



UDC 343.3/7
IRSTI 10.77.51

A.K. Kambarov, E.N. Baigundinov

Alikhan Bukeikhan University, Semey c., the Republic of Kazakhstan

INTERNATIONAL COOPERATION IN COMBATING CRIMINAL OFFENCES IN THE FIELD OF INFORMATIZATION AND COMMUNICATIONS

Abstract. Cybercrimes can be committed by criminals anywhere in the world where there is an Internet connection. The negative consequences of cybercrime can be felt outside the country where the criminal lives. The transnational nature of this crime challenges traditional notions of jurisdiction and requires cooperation between criminal justice officials worldwide. The necessity and validity of collaboration within the framework of international organizations are due to the global spread of this type of crime. International cooperation in cybersecurity should be systematic, holistic and consistent. Despite these and other successful joint efforts of the countries, there are currently obstacles standing in the way of international cooperation in the fight against cybercrime. This article discusses the concepts of sovereignty and jurisdiction concerning cybercrime, mechanisms of international cooperation, and problems related to the implementation of international collaboration.

Keywords: cyberspace; jurisdiction; international cooperation; cybercrime; European convention; information and communication technologies; telecommunications; Internet.

А.Қ. Қамбаров, Е.Н. Байгундинов

Alikhan Bukeikhan University, Семей қ., Қазақстан Республикасы

АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАРСЫ КҮРЕСТЕГІ ХАЛЫҚАРАЛЫҚ ҰНТЫМАҚТАСТЫҚ

Аннотация. Киберқылмыстарды қылмыскерлер интернетке кіру мүмкіндігі бар әлемнің кез келген жерінде жасай алады. Киберқылмыстың теріс салдары қылмыскер тұратын елден тыс жерде сезілуі мүмкін. Бұл қылмыстың трансұлттық сипаты юрисдикцияның дәстүрлі идеяларына қарсы тұрады және бүкіл әлем бойынша қылмыстық сот төрелігі жүйесінің қызметкерлері арасында ынтымақтастық орнатуды талап етеді. Халықаралық ұйымдар шеңберіндегі ынтымақтастықтың қажеттілігі мен негізділігі қылмыстың осы түрінің жаһандық таралуына байланысты. Киберқауіпсіздік саласындағы халықаралық ынтымақтастық жүйелі, тұтас және дәйекті болуға тиіс. Елдердің осы және басқа да табысты бірлескен күш-жігеріне қарамастан, қазіргі уақытта киберқылмыспен күресте халықаралық ынтымақтастық жолында әлі де кедергілер бар. Бұл мақалада киберқылмысқа қатысты егемендік пен юрисдикция ұғымдары, халықаралық ынтымақтастық тетіктері, сондай-ақ халықаралық ынтымақтастықты жүзеге асыруға байланысты мәселелер қарастырылады.

Түйінді сөздер: киберкеңістік; юрисдикция; халықаралық ынтымақтастық; киберқылмыс; еуропалық конвенция; ақпараттық-коммуникациялық технологиялар; телекоммуникация; интернет.

А.Қ. Қамбаров, Е.Н. Байгундинов

Alikhan Bukeikhan University, г. Семей, Республика Казахстан

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С УГОЛОВНЫМИ ПРАВОНАРУШЕНИЯМИ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Аннотация. Киберпреступления могут совершаться преступниками в любой точке мира, где есть выход в Интернет. Негативные последствия киберпреступности могут ощущаться за пределами страны, в которой проживает преступник. Транснациональный характер этой преступности бросает вызов традиционным представлениям о юрисдикции и требует налаживания сотрудничества между сотрудниками системы



уголовного правосудия по всему миру. Необходимость и обоснованность сотрудничества в рамках международных организаций обусловлена глобальным распространением данного вида преступности. Международное сотрудничество в сфере кибербезопасности должно быть системным, целостным и последовательным. Несмотря на эти и другие успешные совместные усилия стран, в настоящее время существуют препятствия, все еще стоящие на пути международного сотрудничества в борьбе с киберпреступностью.

В данной статье рассматриваются понятия суверенитета и юрисдикции применительно к киберпреступности, механизмы международного сотрудничества, а также проблемы, связанные с осуществлением международного сотрудничества.

Ключевые слова: киберпространство; юрисдикция; международное сотрудничество; киберпреступность; европейская конвенция; информационно-коммуникационные технологии; телекоммуникация; интернет.

