Law Review • vol. X, issue 2, July-Decembre 2019, pp. 218-227

Regionalization of international cooperation in the fight against cybercrime*

*Nataliya MAROZ***

Abstract

International legal cooperation in the fight against cybercrime is carried out primarily on the basis of regional treaties. Since every regional legal regime is unique and has its own specific characteristics the article addresses possible implications of such regionalization. Therefore, the goal of the research is to reveal characteristics of an ongoing trend on regionalization of international legal cooperation in the fight against cybercrime and its possible impact on practical aspects of combating these crimes. It doesn't address any institutional developments in the area and covers only treaty cooperation on the matter. The applicability of universal treaties on combating different types of crimes to cybercrime suppression is identified. An analysis of regional cybercrime treaties is carried out. On the basis of the undertaken research author makes a conclusion, that regionalization of the international legal cooperation in the fight against cybercrime has its positive and negative sides and has led to a paradoxical situation which partly might be explained by a transnational nature of cybercrime. From one point, regional treaty is the best way to address cybercrime problem within a certain regional organization. From the other side different approaches to the criminalization of acts committed on the Internet or with the use of computer technologies might lead to creation of save heavens for cyber criminals, impede mutual legal assistance or extradition between countries that belong to different regions.

Keywords: *Public law, regionalisation, fragmentation of international law, cybercrime, international cooperation in the fight against cybercrime*

Introduction

Cybercrime has an adverse impact on different aspects of social life and economics. As it was emphasized by the United Nations [hereafter – UN] Information Service "threats to Internet safety have spiked dramatically in recent years, and cybercrime now affects more than 431 million adult victims globally"[1].

* The article was prepared for the International Law Conference, "*Current Issues within EU and EU Member States: Converging and Diverging Legal Trends*", 3rd edition, organized by the Faculty of Law – Transilvania University of Braşov on the 29th-30th of November 2019. All links were last accessed on 25 September 2019.

Cybercrime is not only one of the fastest growing threats it also might be really destructive. In 2016 a British hacker Daniel Kaye developed a botnet which attack, finally, resulted in the shutdown of the Internet in most countries of West Africa[2]. Other well-known examples of disruptive cyber incidents are Petya and NotPetya virus attacks. The latter spread to more than 10 countries and lead to more than $10 billion in total damage, according to the US Homeland Security adviser Tom Bossert[3].

These cases perfectly demonstrate the need for strong international legal cooperation in the fight against cybercrime. In particular, it concerns the need for harmonization of criminal legislation, both material and procedural, and legal framework for mutual legal assistance on criminal matters and extradition.

Unfortunately, computer technologies are being developed too fast so that national criminal law can't keep pace with all the changes. Moreover, cybercrime tends to be transnational and, therefore, needs a comprehensive international legal framework to suppress it. Despite the fact states and intergovernmental organizations recognize transnational nature of cybercrime, there is a considerable debate concerning the necessity to conclude a treaty on cybercrime of universal character. Basically, international legal cooperation in the fight against cybercrime is promoted at regional level. Different approaches to criminalization of conduct in cyber space, preservation and collection of electronic evidence might impede effective collaboration of competent authorities and, thus, combating cybercrime.

The goal of the research is to reveal characteristics of an ongoing trend on regionalization of international legal cooperation in the fight against cybercrime and its possible impact on practical aspects of combating these crimes. It doesn't address any institutional developments in the area and covers only treaty cooperation on the matter.

Therefore, the article attempts to cover two major issues. First of all, it concerns international legal framework for cybercrime suppression and regional conventions establishing legal basis for international cooperation in the fight against cybercrime. Secondly, it addresses the influence of regionalization of international cooperation in the area discussed on the effectiveness of cybercrime suppression.

** Assistant Professor, Ph.D. – Belarusian State University (nataliya.maroz@gmail.com).

[1] UN Information Service, *Cybercrime*, available on http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html.

[2] The Sunday Times, *British hacker Daniel Kaye shut down web for entire nation of Liberia*, available on https://www.thetimes.co.uk/article/british-hacker-daniel-kaye-shut-down-web-for-entire-nation-of-liberia-dn9kzslhd, consulted on 10.10.2019.

[3] R. Brewer. *NotPetya malware estimated to have caused $10bn damage*, available on http://insights.threatmanagement.info/post/102f15f/notpetya-malware-estimated-to-have-caused-10bn-damage.

