https://doi.org/10.31489/2025L4/50-62
UDC 340.341
Received: 28 July 2025 | Accepted: 18 September 2025

L.K. Amandykova[1*], S.N. Sarsenova[2]

[1,2]*Astana International University, Astana, Kazakhstan*
(E-mail: monamie2000@mail.ru, saniyacreating@gmail.com)
[1] *ORCID ID: 0000-0001-5341-1776*
[2] *ORCID ID: 0000-0003-3134-284X*

Practical aspects of Kazakhstan's interaction with the UN in the field of cybersecurity

To enhance the security of its digital environment, the Republic of Kazakhstan closely cooperates with the UN and other international organizations, applying a variety of strategic methods and regulatory instruments to create and implement effective international cybersecurity standards. The increasing risks associated with cyberterrorism, cyberintelligence, and interference in the sovereignty of states through cyberspace necessitate expanded international cooperation. Consequently, the UN's role in coordinating efforts to establish common principles and rules of conduct for states in the cyber environment is growing, reflected in the adoption of new resolutions and the expansion of the mandate of the Open-Ended Working Group on Cybersecurity. Structural, logical, and dialectical approaches were used to analyze Kazakhstan's cybersecurity legislation. The theoretical foundation of the study was formed by examining international law, academic papers, and materials from international organizations. International commitments, particularly within the United Nations, are key to the development and evolution of Kazakhstan's cyber policy. Active engagement in international projects, aligning national legislation with international standards, and implementing strategic programs contribute to enhancing the state's cybersecurity and its integration into the global digital community. A significant factor in this process is the incorporation of international law into national legislation.

Keywords: cybersecurity, UN, cyber threats, international cyber regulation, international law, information law.

Introduction

The relevance of this study stems from the dynamics of recent global trends. The period 2022–2024 was marked by a wave of large-scale cyberattacks targeting both public and private entities in many countries, including the Republic of Kazakhstan. There is an alarming increase in cyberterrorism, cyberespionage, and attempts to destabilize national processes through cyberspace, highlighting the need for intensified international cooperation.

In this context, the UN's role as a coordinator in developing universal principles and norms for state behavior in the digital environment is growing, as reflected in the adoption of new resolutions and the expansion of the mandate of the Open-Ended Group on Cybersecurity. Furthermore, the legal regulation of cybersecurity faces additional challenges associated with the rapid development of artificial intelligence, the Internet of Things, and automated systems. These innovations are generating new types of threats while transforming existing risks. In response to these changes, states are increasingly turning to bilateral and multilateral agreements aimed at strengthening cooperation in the cyberspace domain. This makes an in-depth study of the international legal framework for cybersecurity particularly important, especially in the context of increasing global competition in the technological sphere. Recognizing the scale of threats in cyberspace, states are actively developing national cybersecurity strategies. They are also adopting legislative measures to prevent, detect, and combat cyberthreats, as well as to protect critical infrastructure and guarantee the rights of citizens in the digital space.

In the 21st century, cyberspace has become a new arena for international interaction, where digital technologies play a key role in economics, security, and diplomacy. Amid the rapid growth of cyber threats, the global community faces the need to develop internationally recognized norms and standards of conduct in the information space. The United Nations, as a universal intergovernmental body, serves as the coordinating center for these processes, including through the platforms of the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG).

* Corresponding author's e-mail: *monamie2000@mail.ru*

International experience in interacting with the UN in this area provides important guidance for states developing their own cybersecurity strategies. Particularly illustrative is the experience of the European Union and the Russian Federation: two actors representing different legal, political, and technological approaches to international information security.

Further research requires examining the experiences of other countries in interacting with the UN and other international bodies responsible for cybersecurity. This can be achieved by analyzing case studies of various countries, which will reveal different strategies and approaches to building both their own cybersecurity and legal policies related to cybersecurity in national and international law.

The study draws on the work of Sh. Zabikh, S.A. Shulgin, E. Tikk and M. Kerttunen, identifying problems that, despite the development of the digital economy in Kazakhstan, there is a growing dependence on information technology. This creates new vulnerabilities in cyberspace, requiring additional security measures.

As part of the "Digital Kazakhstan" national program, the country is actively pursuing digital transformation, necessitating the continuous updating of cybersecurity legislation and active international cooperation. These factors underlie the importance of this topic.

The findings of this study will be useful for legal professionals and policymakers. The results can be used to develop state policy in the area of cybersecurity, shape Kazakhstan's foreign policy, and draft international treaties. They can also serve as the foundation for educational and analytical materials on international law and ICT security.

The purpose of the study is to identify practical aspects of Kazakhstan's interaction with the UN in the field of cybersecurity, as well as to develop recommendations for improving the legal framework for international cooperation.

Research objectives:

- to study existing international legal norms governing cybersecurity;
- to analyze Kazakhstan's participation in international agreements and UN initiatives on this topic;
- to consider mechanisms of cooperation between Kazakhstan and other countries with international organizations in the field of information security;
- to identify ways to improve international legal regulation of cyber threats.

The object of study is the scope of international legal regulation of cybersecurity, with particular attention to the forms and content of interaction between the Republic of Kazakhstan and the United Nations and other international organizations in the context of ensuring digital security.

The subject of research is legal instruments and processes that ensure the implementation of international norms and obligations in the national cybersecurity policy of the Republic of Kazakhstan. Specifically, the adaptation of international standards, the country's participation in UN initiatives, and their cumulative impact on the evolution of domestic legislation and the development of information security infrastructure are analyzed.

Methods and materials

This study included an in-depth analysis of the theoretical and legal aspects of cybersecurity in Kazakhstan, encompassing both international and national norms. The methodological basis of the work was a systemic-structural, logical, and dialectical approach to studying scientific and legal literature. Key sources of information included regulatory legal acts of the Republic of Kazakhstan, as well as academic works, including monographs, dissertations, and educational materials. Information provided by the United Nations was used to form the theoretical basis of the article.

Results

The United Nations has consistently affirmed the applicability of international law to cyberspace. The UN Charter, along with fundamental principles such as state sovereignty, non-interference in internal affairs, the prohibition of the use of force, and respect for human rights, also apply to the field of information and communications technology [1–3]. These provisions were recognized in the 2013 and 2015 reports of the Group of Governmental Experts (GGE), as well as in the 2021 report of the Open-Ended Working Group (OEWG). Consequently, states are obliged to comply with international legal norms when conducting cyber operations.

Resolution A/RES/79/243: UN Convention against Cybercrime

Resolution A/RES/79/243, adopted on December 24, 2024, endorsed the first-ever global, legally binding UN Convention against Cybercrime. This international instrument aims to prevent and combat cybercrime, as well as strengthen cooperation between states in this area [4].

