BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg
BG PULSE JOURNAL

INNOVATIVE APPROACHES TO SYSTEMATIZING AND DISSEMINATING MODERN KNOWLEDGE ON NATIONAL SECURITY

Feruza Muratkhodjaeva Hotamovna

Associate Professor at Oriental University

E- mail: fmuratkhodjaeva@gmail.com

Fayzullayeva Khilola Djuraxodjayevna

Captain, senior officer of a subdivision of military unit 29013

Email: xilolaf15@gmail.com

Doi: https://doi.org/10.5281/zenodo.22877485

Abstract. The rapid transformation of the global information environment, the expansion of digital technologies, and the emergence of new forms of cyber and information threats have significantly increased the importance of systematic knowledge management in the field of national security. Modern national security knowledge is characterized by its interdisciplinary nature, rapid renewal, and dependence on continuously changing technological, social, economic, and geopolitical conditions. In this context, traditional approaches to collecting, organizing, and disseminating security-related knowledge require further development through innovative digital solutions. This article examines contemporary approaches to the systematization and dissemination of national security knowledge with particular attention to digital platforms, artificial intelligence, knowledge management systems, cybersecurity awareness tools, and innovative educational technologies. The study analyzes recent academic and institutional literature published between 2020 and 2026 and identifies key principles for developing an integrated knowledge dissemination framework. Particular attention is given to the role of artificial intelligence in knowledge organization, semantic analysis, information retrieval, personalization, and the rapid dissemination of relevant security information. Recent research indicates that AI-enabled techniques can contribute to secure knowledge management and cybersecurity by supporting data analysis, knowledge representation, and decision-making processes. At the same time, effective dissemination of national security knowledge requires not only technological infrastructure but also information literacy, cybersecurity awareness, ethical standards, and human oversight. UNESCO emphasizes transparency, fairness, human oversight, and AI literacy as important principles for the responsible use of artificial intelligence. The article also considers the relevance of structured cybersecurity frameworks for organizing and communicating security knowledge. The NIST Cybersecurity Framework 2.0, for example, provides a common taxonomy for understanding, assessing, prioritizing, and communicating cybersecurity risks. Based on the reviewed literature, the article proposes that an effective national security knowledge system should combine centralized knowledge repositories, AI-supported analytical tools, digital learning platforms, interactive awareness mechanisms, and continuous knowledge updating. Such an integrated approach can contribute to improving the accessibility, relevance, reliability, and practical applicability of national security knowledge in the contemporary digital environment.

Keywords: national security; knowledge management; knowledge systematization; knowledge dissemination; artificial intelligence; digital technologies; cybersecurity awareness; information security; digital platforms; information literacy; knowledge management systems; innovative educational technologies.

Introduction. The rapid development of digital technologies, artificial intelligence, interconnected information systems, and cyberspace has fundamentally transformed the contemporary national security environment. In the twenty-first century, national security is no longer limited to the protection of territorial integrity, military capabilities, and state institutions. It increasingly encompasses cybersecurity, information security, technological resilience, protection of critical information infrastructure, digital literacy, and the ability of institutions and citizens to identify, interpret, and respond to emerging threats. Consequently, knowledge has become an important strategic resource for national security, while the capacity to collect, systematize, update, and disseminate security-related knowledge has become an essential component of effective security governance. The contemporary information environment is characterized by an unprecedented volume, speed, and diversity of information. Digital platforms enable security-related information to be produced and disseminated almost instantaneously across institutional and national boundaries. At the same time, the growing complexity of information environments creates challenges associated with information overload, fragmented knowledge resources, misinformation, rapidly changing cyber threats, and unequal access to reliable information. These developments demonstrate that simply accumulating large amounts of security-related information is insufficient. Knowledge must be organized into accessible and meaningful structures that enable users to identify relevant information, understand its significance, and apply it appropriately in different security contexts.

The increasing integration of artificial intelligence into information processing has created new opportunities for addressing these challenges. AI-based technologies can support the classification, analysis, retrieval, and personalization of large volumes of information, thereby facilitating more efficient knowledge management. Recent developments in digital technologies have also expanded the possibilities for personalized learning, interactive educational resources, intelligent information retrieval, and automated knowledge organization. UNESCO (2023), for example, emphasizes that digital technologies are transforming the production, distribution, and use of educational content and creating new opportunities for personalized and technology-supported learning. These developments are particularly relevant to national security education and awareness, where information needs to be continuously updated in response to emerging technological and security challenges. An important aspect of contemporary national security knowledge management is the development of common conceptual and organizational frameworks. The NIST Cybersecurity Framework 2.0, published in 2024, provides a structured taxonomy of cybersecurity outcomes designed to help organizations understand, assess, prioritize, and communicate cybersecurity risks (Pascoe, Quinn, & Scarfone, 2024). The framework is organized around six core functions—Govern, Identify, Protect, Detect, Respond, and Recover—which provide a structured approach to managing cybersecurity risks. Such frameworks demonstrate the importance of structuring complex security knowledge into interconnected categories that can be understood and applied by different groups of users. At the same time, the dissemination of national security knowledge requires more than the availability of digital resources. Effective dissemination depends on the reliability, accessibility, relevance, comprehensibility, and timeliness of information.

