CYBERSECURITY AS A NEW DIMENSION OF INTERNATIONAL SECURITY: CHALLENGES, GOVERNANCE, AND GLOBAL PERSPECTIVES

Zayniddinova Dilfuza Sherali qizi
Toshkent Xalqaro moliyaviy boshqaruv va texnologiyalar universiteti
4-kurs xalqaro munosabatlar talabasi
Sayfullayev Behruz
Ilmiy rahbar Tarix fanlari bo'yicha falsafa doktori (PhD), dotsent
https://doi.org/10.5281/zenodo.21833826

Introduction

In the modern era of globalization, the rapid development of Information and Communication Technologies (ICT) has fundamentally transformed every sphere of human life. The Internet, artificial intelligence, cloud computing, and digital infrastructures have elevated economic growth, social interaction, and public administration to a new level. However, this development has simultaneously turned cyberspace into a new, complex, and highly dangerous dimension of international security. Today, cybersecurity is no longer merely a technical or economic issue; it has become a central element of interstate relations, strategic competition, and global stability.

Cyberspace has been recognized as the fifth domain of warfare, following land, sea, air, and space. Within this domain, states, non-state actors, and even individuals can employ cyber capabilities as strategic weapons to achieve political, military, or economic objectives. Cyberattacks such as Stuxnet (2010), WannaCry (2017), NotPetya, and others have clearly demonstrated the destructive potential of cyber weapons against critical physical infrastructure and their far-reaching global consequences. These incidents pose significant threats to national security, economic stability, and social resilience while also requiring a reassessment of international legal norms, state sovereignty, and the balance of power.

Relevance of the Research Topic

The growing importance of cybersecurity as a new dimension of international security can be explained by several factors. First, the increasing level of digital interdependence has made the global economy and critical infrastructure—including power grids, financial systems, transportation, and healthcare—highly dependent on cyberspace. A single successful cyberattack can disrupt entire regions or even global supply chains. Second, intensifying geopolitical competition has encouraged major powers, particularly the United States, China, and Russia, to actively use cyberspace as a tool for influence and strategic advantage. Third, the spread of hybrid threats has led to the integration of cyber operations with conventional military actions, thereby blurring the distinction between war and peace.

The United Nations Security Council and other international organizations have recognized cyber threats as serious risks to international peace and security. According to reports published in 2025, both the frequency and sophistication of cyberattacks continue to increase, causing significant economic losses, undermining trust, and intensifying geopolitical tensions. For developing countries such as the Republic of Uzbekistan, this issue is particularly important because the process of digital transformation requires stronger protection of national sovereignty alongside enhanced international cooperation.

The significance of this topic is also evident from a theoretical perspective. Major theories of international relations—including realism, liberalism, and constructivism—suggest that

cyberspace requires a reconsideration of traditional concepts such as power, sovereignty, and cooperation. Realism views cyberspace as a new arena of strategic competition, whereas liberalism emphasizes the role of international norms and institutions in regulating cyber activities.

Research Objective

The primary objective of this study is to analyze cybersecurity as a new dimension of international security, examine its impact on the global security system, and propose effective strategies for addressing contemporary cyber threats.

Research Objectives

- To define the concept of cybersecurity from a theoretical perspective and examine its place within international security theories.
- To analyze contemporary forms of cyber threats, including state-sponsored cyberattacks, ransomware, and hybrid warfare, supported by relevant case studies.
- To examine the interrelationship between cybersecurity at the national and international levels.
- To evaluate international cooperation mechanisms, including those of the United Nations (UN), the North Atlantic Treaty Organization (NATO), the Shanghai Cooperation Organization (SCO), and other institutions, as well as the existing international legal and regulatory frameworks.
- To develop recommendations for strengthening cybersecurity in the context of Uzbekistan by considering international experience and best practices.

Abstract

This article presents a comprehensive analysis of cybersecurity as a contemporary strategic dimension of international security. The study examines how the processes of globalization and digitalization have transformed cyberspace into the fifth domain of warfare, characterized by transnational, hybrid, and increasingly sophisticated cyber threats, as well as the growing interdependence of global digital infrastructure.

The primary objective of the research is to analyze the theoretical foundations of cybersecurity, evaluate its role within the international security system, compare Uzbekistan's experience with international best practices, and develop practical recommendations for strengthening national cybersecurity.