The development of the Convention dates back to 2019, when an intergovernmental expert group was established to analyze cybercrime issues. In 2021, the General Assembly established an Ad Hoc Committee to draft a comprehensive convention. A series of sessions was held in New York and Vienna from 2022 to 2024, culminating in the adoption of the final text in August 2024.

The Convention comprises nine chapters addressing key aspects of the fight against cybercrime. It establishes provisions for the criminalization of acts, such as unauthorized access to information systems, interference with data, the use of malware, and the commission of crimes using ICTs, including fraud and extortion. Procedural rules provide for effective methods of investigation and collection of digital evidence while respecting human rights. Significant attention is paid to international cooperation: extradition procedures, legal assistance, and joint investigations are regulated. Furthermore, the text of the Convention contains provisions on providing technical assistance to developing countries and measures to build their capacity [4].

The document represents an important step towards the development of universal standards and the harmonization of national legislation by providing minimum mandatory legal provisions to be implemented by participating States. This helps eliminate legal conflicts in cross-border cybercrime investigations and increases the level of cooperation between jurisdictions [4].

The Convention places particular emphasis on the protection of human rights. It prohibits the arbitrary collection and transfer of personal data, requires legal oversight of law enforcement actions, upholds the principle of proportionality in the application of investigative measures, and draws on the International Covenant on Civil and Political Rights. This ensures a balance between the interests of law and order and the fundamental rights of the individual [4].

An important aspect is the establishment of technical support mechanisms for developing countries. The Convention provides financial and expert assistance in drafting legislation, training personnel, and establishing national cyber incident response teams. It also promotes technology transfer and the development of resilient digital infrastructure [4].

The document will be opened for signature in 2025 at a ceremony in Hanoi, and then at UN headquarters in New York until the end of 2026. To enter into force, the Convention must be ratified by 40 states. A Conference of States Parties will subsequently be established to monitor its implementation and consider possible amendments [4].

Thus, the UN Convention against Cybercrime represents a significant achievement in institutionalizing the global fight against digital crime. It strengthens norms of international cooperation, promotes greater legal certainty, and emphasizes the need to respect human rights in the context of digital transformation.

Discussion

The Group of Governmental Experts (GGE): History and Contributions

The Group of Governmental Experts on Developments in the Field of Computer Science in the Context of International Security (GGE) was established by the UN General Assembly in response to growing concern among states about the risks associated with the use of information and communications technologies (ICT) for purposes threatening international security. The reasons for the creation of the GGE were the lack of generally accepted rules of conduct for states in cyberspace, the increasing number of cross-border cyber incidents, and the need to interpret the applicability of existing international law to action in the digital environment, as well as the desire to prevent an arms race in cyberspace.

Since its inception, the GGE has conducted seven working cycles. The first group (2004–2005) did not reach consensus but laid the foundation for subsequent discussions [1]. The second GGE (2009–2010) recognized the need to apply international law and norms to the ICT sphere [1]. The third GGE (2012–2013) formally reaffirmed for the first time the applicability of the UN Charter and the principles of international law in cyberspace [5]. The fourth GGE (2014–2015) developed 11 voluntary norms of responsible state behavior. The fifth GGE (2016–2017) concluded without a final report due to disagreements among participating states [2]. The sixth GGE (2019–2021) presented a new final report with clarifications on international law, norms, and confidence-building measures [3]. The seventh GGE (2023–2024) focused on transparency measures, capacity building and conflict prevention in the digital environment; its report is expected in 2025 [6].

Among the key documents of the GGE, the 2013 GGE Report (A/68/98) recognized the application of international law to cyberspace, the 2015 GGE Report (A/70/174) contained 11 norms of responsible behavior of states, and the 2021 GGE Report (A/76/135), which developed approaches to international law, confidence-building measures, and technical cooperation. These documents formed the basis of the normative architecture in the field of international cybersecurity and serve as a guide for subsequent work within the UN [5][3].

Thus, the GGE has played a fundamental role in legitimizing the application of international law to cyberspace, shaping basic norms of state behavior, and promoting confidence-building measures between states.

Open-Ended Working Group (OEWG): Rationale, Documents, and an Inclusive Approach to Cybersecurity

The Open-Ended Working Group on ICTs and International Security (OEWG) was established by UN General Assembly Resolution 73/27 in 2018 in response to criticism of the GGE's limited membership and the need for an inclusive approach. Its creation was prompted by demands from developing countries for broader representation in the development of international cyber rules, a desire to ensure transparency and legitimacy in negotiations, and the need to discuss cybersecurity issues in a multilateral format, rather than solely among experts.

The OEWG became the first UN platform open to participation by all Member States. Its key documents were the OEWG Final Report (A/75/816) of March 2021, which reaffirmed the applicability of international law and proposed recommendations for confidence-building, technical assistance, and cooperation, as well as the OEWG Interim Report for the 2023–2025 Cycle (A/78/350), which assessed progress in implementing previously agreed measures [7]. In addition, an Action Plan was developed until 2025, which includes holding global workshops, supporting national incident response centers (CSIRT/CERT), and implementing ICT security standards [8].

Important achievements of the OEWG have included stimulating the development of national cybersecurity strategies, recommending the establishment of computer incident response teams, confidence-building measures (including state-to-state communication channels, joint exercises, and technical information sharing), and promoting the development of developing countries' digital security capabilities.

The OEWG format has significantly strengthened the engagement of countries in the Global South in the dialogue on digital security and has become an important platform for coordinating positions, developing common approaches, and increasing transparency in international cyber policy.

Key provisions of the ITU standards in the field of cybersecurity

One of the key players in shaping the global cybersecurity architecture is the International Telecommunication Union (ITU), a specialized UN agency coordinating standards and initiatives in the field of information and communications technology (ICT). The ITU's strategic instrument for global regulation is the Global Cybersecurity Agenda (GCA), launched in 2007 [9–11]. The GCA is a framework platform aimed at strengthening international cooperation to enhance trust and security in the use of ICTs. This initiative covers five mutually reinforcing areas:

Legal measures — the ITU emphasizes the importance of developing and harmonizing legislation aimed at combating cybercrime and ensuring cybersecurity. This includes the creation of model legislation that can be adapted by member countries to create an effective legal framework. Such measures promote international cooperation and provide a basis for prosecuting cybercrime.

Technical Measures — the ITU actively develops and promotes technical standards and procedures aimed at enhancing the security of ICT infrastructure. This includes recommendations on risk management, data protection, and incident response. The organization also collaborates with other standardization bodies and industry groups to ensure the consistency and effectiveness of technical measures.