DOI: 10.52425/25187252_2023_28_74

Introduction. Territorial sovereignty means the complete and exclusive exercise by a State of its rights and powers concerning its geographical territory. The protection of sovereignty is prominent in international and regional legal documents combating cybercrime. For example, the Arab League Convention of February 15, 2012 on combating Crimes in the Field of Information Technology can be cited. In particular, article 4 of this Convention reads as follows: «Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non interference in the internal affairs of other States.»¹.

Territorial sovereignty may extend to cyberspace, in particular, to the infrastructure of information and communication technologies of States. State sovereignty may be violated when third parties gain unauthorized access to information and communication technologies in foreign countries without the knowledge and permission of the country in which the information and communication technologies are located and its law enforcement agencies. Sovereignty is considered violated even if such unauthorized access is carried out as part of an investigation of a cybercrime committed in another country when that country is trying to identify the source of a cyberattack or prevent its commission [1, p. 318].

Modernity is characterized by the

transformation of the system of international relations and moving global currents. Mechanisms of comprehensive governance are improving, in the context of integration and the economic and political state of states, information factors play a large role. The development of the information sphere becomes one of the main factors affecting the development of society and the state. Depending on the degree of development of the information society, the economy and protective capabilities of the state function, the functional function of the institutions of the state [2, p. 126].

The term computer crime was introduced in the USA in the early 60s by D.B. Parker, who identified a new type of crime in which a computer is both the object of a crime since it causes material damage by physical damage, and an instrument of committing a crime when it is used to obtain political or business advantages [3, p. 215].

In the US Criminal Code, a computer crime is defined as a series of activities using a computer to extract benefits that caused or could cause damage or direct illegal use of computers in the commission of a crime or any criminal action for the successful implementation of which knowledge of computer technology is required.

A jurisdiction tied to sovereignty provides States with the rights and powers to determine and preserve the duties and rights of people on their territory, ensure compliance with legislation and punish violations of laws. States primarily declare their jurisdiction over crimes committed on their territory. Article 22 of the 2001 Council of

¹ Arab Convention on Combating Information Technology Offences, February 15, 2012 [Electronic resource] – Access mode: <https://nsarchive.gwu.edu/document/18573-national-security-archive-arab-convention> (Access data: 19.06.2023).



Europe Convention on Computer Crimes states: «Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with ... this Convention, when the offence is committed: a in its territory».

Nevertheless, as Brenner and Kups rightly point out, determining «whether a crime was committed on the territory of a country is, however, not an easy task when the crime was related to the use of cyberspace» [4, p. 10].

Jurisdiction over cybercrimes is determined by other factors, such as the nationality of the offender, the nationality of the victim and the consequences of cybercrime for the interests and security of the State: «Legal framework and human rights»), if only it is possible to establish «the existence of a sufficient or genuine link» between and the State exercising jurisdiction» [5].

In accordance with these and other national cybercrime laws, jurisdiction is established mainly on the basis of the location of criminals or victims and the consequences of cybercrime.

Materials and methods. The methodological basis of the scientific article consists of general scientific and individual scientific methods: analysis, synthesis, description, generalization, normative legal, formal legal, comparative legal methods, and legal statistics data.

Results and discussion. The development of the information sphere is becoming one of the main factors affecting the overall social and state action, which directly affects the effectiveness of the functioning of state institutions, the economy and the defense capability of states [6, p. 58].

The success of international cooperation depends on the availability of unified national legislation in combating cybercrime, providing for criminal liability for cybercrime, and national procedural legislation on cybercrime, which establish the rules of evidentiary law and rules for the conduct of criminal proceedings. International cooperation can also be facilitated by unifying bilateral, regional and multilateral legal instruments related to cybercrime. Accession to regional and plurilateral instruments on combating cybercrime and their ratification is

also necessary to make these documents legally binding for further familiarization with general issues of international cooperation in the fight against transnational organized crime.

The peculiarity of cybercrimes is their high latency, that is, the emergence of new methods of committing crimes creates difficulties due to the lack of necessary legal, organizational and technical means of proving them. Therefore, the fight against cybercrime is conditioned by the need for joint actions of the relevant state operational impact services, special services and law enforcement agencies. For this reason, the big question is about the creation of new bodies and organizations that control and combat cybercrime, requiring, in turn, the training of representatives and national personnel who can be involved in the activities of transnational bodies and organizations aimed at combating cybercrime [7].

Bilateral, regional and multilateral treaties also facilitate international cooperation in combating cybercrime, provided that the relevant act is mutually recognized as a crime. Without mutual recognition of the relevant act as a crime and unified laws, «safe havens» are created for persons who have committed cybercrimes where perpetrators cannot be prosecuted. This could be observed in 2000 in the example of the creator and distributor of the computer virus «LOVE BUG», who could not be brought to criminal responsibility since, at the time of the incident, his actions were not considered a crime in his country of residence.