The study examines the concept of cybersecurity, the distinctive characteristics of cyberspace, the principal types of cyber threats, state-sponsored cyberattacks, and the role of international organizations in ensuring cybersecurity. It also analyzes Uzbekistan's cybersecurity policy and the National Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030. Furthermore, the cybersecurity policies and practices of the United States, the European Union, and South Korea are comparatively analyzed to identify effective approaches to cybersecurity governance.

The findings demonstrate that cybersecurity has become an indispensable component of both national and international security. The study further emphasizes the necessity of strengthening digital sovereignty, expanding international cooperation, and enhancing modern cyber defense mechanisms to address the evolving challenges of the digital era.

Keywords: cybersecurity, cyberspace, cyber threats, international security, digital sovereignty, cybercrime, state-sponsored cyberattacks, Uzbekistan, National Cybersecurity Strategy.

Chapter 1. The Concept of Cybersecurity and Its Theoretical Foundations

1.1. The Nature of Cybersecurity and Its Fundamental Concepts

Cybersecurity is a comprehensive approach to protecting the digital environment created by modern Information and Communication Technologies (ICT). It encompasses the protection of computer systems, networks, software, data, and users against unauthorized access, modification, disruption, or destruction.

The fundamental principles of cybersecurity are based on the CIA Triad, which consists of Confidentiality, Integrity, and Availability.

Confidentiality ensures that information is accessible only to authorized individuals and protected from unauthorized disclosure. This principle is particularly important for safeguarding personal data, commercial secrets, and classified government information.

Integrity guarantees the accuracy, consistency, and reliability of information by preventing unauthorized modification or corruption. Any unauthorized alteration should be detected and prevented to maintain data authenticity.

Availability ensures that information systems and services remain accessible and operational for authorized users whenever needed. This principle is especially important in protecting critical infrastructure against attacks such as Distributed Denial-of-Service (DDoS) attacks.

In addition to the CIA Triad, cybersecurity also incorporates other essential principles, including authentication (verification of a user's identity), authorization (granting appropriate access rights), accountability and auditing (monitoring and recording user activities), and non-repudiation, which prevents parties from denying their actions or communications.

Cybersecurity is widely regarded as an expanded dimension of information security. While information security primarily focuses on protecting data, cybersecurity encompasses the entire cyberspace ecosystem, including networks, devices, users, applications, and digital processes. Consequently, cybersecurity extends beyond technical protection and incorporates legal, social, economic, and political dimensions.

According to contemporary definitions, cybersecurity refers to the collection of policies, technologies, processes, and practices designed to preserve the confidentiality, integrity, and availability of information within cyberspace. It is implemented at governmental, organizational, and individual levels and relies on risk management, vulnerability mitigation, incident prevention, and effective response mechanisms.

1.2. Cyberspace and Its Role in Contemporary Society

Cyberspace is the virtual environment formed by interconnected computer networks, software systems, digital information, and the human activities conducted through them. The term was first introduced by William Gibson in his 1984 novel Neuromancer and has since evolved into a fundamental platform for global communication, commerce, governance, and social interaction.

Cyberspace possesses several distinctive characteristics.

First, it is borderless, meaning that it transcends geographical boundaries and enables actions in one country to produce immediate consequences across the world.

Second, it provides a high degree of anonymity, while the attribution of cyberattacks remains technically and politically challenging, making it difficult to identify the responsible actors.

Third, cyberspace has a dual-use nature. It supports peaceful activities such as education, business, scientific research, and communication, while simultaneously enabling malicious activities including cyber espionage, sabotage, cybercrime, and cyber warfare.

Finally, cyberspace is dynamic and continuously expanding due to the rapid development of emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), fifth- and sixth-generation mobile networks (5G/6G), and quantum computing.

In contemporary society, cyberspace constitutes the foundation of digital transformation. It supports financial systems, transportation, energy infrastructure, healthcare services, public administration, and social communication. A substantial share of global trade is conducted through digital platforms, while smart cities and Industry 4.0 technologies rely heavily on secure and resilient cyber infrastructure.

However, this increasing dependence also creates significant vulnerabilities. Cyberspace is now widely recognized as the fifth operational domain of warfare, alongside land, sea, air, and space. States increasingly employ cyber capabilities to achieve strategic superiority, conduct intelligence operations, and weaken their adversaries without engaging in conventional military conflict.