Organizational Structures — the establishment and strengthening of national and international institutions responsible for the coordination and management of cybersecurity is a key focus of the GCA. This includes the formation of national Computer Incident Response Teams (CIRTs), the development of crisis management strategies, and the protection of critical information infrastructure.

Capacity Development — the ITU places great importance on the education and training of cybersecurity professionals. The organization conducts training events, such as CyberDrills, and provides methodological recommendations to raise awareness and develop skills. Particular attention is paid to supporting developing countries and promoting the participation of women in international cybersecurity processes.

International Cooperation — The GCA promotes international cooperation in cybersecurity by encouraging information sharing, joint exercises, and the development of common standards. This includes participation in international fora, cooperation with other organizations, and support for countries in developing and implementing national cybersecurity strategies [11, 9, 10].

The GCA's significant regulatory and institutional framework is complemented by ITU resolutions aimed at specifying the functions and objectives of the state and the international community in ensuring digital security. Resolution No. 130 (Bucharest, 2022) emphasizes the need to strengthen the role of the ITU as the central international mechanism for trust and security in the use of ICTs. Resolution No. 174 (Busan, 2014) expands this agenda by establishing ITU's competence in international policy to prevent the illicit use of ICTs. Of particular significance is Resolution No. 179 (Bucharest, 2022), which establishes standards for the protection of children in the digital environment, emphasizing the social responsibility of participants in digital interactions [12].

To monitor and benchmark the cybersecurity status of ITU member states, the ITU developed the Global Cybersecurity Index (GCI). The GCI methodology includes five criteria: the presence of a legal framework, technical measures, organizational structure, capacity development programs, and participation in international cooperation. Published every two years, the GCI rankings enable countries to identify gaps in their national cybersecurity systems and adopt effective practices from more advanced states. According to recent reports, Kazakhstan has demonstrated positive dynamics, moving up the GCI rankings, demonstrating the effectiveness of its measures and adherence to international benchmarks [12].

Along with assessment tools, ITU actively assists countries in developing national cybersecurity strategies and establishing Computer Incident Response Teams (CIRTs). As part of this work, the organization:

- develops methodological recommendations for building cybersecurity strategies and architecture;
- conducts training courses and cyber exercises (CyberDrills) for specialists;
- provides assistance in the creation and modernization of national CIRTs, including readiness diagnostics, planning and technical support [13; 57].

The UN demonstrates a systematic and consistent approach to developing the international legal regime for cyberspace. Through the GGE and OEWG mechanisms, as well as through the development of global treaties, such as the Convention against Cybercrime, the organization is developing universal norms to ensure both international security and the protection of human rights in the digital age. Kazakhstan's participation in these initiatives strengthens its position on the international stage and develops an effective national cybersecurity policy.

ITU's activities also encompass all key aspects of cybersecurity, from international normative initiatives to direct technical and institutional support for states. For Kazakhstan, which is actively involved in these processes, participation in ITU programs contributes to enhancing the resilience of its digital infrastructure and integrating it into the global cybersecurity system [14; 95, 15; 33].

With the rapid development of digital technologies and the growth of cyber threats, international cooperation between states is becoming critical to ensuring global and national cybersecurity. The United Nations (UN) plays a key role in developing universal norms and approaches in this area, creating a platform for dialogue and cooperation between countries. Kazakhstan, recognizing the importance of a multilateral approach to cybersecurity issues, actively participates in UN initiatives aimed at strengthening international information security and developing agreed standards for state behavior in cyberspace. This subchapter examines Kazakhstan's interactions with the UN, including its areas, achievements, and existing challenges.

Examples of interaction between the Republic of Kazakhstan and the UN and international organizations in the field of cybersecurity

The Republic of Kazakhstan actively participates in the activities of the UN Open Working Group on Promoting Responsible State Behavior in the Cyberspace. During the ninth session of the OEWG (2021–2025), Kazakhstan proposed developing standardized templates for classifying cyber threats and post-incident communications to improve the effectiveness of the Global Point of Contact Directory. Furthermore, Kazakhstan emphasized the need to develop global guidelines for ensuring the security of emerging technologies, such as artificial intelligence, quantum computing, and machine learning, and proposed conducting cyber exercises and attack simulations to strengthen states' cybersecurity capacity [16].

Close cooperation with the ITU on various cybersecurity initiatives is also noted. In September 2022, an interregional cyber training seminar for the CIS and Arab States was held in Almaty, organized by the ITU jointly with the Ministry of Digital Development, Innovation, and Aerospace Industry of Kazakhstan and the

Cyberattack Analysis and Investigation Center (CAAC). Participants discussed the role of national computer incident response teams (CIRTs/CSIRTs) and measures to protect critical information infrastructure [17].

In addition, Kazakhstan participated in the global GIGA initiative, together with ITU and UNICEF, with the aim of connecting all schools to the internet and providing young people with access to information and opportunities.

Within the framework of this project, Kazakhstan provided high-speed Internet to 446 rural schools, planning to expand coverage to 1,342 schools [18].

Kazakhstan is implementing the national cybersecurity concept "Kazakhstan Cyber Shield", which includes measures to enhance the legal and industrial culture in the field of cybersecurity, improve preparedness for preventing and responding to incidents, and raise public awareness of cyber threats [19].

In 2024, a regional project on digital transformation of the public sector, funded by the Government of the Republic of Korea and implemented with the support of UNDP, was launched in Almaty. The project aims to develop digital governance in 12 countries of Central Asia, the Caucasus, and the Asia-Pacific region, including Kazakhstan [19].

Kazakhstan also presented innovative solutions in the field of digital transformation of social protection, including the "Digital Family Card" project, at the Asia-Pacific Ministerial Conference on Digital Inclusion and Transformation. The project aims to ensure equal access of citizens to state support in the social sphere and was highly praised by the international community [19].

Kazakhstan actively participates in regional cybersecurity initiatives. In September 2023, interagency consultations of SCO member states were held in Almaty on the establishment of an information security center based at the Regional Anti-Terrorism Structure in Tashkent. Kazakhstan presented a concept for creating such a center that would promptly respond to emerging cyber threats and protect the information space of the SCO region [20].

In addition, in November 2023, Kazakhstan and Azerbaijan signed a memorandum of understanding in the field of information security, aimed at increasing the level of cooperation in responding to information security incidents, exchanging best practices and information on current cyber threats [20].

Kazakhstan, with the support of UNICEF and the European Union, launched the "CYBER TUMAR" information and educational campaign aimed at protecting children online. The campaign includes information materials, practical advice from experts, and educational videos to help children navigate cyberspace safely [21].