It also requires appropriate mechanisms for adapting information to different audiences, including policymakers, security professionals, educators, students, employees, and the wider public. The development of digital learning platforms, interactive simulations, online courses, knowledge repositories, multimedia resources, and AI-supported educational tools can facilitate differentiated approaches to security knowledge dissemination. In this context, digital transformation should be understood not simply as the replacement of traditional information channels with digital ones, but as a transition toward more integrated, interactive, adaptive, and continuously updated knowledge ecosystems. Another significant issue concerns the responsible use of artificial intelligence in the management and dissemination of security-related knowledge. Although AI can facilitate information processing and knowledge discovery, its application also raises questions concerning accuracy, transparency, data protection, algorithmic bias, human oversight, and the potential dissemination of unreliable information. Therefore, innovative national security knowledge systems should combine technological capabilities with appropriate mechanisms of verification, ethical governance, and human supervision. This is particularly important because security-related information may have significant social, institutional, and strategic consequences when it is misinterpreted or disseminated without adequate verification.

The purpose of this study is to identify and theoretically substantiate innovative approaches that can contribute to the systematic organization, continuous updating, and effective dissemination of modern national security knowledge. The study seeks to examine how contemporary digital technologies can support the creation of an integrated knowledge environment in which security information can be organized, retrieved, interpreted, updated, and communicated to different target audiences in an accessible and responsible manner. The research is also aimed at identifying the principal organizational, technological, and methodological conditions necessary for the development of an effective national security knowledge dissemination model.

Main part. *Systematization of Modern National Security Knowledge.* The contemporary national security environment is characterized by the rapid emergence of new technologies, increasing digital interdependence, expanding cyber threats, and the growing complexity of information flows. These processes have transformed knowledge into an important strategic resource for national security institutions. Effective security management increasingly depends not only on access to information but also on the ability to organize, classify, evaluate, update, and disseminate relevant knowledge in a structured and accessible manner. Therefore, knowledge systematization should be considered an essential component of modern national security management. National security knowledge is inherently interdisciplinary. It includes information related to cybersecurity, information security, critical infrastructure protection, technological development, emergency management, digital governance, risk assessment, strategic communication, and public awareness. The interdisciplinary nature of this knowledge creates a need for integrated knowledge structures capable of connecting information from different domains. Fragmented information repositories may limit the ability of institutions and individuals to develop a comprehensive understanding of emerging threats. Consequently, modern knowledge management systems should facilitate the integration of heterogeneous information sources and establish relationships between concepts, risks, preventive measures, and response mechanisms. One important approach to systematization is the development of standardized knowledge frameworks. The National Institute of Standards and Technology's Cybersecurity Framework 2.0 provides an example of such an approach. Published in 2024, the framework establishes a taxonomy of high-level cybersecurity outcomes that organizations can use to understand, assess, prioritize, and communicate cybersecurity risks (Pascoe, Quinn, & Scarfone, 2024). The framework

is designed to be adaptable to organizations of different sizes, sectors, and levels of cybersecurity maturity. This flexibility demonstrates the importance of developing knowledge structures that can be applied across different institutional environments. An important characteristic of a modern knowledge system is its capacity for continuous development. Security knowledge cannot be treated as a static collection of documents because technologies, vulnerabilities, attack methods, regulations, and institutional practices are constantly changing. NIST describes the Cybersecurity Framework as a "living" framework that evolves in response to technological and threat trends and incorporates lessons learned from practice (NIST, 2024). This principle can be extended to national security knowledge management more broadly. A contemporary knowledge system should therefore incorporate mechanisms for continuous monitoring, validation, updating, and removal of obsolete information.

The systematization process should also distinguish between raw information and verified knowledge. Large quantities of digital information do not automatically constitute a useful knowledge base. Information becomes practically valuable when it is contextualized, evaluated for reliability, connected with existing knowledge, and presented in a form that supports interpretation and decision-making. For this reason, national security knowledge repositories should include mechanisms for source verification, metadata classification, semantic organization, version control, and regular expert review.