As a result, cyberspace has become an indispensable component of international security and has contributed to the emergence of a new concept of sovereignty known as digital sovereignty, which emphasizes a state's ability to govern, protect, and control its digital infrastructure, information resources, and cyberspace.

1.3. Main Types of Cyber Threats

Cyber threats refer to potential or actual risks directed against information systems, computer networks, and critical infrastructure. As digital technologies continue to evolve, the nature and complexity of these threats have become increasingly sophisticated. The principal categories of cyber threats include the following:

Malware. Malware encompasses malicious software such as viruses, Trojan horses, ransomware (e.g., WannaCry), spyware, and worms. Its primary objectives include stealing sensitive information, disrupting system operations, encrypting data for ransom, or gaining unauthorized control over targeted systems.

Phishing and Social Engineering. These attacks include phishing, spear-phishing, smishing (SMS phishing), and Business Email Compromise (BEC). They exploit human vulnerabilities by deceiving users into revealing confidential information or granting unauthorized access to computer systems.

Network Attacks. Common forms of network attacks include Distributed Denial-of-Service (DDoS) attacks, which overwhelm systems with excessive traffic and disrupt service availability, and Man-in-the-Middle (MitM) attacks, in which attackers intercept communications to steal, manipulate, or alter transmitted information.

Application and Web-Based Attacks. These attacks exploit vulnerabilities in software applications and websites through techniques such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and zero-day exploits, allowing attackers to compromise systems before security patches become available.

State-Sponsored and Advanced Persistent Threats (APTs). Advanced Persistent Threats are highly sophisticated, long-term, and covert cyber operations, often supported by state actors. Their objectives typically include cyber espionage, intelligence gathering, and sabotage of critical infrastructure. The Stuxnet attack is widely regarded as one of the most significant examples of an APT operation.

Insider Threats. Insider threats originate from employees, contractors, or other authorized individuals who intentionally or unintentionally compromise an organization's information security through negligence, misuse of privileges, or malicious actions.

Emerging Cyber Threats. Recent developments have introduced new forms of cyber threats, including supply chain attacks, cryptojacking, artificial intelligence (AI)-enabled cyberattacks, and vulnerabilities associated with the Internet of Things (IoT). These threats have expanded the cyber risk landscape and present significant challenges for governments and organizations worldwide.

Cyber threats possess several defining characteristics. They are inherently transnational, allowing attacks to spread rapidly across national borders. They can inflict substantial economic damage, with global financial losses estimated to reach trillions of U.S. dollars annually. Moreover, cyber operations have become an integral component of hybrid warfare, often accompanying conventional military, political, and information campaigns. In addition to digital disruption, cyberattacks may produce physical consequences, including the failure of power grids, transportation systems, healthcare services, and other critical infrastructure, thereby posing serious risks to national and international security.

Chapter 2. The Significance of Cybersecurity in the International Security System

2.1. Cybercrime and Threats to International Security

Cybercrime has emerged as one of the most significant threats to contemporary international security. It not only causes financial losses to individuals and private organizations but also poses serious risks to national economies, critical infrastructure, and social stability. According to recent global estimates, the economic cost of cybercrime reached approximately USD 10.5 trillion in 2025, making the hypothetical entity often referred to as «Cyber Rica» the world's third-largest economy after the United States and China. The global cost is projected to increase to USD 11.88 trillion in 2026.

The principal characteristics of cybercrime include the following:

Transnational nature. Cybercriminals operate beyond geographical boundaries, enabling attacks to be launched from one country against targets located anywhere in the world.

Industrialization of cybercrime. The emergence of business models such as Ransomware-as-a-Service (RaaS) and Fraud-as-a-Service (FaaS) has transformed cybercrime into a highly organized and profitable industry. In 2025, cyber extortion attacks increased by 44.5%, while the number of victims nearly tripled compared with 2020.

Threats to critical infrastructure. Sectors such as healthcare, energy, transportation, and finance remain among the most frequently targeted. Cyberattacks against these sectors may disrupt essential public services and jeopardize national security.

Notable examples include the WannaCry ransomware attack in 2017 and subsequent ransomware campaigns, which severely disrupted hospital operations and endangered millions of lives. Reports indicate that ransomware incidents increased by approximately 42% in 2025. Furthermore, cybercrime has become increasingly interconnected with organized

criminal networks and may serve as a source of financing for terrorist activities. Consequently, cybercrime undermines public confidence in state institutions, weakens governance, and contributes to political and social instability.