1. International legal framework for cooperation in the fight against cybercrime

Unfortunately, there is no universal treaty which specifically deals with international legal cooperation in the fight against cybercrime. However, some international treaties that regulate international cooperation in combating other types of crimes, for which cyber aspect might constitute one of the sub elements of *actus reus*, can be applicable to the matter.

The UN Convention on transnational organized crime (2000) and the Optional protocol on the sale of children, child prostitution and child pornography (2000) can be a basis for international cooperation when a particular cybercrime satisfies general requirements set forth in these treaties. So, the Optional protocol can be applicable to producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography when these acts are committed online (art. 3 c) of the Protocol)[4]. The UN Convention on transnational organized crime can apply to the prevention, investigation and prosecution of a serious cyber offence when it is transnational in nature and involves an organized criminal group (art. 3 (1) of the Convention)[5].

However, this international framework is not enough to create a comprehensive and robust mechanism of cybercrime suppression, which requires a well-established system of mutual assistance to ensure preservation and transmission of electronic evidence while investigating a transnational cybercrime. As it was stressed in the Discussion Guide for the Fourteenth UN Congress on Crime Prevention and Criminal Justice "technology and globalization enable criminals to coordinate across regions like never before, increasing their reach, crimes, targeted victims and profits"[6]. Transnational cybercrime can affect different states from different regions challenging an existing system of international legal cooperation in the fight against high-tech crime.

Unfortunately, an initiative to negotiate a treaty on cybercrime under the auspices of the UN wasn't supported by the states[7]. Since the 12th UN Congress

---

[4] *Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography*, New York, 25 May 2000, available on https://treaties.un.org/doc/Treaties/2000/05/20000525%2003-16%20AM/Ch_IV_11_cp.pdf.

[5] *United Nations Convention against Transnational Organized Crime*, New York, 15 November 2000, available on https://www.unodc.org/documents/rpanc/Publications/UN_documents/Crime/TOCebook-e.pdf.

[6] Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, *Discussion Guide*, 24 September 2018, A/CONF.234/PM.1, available on https://www.unodc.org/documents/congress//Documentation_14th_Congress/DiscussionGuide/A_CONF234_PM1_e_V1806329.pdf.

[7] *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, El Salvador, Brazil, April 12–19, 2010, available on http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053830r.pdf.

on Crime Prevention and Criminal Justice this issue hasn't been among the questions for the discussion.

In this regard international regional intergovernmental organizations make substantial effort to create an effective legal framework for cybercrime suppression. For the past 20 years there have been concluded 6 cybercrime conventions: *Council of Europe* [hereafter – COE] *Convention on cybercrime* (2001) and its *Additional protocol on xenophobia and racism* (2003); *African Union Convention on cyber security and personal data protection* (2014); *Collective Security Treaty Organization* [hereafter – CSTO] *protocol on counteracting crimes in information security area* (2014); *Agreement on cooperation of the member-states of the Commonwealth of Independent States* [hereafter – CIS] *in fighting crimes in the sphere of computer information* (2001); *Arab Convention on combating information technology offences* (2010).

All these treaties establish a legal framework for harmonization of criminal legislation and cooperation of law enforcement agencies and courts in the fight against cybercrime in a certain region. However, regional agreements on cybercrime also create various more or less formal regulatory regimes that actually might provoke legal conflicts resulting in deviations of institutional practices and emergence of conflicting jurisprudence, and more importantly, in creating safe havens for cyber criminals[8].

2. Regional treaties on cybercrime and their characteristic

All the regional cybercrime treaties have their own specific features and might be divided into 2 major groups.

The first group includes treaties that are concluded in the Post-soviet space and are aimed at harmonization of criminal legislation rather than regulating mutual legal assistance in criminal matters. It encompasses the CSTO protocol on counteracting crimes in information security area and the Agreement on cooperation of the member-states of the CIS in fighting crimes in the sphere of computer information.

The aforementioned treaties were negotiated to address to a special challenge to cyber security, which can be revealed through the interpretation of their preambles. The Agreement on cooperation of the member-states of the CIS in fighting crimes in the sphere of computer information was concluded to "to create a legal basis for the cooperation of law enforcement and judicial bodies of the state parties in the fight against crimes in the sphere of computer

[8] *Fragmentation of international law: difficulties arising from the diversification and expansion of international law*, Report of the Study Group of the International Law Commission, 13 April 2006, available on http://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf.

information"[9]. At the same time the CSTO protocol on counteracting crimes in information security area is seeking "to ensure effective collective interaction to counter criminal activities in the information sphere and to create the legal basis for cooperation of intelligence services and law enforcement agencies of the Parties in the fight against crimes in the field of information technology"[10]. Thus, the treaties have close, but still different objects of legal regulation.

