https://doi.org/10.18485/iipe_ioscw.2022.1.ch34

THE COUNCIL OF EUROPE AND THE FIGHT AGAINST CYBERCRIME

Zvonimir IVANOVIĆ*

Abstract: The Council of Europe adopted the Convention on Cybercrime in 2001, and it entered into force on July 1, 2004. The Convention represents the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child abuse materials, and violations of network security. The Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, entered into force on March 1, 2006. Serbia has signed and ratified both the Cybercrime Convention and the First Additional Protocol in 2009. On November 17, 2021, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. As a response, the Protocol provides a legal basis for disclosure of domain name registration information and for direct cooperation with service providers for subscriber information; an effective means to obtain subscriber information and traffic data; immediate cooperation in emergencies; mutual assistance tools; and personal data protection safeguards. The signing of the Second Additional Protocol will be held in May 2022, and Serbia will probably sign it. The paper analyzes the solutions achieved in the fight against cybercrime, as well as Serbia's cooperation with the Council of Europe in this area.

Keywords: Council of Europe, Cybercrime, Second protocol, evidence, international cooperation.

INTRODUCTION

The Council of Europe was the pioneer in regulating the cybercrime area (Ivanović et al., 2010; 2012a; 2021). This is due to its international position,

* Professor, University of Criminal Investigation and Police Studies, Belgrade. E-mail: zvonimir.ivanovic@kpu.edu.rs

the possibility not to have political or allied influences, but also the specific position this organization has. At the moment of working on drafting the convention during the 90-ties and early 2000, the world was still in the state of the post-Soviet crash, without any real shaping of multipolar influences. The OSCE and UN recognized the need to regulate this area, and some activities were initiated by the International Telecommunication Union (ITU), an international organization under the UN, but all odds were stacked against the Council of Europe (CoE). In the preamble of the CETS 185, the official title of the CoE Budapest convention, it is stated, " the aim of the Council of Europe is to achieve greater unity among its members; recognizing the value of fostering cooperation with the other States parties to this Convention; convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation; conscious of the profound changes brought about by the digitalization, convergence, and continuing globalization of computer networks; concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; recognizing the need for cooperation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; believing that an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters; convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity, and availability of computer systems, networks and computer data as well as the misuse of such systems, networks, and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation, and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international cooperation" (Council of Europe, 2001, November 23; Gergke et al., 2008; Ivanović et al., 2016). This preamble serves best to describe the status and actual odds between the parties of the treaty, in order to create new boundaries for criminal prosecution of offenders and to provide efficient tools in combating crime in the area of cyber. While building upon the existing Council of Europe conventions on cooperation in the penal field as well as similar treaties which exist between the Council of Europe member States and other States, and stressing that the present Convention is intended

to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence, this convention is the new and very actual legislative effort in the then modern world. This is evidenced by many accessors located outside the European continent, from America, Asia, Australia, and Africa (Ivanović, 2015a). In the preamble is also stated that "Welcoming recent developments which further advance international understanding and cooperation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8; Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications (Ivanović et al., 2012, October 8-9); No. R (88) 2 on piracy in the field of copyright and neighboring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology; Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international cooperation, which duly takes into account the specific requirements of the fight against cybercrime; Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe" (Council of Europe, 2022). All of this serves to strengthen future efforts and provide a solid basis for

