Security Journal
https://doi.org/10.1057/s41284-021-00304-3

ORIGINAL ARTICLE

Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development

Aigul Nukusheva[1] · Roza Zhamiyeva[2] · Viktor Shestak[3] · Dinara Rustembekova[4]

Accepted: 8 June 2021

Abstract
This article analyzes the international legal framework against cybercrime. The international legal framework provides a solution to the problem in three areas: reducing discrepancies between national laws, introducing new powers of authorities, and promoting international cooperation. The study argues that the core documents effectiveness in the field of cybercrime counteraction does not appear to be dependent on the legal applicability of the international measures. Such factors as national security, politics, economics, and public opinion, apparently, stimulate the spontaneous implementation of the international legal framework. The study focuses on the need to develop a system of basic approaches in the field of criminal law cybercrime qualification and consolidate their classification at the supranational level. A qualitatively new approach to cooperation between international relations subjects in combating cybercrime is proposed. The latter is based on all states actions coordination in improving the legal regulation of interaction and implementation of fundamental rules in national legislation, reorganizing the information exchange basics.

Keywords Convention on cybercrime · Cybercrime · Cybersecurity · International cooperation · National legislation

Introduction

The widespread use of modern information technologies in state and non-state structures, as well as in society as a whole, necessitates the search for solution to information security problems (Kersting 2016; Maras 2016). In addition to direct harm from possible cases of unauthorized access to information, its modification,

✉ Aigul Nukusheva
aigul_nukusheva@rambler.ru

Extended author information available on the last page of the article

Published online: 18 June 2021

or destruction, informatization can turn into a source of a serious threat to state security and human rights (Chaikin 2006).

The growth of information technology determines not only progressive changes in the economy, but also negative trends in the development of the criminal world, the emergence of new forms, and types of criminal attacks. This is manifested in the fact that attackers actively use the latest computer tools and new information technologies in their criminal activities (Karpova 2014). Such socially dangerous acts as the creation and dissemination of computer viruses and child pornography, embezzlement of funds from bank accounts of individuals and legal entities, bank card fraud, Internet terrorism—have received the fairly common name of "cybercrime".

There is no universally accepted definition of cybercrime. However, the following definition includes elements common to all existing definitions of cybercrime. Cybercrime is an act that violates the law, which is committed using information and communication technologies (ICT) and is either aimed at networks, systems, data, websites, and/or technologies, or contributes to the commission of a crime (Maras 2016; Wilson 2008). Cybercrime differs from a traditional crime in that it does not recognize physical or geographic boundaries and can be committed with less effort, more ease, and more speed than a traditional crime (although it depends on the type of cybercrime and the type of traditional crime with which it is compared) (Maras 2014).

Europol (2018) divides cybercrime into cyber-dependent crimes (i.e., any crime that can only be committed using computers, computer networks, or other forms of information and communication technologies (McGuire and Dowling 2013) and crimes committed through cyber technology (i.e., traditional crimes committed through the Internet and digital technologies). The key difference between these categories of cybercrime is the role of information and communications technology in the commission of the offense—whether ICT is the purpose of the crime or an integral part of the way of conducting a crime (UNODC 2013). When ICTs are the target of a crime, such cybercrime negatively affects the confidentiality, integrity, and/or availability of computer data or systems (UNODC 2013).

Confidentiality, integrity and accessibility make up the so-called "CIA Triad" (Rouse et al. 2014): simply put, confidential information should remain confidential, it should not be changed without the permission of the owner, and data, services, and systems should be available to the owner at any time. When ICTs are among the means of committing a crime, in this case, cybercrime includes a traditional crime (such as fraud and theft), while the Internet and digital technologies contribute to crime's commitment in one way or another.

In modern conditions, the UN has taken on a coordinating role in developing both conceptual and legal frameworks for regulating key issues in the fight against cybercrime. Hence, back in 1990, the VIII UN Congress on Crime Prevention and Criminal Justice adopted a resolution. The latter calls on governments of different countries to

- increase efforts in the fight against cybercrime;
- introduce innovative solutions into national criminal law;

- contribute to improving the future system of international principles and standards for the prevention, investigation, and punishment of cybercrime (General Assembly 1990).

The growth of the corresponding type of crime and the nature of the crimes committed require an immediate reaction of the international community to the corresponding negative social manifestations. Under the auspices of the UN, which unites the largest number of states of the world, it is advisable to carry out activities to develop and implement international legal regulation of the studied public relations. The adoption of the relevant resolution, which outlined the framework agreements, was one of the first steps towards the creation of an international legal framework to combat cybercrime (Maras 2016).

In 1997, the Ten Principles for Combating High-Tech Crimes were developed and signed between the Ministers of Justice and the Ministers of the Internal Affairs of the G8 countries in Washington. These principles, in particular, include the provision that for those who misuse information technology, and there should be no security zones. Thus, the legal system must ensure the confidentiality, integrity, and suitability of data and systems, and protect against criminal damage, and guarantee the punishment for serious offenses (Holt et al. 2017).

On January 18, 2013, the European Center for the Fight against Cybercrime was officially opened in The Hague. The goals of its creation are as follows:

- collection and processing of data on cybercrime;
- conducting expert assessments of Internet threats;
- development and implementation of advanced methods for the prevention and investigation of cybercrime;
- training new personnel;
- assistance to law enforcement and judicial authorities;
- coordination of joint actions by stakeholders to increase security in European cyberspace (UNODC 2013).

The features of the universal international legal regulation of the fight against cybercrime are the following:

(1) relevant activities accumulate around the UN and its bodies or entities created with its support (Smith 2007);
(2) today, there are strategic documents that should lay the foundations of international legal regulation of the relevant circle of relations (Van Der Hof and Koops 2011);
(3) the main areas of activity should be the creation and development of organizational and legislative measures to counter cybercrime, as well as issues of interaction in this field of activity;
(4) there is a need to create international joint bodies for operational investigative activities to record traces of committed crimes; and

(5) improving interaction between the competent authorities of various states (Karpova 2014). In addition, there is an urgent need to develop and adopt universal conventions on relevant issues that would ensure the participation of most states in relevant anti-crime activities (McGuire and Dowling 2013).