In the context of Uzbekistan, cybercrime has also become a growing concern. Between 2021 and 2024, cybercriminals illegally obtained more than UZS 1.9 trillion from citizens, with financial losses exceeding UZS 603 billion in 2024 alone.

2.2. State-Sponsored Cyberattacks and Their Consequences

State-sponsored cyberattacks have transformed cyberspace into a new arena of geopolitical competition. Governments increasingly employ cyber capabilities for espionage, sabotage, political influence, and hybrid warfare. Consequently, the consequences of such attacks extend far beyond economic damage, producing significant strategic, political, and security implications.

Several major cyber incidents illustrate this trend.

The Stuxnet attack (2010), widely attributed to the United States and Israel, targeted Iran's nuclear program and is considered the first large-scale cyber sabotage operation against critical industrial infrastructure.

The NotPetya attack (2017), attributed to Russia's GRU and the Sandworm group, initially targeted Ukraine but rapidly spread worldwide, causing more than USD 10 billion in damages. Major multinational corporations, including Maersk and Merck, suffered severe operational and financial losses. NotPetya is widely recognized as one of the most costly cyberattacks in history.

The SolarWinds supply chain attack (2020), attributed to Russia's SVR and the APT29 (Cozy Bear) group, compromised numerous U.S. government agencies and hundreds of private companies. This incident demonstrated the growing sophistication of cyber espionage and the strategic importance of supply chain security.

More recent developments include cyber operations targeting Ukraine's energy infrastructure and the Viasat satellite network during the Russia–Ukraine conflict, long-term cyber espionage campaigns attributed to China, and cryptocurrency thefts conducted by North Korean hacking groups, which reportedly exceeded USD 2 billion in 2025.

State-sponsored cyberattacks generate several significant consequences. First, the problem of attribution makes it difficult to accurately identify perpetrators, thereby complicating legal accountability and political responses. Second, cyber operations have become an essential component of hybrid warfare, blurring the distinction between peacetime competition and armed conflict. Third, these attacks weaken digital sovereignty by exposing the vulnerability of national digital infrastructure. Finally, they intensify geopolitical tensions, deepen mistrust among major powers, and contribute to an international cyber arms race.

2.3. The Role of International Organizations in Ensuring Cybersecurity

International organizations play an essential role in promoting cooperation against cyber threats; however, their effectiveness remains constrained by geopolitical disagreements and conflicting national interests.

The United Nations (UN) has become one of the principal platforms for developing international norms governing responsible state behavior in cyberspace. Through mechanisms such as the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG), the UN has sought to promote the application of international law in

cyberspace, strengthen confidence-building measures, and establish common normative principles for responsible state conduct. In 2025, cyber threats were once again recognized as serious challenges to international peace and security, highlighting the growing importance of multilateral cooperation in addressing global cyber risks.The new United Nations Convention on Cybercrime is currently under discussion and represents an important step toward strengthening the global legal framework for combating cybercrime and enhancing international cooperation in cyberspace.

The Budapest Convention on Cybercrime (2001), adopted by the Council of Europe, is widely recognized as the first international legally binding treaty specifically addressing cybercrime. It establishes common legal standards for preventing, investigating, and prosecuting cyber offenses while promoting international judicial and law enforcement cooperation. Many countries have acceded to or cooperate within the framework of the Convention, including Uzbekistan. However, several states, most notably Russia and China, have criticized the Convention as reflecting predominantly Western legal and political perspectives.

NATO officially recognized cyberspace as the fifth operational domain in 2016, alongside land, sea, air, and space. Through initiatives such as the Cyber Defence Pledge and the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, NATO has strengthened the cyber defense capabilities of its member states. The Alliance also cooperates closely with the European Union in addressing hybrid threats and enhancing cyber resilience.

The Shanghai Cooperation Organization (SCO) plays a particularly important role for Uzbekistan in the field of cybersecurity. The organization promotes cooperation through agreements on international information security, including the 2009 Agreement on International Information Security, and supports the development of common information security principles. Under the leadership of China and Russia, the SCO advocates the concept of digital sovereignty or the «sovereign Internet», while encouraging regional cooperation against cyber threats.

