

Article

Social and Philosophical Analysis of The Impact of Cyber Threats on The Security of The Individual, Society And State

Khamidov Shukurullo Muqimjon oglu*¹

1. Researcher at Fergana State University

*Correspondance: shukurulloxamidov2695@gmail.com

Abstract: This article analyzes the impact of cyber threats on the security of the individual, society and state from a socio-philosophical perspective. In the context of the information society, the essence of cyber threats, their impact on human rights, social stability and national security has been revealed. It also covers new forms of cyber threats, their social consequences and socio-philosophical mechanisms for ensuring cybersecurity in the processes of digital transformation.

Keywords: Cyber Threat, Cybersecurity, Information Society, Information Security, Personal Security, Social Security, National Security, Digital Transformation, Disinformation, Cybercrime

1. Introduction

In the 21st century, as a result of the rapid development of information and communication technologies, human development has reached a new level [1]. The formation of the information society has led to the interdependence of economic, political, social and cultural processes with the use of digital technologies [2].

Today, public administration, education, healthcare, the banking and financial system, mass communications, and almost all aspects of everyday life rely on digital infrastructures. At the same time, the expansion of the information space and the popularization of digital technologies cause the emergence of new threats and challenges.

2. Methodology

Cyber threats are emerging as one of the most pressing challenges of modern society. They negatively affect not only information systems and technological infrastructures, but also the rights and freedoms of the individual, the spiritual stability of society, and the national interests of the state. Therefore, it is imperative to study cyber threats not only as a technological phenomenon but also as a complex socio-philosophical phenomenon [3].

In the context of globalization and digital transformation, the scope and sophistication of cyber threats is increasing. Today, cybercrime, disinformation, information manipulation, cyberespionage, cyberterrorism, and artificial intelligence-based threats pose a serious threat not only to individuals, but to entire societies and states [4]. In this regard, the socio-philosophical analysis of this issue is one of the most important tasks facing modern science.

The concept of cyber threat refers to any action, event or process aimed at causing damage to information and communication technologies and digital infrastructures [5]. However, in modern scientific approaches, the cyber threat is being interpreted not only

Citation: Muqimjon oglu, K. S. Social and Philosophical Analysis of The Impact of Cyber Threats on The Security of The Individual, Society And State. Middle European Scientific Bulletin 2026, 46(4), 9-12.

Received: 05th Jun 2025Revised: 30th Jun 2025Accepted: 20th Jul 2026Published: 12th Aug 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/>)

as an attack on technical systems, but also as a factor influencing the system of social relations.

From a socio-philosophical perspective, cyber threats is a complex social phenomenon that negatively affects a person's information freedom, personal immunity, and stability of social relationships. They are an expression of the new security problems that have arisen in modern society as a result of the transformation of information into a strategic resource.

M. Castels describes modern society as a "networked society", in which information flows and digital communications have become the main factor of social progress [6]. Therefore, any threat that arises in the information space has a direct impact on the economic, political and spiritual development of society. The social nature of cyber threats is also manifested in their impact on trust, communication, and cooperative relationships between people [7]. Today, events such as information manipulation, dissemination of false information, and cyber fraud are causing a decline in social trust.

The impact of cyber threats primarily on human interests increases their social vulnerability. Modern people actively use the Internet, social networks, e-commerce, mobile applications and digital services in their daily life [8]. As a result, personal information, financial resources, and communicative activities become closely linked to the digital space.

3. Results and Discussion

Phishing, identity theft, internet fraud, malware, and the illegal dissemination of personal information are shown as the most common forms of cyber threats targeting personal security. These threats bring not only material damage, but also negative psychological and moral consequences. Theft of personal data leads to violation of the human right to information inviolability and privacy [9]. As a result, an individual may form an illusion that he does not feel safe, is under constant control. This leads to psychological pressure, stress, and social alienation.

Incidents of cyberbullying, harassment, blackmail and virtual violence that are spreading on social networks also pose a serious threat to the security of the individual. Especially young people and adolescents are becoming the primary victims of these threats. Therefore, cyber threats affect not only the information, but also the spiritual security of an individual [10]. Another dangerous aspect of cyber threats is how they affect a person's ability to think independently. Information flows formed on the basis of algorithms, manipulative advertising and content created with the help of artificial intelligence can limit a person's ability to make an informed choice [11]. Public security means the maintenance of a stable system of relationships between individuals, social groups, and institutions. Cyber threats continue to manifest themselves as one of the key factors contributing to this particular system outage.

Today, disinformation and ethical manipulation are among the biggest threats to public safety. The rapid spread of fake information and misinformation serves to misshape public opinion. As a result, social trust is diminished, civic solidarity is weakened, and various social conflicts arise.

