GENESIS, NATURE AND STRUCTURE OF CYBERSECURITY IN PHILOSOPHICAL DISCOURSE

SOBIROV ANVAR
Tashkent State University of Economics
Independent researcher of the Department of Philosophy
E-mail: dilmurodernazarov55@gmail.com Mobile: +998997700429

Introduction

The rapid development of information and communication technologies over recent decades has become one of the key factors transforming modern society. The digitalization of the economy, the expansion of global network communications, and the formation of the information society have led to the emergence of a fundamentally new environment of human activity — cyberspace. In the context of the digital transformation of social processes, information resources are becoming a strategic factor in the development of states and international relations. However, alongside the expansion of the possibilities for using information technologies, the number of threats arising in the digital environment is also increasing, which necessitates the formation of an effective cybersecurity system (Singer & Friedman, 2014).

In recent years, a steady increase in the number of cyber incidents affecting government institutions, financial organizations, industrial enterprises, and individual users has been observed. According to international research, the annual global damage caused by cybercrime reaches hundreds of billions of dollars, while the scale and complexity of cyberattacks continue to grow. Consequently, issues related to ensuring the security of digital

infrastructure have acquired not only technological but also socio-political significance (Kshetri, 2021).

Despite the widespread use of such terms as “cyberspace,” “cyber threat,” “cyberattack,” and “cybersecurity,” there is still no unified understanding of these concepts in scientific literature. Terminological ambiguity is largely explained by the interdisciplinary nature of cybersecurity research, which involves philosophy, sociology, law, political science, and computer science (Deibert, 2013).

A particular challenge arises in defining the relationship between the concepts of information security and cybersecurity. In some studies, these categories are used as synonyms; however, many contemporary scholars consider cybersecurity to be a narrower concept related primarily to the protection of digital systems and network infrastructures. Information security, in contrast, encompasses a broader range of threats, including both digital and non-digital forms of information influence (Lopatyn, 2016).

Therefore, the relevance of this research lies in the need for a philosophical analysis of the nature of cybersecurity, the examination of the genesis of this concept, and the identification of its structural elements within the context of the modern information society.

The aim of this study is to analyze the genesis, essence, and structure of cybersecurity in philosophical discourse and to identify the main conceptual approaches to interpreting this phenomenon.

Literature Review

The study of cybersecurity has become one of the central topics in contemporary academic discourse due to the rapid expansion of digital technologies and the growing dependence of modern societies on information infrastructures. The concept of cybersecurity has been explored from multiple disciplinary perspectives, including philosophy, sociology, political science,

law, and information technology. As a result, the theoretical understanding of cybersecurity has evolved significantly over the past decades.

Early research on information security primarily focused on the protection of information systems from technical vulnerabilities and unauthorized access. In this context, cybersecurity was often considered as a technical issue related to computer science and network protection (Anderson, 2020). However, with the expansion of the internet and the increasing integration of digital technologies into everyday life, scholars began to recognize the broader social and political implications of cybersecurity.

One of the influential theoretical frameworks for understanding the digital environment was proposed by Manuel Castells, who introduced the concept of the network society. According to Castells (2010), modern social structures are increasingly organized around digital communication networks that transform economic, political, and cultural processes. Within this context, cyberspace functions not only as a technological infrastructure but also as a new form of social space in which power relations, social interactions, and economic activities are restructured.

Another important contribution to the study of cyberspace was made by Barry Wellman, who emphasized the transformation of social networks in the digital era. Wellman (2001) argued that the development of network communication technologies leads to the emergence of "networked individualism," where individuals participate in multiple online networks rather than being limited to traditional social structures. This transformation significantly increases the importance of cybersecurity, as personal, social, and institutional activities increasingly rely on digital communication channels.

The interdisciplinary nature of cybersecurity research has also been highlighted by Deibert (2013), who analyzed the relationship between digital technologies, surveillance systems, and political power. According to Deibert, cyberspace has become a critical arena in which states, corporations, and non-

state actors compete for control over information flows. This competition creates new forms of cyber conflict and necessitates the development of comprehensive cybersecurity strategies.

From a political science perspective, Joseph Nye introduced the concept of **cyber power**, emphasizing the role of cyberspace in international relations. Nye (2017) argues that cyber capabilities have become an essential component of national power alongside traditional military and economic resources. Cybersecurity therefore represents not only a technical challenge but also a strategic issue related to national security and global governance.