In May 2023, a sub-regional training on ICT security for representatives of Central Asian countries and Mongolia was held in Astana, organized by the OSCE, together with the Ministry of Digital Development, Innovation, and Aerospace Industry of Kazakhstan, with support from the United Kingdom, has provided a significant platform for international cooperation aimed at strengthening cybersecurity and ICT development in the region [22].

Thus, Kazakhstan actively participates in international and regional cybersecurity initiatives, cooperates with key international organizations, implements national projects and programs aimed at strengthening cybersecurity, and actively participates in educational and awareness-raising initiatives. These efforts contribute to strengthening national and international security in the digital space.

The Republic of Kazakhstan considers cybersecurity as a key area of national and international security, while recognizing the important coordinating role of the United Nations in the development of global legal standards in this area [5; 7; 6]. In the context of active digital development, Kazakhstan is consistently integrating the provisions of international documents developed within the UN into its own regulatory framework.

One of the most important areas of cooperation with the UN has been Kazakhstan's participation in the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE) on International Information Security. Kazakhstan officially supports the core principles developed by these formats, including respect for state sovereignty in cyberspace, the prohibition of interference in the internal affairs of states, the principle of non-discriminatory access to ICTs, and the need for international cooperation to prevent cyber conflicts [6; 8; 11; 22].

In the context of adapting international norms, Kazakhstan has taken a number of steps to reform its legislative system. Thus, articles aimed at combating cybercrime were introduced into the Criminal Code of the Republic of Kazakhstan (2014 and subsequent amendments) (e.g., Article 205 "Unauthorized access to information", Article 207 "Creation, use, or distribution of malicious software", etc.). These provisions largely correlate with international standards enshrined in the Budapest Convention of the Council of Eu-

rope, as well as UN recommendations, despite the fact that Kazakhstan has not officially acceded to the convention [5; 23].

The European Union: An Integrative Approach to International Cybersecurity

The EU actively participates in the development of international norms and standards, positioning itself as a leader in promoting the principles of the rule of law, human rights protection, and international cooperation in the digital environment. Although the European Union itself is not a state and does not have formal membership in the UN, its participation in international platforms is carried out both through member states and directly as a regional subject of international law [24].

Within the OEWG and GGE, EU representatives consistently promote the application of existing international law to cyberspace. Particular emphasis is placed on the applicability of the UN Charter, international humanitarian law, and the principle of the inadmissibility of aggression, including in digital form. The EU also emphasizes the need for confidence-building measures, transparency, and accountability, which are the foundation for building a stable cyber environment [25].

At the institutional level, the EU has taken a number of steps to consolidate its cybersecurity efforts internally. A central role here is played by the European Union Agency for Cybersecurity (ENISA), whose mandate was significantly strengthened following the adoption of the Cybersecurity Act in 2019. ENISA has become not only an analytical and technical center but also a link between the national structures of EU Member States and international partners, including UN agencies [26].

Another important element of EU policy has been the introduction of a cybersecurity certification system. This system, based on three levels of trust, serves as a tool for harmonizing the assessment of ICT products and services, reducing digital market fragmentation and promoting trust both within the EU and beyond. It is particularly important that these certification approaches are becoming the subject of international dialogue, being promoted within the UN and ITU platforms.

A key feature of the EU's strategy is its attempt to combine domestic legal regulation and external diplomatic activity. For example, in November 2024, the EU Council adopted a declaration on the applicability of international law in cyberspace, thereby reaffirming its commitment to existing legal regimes and its willingness to promote these norms in international forums. Thus, the EU is effectively exporting its legal approaches to the global level, facilitating the institutionalization of international cybersecurity.

Russia: Digital Sovereignty and Legal Universalization

The Russian Federation exemplifies a different approach to cybersecurity, centered on the principles of state sovereignty, the equality of states, and the inadmissibility of interference in internal affairs. Since the late 1990s, Russia has actively shaped the UN agenda on international information security. Among the first initiatives were UN General Assembly resolutions, beginning with A/RES/53/70, initiated by Russia and forming the basis for the creation of the Global Geographic Environment (GGE).

At the OEWG, Russia emphasizes the need to develop legally binding international documents regulating the behavior of states in cyberspace. In 2021, an initiative was introduced to develop an international convention on information security, enshrining principles, such as digital sovereignty, the prohibition of cyber aggression, and the inadmissibility of using ICTs for military and destabilizing purposes [27].

Along with its efforts within the UN, Russia is actively working within the UN Office on Drugs and Crime (UNODC), promoting the idea of a comprehensive Convention on Cybercrime. At the same time, contacts are developing with the ITU, where Russia is promoting initiatives to strengthen the role of states in the governance of the internet and technical resources such as DNS and IP addressing [28].

At the national level, Russia implements a multi-layered cybersecurity policy, including the Information Security Doctrine (2016), Federal Law No. 187-FL "On the Security of Critical Information Infrastructure" and the National Digital Transformation Strategy. These documents define the regulatory framework for state control over the digital space and measures to reduce dependence on foreign technologies [29].

International cooperation is also pursued within the SCO, CSTO, BRICS, and through bilateral agreements. Particularly significant is the Memorandum of Understanding between Russia and China (2015), which commits both parties to preventing cyberattacks from each other's territory. Similar agreements have also been signed with Kazakhstan, India, Iran, and several other countries.

The United States: International Law and Digital Stability

The United States of America is a key participant in the development of a global cybersecurity architecture, emphasizing the applicability of existing international legal norms in cyberspace and promoting the principles of openness, transparency, and accountability. Since the early 2000s, the United States has con-

sistently participated in the development of norms for state behavior in the digital environment at the UN [30].

US initiatives within the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) aim to reaffirm the applicability of the UN Charter, international humanitarian law, and principles of international responsibility to actions in cyberspace. The US insists that fundamental norms, including the prohibition of the use of force, sovereignty, non-interference, and the need to respect human rights, should apply regardless of the technological environment [16].

Particular attention is being paid to the development of voluntary, yet politically significant, norms. The United States supported the development of 11 norms of responsible state behavior, as outlined in the 2015 GGE report (A/70/174), including:

- refraining from causing damage to critical infrastructure;
- assistance to states affected by cyberattacks;
- vulnerability notification and threat information sharing [3].

At the OEWG, the United States actively promotes the idea of engaging all stakeholders—including the private sector, academia, and NGOs—in the process of shaping international cyber policy. This approach, according to the United States, ensures a more resilient and flexible system for global digital risk management.