Given the characteristics of crimes in the field of ICT, the interaction of the operational unit of the internal affairs at all levels, including with representatives of law enforcement agencies of other countries, is important for the effectiveness of such crimes operational documentation (Li 2007; Shukan et al. 2019). It is important to recognize that cybercrime is a worldwide problem. Cyberattacks can paralyze both private organizations and state structures, and there is no state in the world that would be completely protected from such attacks. Probable sources of cyber threats are not only hackers or their groups, but also individual states, criminal groups, and terrorist organizations (Brenner 2006).

During the development of methods for combating cybercrime, it is necessary to take into account the latency of this type of crime. Experts rate the latency of cybercrime as extremely high: 80% in the USA, 75% in Germany, 85% in the UK, and more than 90% in Russia (Vardanyan and Nikitina 2007). According to Symantec Security, an international cyber threat assessment service, 12 people in the world are susceptible to cyber-attacks every second, and about 556 million cybercrimes are committed worldwide every year, with more than $ 100 billion worth of damage (Karpova 2014).

Crimes in the field of Internet technologies go beyond the level of the phenomenon and testify to the need to single out an independent type of crime—cybercrime, with its inherent features, and also confirm the relevance of further research in the fight against cybercrime.

The effectiveness of countering the phenomenon of cybercrime is seen in the joint actions of the public and private sectors, improving international and national legislation, organizing international units, and structures in the fight against cybercrime. As for Russia, there is yet no comprehensive research on the fight against cyber terrorism and cybercrime as phenomena that include the entire spectrum of crimes that are committed on the Internet today. In most cases, Russian scientists are exploring ways to tighten responsibility for cybercrime, or the criminological component of Internet crime in Russia (Smirnov 2012). The fight against cybercrime, and in particular the international aspect, and cybercrime as a global phenomenon are disclosed in the works of only foreign scientists that are not related to Russian law. Thus, the aim of the study is to find an effective mechanism for controlling cybercrime in the world. The problems of domestic legislation and its ability to withstand the modern challenges of cybersecurity are assessed, and the international legal experience of combating cybercrime is studied. The possibilities of implementing international legal standards to combat cybercrime, as well as the application of other measures to counter illegal activities in the virtual space, have been clarified.

Methods

The study is based on the analysis of international treaties, acts issued by international institutions, and regulatory acts of European countries (France, Great Britain, Germany, the Netherlands, the USA, and Australia) in the field of cybercrime counteraction. Attention is also drawn to the role of the UN in the fight against cybercrime.

The following acts of international cooperation have become research objects:

- Resolution 45/113 as of December 14, 1990 (General Assembly 1990);
- Report of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime (Unites Nations Office on Drugs and Crime 2016);
- Convention against Cybercrime (Council of Europe 2001).

Herewith, study analyzes legislative acts of the Russian Federation and Kazakhstan (including Criminal Code of the Russian Federation, the Criminal Code of the Republic of Kazakhstan) in the scope above. In addition, the Agreement on the Cooperation of the Member States of the Commonwealth of Independent States in the fight against computer information crimes is analyzed.

Through the method of political and legal analysis used in the study, a comprehensive analysis of international methods of combating cybercrime was carried out in terms of their effectiveness, modernity, and scale. The main results of countering this phenomenon at the legislative level, as well as ways to improve information security in different countries are studied.

Results

The inclusion of the population in the Internet space in different countries is significantly different (Statista 2020), which leads to completely different levels of cybercrime in these countries. As of September 2017, the level of Internet penetration in the world is estimated at 51% (Statista 2020). Thus, approximately half of the world's population has access to the Internet and the ability to use the Internet, which makes them potential victims of cybercrime (Fig. 1).

Since the emergence of public relations precedes the legal regulation, legislative measures to combat cybercrime are developing at different speeds as well: in developed countries, this problem arose earlier than in less developed countries, and, accordingly, legal regulation in them is more extensive than in developing countries. Studying the latest statistics on cybercrime in different countries helps to find measures to strengthen information security in domestic legislation, as well as to understand which mechanisms enshrined in international acts will take into account the interests of individual countries.

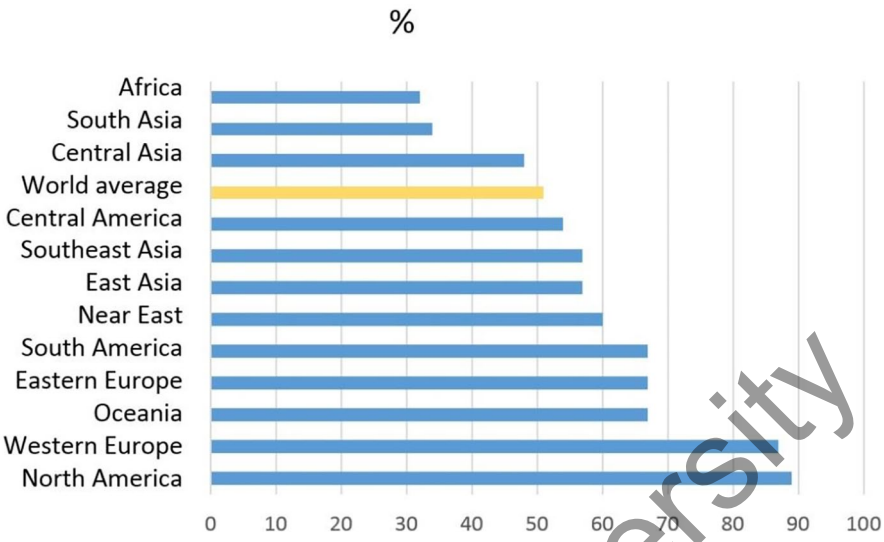

Fig. 1 Worldwide Internet penetration rate as of September 2017, by region. *Source* created by the authors based on (Statista 2020)

In addition, an important issue remains regarding the lack of conceptual certainty, caused by the regular emergence of new types of cybercrimes, as well as the lack of unified criteria for the correct qualification of cybercrimes and the lack of necessary forensic approaches in the fight against them. It should be noted that the question of the relationship between the concepts of cybercrime and offense in cyberspace usually implies the presence of direct intent; therefore, in most studies and in a practical aspect, these concepts are interconnected (Tafazzoli 2018).