international regulations in this area. However, later there will be more dissonant tones about the sovereignty of states in cyberspace, which will encourage Russia not to accede to the convention and officially reject its validity on its territory. This has cast a few shadows of doubt, but the Convention is still here and is being adopted by new members and non-members of the CoE. The First Additional Protocol of the CoE CETS 185 came several years after the adoption of the Convention. The Protocol was opened for signature in Strasbourg on January 28, 2003, on the occasion of the First Part of the 2003 Session of the Parliamentary Assembly. The explanatory protocol provides reasons and grounds for drafting the additional protocol through the following. "As technological, commercial, and economic developments bring the peoples of the world closer together, racial discrimination, xenophobia, and other forms of intolerance continue to exist in our societies. Globalization carries risks that can lead to exclusion and increased inequality, very often along racial and ethnic lines. In particular, the emergence of international communication networks like the Internet provides certain persons with modern and powerful means to support racism and xenophobia and enables them to disseminate easily and widely expressions containing such ideas. In order to investigate and prosecute such persons, international cooperation is vital. The Convention on Cybercrime (ETS 185), hereinafter referred to as "the Convention", was drafted to enable mutual assistance concerning computer-related crimes in the broadest sense in a flexible and modern way. The purpose of this Protocol is twofold: firstly, to harmonize substantive criminal law in the fight against racism and xenophobia on the Internet and, secondly, to improve international cooperation in this area. This kind of harmonization alleviates the fight against such crimes on the national and international levels (Ivanović et al., 2012b; 2012, October 8-9; 2020b). Corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by parties whose laws in this area are less well defined. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced too. International cooperation (especially extradition and mutual legal assistance) is facilitated, e.g., regarding requirements of double criminality" ((Explanatory Report to the Additional Protocol to the Convention on Cybercrime, 2003, January 28, p. 1). There was a task for the agencies of the CoE on preparing "the ratification of Contracting Parties to the Convention, dealing in particular with the following: 1) The definition and scope of elements for the criminalization of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms

of distribution of materials or messages with such content through computer networks; 2) The extent of the application of substantive, procedural and international cooperation provisions in the Convention on Cybercrime to the investigation and prosecution of the offences to be defined under the Additional Protocol. This Protocol entails an extension of the Convention's scope, including its substantive, procedural, and international cooperation provisions, so as to cover offences of racist and xenophobic propaganda. Thus, apart from harmonizing the substantive law elements of such behavior, the Protocol aims at improving the ability of the parties to make use of the means and avenues of international cooperation set out in the Convention in this area" (*Ibidem*). This first additional protocol had as its leading intention the incrimination of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms of distribution of materials or messages with such content through computer networks – and this intention was very much needed, since there were numerous activities online in the rising xenophobic and racist material and hate speech disseminated through different hubs. This was the way to stand up against that internationally, and a successful one. The second idea behind the additional protocol was to extend the extent of the application of substantive, procedural, and international cooperation provisions in the Convention on Cybercrime to the investigation and prosecution of the offences to be defined under the Additional Protocol.

THE SECOND ADDITIONAL PROTOCOL

Following almost four years of negotiations (September 2017–May 2021) and formal approval on November 17, 2021, the Second Additional Protocol to the Budapest Convention on Cybercrime is now open for signature at the Council of Europe in Strasbourg, France, starting on May 12, 2022, within the framework of an international conference on enhanced cooperation and disclosure of electronic evidence, which is scheduled to be held on May 12-13, 2022. The need for the introduction of this Second Additional Protocol came from the striving of the CETS 189 to extend the applicable provisions of the Convention, with special emphasis on the evidentiary and procedural aspects of this area of criminal and criminal procedure law enforcement internationally, or even worldwide. The title of the second protocol is as follows: The Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and the disclosure of electronic evidence. There is a strong emphasis on the enhancement of cooperation and disclosure of

electronic evidence. While cybercrime is proliferating and the complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions is increasing, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities leads to prosecutions or court decisions. The Protocol responds to this challenge and provides tools for enhanced cooperation and disclosure of electronic evidence — such as direct cooperation with service providers and registrars; effective means to obtain subscriber information and traffic data; immediate cooperation in emergencies or joint investigations — that are subject to a system of human rights and the rule of law, including data protection safeguards. This particular area and its implementation aspects were very extensively debated at the scientific and professional community fora, and that was certainly targeted through the negotiations in the drafting of the Second Additional Protocol (Bejatović et al., 2013). The results of the negotiations and the drafted protocol are to be summarized in the following. The Drafted Protocol provides Tools for the Second Additional Protocol. They can be summarized in the following: Direct requests to registrars in other jurisdictions to obtain domain name registration information; Direct cooperation with service providers in other jurisdictions to obtain subscriber information; More effective means to obtain subscriber information and traffic data through government-to-government cooperation; Expeditious cooperation in emergency situations; and Joint investigation teams and joint investigations and video conferencing. It is stipulated that a strong system of human rights and the rule of law safeguards will be developed, including the protection of personal data in the implementation of these tools. On November 17, 2021, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol. The Protocol provides a legal basis for disclosure of domain name registration information and for direct cooperation with service providers for subscriber information; effective means to obtain subscriber information and traffic data; immediate cooperation in emergencies; mutual assistance tools; and personal data protection safeguards. The preparatory work for the Second Protocol started in 2017. At the 17th plenary session of T-CI (June 8, 2017), the preparation of this Protocol was approved based on the proposal prepared by the T-CY Cloud Evidence Group. It was decided to start the drafting of this Protocol at the initiative of T-CY under Article 46, paragraph 1.c, of the Convention. On June 14, 2017, the Deputy Secretary General of the Council of Europe informed the Committee of Ministers (1289th meeting of the Ministers' Deputies) of this T-CY initiative. The terms of reference initially covered the