In 2017, amid a growing number of cyber incidents, the American company Microsoft introduced the Digital Geneva Convention, which received support from expert and diplomatic circles. The document envisaged the introduction of international obligations similar to the Geneva Conventions, aimed at protecting citizens from the consequences of interstate cyberattacks. Proposed measures included a ban on cyberattacks on critical infrastructure, a ban on the introduction of backdoors into products, and the creation of an independent attribution mechanism [26].

The United States also actively opposes alternative concepts of cyber regulation, particularly those promoted by Russia and China under the term "information security". In its speeches at the UN, US officials also emphasize that these concepts replace cybersecurity goals with issues of internal control, undermine freedom of speech, and create risks of internet fragmentation. Thus, during the OEWG discussions in 2021–2022, the US directly rejected the initiative to develop a legally binding convention on information security, proposed by the Russian Federation, citing the lack of broad consensus and the risks of restricting digital rights [31].

At the national level, US cyber policy is based on strategic documents: the Cyberspace Solarium Commission Report (2020), the National Cybersecurity Strategy (2023), and a series of presidential directives and orders, such as Executive Order 14028 "Improving the Nation's Cybersecurity". These documents define the principles of public-private partnerships, incident liability, and deterrence strategy in cyberspace [32].

US international cooperation is implemented through bilateral agreements (e.g., with the UK, Israel, Japan, Australia, etc.), as well as through the Quad initiative, the NATO Cyber Defense Pledge, the Clean Network, and the Paris Call for Trust and Security in Cyberspace.

Conclusion

The European Union emphasizes regionalism, institutionalization, and the promotion of soft law. The EU actively develops and implements regulations and directives that are binding on member states and focuses on the use of structural and administrative mechanisms to ensure cybersecurity within the region. An example is the EU Network and Information Systems Security Directive (NIS Directive), which requires member states to implement national cybersecurity strategies and establish national incident response centers. The EU is also actively engaged in the creation of new norms and standards within the European Cybersecurity Agency (ENISA), providing member states and private companies with recommendations and best practices. This approach encourages coordination and cooperation within the region but generally has limited impact beyond its borders.

Russia, on the contrary, emphasizes the need for global universalism and legal rigor. Russia seeks to transform soft law into hard law, insisting on the adoption of international conventions regulating the behavior of states in cyberspace. Russia's most important initiative is the proposal to develop an international convention on information security within the UN. This convention should include mandatory norms that will ensure protection from cyberattacks and define the rules of conduct for states in cyberspace. Russia emphasizes the importance of creating universal international norms that will be binding on all countries. Also, unlike the EU, Russia emphasizes a legal platform with investigation and coordination mechanisms within the

UN, such as the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), with the aim of creating global mechanisms for legal assistance and investigation of incidents.

The United States, as a leading global power, actively participates in international debates, proposing its approaches to cybersecurity regulation. The United States favors international cooperation and a liberal approach, often focusing on soft law and flexibility in cyberspace regulation. An example is the Digital Geneva Convention initiative, proposed in 2017, which aims to establish international norms of conduct in cyberspace but is not legally binding. The United States actively participates in UN forums, such as the Group of Governmental Experts (GGE), where it promotes the concept of establishing norms and standards for regulating cyber threats, while emphasizing the importance of the private sector and states in coordinating efforts.

Kazakhstan actively participates in the work of the UN Open-Ended Working Group (OEWG), presenting initiatives that address the digital needs and priorities of developing countries. This includes proposals for technical support, exchange of expertise and specialists, and the development of standards to ensure sovereign control of data. The country promotes the creation of a Central Asian Cyber Coordination Center to strengthen cooperation between regional countries, international organizations, and businesses in the field of cybersecurity, accelerates the process of unifying cybersecurity terminology and procedures at the national level, using International Telecommunication Union (ITU) standards and UN recommendations. It is also important to integrate soft law documents into educational programs and regulations. Kazakhstan also develops a system for international evaluation and certification of domestic information security (IS) solutions. It ensures their recognition abroad and compliance with international requirements, which is especially important for IT product exports. Along with it, the country integrates digital diplomacy into the activities of the Ministry of Foreign Affairs and expand the functions of digital attachés in diplomatic missions in key international organizations and countries (UN, EU, ASEAN, etc.).

As noted by Satbaeva A.M. et al. (2023), an important step in rapprochement with international practices was the adoption of the “Kazakhstan Cyber Shield” Cybersecurity Concept aimed at creating a unified legal and organizational approach to protecting digital infrastructure [6; 29]. The concept was developed based on an analysis of best international practices and contains provisions harmonized with UN General Assembly resolutions on ICT in the context of international security.

Furthermore, from 2022 to 2024, Kazakhstan actively developed bilateral and multilateral cooperation with relevant UN agencies, such as the International Telecommunication Union (ITU) and the United Nations Office on Drugs and Crime (UNODC). With the support of these agencies, Kazakhstan participated in training sessions, conducted cyber incident response exercises, and promoted initiatives to provide legal training to specialists and law enforcement officers [2; 7].

Adaptation of international norms is also taking place at the institutional level. For example, the Republic of Kazakhstan has established a State Technical Service (STS) responsible for monitoring cyber threats, a functioning Information Security Coordination Center, and adopted by laws regulating the processing and storage of personal data, user identification, and provider obligations. These measures are aligned with legal practices in force within the European Union and recommended by the UN [10; 14].

Thus, Kazakhstan’s interaction with the UN in the area of cybersecurity is characterized by a comprehensive approach, combining participation in international consultations and working groups with the active adaptation of international law into the national legal system. This demonstrates Kazakhstan’s commitment to integrating into global cyberspace based on international legal responsibility, transparency, and mutual trust.

Acknowledgements

This study was carried out with the financial support of the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (IRN BR24993082 «Comprehensive study of the humanitarian aspects of information security in Kazakhstan and the components of «soft power» in ensuring sustainable development and consolidation of Kazakhstani society»).

References

1 Постановление Республики Казахстан от 24 июля 2024 г. № 592 «Об утверждении Концепции развития искусственного интеллекта на 2024–2029 годы». — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P2400000592.

2 General Assembly of the United Nations. Report the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Distr.: General 24 June 2013. — [Electronic resource]. — Access mode: https://docs.un.org/en/A/68/98.

3 General Assembly of the United Nations. Report the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Distr.: General 22 July 2015. — [Electronic resource]. — Access mode: https://docs.un.org/en/A/70/174.

4 United Nations Convention against Cybercrime; strengthening international cooperation in combating certain crimes committed using information and communication systems and in the exchange of electronic evidence related to serious crimes Adopted by General Assembly resolution 79/243 of December 24, 2024. — [Electronic resource]. — Access mode: https://https://www.un.org/ru/documents/treaty/A-RES-79-243.