At the same time, an attribute of referring certain crimes to the category of cybercrimes in general is the instrument of committing a crime—computer technology, technical devices based on the use of digital technologies, as well as a specific environment for committing crimes—cyberspace. Research suggests that modern conditions indicate the need to separate the concept of cybercrime into a separate category in criminal law and criminal law doctrines and apply to them the entire toolkit of legal measures applied to traditional crimes (Seebruck 2015). In general, terminological ambiguity complicates the issue of properly qualifying cybercrime.

Important issues of state cooperation in combating the criminal use of information and communication technologies were assigned to the International Telecommunication Union. The result of the activity was the adoption by the specified entity of the Global Cybersecurity Program (International Telecommunication Union 2017), which identified the main strategy, goals, and principles that should be laid down in the development of legislation to combat cybercrime. The fundamental objectives of the above Global Program are as follows:

(1) formulating a strategy for the development of model legislation to combat cybercrime, which can be applied on a global scale and which will be compatible with existing national and regional legislative acts;
(2) formulating a global strategy to create appropriate national and regional organizational structures, as well as a cybercrime policy;
(3) developing a strategy for establishing globally acceptable minimum security criteria and authorization schemes for hardware, software applications and systems;
(4) developing a strategy for creating a global framework for monitoring, reporting and responding to incidents to ensure international coordination;
(5) creation and approval of a special digital identification system, as well as the necessary organizational structures in order to recognize digital identity cards without taking into account geographic boundaries;
(6) developing a global strategy to promote human and institutional capacity to increase knowledge and know-how;
(7) preparing proposals based on a global multi-stakeholder strategy with a view to fostering international cooperation, dialog, and coordination (International Telecommunication Union 2017). Subsequently, a number of ITU resolutions have been adopted to implement the planned activities, which are aimed at strengthening confidence and security in the use of information and communication technologies and the fight against computer crimes (Jarvis et al. 2014).

The leading place among the relevant group of international legal instruments is occupied by Convention on Cybercrime as of November 23, 2001 (Budapest) (Council of Europe 2001). Today, it is the most important document that regulates legal relations in the global computer network and so far the only document of such a high level. The Convention imposes obligations on states to take legislative and other measures that may be required to criminalize cybercrimes in accordance with domestic law (Council of Europe 2001). Some organizations for the protection of civil rights and Internet providers even before the Convention was signed, gave weighty arguments against concluding this agreement, since, in their opinion, the Convention is filled with unclear wording and makes excessive demands on providers (Csonka 2004). In particular, the Convention potentially may pose a certain threat to the established rules for the protection of persons and reduce the responsibility of the government in law enforcement (Gercke 2009, 2012). This Convention is not signed, and, accordingly, is not ratified by the Russian Federation.

The significance of this international legal act can be expressed as follows. First, the Convention classifies cybercrimes (computer crimes) by dividing them into

- crimes against the confidentiality, integrity, and availability of computer data and systems (illegal access, unlawful interception, impact on data, impact on the functioning of the system, illegal use of devices);
- offenses related to the use of computer tools (forgery using computer technology, fraud using computer technology);
- offenses related to the content of the data (offenses related to child pornography);

- offenses related to violation of copyright and related rights.

Such offenses are classified in a similar way in the national laws of countries parties to the Convention. Second, the Convention regulates procedural aspects, such as conditions, preventive measures, search, and seizure of stored computer data, collection of real-time data, interception of data, jurisdiction, and the like. Such systematization greatly facilitates the activities of state law enforcement agencies. Third, this document establishes the principles of cooperation of the participating countries in the fight against cybercrime, in particular, extradition and mutual assistance. It should be noted that this aspect is implemented through the conclusion of bilateral agreements by states. As analysis shows, in practice, participating countries prefer the implementation of mutual assistance principle (Kierkegaard 2007). Fourth, the Convention gives parties the right to access publicly accessible computer data without obtaining permission from the other side, which greatly facilitates the investigation of crimes and allows avoiding excessive delays in operational-search activities.

Among the international treaties against cybercrime, to which Russia and Kazakhstan are parties, there is, in particular, the Agreement on Cooperation between the CIS Member States in the fight against computer information crimes as of June 1, 2001 (Codex 2008). This agreement imposes an obligation on States to recognize, in accordance with national legislation, the following as criminal offenses:

(1) unauthorized access to computer information protected by law, if it entailed the destruction, blocking, modification, or copying of information, disruption of the operation of a computer, computer system, or network;
(2) creation, use, or distribution of malware;
(3) violation of computer operation rules, computer system or network by a person having access to a computer, computer system, or network, which entailed the destruction, blocking, or modification of computer information protected by law if it entailed significant harm or serious consequences;
(4) illegal use of computer programs and databases that are objects of copyright, as well as attribution of authorship (Codex 2008). However, for the full implementation of the relevant tasks, it was necessary to agree on a clear list of relevant criminal acts and punishments for them. In practice, not all states that are participants in the CIS have completed the relevant tasks, which significantly reduce the fight against information crime, which requires comprehensive transnational cooperation.

According to a study "Global Cybersecurity Index 2017" (International Telecommunication Union 2017), Singapore is the most informationally protected and ready to fight against cybercrime, followed by the United States and then Malaysia. Among the CIS countries, the most developed in the field of information security is Georgia, which shares eighth place with France. Russia in this ranking goes after Canada and is in 10th place. Kazakhstan, according to the ITU, is not very developed in cybersecurity and is in the 82nd position between Slovakia and Slovenia (Table 1).