period from September 2017 to December 2019, and they were subsequently extended by the T-CY to December 2020 and again to May 2021. This was, of course, due to the COVID-19 pandemic problems, which hit all institutions worldwide. Under these terms of reference, the T-CY set up a Protocol Drafting Plenary (PDP) comprised of representatives of Convention Parties as well as States, organizations, and Council of Europe bodies with observer status in the T-CY. The PDP was assisted in the preparation of the draft protocol by a Protocol Drafting Group (PDG) consisting of experts from the Parties to the Convention. The PDG in turn set up several subgroups and ad hoc groups to work on specific provisions. From September 2017 to May 2021, the T-CY held 10 drafting plenaries, 16 drafting group meetings, and numerous group meetings. Most of this Protocol was prepared during the COVID-19 pandemic. Because of COVID-19-related restrictions, from March 2020 to May 2021, meetings were held in virtual format (more than 65). Such working methods in plenary, drafting groups, and groups (*sub* and *ad hoc*) enabled representatives and experts from Parties to make significant contributions to the drafting of this Protocol and develop innovative solutions. In this work, special significance is provided by the participation of the Commission of the European Union, which participated on behalf of the States Parties to the Convention that were members of the European Union under a negotiation mandate given by the Council of the European Union on June 6, 2019. Once draft provisions had been prepared and provisionally adopted by the PDP, the draft articles were published and stakeholders were invited to provide comments. The T-CY held six rounds of consultations with stakeholders from civil society and the private sector, and with data protection experts. The specialty of these consultations was that they were in conjunction with the Octopus Conference on cooperation against cybercrime in Strasbourg in July 2018; with data protection experts in Strasbourg in November 2018; via invitation for written comments on draft articles in February 2019; in conjunction with the Octopus Conference on cooperation against cybercrime in Strasbourg in November 2019; via invitation for written comments on further draft articles in December 2020; and in May 2021 via written submissions and a virtual meeting held on May 6, 2021. The T-CY furthermore consulted the European Committee on Crime Problems (CDPC) and the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe. The 24th plenary of the T-CY on May 28, 2021, approved the draft of this Protocol and decided to submit it to the Committee of Ministers in view of adoption.

CORE RESULTS AND SUBSTANTIVE NORMS

The starting point was T-CY's assessment of the Convention's mutual assistance provisions (CETS 185) and an analysis of the T-CY Transborder Group and Cloud Evidence Group (2014-2017), with the main issues arising from territorial and jurisdictional puzzles related to digital or electronic evidence. Concretely, specified data needed in a criminal investigation may be stored in multiple, shifting or unknown jurisdictions *(in the cloud),* and solutions are needed to obtain the disclosure of such data in an effective and efficient manner for the purpose of specific criminal investigations or proceedings. The drafters of this Protocol have agreed to focus on the following specific issues:

1. At the time of drafting this Protocol, mutual assistance requests were the primary method to obtain electronic evidence of a criminal offence from other states, including the mutual assistance tools of the Convention. However, mutual assistance is not always an efficient way to process an increasing number of requests for volatile electronic evidence. Therefore, it was considered necessary to develop a more streamlined mechanism for issuing orders or requests to service providers in other parties to produce subscriber information and traffic data.
2. Subscriber information – for example, to identify the user of a specific e-mail or social media account or of a specific Internet Protocol (IP) address used in the commission of an offence – is the most frequently sought information in domestic and international criminal investigations relating to cybercrime and other crimes involving electronic evidence. Without this information, it is often impossible to proceed with an investigation. Obtaining subscriber information through mutual assistance is, in most cases, not effective and overburdens the mutual assistance system. Subscriber information is normally held by service providers. While Article 18 of the Convention already addresses some aspects of obtaining subscriber information from service providers, including in other Parties, complementary tools were found to be necessary to obtain the disclosure of subscriber information directly from a service provider in another Party.[1] These tools would increase the efficiency of the process and also relieve pressure on the mutual assistance system.

[1] T-CY Guidance Note on Article 18.

3. Traffic data is frequently sought in criminal investigations, and their prompt disclosure may be required for tracing the source of communication as a starting point for gathering additional evidence or identifying a suspect.
4. Similarly, as many forms of crime online are facilitated by domains created or exploited for criminal purposes, it is necessary to identify the person who has registered such a domain. Such information is held by entities providing domain name registration services, that is, typically by registrars and registries. An efficient framework to obtain this information from relevant entities in other parties is therefore needed.
5. In an emergency situation where there is a significant and imminent risk to the life or safety of any natural person, rapid action is needed either by providing for emergency mutual assistance or making use of the points of contact for the 24/7 Network established under the Convention (Article 35).
6. In addition, proven international cooperation tools should be used more widely and among all parties. Important measures, such as video conferencing or joint investigation teams, are already available under treaties of the Council of Europe (for example, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No. 182), or other bilateral and multilateral agreements (Bejatović et al., 2013)[2]

However, such mechanisms are not universally available among the parties to the Convention, and this Protocol aims to fill that gap The Convention provides for the collection and exchange of information and evidence for specific criminal investigations or proceedings. The drafters recognized that the establishment, implementation, and application of powers and procedures related to criminal investigations and prosecutions must always be subject to conditions and safeguards that ensure adequate protection of human rights and fundamental freedoms. It was necessary, therefore, to include an article on conditions and safeguards, similar to Article 15 of the Convention. Furthermore, recognizing the requirement for many parties to protect privacy and personal data in order to meet their constitutional and international obligations, the drafters decided to provide for specific data protection safeguards in this Protocol. Such data protection

[2] Serbia signed it on July 4, 2005, and ratified it on April 26, 2007, so the instrument entered into force on August 1, 2007.

safeguards complement the obligations of many of the Parties to the Convention, which are also Parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)[3]. The amending protocol to that convention (CETS No. 223) was opened for signature during the drafting of this Protocol in October 2018.[4] It should also be noted that the drafting process of this Protocol included parties not subject, at the time, to Council of Europe instruments on data protection or to European Union data protection rules. Accordingly, significant efforts were undertaken to ensure a balanced Protocol reflective of the many legal systems of states likely to be parties to this Protocol while respecting the importance of ensuring the protection of privacy and personal data as required by the constitutions and international obligations of other parties to the Convention. Of interest here is also to include the presentation of some measures which were not included in the Protocol. The drafters also considered other measures which, after thorough discussion, were not retained in this Protocol. Two of these provisions, namely, "undercover investigations by means of a computer system" and "extension of searches", were of high interest to the parties but were found to require additional work, time, and consultations with stakeholders, and were thus not considered feasible within the time frame set for the preparation of this Protocol. The drafters proposed that these be pursued in a different format and possibly in a separate legal instrument. This is of particular value for the planning of future procedural coverage by national criminal procedural legislative initiatives. The provisions of this Protocol would add value both from an operational and from a policy perspective to all law enforcement agencies. This Protocol should significantly improve the ability of the parties to enhance cooperation among the parties and between parties and service providers and other entities, and to obtain the disclosure of electronic evidence for the purpose of specific criminal investigations or proceedings. Thus, this Protocol, like the Convention, aims to increase the ability of law-enforcement authorities to counter cyber and other crimes while fully respecting human rights and fundamental freedoms, and it emphasizes the importance and value of an internet built on the free flow of information. The protocol directly aims at furthering and enhancing cooperation on cybercrime and the abilities of law enforcement agencies in finding and

[3] Serbia signed the same on September 6, 2005, ratified it on September 6, 2005, so the instrument entered into force on January 1, 2006.