5 General Assembly of the United Nations. Resolution adopted by the General Assembly [on the report of the Second Committee (A/57/529/Add.3)] 57/239. Creation of a global culture of cybersecurity. Distr.: General 31 January 2003. — [Electronic resource]. — Access mode: https://docs.un.org/en/A/RES/57/239.

6 General Assembly of the United Nations. Report the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Distr.: General 14 July 2021. — [Electronic resource]. — Access mode: https://docs.un.org/en/A/76/135.

7 General Assembly of the United Nations. Resolution adopted by the General Assembly on 5 December 2018 [on the report of the First Committee (A/73/505)]. 73/27. Developments in the field of information and telecommunications in the context of international security. Distr.: General 11 December 2018. — [Electronic resource]. — Access mode: https://docs.un.org/en/a/res/73/27.

8 General Assembly of the United Nations. Report the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Distr.: General 14 July 2021. — [Electronic resource]. — Access mode: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf.

9 ISO/IEC 27035-1:2016 Information security incident management. Part 1: Principles // ISO. — [Electronic resource]. — Access mode: https://www.iso.org/standard/60803.html.

10 ISO/IEC 27032:2012 "Guidelines for cybersecurity" // ISO. — [Electronic resource]. — Access mode: https://www.iso.org/standard/44375.html.

11 General Assembly of the United Nations. Report the Developments in the field of information and telecommunications in the context of international security. Distr.: General 18 March 2021. — [Electronic resource]. — Access mode: https://docs.un.org/en/A/75/816.

12 ISO/IEC 27035-1:2016 "Information security incident management". Part 1: Principles // ISO. — [Electronic resource]. — Access mode: https://www.iso.org/standard/60803.html.

13 Рубан Ю. П. Международно-правовое регулирование киберпространства [Электронный ресурс] / Ю. П. Рубан // Вестник МГИМО-Университета. — 2020. — № 1. — С. 57–64. — Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie- kiberprostranstva.

14 Забих Ш. Международный опыт правового обеспечения информационной безопасности и возможности его применения в Республике Казахстан [Электронный ресурс] / Ш. Забих. — Przegląd Politologiczny. — 2020. — № 3. — С. 95–107. — DOI: 10.14746/pp.2020.25.3.6. — Режим доступа: https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_14746_pp_2020_25_3_6.

15 Шульгина С. А. Правовые аспекты кибербезопасности в международных отношениях: роль международных норм и договоров [Электронный ресурс] / С.А. Шульгина // Человек. Знак. Техника. — 2024. — № 2. — С. 33–37. — Режим доступа: https://repo.ssau.ru/bitstream/Chelovek-Znak-Tehnika/Pravovye-aspekty-kiberbezopasnosti-v-mezhdunarodnyh-otnosheniyah-rol-mezhdunarodnyh-norm-i-dogovorov-110822/1/978-5-93424-903-9_2024_33-37.pdf.

16 Kazakhstan Statement at OEWG 2021–2025. — UNeStatements. — [Electronic resource]. — Access mode: https://estatements.unmeetings.org/estatements/12.1255/20241206100000000/bU WavSrotn/RVjgCXnyc_en.pdf.

17 ITU. Cybersecurity Events — Regional Cyberdrill for CIS and Arab States // International Telecommunication Union. — [Electronic resource]. — Almaty, 2022. — Access mode: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-events.aspx.

18 GIGA Initiative: Connecting Every School to the Internet // International Telecommunication Union. — [Electronic resource]. — Access mode: https://www.itu.int/en/ITU- D/Initiatives/GIGA/Pages/default.aspx.

19 Cyber TUMAR: Informational and Educational Campaign Launched in Kazakhstan to Protect Children Online // UNICEF Kazakhstan. — [Electronic resource]. — Access mode: https://www.unicef.org/kazakhstan/en/press-releases/cyber-tumar-informational-and-educational-campaign-launched-kazakhstan-protect

20 SCO Member States Interdepartmental Consultations on Establishing Information Security Centre // Shanghai Cooperation Organisation. — [Electronic resource]. — Access mode: https://eng.sectsco.org/20230914/SCO-member-states-interdepartmental- consultations-on-establishing-information-security-centre-956495.html.

21 OSCE ICT Security Training in Astana for Central Asia and Mongolia // Organization for Security and Co-operation in Europe. — [Electronic resource]. — Access mode: https://www.osce.org/secretariat/544345.

22 Tikk E. The Role of the UN GGE in Advancing International Norms on Responsible State Behavior in Cyberspace [Electronic resource] / E. Tikk, M. Kerttunen // UNIDIR. — 2020. — Access mode: https://unidir.org/publication/role-un-gge-advancing-international-norms- responsible-state-behaviour-cyberspace.

23 Cybercrime Convention Portal // United Nations Office on Drugs and Crime. — [Electronic resource]. — Access mode: https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

24 European Union Institute for Security Studies. OEWG Side-Event: Cybersecurity for the Common Good: Strengthening Nonprofits Engagement. — [Electronic resource]. — Access mode: https://www.iss.europa.eu/activities/event/oewg-side-event-cybersecurity- common-good-strengthening-nonprofits-engagement.

25 European Union Institute for Security Studies. Advancing the Cyber Programme of Action (PoA). — [Electronic resource]. — Access mode: https://www.iss.europa.eu/projects/advancing-cyber- programme-action-poa.

26 EU statement at the UN OEWG — Norms of responsible State behaviour // European External Action Service. — [Electronic resource]. — Access mode: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2 %80 %93- un-open-ended-working-group-cybersecurity-rules-norms-and-principles- responsible_en.

27 Ministry of Foreign Affairs of the People's Republic of China. Remarks by Mr. Wang Lei, Head of Chinese Delegation and MFA Cyber Affairs Coordinator, at the OEWG. — [Electronic resource]. — Access mode: https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjfywj_665252/20250 3/t20250307_11570776.html.

28 EU Cyber Direct. China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. — [Electronic resource]. — Access mode: https://eucyberdirect.eu/atlas/sources/china-s- submissions-to-the-open-ended-working-group-on-developments-in-the-field-of- information-and-telecommunications-in-the-context-of-international-security.

29 United Nations Economic and Social Commission for Asia and the Pacific. Asia- Pacific Ministerial Conference on Digital Inclusion and Transformation, 3–5 September 2024, Astana. — [Electronic resource]. — Access mode: https://www.unescap.org/events/2024/asia-pacific-ministerial-conference-digital- inclusion-and-transformation.