Other international organizations also contribute significantly to global cybersecurity governance. INTERPOL and Europol facilitate operational cooperation in combating cybercrime, the Organization for Security and Co-operation in Europe (OSCE) promotes confidence-building measures in cyberspace, while regional organizations such as the Association of Southeast Asian Nations (ASEAN) and the African Union (AU) have developed cybersecurity strategies and cooperative mechanisms to strengthen regional cyber resilience.

Chapter 3. Cybersecurity Issues in Uzbekistan and International Practice

3.1. Cybersecurity Policy and Legal Framework in Uzbekistan

In the Republic of Uzbekistan, state policy in the field of cybersecurity has developed rapidly in recent years alongside the country's digital transformation initiatives. A significant milestone was achieved with the adoption of Presidential Decree No. PF-38, signed by President Shavkat Mirziyoyev on 10 March 2026, which approved the Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030. This strategic document establishes the foundation for the development of a comprehensive national cybersecurity system.

The principal objectives of the Strategy include:

- strengthening national cyber resilience and protecting critical information infrastructure;
- systematically reducing cyber risks while enhancing the digital security of citizens, businesses, and public institutions;
- strengthening measures to combat cybercrime;
- promoting digital innovation, artificial intelligence, and technological independence; and
- expanding international cooperation in cybersecurity.

The legal framework for cybersecurity in Uzbekistan is based on several key components. The Law of the Republic of Uzbekistan «On Cybersecurity» serves as the primary legislative foundation governing cybersecurity policy and practice. The State Security Service (SSS) has been designated as the competent authority responsible for cybersecurity at the national level. The legal framework also establishes requirements for the protection, certification, and continuous monitoring of critical information infrastructure. In addition, Uzbekistan is developing Security Operations Centers (SOCs) and national cyber incident response mechanisms to improve early detection and response capabilities. Considerable attention is also devoted to workforce development, improving public cyber literacy, and advancing digital forensic capabilities.

Within the framework of the Digital Uzbekistan–2030 Strategy, the government continues to accelerate the digitalization of public services. While this process contributes significantly to economic modernization, it also increases exposure to cyber threats. Accordingly, the implementation roadmap for 2026–2029 prioritizes the improvement of legislation, modernization of digital infrastructure, and expansion of international cybersecurity cooperation. Nevertheless, several challenges remain, including shortages of qualified cybersecurity professionals, limited participation of the private sector, and continued dependence on imported technologies.

3.2. International Best Practices: The United States, the European Union, South Korea, and Other Countries

The United States possesses one of the world's most advanced cybersecurity systems. Its National Cybersecurity Strategy, updated during 2023–2024, emphasizes close cooperation with the private sector, protection of critical infrastructure, and the development of offensive cyber capabilities. The Cybersecurity and Infrastructure Security Agency (CISA) plays a central role in coordinating national cybersecurity efforts. Key elements of the U.S. approach include cyber threat intelligence sharing, the implementation of Zero Trust Architecture, the application of artificial intelligence for threat detection, and collaboration through international partnerships such as the Five Eyes Alliance. Despite these strengths, concerns remain regarding the protection of personal data and digital privacy.

The European Union (EU) has established a comprehensive cybersecurity framework through the EU Cybersecurity Strategy and the NIS2 Directive, which aim to strengthen the Digital Single Market and reinforce European digital sovereignty. Coordination is primarily carried out by the European Union Agency for Cybersecurity (ENISA). The EU approach emphasizes risk management, the protection of critical infrastructure, and the integration of cybersecurity with personal data protection under the General Data Protection Regulation (GDPR). Member States such as Germany and France further strengthen cyber resilience

through national Computer Emergency Response Teams (CERTs), regular cybersecurity exercises, and close cooperation with NATO in addressing hybrid threats.

South Korea has developed a highly advanced national cybersecurity system in response to persistent cyber threats originating from North Korea. The country's National Cybersecurity Strategy focuses primarily on national defense, economic security, and technological innovation. The Korea Internet & Security Agency (KISA) serves as the leading institution responsible for implementing national cybersecurity policies. Cooperation with the United States has been strengthened through the Strategic Cybersecurity Cooperation Framework (2023), which promotes intelligence sharing, joint cyber exercises, and active cyber defense. South Korea's major strengths include its globally competitive technology sector, represented by companies such as Samsung and LG, a highly cyber-aware population, and an efficient incident response system.

