



Article

Cybersecurity and the Transformation of National Values in the Context of Globalization

Ergashev Shoxrux Rustam ugli¹, Eshonqulov Ulugbek Latibboy ugli²

1. Independent Independent Researcher, Officer of the Samarkand Internal Affairs Department, Uzbekistan
 2. Independent Researcher, Officer of the Samarkand Internal Affairs Department, Uzbekistan
- Correspondance: shoxruxergashev080@gmail.com

Abstract: This article examines the social and philosophical aspects of cybersecurity and the transformation of national values in the context of globalization. It explores the influence of information flows, cyber threats, and global cultural influences in cyberspace on national identity, moral and ethical norms, and social consciousness. Furthermore, the study substantiates the interrelationship between the development of cybersecurity culture, the preservation of national values under contemporary conditions, and the maintenance of moral and spiritual stability.

Keywords: cybersecurity; globalization; national values; digital culture; information security; cyber threats.

1. Introduction

The current stage of global civilization is characterized by globalization, informatization, and the rapid development of digital technologies, which are fundamentally transforming the relationships between individuals, society, and technology. The expansion of information exchange and the increasing integration of the digital environment into social life have transformed cybersecurity from a purely technical issue into an important social and philosophical problem associated with human freedom, personal privacy, social trust, and responsibility [1].

At the same time, global information flows and cultural integration processes significantly influence the transformation of national value systems, social consciousness, and spiritual life. Under these circumstances, preserving national values, reconsidering their significance in accordance with the requirements of contemporary development, and ensuring moral and spiritual renewal are of particular importance.

From this perspective, examining the interrelationship between cybersecurity and the transformation of national values in the context of globalization from a social and philosophical standpoint, substantiating human moral and ethical responsibility in cyberspace, and maintaining a balance between national identity and digital security have become important scientific objectives [2].

According to the Cybersecurity Center's 2025 review, digital

Citation: Rustam ugli, E. S & Latibboy ugli E. U. Cybersecurity and the Transformation of National Values in the Context of Globalization. Web of Scholars: Multidimensional Research Journal 2026, 5(4). 212-216.

Received: 8th Sept 2026

Revised: 17th Sept 2026

Accepted: 14th Sept 2026

Published: 17th Oct 2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

transformation in Uzbekistan reached a new stage of development, with information technologies becoming increasingly integrated into various spheres of public life. The rapid digitalization of public administration, the banking and financial sector, education, and social services, together with increased activity in national cyberspace, also contributed to the emergence of more complex threats to national security [3].

In this regard, cybersecurity should be interpreted not merely as a set of technological protection mechanisms but as a social and philosophical phenomenon that maintains a balance between human freedom and responsibility, technological advancement and security, and individual interests and social well-being in the digital environment [4].

This approach makes it possible to reveal the moral and ethical foundations of cybersecurity, promote digital culture, establish principles of conscious and responsible information use, and develop a deeper understanding of the conceptual foundations for creating a secure digital environment.

2. Methodology

This study systematically and comprehensively employs general scientific methods of inquiry, including the principles of historicism and logical analysis, analysis and synthesis, observation, comparison, and generalization.

These methods are applied to examine the interrelationship between cybersecurity, globalization, and the transformation of national values from a social and philosophical perspective.

3. Results

The extensive sociopolitical, economic, and cultural reforms being implemented in Uzbekistan require the enrichment of national values, their transformation in accordance with contemporary conditions, and their integration with the priority directions of social development [5].

Within this process, national values are manifested not only as historical and cultural heritage but also as an important sociocultural phenomenon contributing to spiritual stability, individual moral development, and the strengthening of national identity.

In particular, globalization and digitalization have intensified the need to reconsider the contemporary significance of national values and harmonize them with transformations occurring in the information environment [6].

From this perspective, it is particularly important to analyze the social and philosophical essence of cybersecurity in the digital society in close connection with the transformation of national values and processes of spiritual renewal.

Cybersecurity is not limited to the technical protection of information

resources and digital infrastructure. Rather, it constitutes a complex social phenomenon aimed at safeguarding human interests, ensuring personal privacy, strengthening social trust, and maintaining social stability.

Its effectiveness depends not only on technological capabilities but also on individuals' information culture, moral and ethical responsibility, and attitudes toward national values [7].

Therefore, examining the interaction between cybersecurity and the transformation of national values under globalization provides an important theoretical foundation for understanding the balance between digital development, national identity, and spiritual stability.

As Mirzarakhimov and Shokirov emphasize, cybersecurity has become an integral part of the modern world, and both organizations and individual users must assume responsibility for protecting their information [8].

International documents adopted in the fields of cybersecurity, information security, and combating cybercrime play an important role in establishing the international legal and institutional foundations for ensuring security in the digital society.