30 U.S. Department of State. Explanation of Position at the Conclusion of the 2016– 2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security 2017. — [Electronic resource]. — Access mode: https://2017-2021.state.gov/explanation- of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental- experts-gge-on-developments-in-the-field-of-information-and- telecommunications-in-the-context-of-international-sec/.

31 Council on Foreign Relations. The Dangers of a New Russian Proposal on a UN Convention on International Information Security // CFR blog. — [Electronic resource]. — Access mode: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention- international-information-security.

32 US Cyber Force Surges Global Operations Amid Rising Threats // BankInfoSecurity 2024. — [Electronic resource]. — Access mode: https://www.bankinfosecurity.com/us-cyber-force-surges-global-operations-amid- rising-threats-a-26889.

Л.К. Амандықова, С.Н. Сәрсенова

Қазақстанның БҰҰ-мен киберқауіпсіздік саласындағы өзара іс-қимылының практикалық аспектілері

Қазақстан Республикасы өзінің цифрлық ортасының қорғалуын арттыру мақсатында Қазақстан Республикасы киберқауіпсіздіктің пәрменді халықаралық нормаларын жасау және іске асыру үшін әртүрлі стратегиялық әдістер мен реттеуші құралдарды қолдана отырып, БҰҰ-мен және басқа да халықаралық құрылымдармен тығыз ынтымақтасады. Кибертерроризмге, кибербарлауға және киберкеңістік арқылы мемлекеттердің егеменді істеріне араласуға байланысты тәуекелдердің артуы байқалады, бұл халықаралық өзара іс-қимылды кеңейту қажеттілігін туғызады. Осыған байланысты БҰҰ-ның кибер ортада мемлекеттердің тәртібінің жалпы қағидаттары мен ережелерін қалыптастыру жөніндегі іс-қимылдарды үйлестірудегі маңыздылығы артып келеді, бұл жаңа қаулар қабылдауда және кибернетикалық қауіпсіздік мәселелері бойынша ашық құрамдағы жұмыс тобының өкілеттіктерін кеңейтуде көрінеді. Киберқауіпсіздік саласындағы қазақстандық заңнаманың ережелерін талдау үшін құрылымдық, логикалық және диалектикалық тәсілдер қолданылды. Зерттеудің теориялық негізі халықаралық құқық нормаларын, ғылыми жұмыстар мен халықаралық ұйымдардың материалдарын зерделеу негізінде қалыптасты. Қазақстан кибер саясатының қалыптасуы мен эволюциясында, атап айтқанда, Біріккен Ұлттар Ұйымы шеңберіндегі халықаралық міндеттемелер шешуші мәнге ие. Халықаралық жобаларға белсенді тарту, ұлттық заңнаманы халықаралық стандарттарға сәйкестендіру және стратегиялық бағдарламаларды жүзеге асыру мемлекеттің киберқауіпсіздік деңгейін арттыруға және оның әлемдік цифрлық қоғамдастыққа интеграциялануына ықпал етеді. Бұл үдерістегі маңызды фактор халықаралық құқық нормаларын ұлттық заңнамаға енгізу.

Кілт сөздер: киберқауіпсіздік, БҰҰ, киберқауіптер, халықаралық кибер реттеу, халықаралық құқық, ақпараттық құқық.

Л.К. Амандыкова, С.Н. Сарсенова

Практические аспекты взаимодействия Казахстана с ООН в области кибербезопасности

Республика Казахстан, в целях повышения защищенности своей цифровой среды, тесно сотрудничает с ООН и другими международными структурами, применяя различные стратегические методы и регуляторные инструменты для создания и реализации эффективных международных норм кибербезопас-

ности. Наблюдается рост рисков, связанных с кибертерроризмом, кибершпионажем и вмешательством во внутренние дела государств через киберпространство, что обуславливает необходимость расширения международного взаимодействия. В связи с этим возрастает роль ООН в координации действий по формированию общих принципов и правил поведения государств в киберсреде, что выражается в принятии новых резолюций и расширении полномочий Рабочей группы открытого состава по вопросам кибернетической безопасности. Для анализа положений казахстанского законодательства в сфере кибербезопасности применялись структурный, логический и диалектический подходы. Теоретический фундамент исследования сформирован на основе изучения норм международного права, научных работ и материалов международных организаций. Ключевое значение в становлении и эволюции киберполитики Казахстана имеют международные обязательства, в частности, в рамках Организации Объединенных Наций. Активное вовлечение в международные проекты, приведение национального законодательства в соответствие с международными стандартами и осуществление стратегических программ способствуют повышению уровня кибербезопасности государства и его интеграции в мировое цифровое сообщество. Существенным фактором в данном процессе является внедрение норм международного права в национальное законодательство.

Ключевые слова: кибербезопасность, ООН, киберугрозы, международное киберрегулирование, международное право, информационное право.

References

1 Postanovlenie Respubliki Kazakhstan ot 24 iiulia 2024 g. № 592 "Ob utverzhdenii Kontseptsii razvitiia iskusstvennogo intellekta na 2024–2029 gody [Resolution of the Republic of Kazakhstan of July 24, 2024 No 592 "On approval of the Concept of Artificial Intelligence Development for 2024–2029]. (n.d.). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/P2400000592 [in Russian].

2 (2013). General Assembly of the United Nations. Report the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *un.org.* Retrieved from https://docs.un.org/en/A/68/98.

3 (2015). General Assembly of the United Nations. Report the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *un.org.* Retrieved from https://docs.un.org/en/A/70/174.

4 (2024). United Nations Convention against Cybercrime; strengthening international cooperation in combating certain crimes committed using information and communication systems and in the exchange of electronic evidence related to serious crimes Adopted by General Assembly resolution 79/243 of December. *un.org.* Retrieved from https://https://www.un.org/ru/documents/treaty/A-RES-79-243.

5 (2003). General Assembly of the United Nations. Resolution adopted by the General Assembly [on the report of the Second Committee (A/57/529/Add.3)] 57/239. Creation of a global culture of cybersecurity. *un.org.* Retrieved from https://docs.un.org/en/A/RES/57/239.

6 (2021). General Assembly of the United Nations. Report the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. *un.org.* Retrieved from https://docs.un.org/en/A/76/135.

7 (2018). General Assembly of the United Nations. Resolution adopted by the General Assembly on 5 December 2018 [on the report of the First Committee (A/73/505)]. 73/27. Developments in the field of information and telecommunications in the context of international security. *un.org.* Retrieved from https://docs.un.org/en/a/res/73/27.