Nevertheless, international cooperation is still possible without a strict interpretation of the requirement for mutual recognition of the relevant act as a crime. Cybercrime is very much a transnational crime. Urgent measures needed to preserve data at the national level are also necessary within the framework of international co-operation.

«Chapter III of the Convention on Cybercrime provides a legal framework for international cooperation with general and specific measures, including the obligation of countries to cooperate to the widest extent possible, urgent measures to preserve data and efficient mutual legal



assistance»².

However, there are exceptions to the requirement for mutual recognition of the relevant act as a crime. For example, article 29 of the Council of Europe Convention on Computer Crimes of 2001 does not require the glory of the relevant applicable act as a crime if it is necessary to «The authority seeking the preservation», «The stored computer data to be preserved and its relationship to the offence» on the primary offences, listed in this Convention. Article 29 provides for the right of States to refuse a request for preservation in cases where, within the framework of mutual legal assistance, a condition on the qualification of an offence as criminally punishable by both Parties is put forward for crimes not listed in the Convention³.

In addition to the requirement of mutual recognition of the relevant act as a crime, another essential need for international cooperation complies with international human rights law obligations. A request for international aid may be rejected if the requested State violates its international human rights obligations due to satisfying this request.

Informal mechanisms of international cooperation, such as information exchange between law enforcement agencies. The type of information exchanged by law enforcement agencies through unofficial channels varies depending on the specific State. In Australia, «the authorities have the opportunity to provide the following types of assistance within the framework of interdepartmental cooperation: taking voluntary witness statements, conducting voluntary interviews of witnesses, taking voluntary testimony by video link, accepting foreign police officers conducting investigations in Australia, exchanging operational data, carrying out physical surveillance, obtaining criminal records or obtaining publicly available materials». Other countries agree to share some personal data [8, p. 88].

Informal cooperation mechanisms facilitate the rapid exchange of information between

law enforcement agencies. In addition, 24/7 networks are created to receive urgent requests for digital evidence and promote international cooperation. Informal channels of cooperation are mainly used to obtain legal and technical advice and assistance in cases related to cybercrime and not for requests for digital evidence collection. For example, in Japan, bids for information through unofficial channels can be executed only if the requesting country does not intend to use this information as evidence. If a government wants to use this information as evidence, sending an official request for mutual legal assistance is necessary. Digital evidence obtained through these channels may be declared inadmissible in the national courts of the requesting State if the evidence protection system is not maintained.

Requests for assistance within the framework of international cooperation may also be rejected due to procedural requirements. Consider, for example, practical methods of storing, securing and accessing data. The execution of a request for the provision of data stored by Internet and communication service providers depends on the terms of service, privacy policy and business practices of the service provider⁴. In this regard, service providers differ not only in the type of data they store but also in the period of their storage, Twitter and the «Data Policy» («Data Usage Policy») Facebook for more information). Data storage and access policies also vary depending on national, regional and international data protection laws.

Requests for data security are sent to service providers by law enforcement agencies to preserve data before it is deleted or modified in any way. The procedure for obtaining access to the stored data is prescribed in national legislation. Legal orders, if any, are required to obtain various data from service providers, varying depending on the specific country. For example, in the United States, subpoenas and court orders are required to obtain non-content data and search warrants are required

² International Cooperation against Cybercrime [Electronic resource] – Access mode: <https://www.coe.int/en/web/cybercrime/international-cooperation> (Access data: 19.06.2023).

³ Convention on Cybercrime. Budapest, 23.11.2001 [Electronic resource] – Access mode: <https://rm.coe.int/1680081561> (Access data: 19.06.2023).

⁴ UNODC. Draft Comprehensive Study on Cybercrime / Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector [Electronic resource] – Access mode: https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf (Access data: 04.04.2023).



to obtain content-related data. «The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers»⁵.

In addition, in certain situations determined by national legislation, voluntary disclosure of information by Internet service providers is allowed without legal orders [9, p. 232]. An example of such a situation is an emergency request for data to prevent serious bodily injury or death. If service providers refuse to provide the requested data voluntarily, then under certain circumstances and depending on the specific case, the required evidence, the burden of proof and national legislation, these service providers may be forced to provide this information under the procedure provided by law.

Even with formal and informal mechanisms of international cooperation, problems arise when identifying and collecting digital evidence stored in cloud storage and from other service providers. The problem with cloud computing is that it's hard to know where the data is stored.