Table 1 Ranking the countries with the highest cybersecurity index in 2017

Country	Score	Global rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10

Source Created by the authors based on (International Telecommunication Union 2017). The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness. The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building, and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighed in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Thus, it can be stated that in Russia, the issue of the country's cybersecurity is quite important and open. It should be said that the methods of combating cybercrime show their effectiveness and relevance. The opposite situation is in Kazakhstan and other countries of Central Asia.

The current criminal law of Russia defines crimes in the field of computer information as acts committed in the field of information processes and encroaching on information security. This group of criminal offenses is a special part of the criminal law, the responsibility for the commission of which is provided for by Chapter 28 of the Criminal Code of the Russian Federation. According to the Criminal Code of the Russian Federation, crimes in the field of computer information are as follows:

- unlawful access to computer information (The Criminal Code of the Russian Federation 2019);
- the creation, use, and distribution of malicious computer programs (The Criminal Code of the Russian Federation 2019);
- violation of the rules for the operation of means of storage, processing, or transmission of computer information and information telecommunication networks and the spread of pornography (The Criminal Code of the Russian Federation 2019).

In Russia, the Office "K" of the Ministry of Internal Affairs and departments "K" of the regional internal affairs departments (which are part of the Bureau of Special Technical Events of the Ministry of Internal Affairs) are engaged in the fight against cybercrime (Ministry of Internal Affairs of the Russian Federation 2019).

It is worth saying about the positive aspects that exist in the legislation regarding Kazakhstan. For example, the K department, established at the Ministry of Internal Affairs (MIA) of Kazakhstan in April 2003, is fighting a wide range of crimes related to computer and Internet technologies, including cyberbullying, production of counterfeit video disks, and the dissemination of information conducive to extremism, terrorism, cruelty, and violence. In 2006, the Kazakh authorities created a National Contact Point for the fight against crimes in the field of information technology and the exchange of information with countries of the Commonwealth of Independent States and partners in foreign countries (Koksegenova 2011).

To date, a system of cooperation has been established in many foreign countries, and the need for the exchange of experience at the international level is determined. These issues are coordinated by each country in accordance with the developed and existing cybersecurity strategy: For instance, the US and most EU countries against the background of other cyber threats, in their strategies prioritize the fight against cybercrime namely (Forst 2009).

The following features of the regional international legal response to cybercrime can be determined:

(1) significant attention from various regional international organizations to the issues of combating cybercrime;
(2) development of numerous regional cooperation agreements in the field of combating information crime;
(3) the corresponding activity is at the stage of its inception, since most of the documents began to be formed in the late 1990s–in the early 2000s;
(4) such activities are an integral part of both international information relations and criminal proceedings.

Today, actions are being taken to establish the foundations of international cooperation in the field of combating cybercrime within the framework of both universal and regional treaties. At the same time, such measures for full-fledged activity are not enough, which require revitalization of activity by each subject of the international community in order to create an effective mechanism for international legal regulation of combating cybercrime.

In the context of considering the issue of combating cybercrime, the concept of cyberterrorism deserves special attention. Terrorism as a criminal law phenomenon is international in nature and in accordance with a number of international documents is classified as an international crime. This fully applies to new forms of its manifestation—cyber terrorism or electronic terrorism. Analysis of global trends in the development of electronic terrorism with a high degree of probability makes it possible to predict that its threat will increase every year.

Based on generalized views, cyber terrorism can be defined as a complex of illegal actions in cyberspace that pose a threat to state security, individuals, and society. The ultimate goal of cyber terrorism is to influence the solution of social, economic, and political problems (Macdonald et al. 2019).

Based on the definitions of terrorism in common understanding, cyber terrorism, as its variety, is a criminal offense. A characteristic feature of cyber terrorism and its difference from cybercrime are its openness when the terrorist's conditions are widely publicized. Cyber terrorism is a serious threat to humanity, comparable to nuclear, bacteriological, and chemical weapons, and the degree of this threat, due to its novelty, is not yet fully understood and studied. The experience that the world community already has in this area clearly indicates the undoubted vulnerability of any state, especially since cyber terrorism has no state borders, a cyber terrorist is capable of equally threatening information systems located almost anywhere in the world. It is very difficult to detect and neutralize a virtual terrorist due to too few traces left by him, in contrast to the real world, where there are still more traces of what offender has done.

The absence of a universally accepted definition of cybercrime determines the current state of the developed classifications of cybercrimes. Some definitions and classifications follow the logic of "traditional crime," others use approaches based on technology, offender or threat, etc. Among the various classifications, there are many intersection points, but there are also many differences in structure, definitions, and content. There is a clear difference between the approaches, which is reflected in the application of the technical nature of cybercrime as a basis on the one hand and the consequences of the crime on the other hand. Researchers have studied aspects of crime, such as technical (types of malicious software and methods of prevention), aspects of committing crimes, or the human aspect (human error, victimization); however, the understanding of cybercrime as a process and system remains less explored (Somer 2019).

Criminology and criminal law approaches treat cybercrime in terms of its classification as "traditional" offenses. The studies say that defining cybercrime as "a crime committed on a computer network" should reflect the existing legal framework, both national and international. There are often controversial points between the concepts of cybercrime and cyberterrorism, and it is noted that cybercrime is usually committed with the aim of obtaining personal gain. Terrorism has other motives, but it can use the same methods, while the concept of cyber war can bear the same features, where technical means can be identical to those used in cybercrimes (Somer 2019).