Digital Technologies and Artificial Intelligence in Knowledge. Management Digital transformation has created new opportunities for improving the organization and dissemination of national security knowledge. Cloud-based repositories, digital libraries, knowledge graphs, online databases, learning management systems, and artificial intelligence can support the collection and processing of large volumes of heterogeneous information. Such technologies can make knowledge more searchable, interconnected, and accessible to authorized users. Artificial intelligence is particularly significant because of its capacity to process large datasets and identify relationships that may be difficult to detect through conventional information-processing methods. AI-supported systems can assist with document classification, semantic search, text summarization, pattern recognition, information retrieval, and personalized knowledge delivery. These capabilities can be particularly valuable in security environments where large quantities of information must be analyzed rapidly. However, the application of AI to national security knowledge management should not be understood as a complete replacement for human expertise. AI-generated information may contain inaccuracies, incomplete interpretations, or contextual limitations. Consequently, human verification remains important when security-related information is used for institutional decisions, education, or public communication. The development of responsible AI-based knowledge systems therefore requires a combination of automated processing and expert supervision.

The NIST approach also illustrates the potential for AI-supported cybersecurity knowledge management. Current NIST resources include guidance exploring how AI can support analysis, planning, implementation, and monitoring of cybersecurity framework outcomes, while emphasizing continuous evaluation and improvement. This suggests that AI can function not only as an information-processing technology but also as an instrument for connecting security knowledge with organizational risk-management processes.

Innovative Methods of Disseminating National Security Knowledge. The effectiveness of a knowledge system depends not only on how knowledge is organized but also on how effectively it reaches its intended users. Traditional dissemination mechanisms, such as printed manuals, formal lectures, and institutional documents, remain relevant, but they are increasingly complemented by

digital and interactive methods. Online courses, digital repositories, webinars, mobile applications, interactive simulations, multimedia materials, and social learning platforms can expand access to security-related knowledge. Rather than presenting security knowledge exclusively through theoretical explanations, interactive environments can allow users to respond to simulated security situations, identify risks, make decisions, and receive immediate feedback. Such approaches can contribute to the development of practical competencies rather than simply increasing the amount of information memorized by learners. Research on cybersecurity training provides empirical support for the importance of innovative dissemination methods. Prümmer, van Steen, and van den Berg (2024) conducted a systematic review that examined 142 relevant studies from a much larger initial literature set. Their analysis found that most reviewed studies reported positive effects of cybersecurity training, while game-based approaches were among the most frequently used training methods. These findings indicate that security knowledge dissemination can benefit from active and engaging learning formats. At the same time, the effectiveness of training should not be evaluated solely according to whether participants acquire theoretical knowledge. A 2024 meta-analysis of cybersecurity training studies found positive overall effects on end-users and particularly strong effects on knowledge and attitudes, while effects on actual behavioral change were more limited (Prümmer et al., 2024). This distinction is important for national security education because the ultimate objective of knowledge dissemination is not simply awareness but the development of appropriate and responsible behavior in security-relevant situations. Digital dissemination should therefore combine several complementary approaches. First, centralized repositories can provide authoritative and regularly updated information. Second, online learning platforms can transform complex security concepts into structured educational modules. Third, interactive simulations and scenario-based learning can support practical skills. Fourth, AI-based recommendation systems can help users identify information relevant to their professional or educational needs. Finally, analytical dashboards and feedback mechanisms can help institutions evaluate which knowledge resources are being used and where additional educational interventions may be necessary.

Information Literacy and Cybersecurity Awareness. The dissemination of national security knowledge is closely connected with information literacy. In the digital environment, individuals are exposed to large quantities of information from official websites, social media, online news platforms, messaging applications, and other sources. The ability to distinguish reliable information from inaccurate or misleading content is therefore an increasingly important element of security awareness. Cybersecurity awareness should be understood as a multidimensional construct that includes knowledge of threats, understanding of protective measures, recognition of risky behavior, and the ability to apply appropriate security practices. From this perspective, knowledge dissemination should be designed around the needs and competencies of particular target groups. A security professional may require technically detailed information, whereas students or members of the general public may require accessible explanations and practical examples.