[4] Serbia signed the same on November 22, 2019, and ratified it on May 26, 2020.

collecting and sharing electronic evidence; providing additional tools in this matter and mutual legal and other assistance and other forms of cooperation between competent authorities; cooperation in emergencies (that is, in situations where there is a significant and imminent risk to the life or safety of any natural person); and direct cooperation between competent authorities and service providers and other entities in possession or control of pertinent information.

PROVISIONS

Continuing the solutions prescribed by the Convention and the First Additional Protocol, the Second Additional Protocol has foreseen some new solutions, the implementation of which could improve the situation in the fight against cybercrime. The Protocol is divided into four chapters: I. "Common provisions"; II. "Measures for enhanced cooperation"; III. "Conditions and safeguards"; and IV. "Final provisions". Chapter I of this Protocol relates to specific criminal investigations or proceedings, not only with respect to cybercrime but any criminal offence involving evidence in electronic form, also commonly referred to as "electronic evidence" or "digital evidence". This chapter also makes definitions of the Convention applicable to this Protocol and contains additional definitions of terms used frequently in this Protocol. Moreover, considering that language requirements for mutual assistance and other forms of cooperation often hinder the efficiency of procedures, an article on "language" was added to permit a more pragmatic approach in this respect. The scope of the application is defined by the area of either where the crime is committed by the use of a computer system, or where a crime not committed by the use of a computer system (for example, a murder) involves electronic evidence, the powers, procedures, and cooperation measures created by this Protocol are intended to be available. Also, it is applicable to the criminal offences established pursuant to the First Protocol. It should be envisaged that each party is required to have a legal basis to carry out the obligations set out in this Protocol if its treaties, laws, or arrangements do not already contain such provisions. This does not change explicitly discretionary provisions into mandatory ones, and some provisions permit declarations or reservations. Some of the definitions are reused from the Convention and First Protocol, but some are genuine for this protocol – like "central or competent authority" or "emergency". For instance, the very important definition of the latter "covers situations in which the risk is significant and imminent, meaning that it does not include situations in which the risk to the life or

safety of the person has already passed or is insignificant, or in which there may be a future risk that is not imminent". The reason for these significance and imminence requirements is that Articles 9 and 10 place labor-intensive obligations on both the requested and requesting parties to react in a greatly accelerated manner in emergencies, which consequently requires that emergency requests be given a higher priority than other important but somewhat less urgent cases, even if they had been submitted earlier. Situations involving "a significant and imminent risk to the life or safety of any natural person" may involve, for example, hostage situations in which there is a credible risk of imminent loss of life, serious injury or other comparable harm to the victim; ongoing sexual abuse of a child; immediate post-terrorist attack scenarios in which authorities seek to determine with whom the attackers communicated in order to determine if further attacks are imminent; and threats to the security of critical infrastructure in which there is a significant and imminent risk to the life or safety of a natural person" (Explanatory Report to the Additional Protocol to the Convention on Cybercrime, 2003, January 28, p. 7; Ivanović et al., 2015b; 2020a). An interesting solution in the Additional Protocol refers to the possibility of using English or other so-called acceptable languages such as Spanish or French. Thus, for requests in a language other than the language prescribed in domestic law or in contracts, there is a possibility of using it. But T-CY, once a year, will engage in an informal survey of acceptable languages for requests and orders. They may state that they accept only specified languages for certain forms of assistance. The results of this survey will be visible to all parties to the Convention, not merely parties to this Protocol. Chapter II contains the primary substantive articles of this Protocol, which describe various methods of co-operation available to the parties. Different principles apply to each type of cooperation. For this reason, it was necessary to divide this chapter into sections with (1) general principles applicable to Chapter II; (2) procedures enhancing direct cooperation with providers and entities in other parties; (3) procedures enhancing international cooperation between authorities for the disclosure of stored computer data; (4) procedures pertaining to emergency mutual assistance; and (5) procedures pertaining to international cooperation in the absence of applicable international agreements. Paragraphs 2-5 introduce seven cooperation measures. These sections are divided by the types of cooperation sought: Section 2 covers direct cooperation with private entities (Article 6, "Request for domain name registration information", and Article 7, "Disclosure of subscriber information"), which allows competent authorities of a party to engage directly with private entities, and it applies whether or not there is