Discussion

Despite the many regional international treaties to combat cybercrime, there is no such global act that would satisfy all participants in the international community. A group of states, including China, Russia, and a number of other developing countries, would like to see a global tool to combat cybercrime, arguing that a new global treaty is needed (Hakman 2017). This argument is based on the fact that these states have not been involved in the process of developing the Budapest Convention

(which, as proposed, should serve as the basis for an international agreement). Many argue that the convention does not reflect their concerns, in particular, concerns about national sovereignty regarding cross-border access to information and electronic evidence, even if many of these issues are being addressed now (Hakman 2017). This serious statement concerns one article—article 32 (b), which allows one state to receive information in another country if the legal owner of the data agrees, without the need for government approval (Council of Europe 2001).

In 2017, BRICS members reiterated their desire to create a universal legal binding document on the fight against the criminal use of ICT under the auspices of the UN (Xinhua 2017). This debate also raged during the Conference of the Parties to the UN Convention against Transnational Organized Crime in October 2016. At that time, some states called for the development of a new legal instrument on cybercrime, arguing that the Budapest Convention does not provide sufficient opportunities for cooperation on this issue. Others said that strengthening existing instruments, including the UN Convention and the Budapest Convention, was the right direction (Unites Nations Office on Drugs and Crime 2016).

Russia (a member of the Council of Europe that has not signed the Budapest Convention) has pushed the UN to a multilateral agreement on cybercrime. In October 2017, Russia submitted to the Secretary General a new draft UN Convention on Cooperation in the Fight against Cybercrime (General Assembly 2019) and was supposed to propose it as a subject of discussion at the GA in 2018 (TASS 2018) but instead received a resolution that instructed the Secretary General to prepare a report on the problems of countering the criminal use of ICT (General Assembly 2018).

In terms of arguments against the need to start a new treaty process, most EU and OECD member states support the Budapest Convention and consider it a solid basis for a global document, claiming that it encourages multilateral cooperation in the fight against cybercrime and includes many signatories from other regions of the world (Kavanagh 2017). The Budapest Convention is a binding instrument on cross-border cooperation in the field of cybercrime and contributing to the harmonization of laws. Entered into force in 2004, the Convention has 56 States Parties, including several countries outside the Council of Europe, such as the United States, Japan, Canada, Senegal, Sri Lanka, the Philippines, Turkey, Morocco, and the Dominican Republic and is open for ratification by other states. Observer countries include South Africa, Ghana, Colombia, and Mexico (Council of Europe 2018). Many Western countries believe that the convention has established best practices for cooperation and provides adequate guarantees for digital rights. They emphasize inter-regional membership as a sign that it can be used as an international basis (Shore et al. 2011).

Cybercrime violates the legitimate interests of both the state and individuals. Undoubtedly, the functioning of the Internet, information, and telecommunication systems requires paying attention to solving cybersecurity issues, as well as the efforts of various public and private entities (Huey et al. 2013). However, it is the state that is able and obligated to effectively counter cybercrime, create the necessary conditions so that the entities that are most susceptible to cybercriminal attacks (for example, banks, individuals, transnational corporations) can build the most

reliable information protection system. In the modern world, there are enough systems that effectively counteract the commission of cybercrime. Currently, the most developed countries are actively creating separate units and services in the armed forces that can combat cybercrime (Sindhu et al. 2014). The cybersecurity features in a number of countries are shown in Table 2.

For example, in the United States, along with the existing National Cybersecurity Center, United States Army Cyber Command was created as part of the Armed Forces, which on a global scale should coordinate the actions of all Pentagon structures during the conduct of hostilities, provide the necessary support to civilian federal institutions, and also interact with departments of other states that are similar in tasks (Berd 2009). At the same time, these organizations are controlled departments, since the main controlling structure is the National Security Council and special committees, whose responsibility includes the implementation of the information strategy (Finklea 2009), including anti-cybercrime. Great Britain implements cyber weapons programs that will ensure the ability of the state to withstand growing cyber threats (Hunton 2009). Email Security Coordination Group (ESCG) was established in Australia. Its main task is to create a safe and reliable information operational space for the public and private sectors (Australia House Standing Committee on Communications, & Australia 2010).

The development of the cybersecurity sphere is a priority of the state, since Israel is one of the most computerized countries in the Middle East. To admit vulnerability in the operation of the information, infrastructure for the state is tantamount to inflicting heavy damage on the defense of the state and national security.

The responsibility for protecting information lies with the Israeli security agency Shabak. It is traditionally responsible for ensuring the security of government agencies and basic infrastructure—power supply facilities, water supply facilities and financial institutions. Also in 2010, the Israel National Cyber Bureau (INCB) was created to advance Israel's cyber policy in three main areas:

- improving the protection and strengthening of national capacities in cyberspace;
- strategic issues of Israel information technology policy;
- encouraging collaboration between scientists, industrialists, the private sector, government officials and the public on security issues (Tabansky and Ben Israel 2015; Zernik 2019).

While some elements of the defense and intelligence community have long had best practices in using cyber technology to accomplish their missions, it was not until the mid-1990s that such efforts took shape in the Israeli government. Defense leaders, bridging the knowledge gap with the civilian branches of government, fostered cybersecurity efforts that culminated in the adoption in 2002 of one of the first Centralized Critical Infrastructure Protection Policies (CIPs) in the developed world. A shared responsibility scheme, in which the Israel National Security Agency (NISA) was the professional regulatory body, proved to be viable, but as cyberspace evolved, risks and opportunities grew.

Israel's 2002 Critical Infrastructure Protection Approach required controlled entities ("users") to appoint and recruit dedicated IT security personnel on behalf of

Table 2 Features of ensuring cybersecurity in a number of countries

Country	Participation in the Convention on Cybercrime	Development of the UN Convention on International Information Security	Key cybersecurity organizations
The UK	+	−	Communications-Electronic Security Group within the UK Government Communications Headquarters; Ministry of Defense Virtual Threat Protection Unit
Germany	+	−	Special group at the Ministry of Internal Affairs of Germany
India	+	−	Foreign Intelligence Research and Analysis Division and Internal Intelligence Bureau
China	−	+	Implementation of a program of protection against unauthorized connection to a computer
Russia	−	+	Office "K" of the Ministry of Internal Affairs and departments "K" of the regional departments of the Ministry of Internal Affairs; National contact point at the Bureau of Special Technical Events of the Ministry of Internal Affairs of Russia
USA	+	−	National Cybersecurity Center; United States Army Cyber Command

Source Created by the authors

the National Information Security Agency (NISA) and public utilities. NISA auditors can access any relevant information and assets of the organization to ensure compliance with regulations or assess new risk vectors. The supervised organization continues to fund all operations, protection, maintenance, upgrades, backup and recovery of its critical important IT systems, including changes, improvements and equipment authorized by NISA, and exchange information and actions with the specific requirements set by NISA (Tabansky and Ben Israel 2015).