Interestingly, that the list of state-parties to these conventions almost coincides. For example, Armenia, Belarus, Russian Federation, Kazakhstan, Kyrgyzstan, Tadzhikistan are state-parties to both multilateral cybercrime conventions concluded within the post-Soviet space[11]. Since the aforementioned conventions are not treaties relating to the same subject matter, they don't create conflicting obligations for the state parties to both of them.

The CSTO protocol on counteracting crimes in information security area establishes a legal framework for suppression three types of conduct, which is considered as a crime in accordance with national legislation of state-parties to the Protocol: against constitutional system and state security, against peace and security of mankind, in the field of information technology.

The scope of the Agreement on cooperation of the member-states of the CIS in fighting crimes in the sphere of computer information is relatively narrow. The treaty regulates cooperation in combating only crimes against computer information (illegal access to computer information; creating, using, or distributing malware; violation of the rules of operation of a computer, computer system or their network by a person that has a legal access to a computer; illegal use of computer programs and databases protected under copyright law). So, this regional agreement doesn't deal with any other offences. However, the vast majority of cybercrimes are criminal offences against property such as cyber theft, cyber fraud etc. Moreover, it worth noting that this treaty doesn't contain any legal provisions on harmonization of criminal procedural legislation in terms of collecting and using electronic evidence.

---

[9] *Agreement on cooperation of the member-states of the Commonwealth of Independent States in fighting crimes in the sphere of computer information*, Minsk, 1 June 2001 (rus), available on http://www.cis.minsk.by/page.php?id=866.

[10] *Collective Security Treaty Organization protocol on counteracting crimes in information security area, Moscow*, 23 December 2014 (rus), available on http://pravo.by/upload/docs/op/E71400003_1438290000.pdf.

[11] *Agreement on cooperation of the member-states of the Commonwealth of Independent States in fighting crimes in the sphere of computer information* (rus), document characteristic available on http://etalonline.by/document/?regnum=n00100021&q_id=1118554&type=card; *Collective Security Treaty Organization protocol on counteracting crimes in information security area* (rus), document characteristic available on http://etalonline.by/document/?regnum=e71400003&q_id=1118566&type=card.

The CIS Agreement and CSTO Protocol regulate possible conflict situations emanating from the participation of the state parties in other international treaties. Both treaties stipulate that they "shall not affect the rights and obligations of the High Contracting Parties arising from other international treaties to which they are parties"[12].

In 2018 member states of the CIS signed an Agreement on cooperation in the fight against information technology crimes which aim is to replace the Agreement of 2001[13]. This new treaty significantly extends the area of cooperation between the CIS member-states in combating cybercrime, requesting to criminalize not only the crimes in the sphere of computer information but also cyber theft, computer sabotage, online calls for terrorist acts and extremism activity, dissemination of child pornography through electronic means of communication. Nevertheless, it hasn't come into force yet.

Unfortunately, none of the first group treaties contains provisions with regard any procedural measures to be taken at the national level for the purpose of criminal investigation of cybercrimes and the collection of evidence in electronic form. However, one of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act[14]. Another drawback of this type of treaties is that they are based on a traditional approach to mutual legal assistance on criminal matters.

The second group of treaties includes the COE Convention on cybercrime and other regional conventions based on it.

The COE Convention on cybercrime is considered to be the most detailed and progressive treaty in this field. It covers harmonization of legislation, human rights challenges arising out of combating cybercrime, jurisdiction issues and mutual legal assistance[15]. It was ratified by 64 states, including Argentina, Australia, Cabo Verde, Canada, Costa Rica, Chile, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Panama, Paraguay, Peru, Philippines, Senegal, Sri Lanka, the United States, Tonga, which are non-member states of the Council

[12] *Agreement on cooperation of the member-states of the Commonwealth of Independent States in fighting crimes in the sphere of computer information*, Minsk, 1 June 2001; *Collective Security Treaty Organization protocol on counteracting crimes in information security area, Moscow*, 23 December 2014 (rus).

[13] *Agreement on cooperation of the member-states of the Commonwealth of Independent States in the fight against information technology crimes*, Dushanbe, 28 September 2018 (rus), available on https://base.spinform.ru/show_doc.fwx?rgn=110821.

[14] Police Executive Research Forum, *The Changing Nature of Crime And Criminal Investigations*, available on https://www.policeforum.org/assets/ChangingNatureofCrime.pdf.

