

CYBERSECURITY AS A CRUCIAL ASPECT OF CROSS-CULTURAL COMMUNICATION IN THE XXI CENTURY

The rapid digitization of all areas of public life has fundamentally transformed the landscape of international relations. Cyber space has become not just a medium for intercultural communication, but also an arena of geopolitical confrontation. Conflicts were previously concentrated in the physical realm, but challenges of informational space as a fourth dimension of conflicts is increasingly apparent. The relevance of the study is due to several factors:

- the transformation of the nature of conflicts towards hybrid forms;
- the absence of universal international legal norms regulating cyber space;
- the emergence of artificial intelligence (AI) technologies that multiplied the potential of destructive informational impact.

In the educational environment, this concept takes on a special meaning because participants in digital interaction are young people who are not always aware of potential risks.

Cybersecurity is about the technologies, processes, and policies that help to prevent or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor. Given the challenges of preventing such negative impacts, increasing attention has been focused on building the capacity of nations to be resilient in the face of security problems, including the development of social and cultural aspects of capacity building. The capacity of a nation to build online security might depend on the attitudes, values, and practices of internet users, such as their awareness of security risks, their online habits and practices, and the prioritisation they place on their security. Moreover, there are social and political factors that might affect their cybersecurity.

The massive spread of social media has fundamentally changed the architecture of cross-cultural communication. A policy-oriented researcher and a private consultant in the fields of cyber security, Lev Topor notes in the “Cyber Sovereignty” that the internet has become a battleground for global dominance where the absence of binding international norms creates a situation of “Digital wild west” [1]. Modern technologies are changing the world, resulting in increased online conflicts. The development of powerful quantum computers threatens the digital locks security, and the proliferation of smart devices makes societies more vulnerable to cyber attacks.

The decentralized nature of social media has demolished traditional information filtering mechanisms. According to research from the Massachusetts Institute of Technology, fake news spreads on social media much faster than credible news. Misinformation campaigns are effective because of psychological mechanisms. The democratization of AI technologies is a qualitatively new stage. According to the Mandiant Company’s research, there has been a significant increase in the use of AI for manipulative campaigns. Deepfake technology is a type of artificial intelligence used to create convincing fake images, videos and audio recordings. The greatest danger posed by deepfakes is the ability to spread false information that appears to come from trusted sources. It’s particularly worrisome that the deepfake technologies are almost indistinguishable from the original images.

In response to escalating threats, nations are developing various strategies for ensuring information security, taking care for people’s rights through rules and laws. For example, there is a data protection law that ensures that no one uses personal data without permission. There are also laws that help to control internet services and markets so that they are fair and safe for all. The concept of “Cyber Sovereignty” implies strict control over internal cyber processes.

Cyber sovereignty is a rapidly spreading concept in the fields of foreign policy and internet governance. Many countries around the world are seeking to apply the concept of cyber sovereignty and expand it for various purposes. This has led to widespread changes in how the internet operates and the user experience. These changes are on the rise and they impact many individuals’ and institutions’ interests associated with the internet. They particularly affect individuals’ exercise of their digital rights through their daily interactions with the network [2].

The main objective of cyber sovereignty is to provide states with the capabilities to protect their national security, their institutions, facilities, and their citizens against the threats of cyber attacks. States are also seeking the means to counter traditional risks that can be exploited using information networks, such as the use of information and communication networks by terrorist groups and other criminal organizations to coordinate their efforts and carry out their operations. One of the objectives of implementing cyber sovereignty policies is to exert control over the flow of information into and out of their borders, to protect its cultural, social, and religious values [2].

In response to cyber challenges, countries should tighten control over the internet and develop their own technologies. At the international level, there is a need to continue negotiations on rules of conduct on the internet, but so far it has been difficult for all countries to come to an agreement.

States' response varies from the concept of cyber sovereignty to regulatory mechanisms for protecting citizens' rights. International legal regulation remains minimal, making information conflicts an attractive instrument of geopolitical confrontation. Effective counteraction requires a comprehensive approach that combines technological, legal, educational, and ideological measures. Among them the creation of standards of information hygiene and the development of critical thinking play key roles.

The rising generation uses cyberspace to search for information, do homework, listen to music, watch movies, play online games, communicate in social networks, try to make some money, creatively achieve their potential, and many other things. For students, the digital environment is not only a learning tool, but also a professional development space. This kind of interaction of a young person with cyberspace is accompanied by the underlying cyber dangers at every step – phishing, bullying in the network, unwanted content, fraudsters of various levels, manipulation of consciousness, etc.

Thus, to protect against cyber threats, everyone needs to learn how to estimate information critically. This means you should check whether the news is true, compare different viewpoints, and use reliable sources to understand what is true and what is false.

Cybersecurity culture refers to the body of knowledge, skills, values and behaviors that ensure the safe and responsible use of digital technologies. Cybersecurity is a set of measures aimed at protecting information systems, data and users from cyberthreats. Cybersecurity in education includes protecting personal data, providing secure access to digital educational resources, preventing cybercrime and online deviant behavior, fostering responsible and ethical behavior in the digital space.

Insufficient level of knowledge and skills in cybersecurity can lead to personal data leakage, cyberfraud, and breaches of information security in educational institutions. Therefore, the formation of a culture of cybersecurity among students becomes an important task directly related to the training of competitive and socially responsible specialists.

References

1. **Topor, L.** Cyber sovereignty : international security, mass communication, and the future of the Internet. / L. Topor. – Cham : Springer, 2024. – 207 p.
2. **Cyber Sovereignty and the Future of the Internet and Digital Rights.** – Masaar: Technology and Law Community, October 30, 2023. – URL: <https://masaar.net/en/cyber-sovereignty-and-the-future-of-the-internet-and-digital-rights> (date of access: 18.03.2026).