Counteraction to the commission of cybercrime is carried out both by individual states and their blocs, for example, NATO. The importance of this problem is reflected in all the governing documents of the bloc adopted in recent years. NATO's strategic concept now includes a provision on cyberspace as a new alliance's military field (Kavanagh 2017).

Thus, both individual states and the international community should focus on the fight against cross-border crimes, which include the majority of cybercrimes. Only with well-coordinated work of the security and information agencies of various countries is possible to reduce the number of committed offenses in the field under study.

The fundamentally different concepts of the role of ICT and the Internet in society limit the ability of states to respond to cybercrime in a collective and coordinated manner (Rowe et al. 2011). States will continue to discuss their key differences when it comes to their citizens' right to privacy and national sovereignty.

The steps taken by some UN committees and UN initiatives are aimed at finding areas where countries can ultimately become more coherent in their response to this complex and controversial area of crime (Holt et al. 2017). At the same time, there are still disagreements between different countries on critical digital issues: the current geopolitical distrust hinders the UN's ability to fight cybercrime.

Ultimately, the states will decide whether a multilateral agreement to combat cybercrime is needed. Whatever the outcome, the invasion and changing nature of cybercrime indicate that the UN needs a flexible approach that can adapt to new risks and identify appropriate joint measures among states that take significantly different approaches to cyberspace (Hunton 2011).

Herewith, the main legal challenges in investigating cybercrimes and prosecuting cybercriminals are factors such as different legal systems in different countries, differences in national cybercrime laws, differences in the rules of evidence and criminal justice (for example, in the procedures for obtaining access to digital evidence by law enforcement agencies; for example, with or without a legal order such as a search warrant), differences in the scope and geographic applicability of regional and multilateral cybercrime treaties and differences in approaches to data protection and respect for human rights (UN 2019).

At the same time, taking into account the above, it can be argued with confidence that the introduction of effective legislation is not always able to solve the problem of cybercrime without the necessary law enforcement and appropriate personnel and incentive policies. In most countries, the number of primary law enforcement officers (usually police officers involved in cybercrime investigations) is small, and their career prospects are also low, as it is difficult for the police to compete for the best employees with commercial structures. Police may not always be able to detect

most cybercrimes on their own, and it often has to rely on private companies such as Internet service providers, mobile operators, and other specialized agents to detect and prosecute such crimes (Selby 2017).

With regard to the classification and criminal qualification of cybercrimes, it should be noted that although there are few schemes for the classification of cybercrime, even they are largely incompatible (Donalds and Osei-Bryson 2018). In this regard, the issue of the development of unified approaches in the field of criminal law qualification of cybercrime, and the consolidation of their classification at the supranational level are especially important as it is a necessary tool for correctly assessing the degree of social danger of a crime, determining the harm caused by the crime, determining a just punishment, its type, and volume. At the same time, the issue of classification of cybercrimes according to the criterion of the amount of material damage should be based on the norms and practice of national legislation and socio-legal realities, since the amount of damage can be differently assessed in different states.

The conducted doctrinal study gives grounds to assert that the resources of one law enforcement agency or law enforcement agencies of a certain state are insufficient to create the conditions for proper and effective activities to combat cybercrime. Such activities should be comprehensive and include the participation of many countries, which requires the necessary regulatory framework at the global level.

Conclusion

The current state of cybercrime is characterized by the absence of a single act of global significance that would regulate the procedure for countering cybercrime. Despite this, the international community is cooperating at regional levels and is making attempts to legislatively regulate the actions of entities in cyberspace, to combat cybercrime.

One of the decisive factors in the fight against cybercrime should be not only the ratification of the Convention by individual states, but also the harmonization of national legislation, taking into account the main provisions of the convention. Namely, the mechanisms should be developed at the national level. If the national legislation of one of the parties does not provide the authority to search for evidence in the Internet environment, and then this side will not be able to fully provide assistance to the other side in the investigation of cybercrimes. Thus, the coordination of functions and powers between states to implement measures to investigate cybercrimes is an extremely important aspect of international cooperation. The main reasons, due to which there is a rapid increase in cybercrime, are the lack of a unified base of law enforcement agencies (whose competence includes the fight against cybercrime) and the limited domestic legislation. It can be stated that the most important component of the strategy to combat cybercrime should be comprehensive international cooperation in this industry, since it is not possible to counteract cyber threats at the level of individual states due to the cross-border nature of this type of crime.

Special attention is required to the issue of the need to develop a system of basic approaches in the field of criminal law qualification of cybercrime and to consolidate their classification at the supranational level. The classification of cybercrimes used in the Budapest Convention today is not all encompassing: with the development of scientific and technological progress and the emergence of new types of legal relations in cyberspace, this classification will only expand. In addition, modern conditions indicate the need to single out the concept of cybercrimes in a separate category in criminal law and criminal law doctrines and apply to them the entire set of legal measures applied to traditional crimes. In addition, the mechanisms of cooperation between agencies in the field of participation and exchange of information in the course of investigation of cybercrimes require constant improvement.

Analyzing the cybersecurity strategies of different countries, the authors identify the unifying key positions that must be followed:

- development of an adequate mechanism of public-state partnership, which might allow both public and private stakeholders to develop and approve a policy to combat the problem of cybercrime;
- determination of the main goals and ways of developing state capabilities, as well as the introduction of the necessary regulatory framework for participation in the international fight against cybercrime;
- increasing preparedness, accelerating the response to individual incidents, developing a plan for recovery from failures, and developing mechanisms for protecting central information infrastructures.