This differentiation suggests that a unified dissemination model should not necessarily provide identical content to all users. Instead, modern digital systems can provide different levels of information according to professional role, prior knowledge, educational needs, and security responsibilities. Such personalization can make national security education more relevant and potentially more effective. The NIST CSF 2.0 provides an example of how complex cybersecurity knowledge can be organized into structured outcomes and profiles. Its Organizational Profiles allow organizations to compare current and target cybersecurity outcomes and identify gaps between existing and desired states (Rigopoulos et al., 2024). A similar principle can be applied to

educational and knowledge-dissemination environments by identifying users' existing knowledge levels and designing appropriate learning pathways.

CONCLUSION. The rapid development of digital technologies, artificial intelligence, cyberspace, and information systems has fundamentally changed the nature of contemporary national security knowledge. The findings of this study demonstrate that the effectiveness of national security knowledge management depends not only on the availability of information but also on its systematic organization, verification, continuous updating, and effective dissemination. In this context, knowledge should be regarded as a dynamic strategic resource that requires permanent development in accordance with technological, social, and security-related changes. The analysis of recent academic and institutional literature from 2020 to 2026 indicates that traditional information-transfer approaches are increasingly complemented by digital knowledge management systems, artificial intelligence, interactive educational technologies, online platforms, and structured cybersecurity frameworks. These technologies create opportunities to improve the accessibility, relevance, and timeliness of national security knowledge. At the same time, technological solutions cannot independently guarantee the reliability or practical effectiveness of disseminated information. Human expertise, source verification, ethical principles, information literacy, and responsible governance remain essential components of an effective knowledge ecosystem. The study identified six interconnected elements of innovative national security knowledge management: knowledge acquisition, systematization, analytical processing, verification and governance, digital dissemination, and continuous feedback and updating. Their integration makes it possible to transform fragmented security-related information into a structured and practically applicable knowledge system. The proposed knowledge cycle—Knowledge Acquisition → Systematization → AI-Supported Analysis → Verification and Governance → Digital Dissemination → Application → Feedback → Continuous Updating—provides a conceptual basis for developing adaptive approaches to national security knowledge management. Particular attention should be given to the responsible integration of artificial intelligence. AI can facilitate information classification, semantic analysis, information retrieval, summarization, personalization, and the identification of relationships among large volumes of security-related data. However, AI-generated outputs require appropriate verification and human oversight, especially when the information concerns sensitive or strategically important security issues. Therefore, AI should be regarded primarily as a supportive analytical instrument within a broader human-centered knowledge management system. The study also demonstrates the importance of audience-oriented dissemination. National security knowledge should be adapted to the specific needs and competencies of different user groups, including researchers, security professionals, educators, students, public-sector employees, and the general population. Online learning platforms, interactive simulations, multimedia resources, digital repositories, and scenario-based learning can complement conventional educational approaches and facilitate the practical application of security knowledge. Consequently, an innovative approach to national security knowledge dissemination should be based on the integration of technological innovation and human-centered governance. The long-term effectiveness of such systems requires continuous evaluation, regular updating of knowledge resources, protection of information integrity, development of digital and information literacy, and systematic assessment of users' knowledge and practical competencies.

In conclusion, the systematization and dissemination of modern national security knowledge should be understood as a continuous, adaptive, and multidimensional process rather than as a one-time transfer of information. The integration of digital technologies, artificial intelligence, structured knowledge frameworks, innovative educational methods, expert verification, and

feedback mechanisms can provide a conceptual foundation for more coherent and sustainable national security knowledge ecosystems. Future research may focus on empirically testing the proposed model, developing AI-supported knowledge repositories, and evaluating the effectiveness of different digital dissemination methods across specific professional and educational contexts.

REFERENCES

1. European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. Publications Office of the European Union.
2. European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. Publications Office of the European Union.
3. International Telecommunication Union. (2021). Global cybersecurity index 2020. ITU.
4. International Telecommunication Union. (2024). Global cybersecurity index 2024. ITU.
5. Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585.
6. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3), e14234.
7. Samtani, S., Zhao, Z., & Krishnan, R. (2023). Secure knowledge management and cybersecurity in the era of artificial intelligence. Information Systems Frontiers, 25, 425–429. https://doi.org/10.1007/s10796-023-10372-y
8. World Economic Forum. (2025). The global cybersecurity outlook 2025. World Economic Forum.
9. OECD. (2024). OECD digital economy outlook 2024 (Volume 1): Embracing the technology frontier. OECD Publishing. https://doi.org/10.1787/a1689dc5-en
10. UNESCO. (2022). Artificial intelligence and education: Guidance for policy-makers. UNESCO.
11. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
12. Xotamovna, M. F. (2024). PHENOMENOLOGY AND THINKING OF THE HUMAN PSYCHE. *IMRAS*, *7*(9), 193-195.