Economic analyses of cybersecurity have also become increasingly significant. Kshetri (2021) examined the economic impact of cybercrime and emphasized that cyber threats represent a growing risk for global markets and digital economies. According to his research, cybercrime has become one of the fastest-growing forms of transnational crime, requiring coordinated responses from governments, international organizations, and private sector actors.

Within the field of information security studies, Singer and Friedman (2014) provided a comprehensive analysis of cyber warfare and cyber threats. Their research highlights the increasing militarization of cyberspace and the growing role of cyber operations in contemporary conflicts. The authors argue that the boundaries between traditional warfare and cyber conflict are becoming increasingly blurred, which further complicates the development of effective cybersecurity policies.

In addition to Western academic traditions, significant contributions to cybersecurity research have also been made by scholars from post-Soviet academic environments. For example, Vojskunsky (2010) examined the psychological aspects of cyberspace, focusing on the interaction between human behavior and digital environments. His work emphasizes that cybersecurity cannot be understood solely in technical terms but must also

account for human factors, including user behavior, digital culture, and online communication patterns.

Similarly, Lopatyn (2016) analyzed the legal and institutional aspects of information security and emphasized the importance of regulatory frameworks in protecting national information infrastructures. His research demonstrates that cybersecurity policies must integrate legal, organizational, and technological mechanisms in order to effectively address emerging cyber threats.

International organizations have also contributed significantly to the development of cybersecurity standards. One of the most influential frameworks is the ISO/IEC 27032 standard, which provides guidelines for cybersecurity and defines cyberspace as a complex virtual environment formed through the interaction of people, software, and communication technologies (ISO/IEC, 2012). This standard emphasizes the importance of risk management and cooperation between governments, private companies, and civil society in addressing cybersecurity challenges.

Overall, the analysis of existing literature demonstrates that cybersecurity is increasingly understood as a multidimensional phenomenon that encompasses technological, social, political, and economic dimensions. Contemporary research highlights the need for interdisciplinary approaches to cybersecurity that integrate insights from various academic disciplines. Such approaches enable a more comprehensive understanding of cyber threats and contribute to the development of effective strategies for protecting digital infrastructures and ensuring the stability of the global information society.

Methods

The methodological basis of this study is grounded in philosophical and interdisciplinary approaches applied to the analysis of cybersecurity as a socio-technical phenomenon.

A systemic approach was employed to examine cybersecurity as a complex structure consisting of technological, social, political, and cultural components. This approach allows cyberspace to be interpreted as a socio-technical system in which technological infrastructure and human activity interact in a dynamic environment.

The comparative method was used to analyze and compare different theoretical interpretations of information security and cybersecurity presented in domestic and international academic literature.

In addition, content analysis of regulatory documents and strategic frameworks related to cybersecurity at national and international levels was conducted. Particular attention was paid to international information security standards, including ISO/IEC 27032, as well as national cybersecurity strategies implemented in various countries.

The method of theoretical modeling was also applied to identify the structural components of cybersecurity. This method allowed cybersecurity to be conceptualized as a system consisting of several interconnected elements, including technical protection mechanisms, organizational security policies, and social factors influencing the protection of digital infrastructure.

The use of these methodological approaches ensured a comprehensive and multidimensional examination of cybersecurity within philosophical discourse.

Results

The analysis of scientific literature demonstrates that the concept of cybersecurity is closely related to the development of the idea of the information space. In academic discourse, the information space is generally understood as a complex system consisting of information resources, communication networks, and social interactions associated with the production, distribution, and consumption of information.

Several approaches to interpreting the information space can be identified in scientific research.

The geopolitical approach interprets the information space as a virtual territory of a state that has certain boundaries and is subject to national jurisdiction. Within this framework, information resources, telecommunication infrastructure, and users are viewed as elements of a national information system. The primary responsibility of the state is to protect its information space from external threats and to ensure information sovereignty.

The social approach considers the information space as a sphere of social communication in which individuals and institutions exchange information and knowledge. In this context, the information space functions as an essential component of social interaction and the formation of public consciousness (Castells, 2010).

The noospheric-informational approach views the information space as a global system of information resources and technologies that support the development of human civilization and contribute to the formation of the global information society.