a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force; Section 3 contains forms of enhanced international cooperation between authorities for the disclosure of stored data; Article 8, entitled "Giving effect to orders from another party for expedited production of subscriber information and traffic data", and Article 9, entitled "Expedited disclosure of stored computer data in an emergency". It provides for cooperation between competent authorities, but of a different nature than traditional international cooperation, and it applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested parties; Section 4 provides for mutual assistance in an emergency; there are two possibilities. When the parties concerned are mutually bound by an applicable mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, section 4 is supplemented by the provisions of that agreement unless the parties concerned mutually determine to apply certain provisions of the Convention in lieu thereof (see Article 10, paragraph 8, of this Protocol).When the parties concerned are not mutually bound by such an agreement or arrangement, the parties apply certain procedures set out in Articles 27 and 28 of the Convention, concerning mutual assistance in the absence of a treaty (see Article 10, paragraph 7, of this Protocol) and Section 5 concludes with international cooperation provisions to be applied in the absence of a treaty or arrangement on the basis of uniform or reciprocal legislation between the parties concerned. These sections are also organized roughly in a progression from the forms of investigatory assistance often sought early in an investigation – to obtain the disclosure of domain name registration and subscriber information – to requests for traffic data and then content data, followed by video conferencing and joint investigative teams, which are forms of assistance that are often sought in the later stages of an investigation. Article 11, entitled "Video conferencing", and Article 12, entitled "Joint investigation teams and joint investigations". These provisions are measures of international cooperation, which apply only where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested parties. These measures do not apply where such a treaty or arrangement exists, except that Article 12, paragraph 7, applies whether or not such a treaty or arrangement exists. However, the parties concerned may mutually determine to apply the provisions of Section 5 in lieu of such an existing treaty or arrangement unless this would be prohibited by the terms of the treaty or arrangement. Chapter III provides for conditions and

safeguards. They require that parties apply conditions and safeguards similar to Article 15 of the Convention also to the powers and procedures of this Protocol. In addition, this chapter includes a detailed set of safeguards for the protection of personal data. Most of the final provisions of Chapter IV are similar to standard final provisions of the Council of Europe treaties or make provisions of the Convention applicable to this Protocol. However, Article 15 on "Effects of this Protocol", Article 17 on the "Federal clause" and Article 23 on the "Consultations of the Parties and assessment of implementation" differ in varying degrees from analogous provisions of the Convention. This last article not only makes Article 46 of the Convention applicable but also provides that the effective use and implementation of the provisions of this Protocol shall be periodically assessed by the parties.

CONCLUSIONS

It is not only that the Second Protocol is a logical and natural furthering of the Convention and the First Additional Protocol related to cybercrime, but it represents a very significant step in fortifying the structures of international combat against wider organized criminal and transnational (transnational or transborder organized crime) activities. In this very vivid and dynamic world, there is a need to have forums and international wisdom focused on specific areas of life, primarily in the cyber area. The difference in the evolution of state actors of different states in this area defines discrepancies in the levels of capabilities to resist such threats from various actors. In that sense, it is very important to have one or more centers where they would serve as intelligence and strategic hubs in the development of different levels reached by parties. The Council of Europe (CoE) is serving as one, with the respectable exclusion of the Russian Federation. In this way, the members of the CoE will have a standardized approach with respect to their sovereignties and their local and national demands in the area, but with respect for majority trends, mainstream activities, and development in the cyber area. As previously stated, the Second Additional Protocol to the Cybercrime Convention represents the normal and natural development of the norms stipulated in it, as well as the further evolution of respectable measures. It provides parties with much more qualitative solutions in the area that needs international rules in communication and realization of measures provided by the international conventions, and also ensures that all interests are taken into account and that no country or party (or their citizens) is discriminated against in the implementation of the measures. This protocol is a must for our country