Other countries also provide valuable examples of effective cybersecurity governance. Singapore and Australia have successfully implemented cybersecurity strategies based on the Smart Nation concept, advanced cyber threat intelligence sharing, and strong public-private cooperation. Overall, international experience demonstrates several common trends, including the expansion of Public–Private Partnerships (PPPs), the adoption of international legal standards such as the Budapest Convention on Cybercrime, and the increasing integration of Artificial Intelligence (AI) into cybersecurity management and threat detection systems.

Conclusion

This study demonstrates that cybersecurity has become a new, essential, and strategic dimension of international security in the contemporary international system. Recognized as the fifth domain of warfare, cyberspace has evolved into an arena in which states, non-state actors, and criminal organizations employ cyber capabilities to pursue political, military, and economic objectives. Consequently, cybersecurity is no longer merely a technical issue but has become a critical factor influencing geopolitical competition, national sovereignty, economic resilience, and international peace and security.

The findings of this research lead to several important conclusions.

First, cybersecurity is fundamentally based on the principles of the CIA Triad—Confidentiality, Integrity, and Availability—together with other essential security principles. As cyberspace permeates virtually every aspect of modern society, cyber threats have become increasingly transnational, anonymous, and hybrid in nature, distinguishing them significantly from traditional security threats.

Second, cybercrime and state-sponsored cyberattacks represent serious challenges to international security. Incidents such as WannaCry, NotPetya, and SolarWinds demonstrate that a single successful cyber operation can inflict substantial global economic losses, disrupt critical infrastructure, and intensify geopolitical tensions. These developments further blur the distinction between peace and armed conflict while highlighting the need to reassess existing principles of international law in cyberspace.

Third, although international organizations—including the United Nations (UN), NATO, the Shanghai Cooperation Organization (SCO), and the Budapest Convention on Cybercrime—play an important role in promoting cybersecurity cooperation, existing legal gaps and geopolitical disagreements continue to limit the effectiveness of international governance.

Consequently, states must develop comprehensive national cybersecurity strategies while simultaneously strengthening international cooperation.

In the context of the Republic of Uzbekistan, both the Digital Uzbekistan–2030 Strategy and the Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030 represent significant milestones in establishing a national cybersecurity framework. Nevertheless, several challenges remain, including the shortage of qualified cybersecurity professionals, the need to enhance technological independence, and greater involvement of the private sector. International experience, particularly that of the United States, the European Union, and South Korea, demonstrates that successful cybersecurity policies are founded upon effective public–private partnerships, strong institutional capacity, technological innovation, and active international cooperation.

Based on the findings of this study, the following practical recommendations are proposed:

- Ensure the comprehensive and effective implementation of Uzbekistan's National Cybersecurity Strategy.

- Strengthen cybersecurity education, professional workforce development, and public cyber awareness.

- Modernize critical information infrastructure through the implementation of Zero Trust Architecture principles.

- Deepen international cooperation through active participation in organizations and platforms such as the United Nations, the Shanghai Cooperation Organization, and other multilateral cybersecurity initiatives.

- Promote the development of domestic digital technologies to strengthen national digital sovereignty and reduce dependence on foreign technologies.

Overall, recognizing cybersecurity as a new dimension of international security and allocating adequate political, legal, and institutional attention to this field has become a strategic necessity for all modern states. By strengthening its digital resilience and expanding international cooperation, Uzbekistan has the potential to secure a meaningful position within the global cybersecurity community. Ensuring that cyberspace remains secure, stable, and beneficial to humanity will require sustained and coordinated efforts at national, regional, and international levels.

This study contributes to both the theoretical and practical understanding of cybersecurity while proposing a policy-oriented framework that may be particularly relevant for developing countries such as Uzbekistan. Future research should further explore emerging technological developments and evolving cyber threats in order to support more effective cybersecurity governance and international cooperation.

Adabiyotlar, References, Литературы:

1. President of the Republic of Uzbekistan. Presidential Decree No. PF-38 on the Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030 (2026).

2. United Nations. Reports of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2025).

3. NATO. Cyber Defence Pledge (2024).

4. Cybersecurity Ventures. Cybercrime Report 2025–2026.
5. Additional scholarly publications, policy documents, and international reports relevant to cybersecurity and international security.