kadyrov Sh.J., Rakhmonov AS Information security and cryptography. – Tashkent: Innovation, 2020.
7. Joint Chiefs of Staff (USA). Cyberspace Operations JP 3-12, US Department of Defense, 2018.
8. Ivanov AA Cyber threats in the military sphere: analysis and countermeasures. - Moscow: Military University, 2021.
9. ITU (International Telecommunication Union). Global Cybersecurity Index (GCI), 2021.
10. Djalilova MZ Digital threats and information security: national approaches. – Journal of "Security and Defense", 2023, No. 2(14), pp. 35–42.
11. Ministry of Defense of the Republic of Uzbekistan. Concept of digitalization of military infrastructure and cybersecurity (internal document, version 2023).
12. Clarke R., Knake R. Cyber War: The Next Threat to National Security and What to Do About It. – HarperCollins, 2012.
13. Singer PW, Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford University Press, 2014.