[15] *Convention on Cybercrime*, Budapest, 23.11.2001, available on https://rm.coe.int/1680081561.

of Europe[16]. Moreover, Benin, Colombia, Nigeria, Tunisia have been invited to accede to the COE Convention on cybercrime[17].

Its comprehensive legal framework became one of the arguments against the concluding a universal convention under the auspices of the UN during the 11th and 12th Congresses on crime prevention and criminal justice. The delegates believed that the COE Convention could have become a universal legal framework for international legal cooperation in the fight against cybercrime[18]. However, some states argued that the convention contained some provisions that could have posed threats to sovereignty and national security (in particular, it concerned art. 32 (b) of the convention, which was dedicated to transboundary access to computer information). These arguments are still being put forward by some countries (for example, Russian Federation)[19].

The mechanism of accession to the COE Convention on cybercrime is quite complicated to the non-member states of the COE. In accordance with art. 37 a candidate state seeking for accession to the convention should get a unanimous consent of the contracting states to the convention and the consent of the Committee of Ministers of the Council of Europe[20]. It's not difficult to imagine that even a slight political misunderstanding exiting between a candidate state and a state party to the treaty might be a serious obstacle to its accession. The final decision of a state party on this matter is not supposed to be supported by any argument. It's a sovereign right of a state party to give or refuse to give this kind of consent. Therefore, despite the fact the number of the state parties to the COE Convention on cybercrime that are non-member states of the COE has been grown during the past five years; it would be still unfair to assert the Convention could be a universal legal framework for cybercrime suppression.

The Convention on cybercrime was concluded in 2001, and, thus, didn't address all the modern trends in cybercrime. Therefore, there hadn't been taken into consideration botnets, child grooming over the Internet or crypto-currency fraud while drafting this treaty. In this regard, the Conventional committee (T-CY) issues guidelines aimed at facilitating the effective use and implementation

---

[16] *Chart of signatures and ratifications of Treaty 185*, available on https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=BUuD8GPy.

[17] *Non-members States of the Council of Europe*, available on https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22.

[18] *Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice*, Bangkok, April 18–25, 2005, available on http://www.un.org/russian/events/11thcongress/a_conf203_18.pdf.

[19] A. Arsentiev, *Putin has refused to sign the Convention on cybercrime* (rus), available on http://safe.cnews.ru/news/top/putin_otkazalsya_podpisat_konventsiyu.

[20] *Convention on Cybercrime*, Budapest, 23.11.2001, available on https://rm.coe.int/1680081561.

of the COE Convention on cybercrime in the light of legal, policy and technological developments[21].

Despite positive results achieved in terms of interpretation of the COE Convention on cybercrime by the T-CY, some recent trends in cybercrime need to be addressed only through a specific legal instrument. In particular, there exists a widespread practice of the cloud computing used for commercial and private purposes, which poses new challenges to collection of electronic evidence. Therefore, in 2017 the states parties to the COE Convention on cybercrime agreed to launch the preparation of a protocol to this treaty to help law enforcement secure evidence on servers in foreign, multiple or unknown jurisdictions[22]. The protocol is expected to contain provisions "for more effective mutual legal assistance; direct cooperation with service providers, including production orders for subscriber information to be issued directly to a service provider in another Party; extending searches transborder" etc.[23]

While analyzing the treaties that belong to the second group it's worth mentioning the Arab convention on combating information technology offences which content was basically developed on the basis of COE Convention on cybercrime. This treaty also consists of two major parts. The first part is dedicated to the harmonization of criminal legislation, both material and procedural. The second one concerns legal and judicial cooperation on the matter. Remarkably, that the convention attempts to provide a comprehensive list of computer-related offences (forgery, fraud, theft, pornography, child pornography, terrorism, organized crime, traffic in human beings etc). However, the treaty has a significant drawback. It prescribes the state parties to criminalize some conduct not giving any explanation of its *actus reus* (art. 14-15 of the Arab convention stipulating "other offences related to pornography" and "offence against privacy by means of information technology").

The Arab convention contains some important legal provisions with regard to mutual legal assistance. First of all, in accordance with this treaty mutual legal assistance is granted only on a basis of a legal request sent by one appointed central authority directly to another (which is similar to a corresponding provision of the COE Convention on cybercrime). Secondly, a state party can

---

[21] *Guidance Notes*, available on https://www.coe.int/en/web/cybercrime/guidance-notes.