The fight against cybercrime in an international format necessitates coordination of actions of the public and private sectors through the following means:

- combination of financial, technical, communication, and organizational resources;
- limiting the anonymity of users on the Internet, social networks, and during banking operations.

There is a need for the creation of international units and structures to combat cybercrime. It is also necessary to develop international or cross-border communication networks for real-time tracking and transmission of information about cybercrimes.

Acknowledgements Aigul Nukusheva and Roza Zhamiyeva were financially supported as holders of the title and state Grant "The best teacher of the university—2020".

Data availability All data will be available on request.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Australia House Standing Committee on Communications, & Australia. 2010. *The Report of the Inquiry into Cyber Crime, Standing Committee on Communications. The Parliament of the Commonwealth of Australia*. https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/report.htm. Accessed 15 October 2020.

Berd, K. 2009. A War with many unknown quantities. *Computerra* 20: 26–29.

Brenner, Susan W. 2006. Cybercrime jurisdiction. *Crime, Law and Social Change* 46: 189–206. https://doi.org/10.1007/s10611-007-9063-7.

Chaikin, David. 2006. Network investigations of cyber-attacks: The limits of digital evidence. *Crime, Law and Social Change* 46: 239–256. https://doi.org/10.1007/s10611-007-9058-4.

Codex. 2008. *The Agreement on Cooperation between the CIS Member States in the fight against computer information crimes*. http://docs.cntd.ru/document/902140948. Accessed 15 October 2020.

Council of Europe. 2001. *Convention on Cybercrime: Explanatory Report*. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. Accessed 15 October 2020.

Council of Europe. 2018. *Towards a protocol to the Budapest Convention.* https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713. Accessed 15 October 2020.

Csonka, Peter. 2004. The Council of Europe Convention on cyber-crime: A response to the challenge of the new age? In *Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatico*, ed. I. Giovanni, and M. Gianfranco, 3–29. Milano: Giuffrè.

Donalds, Charlette, and Kweku-Muata Osei-Bryson. 2018. An Ontological approach to classifying cybercrimes in an ICT4D context. Lecture Notes in Computer Science. In *Designing for a Digital and Globalized World. DESRIST 2018. Lecture Notes in Computer Science, vol 10844*, 253–267. Cham: Springer. https://doi.org/10.1007/978-3-319-91800-6_17.

Europol. 2018. *Internet organised crime threat assessment*. https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2018. Accessed 15 October 2020.

Finklea, Kristin M. 2009. *Organised crime in the United States: Trends and issues for Congress*. Darby: DIANE Publishing.

Forst, Brian. 2009. *Terrorism, crime and public policy*. New York: Cambridge University Press.

General Assembly. 1990. *United Nations Rules for the Protection of Juveniles Deprived of their Liberty*. UN General Assembly Resolution 45/113 as of December 14. https://undocs.org/A/RES/45/113. Accessed 15 October 2020.

General Assembly. 2018. *Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General*. https://undocs.org/A/C.3/72/12. Accessed 15 October 2020.

General Assembly. 2019. *Resolution adopted by the General Assembly on 17 December 2018*. https://undocs.org/A/RES/73/187. Accessed 15 October 2020.

Gercke, Marco. 2009. Europe's legal approaches to cybercrime. *ERA Forum* 10: 409–420. https://doi.org/10.1007/s12027-009-0132-5.

Gercke, Marco. 2012. *Understanding cybercrimes: Phenomena, challenges and legal response*. Geneva: International Telecommunication Union.

Hakman, Joyce. 2017. *Building a stronger international legal framework on cybercrime*. https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime. Accessed 15 October 2020.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2017. *Cybercrime and digital forensics*, 2nd ed. Abingdon: Routledge.

Huey, Laura, Johnny Nhan, and Ryan Broll. 2013. Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime. *Criminology & Criminal Justice* 13: 81–97. https://doi.org/10.1177/1748895812448086.

Hunton, Paul. 2009. The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. *Computer Law & Security Review* 25: 528–535. https://doi.org/10.1016/j.clsr.2009.09.005.

Hunton, Paul. 2011. A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation* 7: 105–113. https://doi.org/10.1016/j.diin.2011.01.002.

International Telecommunication Union. 2017. Global Cybersecurity Index 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf. Accessed 15 October 2020.

Jarvis, Lee, Lella Nouri, and Andrew Whiting. 2014. Understanding, locating and constructing cyberterrorism. In *Cyberterrorism: Understanding, assessment and purpose*, ed. T.M. Chen, L. Jarvis, and S. Macdonald, 25–41. Heidelberg: Springer.

Karpova, Daria N. 2014. Cybercrimes: A Global issue and its solution. *Power* 8: 46–50.

Kavanagh, Camino. 2017. *The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century*. Geneva: United Nations Institute for Disarmament Research.

Kersting, Norbert. 2016. Participatory turn? Comparing citizens' and politicians' perspectives on online and offline local political participation. *Lex Localis - Journal of Local Self-Government* 14: 251–263.

Kierkegaard, Sylvia. 2007. Cybercrime convention: Narrowing the cultural and privacy gap? *International Journal of Intercultural Information Management* 1: 17–32. https://doi.org/10.1504/IJIIM.2007.014368.

Koksegenova, Oksana. 2011. Hackers threaten Kazakhstan. Computer Crime Research Center. http://www.crime-research.ru/analytics/cyber_kaz/. Accessed 15 October 2020.

Li, Xingan. 2007. International actions against cybercrime: Netwroking legal systems in the networked crime scene. *Webology* 4: 45.