since there were different problems in implementing previously designed measures in international cooperation, of which some were even nationally related. Implementation of this protocol will certainly ease procedural measures in law enforcement and will provide quick reactions to incidents and cybercrime activities, very much needed by all parties to the Convention. This will also result in quicker detection of criminal activities and criminals in the area and their bringing to justice, as well as lowering the dark figure of victims reporting the crime. Ultimately, it will take its tow on cybercrime in general, so as soon as we sign and ratify this protocol after June 2022, it will be better. Of course, it needs to be implemented fully as stipulated, and for that, we need to wait and see.

REFERENCES

Bejatović, S. Škulić, M. Ilić, G. (eds). (2013). *Manual for the implementation of the new CPC*. Belgrade, Fiduciary OSCE Mission to Serbia.

Council of Europe. (2001, November 23). Convention on Cybercrime. *ETS* (185).

Council of Europe. (2022). *Detail of Treaty No. 185.* Retreived from: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. Accessed 1.2.2022.

Explanatory Report to the Additional Protocol to the Convention on Cybercrime. (2003, January 28). Report concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, *ETS* (189). Retrieved from: Internet: https://rm.coe.int/16800d37ae. Accessed. 09.01.2022.

Gerke, M. Djokic, D. Radulović, S. Petrović Z. Lazović, V. Dust, R. (2008). *Manual for investigation of crimes inthe area of cybercrime.* Council of Europe.

Ivanović, Z., Urosević, V. (2010). The role of Serbia in the international fight against high technology crime, in: *Role and place of the Republic of Serbia and international organizations,* Institute of International Politics and Economics, Belgrade.

Ivanović, Z., Lajić, O. (2012a). Uporednopravna analiza mera suprotstavljanja visokotehnološkom kriminalu, *Kultura polisa,* 9(1).

Ivanović, Z. (2012b). Harmonization of the laws of the Republic of Serbia with the EU law, analysis of harmonization of regulations in the field of VTK, IMPP, IUP, HSS Belgrade.

Ivanović, Z., Banutai, E. (2012, October 8-9). Cyber crime cooperation in see through the view of PCC SEE and Cybercrime@IPA SEE 2012, Str. 52-65, in: *Improvement of relations between Serbia and Southeast European states*, Belgrade.

Ivanović, Z., Čvorović, D. (2012, May 18-19). Srpski paradoks presretanja komunikacija, u: *Zloupotreba informacionih tehnologija i zaštita* (ZITEH-12), Beograd.

Ivanović, Z. (2015a). Pitanje postupanja sa digitalnim dokazima u srpskom zakonodavstvu- *Kriminalistička teorija i praksa*.

Ivanović, Z., Živković, T. (2015b). *SM Megraf: Issue of state agencies jurisdictions in the cybercrime area in the Republic of Serbia*. Им. ГА Крестова Российской Академии наук (ИХР-РАН)/GA Krestov Institute of Solution Chemistry of Russian Academy of Sciences (ISC-RAS).

Ivanović, Z., Žarković, M., Žarković, I. (2016). Public Video Surveillance: A Puzzling Issue for Serbian Lawmakers. Varstvoslovje, *Journal of Criminal Justice & Securit*y.

Ivanović, Z., Banović, B. (2020a). Sexual exploitation of minors/analysis in Serbian law enforcement practice, *Culture of Polis - Journal for Nurturing of Democratic Political Culture* 17 (42).

Ivanović, Z., Lajić, O. (2020b). Search and seizure of devices in relation to the automatic procession of data, *Culture of polis Journal for Nurturing of Democratic Political Culture,* 17 (41).

Ivanović, Z., Dragović, R, Ulyanov, S. (2021). The role of regonal organization in combating cybercrime and the Western Balkans and the Western Balkans: from stabilization to integration, in: Miroslav Antevski, Dragana Mitrović (eds). Belgrade, Institute for International Politics and Economics.