[22] Council of Europe, *Cybercrime: towards a Protocol on evidence in the cloud*, available on https://www.coe.int/en/web/human-rights-rule-of-law/-/cybercrime-towards-a-protocol-on-evidence-in-the-clo-1.

[23] Directorate of Legal Advice and Public International Law, *Use of a 'disconnection clause' in the second additional protocol to the Budapest Convention on Cybercrime*, 29.04.2019, available on https://www.coe.int/en/web/dlapil/-/use-of-a-disconnection-clause-in-the-second-additional-protocol-to-the-budapest-convention-on-cybercri-1.

refuse to provide any legal assistance if a dual criminality clause is not satisfied (art. 32 (5) of the Arab convention)[24].

African Union Convention on cyber security and personal data protection is a complex treaty covering civil and public aspects of cybersecurity. The convention enlarges a list of cyber-offences in comparison with the COE Convention on cybercrime, paying particular attention to computerized data breaches and content-related offences. Unfortunately, the African Union Convention doesn't stipulate a procedure of mutual legal assistance precisely. In particular, art. 28 of the treaty provides that "state parties that don't have agreements on mutual legal assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double liability, while promoting the exchange of the information as well as the efficient sharing of data between the organizations of state parties on a bilateral or multilateral basis"[25]. So, the African Union Convention mostly leaves aside the question of mutual legal assistance in criminal matters encouraging state parties to regulate them in specific international agreements.

Both the COE convention on cybercrime and the African Union Convention on cyber security and personal data protection establish conventional monitoring mechanisms, which functions, actually, differ in many respects.

The T-CY was established in accordance with art. 46 of the COE Convention on cybercrime with the aim to coordinate consultations of the state parties in three major areas (facilitating the effective use and implementation of the convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under the convention; the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form; consideration of possible supplementation or amendment of the convention).

Pursuant to art. 32 the African Union Convention's Operational mechanism has a wider competence than T-CY and fulfils a range of functions covering all the areas regulated by this treaty. In particular, it formulates and promotes the adoption of harmonized codes of conduct for the use of public officials in the area of cyber security; submits reports to the Executive Council of the African Union concerning the implementation of the convention; establishes partnerships

[24] *Arab Convention on Combating Information Technology Offences*, Cairo, 21.12.2010, available on https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

[25] *African Union Convention on cyber security and personal data protection*, Malabo, 27.06.2014, available on https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

with the African Union bodies, civil society, intergovernmental and non-governmental organizations in the area discussed etc.

To conclude, regional treaties establish different legal regimes for international legal cooperation in the fight against cybercrime. The treaties concluded in the Post-Soviet space are aimed at harmonization of criminal law and rely on traditional mechanism of mutual legal assistance in criminal matters. The treaties developed on the basis of the COE convention on cybercrime regulate international cooperation in the fight against cybercrime more comprehensively establishing a framework for harmonisation of material and procedural criminal legislation, as well as mutual legal assistance. Unfortunately, the list of cybercrimes enshrined in the treaties differs from region to region. This situation might give rise to a problem in prosecuting those committed these types of transnational offences.

Conclusions

Regionalization of the international legal cooperation in the fight against cybercrime has its positive and negative sides and has led to a paradoxical situation which partly might be explained by a transnational nature of cybercrime. From one point, regional treaty is the best way to address cybercrime problem within a certain regional organization. From the other side different approaches to the criminalization of acts committed on the Internet or with the use of computer technologies might lead to creation of save heavens for cyber criminals, impede mutual legal assistance or extradition between countries that belong to different regions.

The lack of international legal framework for mutual assistance in the field might lead to a situation when law enforcement agents have to cooperate directly on the base of their personal contacts of their colleagues in foreign countries. In the absence of specific legal framework providing the widest and quickest cooperation possible it's quite difficult to combat cybercrime effectively.

The COE Convention on cybercrime can't establish a universal mechanism for international cooperation in the fight against cybercrime. It contains a very complicated mechanism for accession, which is reasonable for a regional treaty, however, inadmissible to any convention to be considered as of universal level. Moreover, there is no global consensus concerning the content of its several provisions concerning transboundary access to computer data.

The more authentic regional treaties on cybercrime are, the more fragmented international legal framework for international cooperation in the fight against cybercrime is. The more regional organizations focus on their specific needs in the field discussed, the less it's possible to create a robust and effective mechanism of international cooperation in the fight against cybercrime. Therefore, any regional treaty-drafting process should be accompanied by a comprehensive research of existing treaty instruments on cybercrime.