These documents are aimed at protecting information systems, preventing threats in cyberspace, identifying and investigating cybercrime, and strengthening cooperation among states [9].

In particular, documents developed within the framework of the Council of Europe and the Shanghai Cooperation Organization play an important role in establishing legal and organizational mechanisms for ensuring security in cyberspace, promoting cooperation in the information sphere, and facilitating joint action against transnational threats [10].

From a social and philosophical perspective, these international initiatives also demonstrate the necessity of maintaining a balance between security, state responsibility, human rights, and freedom of information in the digital environment.

Consequently, improving international norms and cooperation mechanisms is an important prerequisite not only for strengthening cybersecurity but also for ensuring social trust and stability in the digital society [11].

Under contemporary conditions of digital development, cybersecurity constitutes an important factor in protecting personal privacy, individual

freedom, and property interests.

The widespread circulation of personal information in cyberspace exposes individuals to risks associated with unauthorized data use, fraud, and other cyber threats.

As Rustamov emphasizes, vigilance and compliance with information security rules are among the most effective measures for combating cybercrime [12]. Avoiding unfamiliar links, refraining from disclosing SMS verification codes and banking information, verifying urgent money-transfer requests before taking action, and confirming suspicious messages through reliable alternative sources are important steps toward ensuring individual cybersecurity [13], [14].

Therefore, cybersecurity is not merely a matter of technical protection but also an essential condition for ensuring human dignity, ethical responsibility, and digital freedom [15].

A secure digital environment develops through the harmonious interaction of conscious decision-making, information culture, and personal responsibility. International frameworks on cybersecurity, digital culture, privacy, and network society further contextualize these issues.

5. Conclusions

In conclusion, the close relationship between cybersecurity and national values is reflected in individuals' ethical attitudes, information-use culture, and social responsibility in cyberspace. Values such as honesty, mutual respect, responsibility, and respect for human dignity, which are embedded in national traditions, provide moral guidance for individual behavior in the digital environment. These principles have practical significance in protecting personal information, respecting the rights of others, refraining from disseminating false information, and demonstrating responsible attitudes toward cyber threats. At the same time, cybersecurity creates the necessary conditions for preserving national values in cyberspace, promoting them through reliable information, and protecting young people from manipulative influences. Thus, the relationship between cybersecurity and national values is manifested, on the one hand, in the influence of ethical values on digital behavior and, on the other hand, in the opportunities provided by a secure digital environment for preserving and developing national spiritual and cultural heritage.

REFERENCES

- [1] Shanghai Cooperation Organization, 'Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security', *Bulletin of International Treaties*, no. 1. pp. 13–21, 2012.
- [2] UNESCO, *Convention for the Safeguarding of the Intangible Cultural Heritage*. Paris, France: UNESCO, 2003.
- [3] Council of Europe, 'Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols'. Accessed: Oct. 17, 2026. [Online]. Available: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- [4] Cybersecurity Center, 'Cybersecurity Center: Year in Review (2025)'. Accessed: Oct. 17, 2026. [Online]. Available: <https://csec.uz/en/news/list/69>
- [5] B. Mirzarakhimov and B. T. Shokirov, *Cybersecurity: Modern Threats and Strategies for Moral and Legal Protection*. Fergana, Uzbekistan, 2025.
- [6] N. K. Khakkulov and I. I. Rizaev, 'Digital Culture and Personal Inviolability', in *New Technologies in the Educational Process and Production*, 2023, pp. 605–606.
- [7] European Union Agency for Cybersecurity, 'ENISA Threat Landscape 2024', European Union Agency for Cybersecurity, Athens, Greece, 2024.
- [8] International Telecommunication Union, 'Global Cybersecurity Index 2024', International Telecommunication Union, Geneva, Switzerland, 2024.
- [9] A. Rustamov, 'How to Recognize Cybercriminals?' Accessed: Oct. 17, 2026. [Online]. Available: https://uza.uz/oz/posts/kiberjinoyatchilarni-qanday-tanish-mumkin_911172
- [10] L. Floridi, *The Ethics of Information*. Oxford, U.K.: Oxford University Press, 2013.
- [11] I. I. Rizaev and N. K. Khakkulov, 'The Influence of Digital Culture on the Inviolability of Human Life in Society', in *Organizing Committee*, 2023, p. 342.
- [12] National Institute of Standards and Technology, 'The NIST Cybersecurity Framework (CSF) 2.0', National Institute of Standards and Technology, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [13] United Nations Human Rights Council, 'The Right to Privacy in the Digital Age', no. A/HRC/RES/48/4. Oct. 2021.
- [14] M. Castells, *The Rise of the Network Society*, 2nd edn. Chichester, U.K.: Wiley-Blackwell, 2010.
- [15] UNESCO, *Universal Declaration on Cultural Diversity*. Paris, France: UNESCO, 2001.