Cloud data can be fragmented and stored in different locations and several countries. The example of the case *United States v. Microsoft* can illustrate this problem of data fragmentation. As part of the investigation into the case, the U.S. government issued a search warrant under the U.S. Stored Communications Act of 1986 to obtain evidence in a drug trafficking case. Microsoft granted this request by transferring relevant non-content data stored on servers in the United States. Still, it did not provide the US government with relevant content-related data, since it was held in Dublin's Microsoft data center.

The effectiveness of international cooperation depends on the ability of States to comply with requests for evidence in such a way as to ensure the admissibility of this evidence in court. To do this, it is necessary to have qualified specialists in the field of cybercrime who can provide the receipt of proof following national standards of evidentiary law and the rules of criminal procedure. However, there are not enough such specialists. Moreover, countries worldwide

lack the national capacity needed to combat cybercrime.

This lack of national capacity results from a lack of human, financial and technical resources. Firstly, many countries lack a sufficient number of qualified specialists to conduct investigations of cybercrimes, as well as to prosecute cybercriminals and consider requests for assistance in the framework of international cooperation in cases related to cybercrime. Secondly, countries may lack the financial resources necessary to recruit, hire and retain qualified personnel, as well as to organize regular and up-to-date training for cybercrime investigators and other relevant specialists. Thirdly, countries lack the necessary material base to analyze digital evidence and the funds to purchase the equipment and digital forensics tools for properly investigating cybercrime [10, p. 126].

To address the national capacity deficit, partnerships have been installed and continue to be established with national, regional and international organizations, as well as private companies, to provide financial, personnel and technical assistance on issues related to cybercrime to countries in need of such aid. Help and support their efforts to develop national capacities combating cybercrime.

Per United Nations General Assembly resolution №65/230, resolution №22/8 of the UN Commission on Crime Prevention and Criminal Justice «United Nations Office on Drugs and Crime, on the basis of the needs of requesting States, to strengthen partnerships for technical assistance and capacity-building to counter cybercrime with Member States, relevant organizations, the private sector and civil society», «United Nations Office on Drugs and Crime to serve as a central data repository of cybercrime laws and lessons learned with a view to facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance», UNODC is mandated to assist States in combating cybercrime by providing technical training for capacity-building and implementing cybercrime prevention programmes and

⁵ Electronic Communications Privacy Act of 1986 (ECPA) [Electronic resource] – Access mode: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically> (Access data: 19.06.2023).



awareness-raising campaigns. These training, programs and campaigns are necessary because they offer long-term solutions to the existing national capacity shortage by increasing the knowledge, skills and capabilities needed to conduct cybercrime investigations⁶.

Conclusion. Mutual recognition of the relevant act as a crime and unification of national, bilateral, regional and multilateral laws on cybercrime is essential for international cooperation. Even if there is a requirement for mutual recognition of the relevant act as a crime and unified laws, international cooperation cybercrime investigation may be complex. The situation is aggravated by the lack of agreements regarding the timely collection and preservation of digital evidence and their exchange between countries

through official cooperation mechanisms. Countries worldwide also lack the national capacity to investigate cybercrimes in terms of human, financial and technical resources. In addition to the problem of the lack or shortage of the necessary funds, qualified personnel, specialised equipment and tools for conducting investigations of cybercrimes, there are also no generally accepted standards and protocols related to digital forensics and evidence collection that ensure the admissibility of digital evidence in the national courts of cooperating countries. Only a multilateral approach aimed at solving the problems mentioned above can improve the quality of international cooperation in cases related to cybercrime.

List of used literature:

1. Pål, W. Intervention in national and private cyberspace and international law / In Ebbesson, Jonas, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrange (eds) // International Law and Changing Perceptions of Security. – Brill/Nijhoff. – 2017. – Pp. 307-326.
2. Аратұлы, Қ. Ақпараттық құқық бұзушылықтармен күресу аспектілері: монография / Қ. Аратұлы. – Алматы: Қазақ университеті, 2019. – 143 б.
3. Медведевский, И.Д. Атака через Internet: под науч. ред. проф. Зегжды П.Д. – СПб.: Мир и Семья – 95, 2007. – 366 с.
4. Brenner, S.W. Approaches to cybercrime jurisdiction / S.W. Brenner and B.-J. Koops // Journal of High Technology Law. – 2004. – №4(1). – Pp. 1-46.
5. Голубев, В.А. Проблемы борьбы с кибертерроризмом в современных условиях [Электронный ресурс] – Режим доступа: <https://www.crime-research.org/library/e-terrorism.htm> (дата обращения: 05.04.2023).
6. Қамбаров, А.Қ. Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтармен күресудің кейбір теориялық аспектілері / А.Қ. Қамбаров, М.Д. Қаражанов // Құқық қорғау органдары академиясының жаршысы. – 2022. – №3(25). – 58-67 б.
7. Протасевич, А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, П.П. Зверьянская // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – №3. – С. 28-33.
8. Volker, E. Key Contours of Citizenship and Ius Doni / E. Volker, C. Gloria. – In: Knut Ipsen (ed.). – Der Staat im Volkerrecht; 5th ed. Munich: C.H. Beck. – 2004. – 115 p.
9. Kate, W. International Law Enforcement Access to User Data: A Survival Guide and Call for Action / W. Kate, K. Gail // Canadian Journal of Law and Technology. – 2015. – №13(2). – Pp. 225-254.
10. Dan, S. Guide to Obtaining Communication Service Provider Evidence from the United States / S. Dan. – 2016. – 182 p.