Macdonald, Stuart, Lee Jarvis, and Simon M. Lavis. 2019. Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism,* in press. https://doi.org/10.1080/1057610X.2019.1696444

Maras, Marie H. 2014. *Computer forensics: Cybercriminals, laws and evidence*, 2nd ed. Massachusetts: Jones and Bartlett.

Maras, Marie H. 2016. *Cybercriminology*. Oxford: Oxford University Press.

McGuire, Mike, and Samantha Dowling. 2013. *Cybercrime: A review of the evidence. Summary of key findings and implications*. Home Office Research report No. 75. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Accessed 15 October 2020.

Ministry of Internal Affairs of the Russian Federation. 2019. *Website of the Office "K" of the Ministry of Internal Affairs of the Russian Federation*. https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii. Accessed 15 October 2020.

Rouse, Margaret, Matthew Haughn, and Stan Gibilisco. 2014. *Confidentiality, integrity, and availability (CIA triad)*. TechTarget. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. Accessed 15 October 2020.

Rowe, Brent, Dallas Wood, Douglas Reeves, and Fern Braun. 2011. *The role of internet service providers in cybersecurity*. Durham: Institute for Homeland Security Solutions.

Seebruck, Ryan. 2015. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation* 14: 36–45. https://doi.org/10.1016/j.diin.2015.07.002.

Selby, Nick. 2017. *Local police don't go after most cybercriminals. We need better training*. The Washington Post. https://www.washingtonpost.com/posteverything/wp/2017/04/21/local-police-dont-go-after-most-cybercriminals-we-need-better-training/. Accessed 15 October 2020.

Shore, Malcolm, Du. Yi, and Sherali Zeadally. 2011. A public-private partnership model for national cybersecurity. *Policy & Internet* 3: 1–23. https://doi.org/10.2202/1944-2866.1114.

Shukan, Aliya, Aitugan Abdizhami, Gulnar Ospanova, and Dana Abdakimova. 2019. Crime control in the sphere of information technologies in the Republic of Turkey. *Digital Investigation* 30: 94–100. https://doi.org/10.1016/j.diin.2019.07.005.

Sindhu, K.K., Rupali Kombade, Reena Gadge, and B.B. Meshram. 2014. Forensic Investigation processes for cybercrime and cyber space. In *Proceedings of International Conference on Internet Computing and Information Communication*, 193–206. New Delhi: Springer.

Smirnov, A.A. 2012. International legal aspects of fighting cybercrimes and cyber-terrorism. *Issues of Strengthening Legality and Rule: Science, Practice, Trends* 5: 323–329.

Smith, Russel G. 2007. Crime control in the digital age: An exploration of human rights implications. *International Journal of Cyber Criminology* 1: 167–179.

Somer, Tiia. 2019. Taxonomies of cybercrime: An overview and proposal to be used in mapping cyber criminal journeys. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security,* 475. Academic Conferences and publishing limited.

Statista. 2020. *Global internet penetration rate*. https://www.statista.com/statistics/269329/penetration-rate-of-theinternet-by-region/. Accessed 15 October 2020.
Tabansky, Lior, and Isaac Ben Israel. 2015. *Cybersecurity in Israel*. New York: Springer.
Tafazzoli, Tala. 2018. *Cyber Crime Legislation*. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf. Accessed 15 October 2020.
TASS. 2018. *Russia to propose draft cybersecurity convention to UN General Assembly*. http://tass.com/politics/1011749. Accessed 15 October 2020.
The Criminal Code of the Russian Federation as of 13 Jun 1996 N 63-FZ. 2019. http://www.consultant.ru/document/cons_doc_LAW_10699/. Accessed 15 October 2020.
UN. 2019. *Cybercrime 1. INTRODUCTION TO CYBERCRIME. Resource for lecturer*. https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf. Accessed 15 October 2020.
Unites Nations Office on Drugs and Crime. 2016. *Report of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime on its eighth session, held in Vienna from 17 to 21 October 2016*. https://undocs.org/en/CTOC/COP/2016/15. Accessed 15 October 2020.
UNODC. 2013. *Comprehensive study of cybercrime*. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed 15 October 2020.
Van Der Hof, Simone, and Bert-Jaap. Koops. 2011. Adolescents and cybercrime: Navigating between freedom and control. *Policy & Internet* 3: 1–28. https://doi.org/10.2202/1944-2866.1121.
Vardanyan, A.V., and E.V. Nikitina. 2007. *Investigation of hi-tech and computer information crimes*. Moscow: Yurlitinform Publ.
Wilson, Clay. 2008. *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*. https://fas.org/sgp/crs/terror/RL32114.pdf. Accessed 15 October 2020.
Xinhua. 2017. *Full text of BRICS leaders Xiamen Declaration*. Brics Summit Media Center. http://www.bricschn.org/English/2017-09/05/c_136583711_2.htm. Accessed 15 October 2020.
Zernik, Joseph. 2019. Cybersecurity and law in Israel - A case study. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 205–212. IEEE. https://doi.org/10.1109/icgs3.2019.8688318

Authors and Affiliations

Aigul Nukusheva[1] · Roza Zhamiyeva[2] · Viktor Shestak[3] · Dinara Rustembekova[4]

Roza Zhamiyeva
zhamiyeva_1@rambler.ru

Viktor Shestak
viktor_shestak@rambler.ru

Dinara Rustembekova
rustembekova_1@rambler.ru

1 Department of Civil and Labour Law, Karaganda State University Named After Academician E. A. Buketov, 28 University Str., Karaganda 100024, Republic of Kazakhstan

2 Department of Criminal Law, Procedure and Forensic Science, Karaganda State University Named After Academician E. A. Buketov, 28 University Str., Karaganda 100024, Republic of Kazakhstan

3 Department of Criminal Law, Criminal Procedure and Criminology, MGIMO University, 76, Prospekt Vernadskogo, 11945 Moscow, Russian Federation

4 Department of Civil and Labour Law, Karaganda State University Named After Academician E. A. Buketov, 28 University Str., 100028 Karaganda, Republic of Kazakhstan