The development of the concept of information space has led to the emergence of another important category — cyberspace. In contemporary academic discourse, cyberspace is typically understood as a virtual environment formed through the interaction of computer networks, software systems, and users.

The concept of cyberspace was initially popularized by the American writer William Gibson, who used the term to describe a virtual reality created by computer networks. Over time, the concept has been widely adopted in academic literature and has become a key category for analyzing digital environments.

From a sociological perspective, cyberspace can be considered a specific form of social space in which various forms of human activity occur.

Barry Wellman argues that the development of network technologies contributes to the formation of new patterns of social organization based on network interactions (Wellman, 2001).

Similarly, A. E. Vojskunsky defines cyberspace as a virtual environment that contains virtually unlimited volumes of information and provides opportunities for communication and interaction among users through computer networks (Vojskunsky, 2010).

International standards also provide their own interpretation of cyberspace. In the ISO/IEC 27032 standard, cyberspace is defined as a complex virtual environment formed through the interaction of people, software systems, and network technologies. In this context, cybersecurity is understood as the protection of information assets from threats affecting confidentiality, integrity, and availability of data.

Contemporary studies generally distinguish two main approaches to defining cybersecurity.

The broad approach considers cybersecurity as a comprehensive system that includes technological, organizational, social, and psychological aspects of digital security.

The narrow approach interprets cybersecurity primarily as a set of technological mechanisms aimed at protecting computer networks and digital infrastructures.

In practical terms, cybersecurity includes several key areas: network security, application security, cloud security, and the protection of critical information infrastructure.

Particularly important is the protection of critical information infrastructure, which includes government information systems, energy networks, transportation systems, financial institutions, and other strategic sectors.

The rapid development of digital technologies has also led to the emergence of various types of cyber threats. The most common types include malicious software, phishing attacks, social engineering, cryptojacking, and attacks based on artificial intelligence technologies.

Discussion

The analysis of contemporary research indicates that cybersecurity should not be considered solely as a technological issue. Instead, it represents a complex interdisciplinary phenomenon that encompasses social, political, economic, and cultural dimensions.

In the context of digital transformation, cybersecurity has become one of the most important elements of national security policy. Governments around the world are developing national cybersecurity strategies, establishing specialized cyber defense centers, and implementing advanced technologies to protect digital infrastructures.

Special attention is given to the protection of critical information infrastructure, since disruptions to these systems can cause severe economic and social consequences.

In the Republic of Uzbekistan, significant steps have also been taken to strengthen national cybersecurity systems. In 2023, a regulatory framework was adopted to establish procedures for assessing the level of cybersecurity protection of critical information infrastructure facilities. This framework includes the evaluation of security management systems, cyber threat monitoring mechanisms, and incident response procedures.

One of the most promising modern approaches to cybersecurity is the Zero Trust security model. The fundamental principle of this model is that no user, device, or system should automatically be trusted. Instead, all access requests must be verified and authenticated continuously.

From a philosophical perspective, cybersecurity can therefore be understood not only as a technical system designed to protect information but

also as a complex social institution that regulates the functioning of digital environments and ensures the stability of the information society.

REFERENCES

Castells, M. (2010). *The rise of the network society*. Wiley-Blackwell.

Chebotareva, A. A. (2018). *Information security in modern society*. Moscow: Nauka.

Deibert, R. (2013). *Black code: Surveillance, privacy, and the dark side of the Internet*. McClelland & Stewart.

Dzyaloshinsky, I. M. (2001). *Information space of Russia*. Moscow.

Frolov, I. T. (2010). *Philosophical dictionary*. Moscow.

ISO/IEC. (2012). *ISO/IEC 27032: Guidelines for cybersecurity*. Geneva: International Organization for Standardization.

Kshetri, N. (2021). *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan.

Likhtin, A. A., & Kovalev, A. A. (2015). *Information space as a social phenomenon*. Moscow.

Lopatyn, V. N. (2016). *Information security of Russia*. Moscow.

Nye, J. (2017). Deterrence and dissuasion in cyberspace. *International Security*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Vojskunsky, A. E. (2010). *Psychology of cyberspace*. Moscow.

Wellman, B. (2001). Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research*.

Cybersecurity Center of Uzbekistan. (2023). Regulation on cybersecurity assessment of critical infrastructure facilities.