References:

1. Pål, W. Intervention in national and private cyberspace and international law / In Ebbesson, Jonas, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrange (eds) // International Law and Changing Perceptions of Security. – Brill/Nijhoff. – 2017. – Rr. 307-326.

⁶ Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime [Electronic resource] – Access mode: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf (Access data: 19.06.2023).



2. Aratǵly, Q. Aqparattyq qúqyq bızushylyqtarmen kyresu aspektileri: monografija / Q. Aratǵly. – Almaty: Qazaq universiteti, 2019. – 143 b.
3. Medvedovskij, I.D. Ataka cherez Internet: pod nauch. red. prof. Zegzhdy P.D. – SPb.: Mir i Sem'ja – 95, 2007. – 366 s.
4. Brenner, S.W. Approaches to cybercrime jurisdiction / S.W. Brenner and B.-J. Koops // Journal of High Technology Law. – 2004. – №4(1). – Rr. 1-46.
5. Golubev, V.A. Problemy bor'by s kiberterrorizmom v sovremennyh uslovijah [Jelektronnyj resurs] – Rezhim dostupa: <https://www.crime-research.org/library/e-terrorism.htm> (data obrashhenie: 05.04.2023).
6. Qambarov, A.Q. Aqparattandyru zhəne bajlanys salasyndary qylmystyq qúqyq bızushylyqtarmen kyresudiń kejbir teorijalyq aspektileri / A.Q. Qambarov, M.D. Qarazhanov // Qúqyq qorǵau organdary akademijasynuń zharshysy. – 2022. – №3(25). – 58-67 b.
7. Protasevich, A.A. Bor'ba s kiberprestupnost'ju kak aktual'naja zadacha sovremennoj nauki / A.A. Protasevich, P.P. Zverjanskaja // Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta jekonomiki i prava. – 2011. – №3. – S. 28-33.
8. Volker, E. Key Contours of Citizenship and lus Doni / E. Volker, C. Gloria. – In: Knut Ipsen (ed.). – Der Staat im Volkerrecht; 5th ed. Munich: C.H. Beck. – 2004. – 115 p.
9. Kate, W. International Law Enforcement Access to User Data: A Survival Guide and Call for Action / W. Kate, K. Gail // Canadian Journal of Law and Technology. – 2015. – №13(2). – Rr. 225-254.
10. Dan, S. Guide to Obtaining Communication Service Provider Evidence from the United States / S. Dan. – 2016. – 182 p.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Азамат Қамбарұлы Қамбаров – Alikhan Bokeikhan University докторанты, заң ғылымдарының магистрі, e-mail: aza_kambarov@mail.ru.

Қамбаров Азамат Қамбарұлы – докторант Alikhan Bokeikhan University, магистр юридических наук, e-mail: aza_kambarov@mail.ru.

Kambarov Azamat Kambaruly – doctoral student of Alikhan Bokeikhan University, Master of Law, e-mail: aza_kambarov@mail.ru.

Елдос Нағымбайұлы Байгундинов – Alikhan Bokeikhan University заң факультетінің қылмыстық құқықтық пәндер кафедрасының аға оқытушысы, философия докторы (PhD), e-mail: ben_semcity@mail.ru.

Байгундинов Ельдос Нағымбаевич – старший преподаватель кафедры уголовно-правовых дисциплин юридического факультета Alikhan Bokeikhan University, доктор философии (PhD), e-mail: ben_semcity@mail.ru.

Baigundinov Eldos Nagymbaevich – Senior Lecturer of the Department of Criminal Law Disciplines of the Faculty of Law Alikhan Bokeikhan University, Doctor of Philosophy (PhD), e-mail: ben_semcity@mail.ru.