From a socio-philosophical perspective, disinformation blurs the boundaries between truth and falsehood. This has a negative impact on people's correct perception of reality. As confidence in the reliability of information decreases, social instability in society increases [12]. The impact of cyber threats on public safety is also evident in the spiritual realm. Violence, extremism, radicalism, immorality and destructive ideas being propagated in the virtual space can weaken the moral foundations of society [13]. Ideological threats to the minds of young people, in particular, have a negative impact on the spiritual image of future generations.

Cyber threats also pose a threat to cultural identity and national values. In the context of globalization, certain information flows can lead to the suppression of local cultures and traditions. That is why the link between information security and moral security is becoming increasingly strong.

The issue of state security is one of the most important areas of modern cyber threats. As a result of digital transformation, public administration, defense, energy, transport, banking and financial and communication systems are increasingly connected to digital infrastructures.

This situation increases the vulnerability of states to cyber threats. Cyberespionage, theft of strategic information resources, illegal access to government information systems, and orchestrated cyberattacks on critical infrastructures can seriously harm national security.

Cyberterrorism is also emerging as a new threat to state security. The use of the Internet by terrorist and extremist groups, conducting virtual propaganda and their attempts to carry out cyber attacks pose a serious threat to international security [14].

In the context of globalization, the transnational nature of cyber threats makes it more difficult to detect and eliminate them. Cyber attacks do not recognize state borders and can be carried out from anywhere in the world. Therefore, national security issues are increasingly linked to international cooperation [15].

Today, many countries are recognizing cybersecurity as one of their national security priorities. This suggests that cyberspace is becoming a space of modern geopolitical competition.

The societal consequences of cyber threats are manifold in nature. They manifest themselves in the form of economic damage, erosion of social trust, weakening of moral values, political instability and threats to national security.

From a socio-philosophical perspective, the main danger posed by cyber threats is that they erode the relationship of trust between people and society. Because the level of security in the information space is directly related to stability and progress in society.

To solve these problems, along with technological means, the development of information culture, digital literacy and social responsibility is important. A sustainable model of cybersecurity relies not only on technical protection systems, but also on the advanced human factor. In addition, the formation of a culture of cybersecurity in the education system, teaching young people to think critically and developing competencies for working with information is an urgent task. Because most modern cyber threats are based on the use of the human factor.

4. Conclusion

In conclusion, cyber threats are one of the complex socio-philosophical problems of the information society. They have a direct impact on the individual's freedom of information and personal inviolability, the spiritual stability of society, and the national security of the state. The transnational, anonymity, agility, and popularity of cyber threats make them one of the most pressing challenges for modern security systems. Therefore, in the fight against cyber threats, it is necessary to make widespread use of socio-philosophical approaches along with technological, legal and organizational measures. One of the most effective ways to mitigate the negative consequences of cyber threats is the development of information culture, digital literacy, critical thinking and social responsibility. And a sustainable cybersecurity system serves the safe development of an information society by ensuring a harmony of the interests of the individual, society and the state.

REFERENCES

- [1] A. Toffler, *The Third Wave*. New York, NY, USA: Bantam Books, 1980.
- [2] N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, 2nd ed. Cambridge, MA, USA: MIT Press, 1961.
- [3] Q. G. Nazarov and N. A. Shermuhamedova, *Falsafa Asoslari [Fundamentals of Philosophy]*. Tashkent, Uzbekistan: O'zbekiston, 2018, (in Uzbek).
- [4] E. Kaspersky, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, U.K.: Oxford Univ. Press, 2018.
- [5] Republic of Uzbekistan, Law of the Republic of Uzbekistan "On Cybersecurity," Tashkent, Uzbekistan, 2022, (in Uzbek).
- [6] M. Castells, *The Rise of the Network Society*, 2nd ed. Oxford, U.K.: Wiley-Blackwell, 2010.
- [7] Z. Bauman and D. Lyon, *Liquid Surveillance: A Conversation*. Cambridge, U.K.: Polity Press, 2013.
- [8] D. Bell, *The Coming of Post-Industrial Society*. New York, NY, USA: Basic Books, 1973.
- [9] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs, 2019.
- [10] J. T. Tulenov and Z. G'ofurov, *Falsafa [Philosophy]*. Tashkent, Uzbekistan: O'qituvchi, 2016, (in Uzbek).
- [11] M. Foucault, *Discipline and Punish: The Birth of the Prison*, A. Sheridan, Trans. New York, NY, USA: Pantheon Books, 1977.
- [12] J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, T. Burger, Trans. Cambridge, MA, USA: MIT Press, 1989.
- [13] Y. N. Harari, *21 Lessons for the 21st Century*. New York, NY, USA: Spiegel & Grau, 2018.
- [14] E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY, USA: PublicAffairs, 2011.
- [15] International Telecommunication Union (ITU), *Global Cybersecurity Index 2024*. Geneva, Switzerland: ITU, 2024.