8 (2021). General Assembly of the United Nations. Report the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. *un.org.* Retrieved from https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf.

9 (2016). ISO/IEC 27035-1:2016 Information security incident management. *iso.org.* Retrieved from https://www.iso.org/standard/60803.html

10 (2012). ISO/IEC 27032:2012 "Guidelines for cybersecurity". *iso.org.* Retrieved from https://www.iso.org/standard/44375.html.

11 (2021). General Assembly of the United Nations. Report the Developments in the field of information and telecommunications in the context of international security. *un.org*. Retrieved from https://docs.un.org/en/A/75/816.

12 (2016). ISO/IEC 27035-1:2016 "Information security incident management". *iso.org.* Retrieved from https://www.iso.org/standard/60803.html.

13 Ruban, Yu.P. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstva [International legal regulation of cyberspace]. *Vestnik MGIMO-Universiteta — MGIMO Review of International Relations, 1,* 57–64. Retrieved from https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie- kiberprostranstva [in Russian].

14 Zabikh, Sh. (2020). Mezhdunarodnyi opyt pravovogo obespechenia informatsionnoi bezopasnosti i vozmozhnosti ego primeneniia v Respublike Kazakhstan [International experience in the legal provision of information security and the possibility of its application in the Republic of Kazakhstan]. *Przegląd Politologiczny, 3,* 95–107. Retrieved from https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi- 10_14746_pp_2020_25_3_6 [in Russian].

15 Shulgina, S.A. (2024). Pravovye aspekty kiberbezopasnosti v mezhdunarodnykh otnosheniiakh: rol mezhdunarodnykh norm i dogovorov [Legal aspects of cyber security in international relations: the role of international norms and treaties]. *Chelovek. Znak.*

Tekhnika. — Human. Sign. Technology, 2, 33–37. Retrieved from https://repo.ssau.ru/bitstream/Chelovek-Znak-Tehnika/Pravovye-aspekty- kiberbezopasnosti-v-mezhdunarodnyh-otnosheniyah-rol-mezhdunarodnyh-norm-i-dogovorov-110822/1/978-5-93424-903-9_2024_33-37.pdf [in Russian].

16 (2025). Kazakhstan Statement at OEWG 2021–2025. *estatements.unmeetings.org.* Retrieved from https://estatements.unmeetings.org/estatements/12.1255/20241206100000000/bU WavSrotn/RVjgCXVnyc_en.pdf.

17 ITU (2022). Cybersecurity Events — Regional Cyberdrill for CIS and Arab States. *itu.int.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-events.aspx.

18 GIGA Initiative: Connecting Every School to the Internet // International Telecommunication Union. *itu.int.* Retrieved from https://www.itu.int/en/ITU- D/Initiatives/GIGA/Pages/default.aspx.

19 Cyber TUMAR: Informational and Educational Campaign Launched in Kazakhstan to Protect Children Online. UNICEF Kazakhstan. (n.d.). *unicef.org.* Retrieved from https://www.unicef.org/kazakhstan/en/press-releases/cyber-tumar-informational- and-educational-campaign-launched-kazakhstan-protect.

20 Shanghai Cooperation Organisation. SCO Member States Interdepartmental Consultations on Establishing Information Security Centre. (n.d.). *sectsco.org.* Retrieved from https://eng.sectsco.org/20230914/SCO-member-states-interdepartmental-consultations-on-establishing-information-security-centre-956495.html.

21 OSCE ICT Security Training in Astana for Central Asia and Mongolia // Organization for Security and Co-operation in Europe. *osce.org*. Retrieved from https://www.osce.org/secretariat/544345.

22 Tikk, E., & Kerttunen, M. (2020). The Role of the UN GGE in Advancing International Norms on Responsible State Behavior in Cyberspace. *UNIDIR.* Retrieved from https://unidir.org/publication/role-un-gge-advancing-international-norms- responsible-state-behaviour-cyberspace.

23 United Nations Office on Drugs and Crime. Cybercrime Convention Portal. (n.d.). *unodc.org.* Retrieved from https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

24 European Union Institute for Security Studies. OEWG Side-Event: Cybersecurity for the Common Good: Strengthening Nonprofits Engagement. *iss.europa.eu.* Retrieved from https://www.iss.europa.eu/activities/event/oewg-side-event-cybersecurity-common-good-strengthening-nonprofits-engagement.

25 European Union Institute for Security Studies. Advancing the Cyber Programme of Action (PoA). *iss.europa.eu.* Retrieved from https://www.iss.europa.eu/projects/advancing-cyber- programme-action-poa.

26 EU statement at the UN OEWG — Norms of responsible State behavior. *eeas.europa.eu.* Retrieved from https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2 %80 %93- un-open-ended-working-group-cybersecurity-rules-norms-and-principles- responsible_en.

27 Ministry of Foreign Affairs of the People's Republic of China. Remarks by Mr. Wang Lei, Head of Chinese Delegation and MFA Cyber Affairs Coordinator, at. *mfa.gov.cn.* Retrieved from https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjfywj_665252/20250 3/t20250307_11570776.html.

28 EU Cyber Direct. China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. *eucyberdirect.eu.* Retrieved from https://eucyberdirect.eu/atlas/sources/china-s- submissions-to-the-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security.

29 (2024). United Nations Economic and Social Commission for Asia and the Pacific. Asia- Pacific Ministerial Conference on Digital Inclusion and Transformation, 3–5 September Astana. *unescap.org.* Retrieved from https://www.unescap.org/events/2024/asia-pacific-ministerial-conference-digital- inclusion-and-transformation.

30 (2017). U.S. Department of State. Explanation of Position at the Conclusion of the 2016– 2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. *state.gov.* Retrieved from https://2017-2021.state.gov/explanation- of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental- experts-gge-on-developments-in-the-field-of-information-and- telecommunications-in-the-context-of-international-sec/.

31 Council on Foreign Relations. The Dangers of a New Russian Proposal on a UN Convention on International Information Security. *cfr.org.* Retrieved from https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention- international-information-security.

32 (2024). US Cyber Force Surges Global Operations Amid Rising Threats. *bankinfosecurity.com.* Retrieved from https://www.bankinfosecurity.com/us-cyber-force-surges-global-operations-amid- rising-threats-a-26889.

Information about the authors

Amandykova Leila Koshkenovna — Candidate of Law, Associate Professor, Higher School of Law, Astana International University; Astana, Kazakhstan; e-mail:monamie2000@mail.ru.

Sarsenova Sania Nurzhanovna — Candidate of Law, Higher School of Law, Astana International University, Astana, Kazakhstan; e-mail: saniyacreating@gmail.com.