International Regulations of Cybersecurity

Filip Radoniewicz

Abstract There is no doubt that, due to the global nature of modern ICT networks, international cooperation plays a key role in ensuring cybersecurity, including in the fight against cybercrime.

This chapter describes initiatives taken within international organizations to ensure cybersecurity and the prevention of cybercrime. The presentation will start with the initiatives of the OECD and the Council of Europe. This is due not only to some kind of “Eurocentrism” but above all to the fact that these two organisations were the first to address cybersecurity and cybercrime issues. In addition, the Council of Europe Convention 185 on CyberCrime of November the 23rd, 2001, an international agreement concluded in the Council of Europe, is a milestone in the prevention of computer crime, remaining the only binding act of international law to combat it. Its importance is best demonstrated by the constantly growing number of signatories (and countries that model without signatures after the provisions, e.g. Pakistan) and the fact that international organisations, or recommend that their members accept (UN, G7/G8, European Union) or “copy” provisions, creating their own model legal acts (e.g. Commonwealth).

1 General Remarks

Given the global character of modern tele-information systems, international cooperation undoubtedly plays an instrumental role in ensuring cybersecurity and combating cybercrime. Therefore, efforts to establish legal frameworks of the interstate cooperation aimed at ensuring computer data and information system security have been made on the international arena since tele-information became supranational. It should be stressed that, for any cybersecurity-oriented measures to be effective,

F. Radoniewicz (✉)

Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: filip.radoniewicz@radoniewicz.eu

© The Author(s) 2022

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_5

international cooperation must be pursued not only at the national level, but it must also involve private entities, representatives of the IT industry, and including in particular Internet service providers.

Initiatives launched by international organisations to ensure cybersecurity and to combat cybercrime are outlined below, starting with those devised by OECD and the Council of Europe. This line of presentation was motivated not only by the Euro-centric approach, but also by the fact that these two organizations had been the first to deal with cybersecurity and cybercrime issues. Furthermore, Convention on Cybercrime No. 185 of the Council of Europe of the 23rd of November 2001,¹ being an international treaty drawn up within the Council of Europe, was a milestone in the field of combating computer crime. It has also served a binding international legal act adopted with this objective in mind. Its importance is best reflected in the still growing number of signatories (as well as non-signatories, which otherwise commit to follow its provisions, e.g. Pakistan) and in the fact that international organizations either recommend their members to adopt the Convention (the UN, G7/G8, the European Union) or “map” its content when drawing up their own governing agreements (e.g. The Commonwealth of Nations).²

2 Organisation for Economic-Cooperation and Development

Recommendation C (92)188³ was the first document on cybercrime within the Organisation for Economic-Cooperation and Development (French: *Organisation de coopération et de développement économiques*, abbreviated as OECD), adopted on the 26th of November 1992 by the OECD Council. In 2000, following its revision, it was deemed indispensable to draw up entirely new guidelines.⁴ Work that was launched to this end took on momentum after 9/11, and eventually resulted in the formulation of the Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security,⁵ which replaced Recommendation C(92)188. For nearly 13 years, it was the landmark OECD legal act dealing with widely understood computer network security. It drew attention to the increasing role of, and the fact that national economies, international trade, as well as social, cultural and political life are becoming

¹<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>, Accessed on 1 September 2020.

²Cf. Chałubińska-Jentkiewicz (2019), pp. 261–262.

³Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 (C(92)188/FINAL).

⁴Gercke (2011), Accessed on 1 September 2020.

⁵Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security of 25 July 2002, (C (2002) 131).

increasingly dependent on information systems and networks, which should prompt efforts to protect and foster confidence in such systems and networks. At the same time, as was also stressed in the Recommendation, information systems and networks, as well as data stored on, or transmitted over, such systems and networks, are subject to new and increasing threats (various types of unauthorized access, use or alteration, malicious code transmissions, and mass denial-of-service attacks affecting a significant number of computers and paralyzing tele-information systems). In consequence, governments of Member States were advised, in particular, to develop new or revise existing policies, practices, measures and procedures based on the Guidelines attached to Recommendation C(2002)131, and at the same time to promote a culture of security as set out in these Guidelines among all concerned parties (which are understood as including all entities which develop, own and use information systems and networks, and which provide related services, i.e. governments, enterprises, other organizations and individual users). Given the technological progress, work to revise the Guidelines commenced in 2012 and resulted in adopting, on the 17th of September 2015, the Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity (C(2015)115).⁶ It was stressed in the Recommendation that the global interconnectedness has created considerable opportunities, but the risks emerging throughout its development are becoming more common and refined, and may affect the functioning of both the public and private sectors. The problem should, therefore, be now approached from a bigger perspective, one that is not limited to technological aspects. For this reason, the terms “cybersecurity” and “cyberspace” were abandoned in the Recommendation, and broader terms, “digital security risk” and “digital environment”, were used instead. The Recommendation clearly stated that governments and private enterprises should share responsibility for combating digital security risks. It laid down the principles of digital security risk management to be followed by all concerned parties (governments, public and private organizations, as well as natural persons whose social or economic activities are pursued, whether in whole or in part, in the digital environment), along with guidelines for national strategies to ensure digital security, the implementation of which should be advocated by governments. These strategies are expected to present a clear and ‘whole-of-government’ approach, which should be flexible, technology-neutral and coherent with other strategies fostering economic and social prosperity. It should also cover best practices for the public sector, large, medium-sized and small enterprises, and individual citizens.⁷

Among other OECD guidelines related to widely understood information technologies, the following are worth noting:

⁶Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity of 17 September 2015 (C(2015)115).

⁷See more in Radoniewicz (2016), pp. 152–156.

1. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of the 23rd of September 1980 (C(80)58)⁸ (still in force but revised in 2013), which was the first set of principles established at the international level, which countries should be guided by when developing regulations on the protection of privacy in connection with cross-border flows of personal data;
2. Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of the 12th of December 2007 (C(2007)67)⁹ (revised in 2013), including proposals of measures to be taken with a view to streamlining international co-operation in the field of privacy protection in connection with cross-border flows of personal data;
3. Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam of the 13th of April 2006;¹⁰
4. Recommendation of the Council on Protection of Critical Information Infrastructures of the 30th of April 2008 (C(2008)35)¹¹ containing guidelines for countries on ensuring the protection of critical information infrastructures (CIIs) at the national and international level.¹²

To sum up OECD's activities in the field of regulations on new technologies, it should be stressed that, although the Organization was first to implement measures aimed at combating cybercrime, its major interest is now limited to cybersecurity.¹³

3 Council of Europe

A discussion on the Council of Europe activities in the field of cybersecurity and combating cybercrime should start with Recommendation No. R(89)9 on Computer-Related Crime, adopted by the Committee of Ministers of the Council of Europe on the 13th of September 1989.¹⁴ The document required Member States to take into account, in the course of legislative work on regulations directed at eliminating computer crime, the proposed solutions included in the report attached to it.¹⁵

⁸Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 (C(80)58(final)).

⁹Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of 12 December 2007 (C (2007) 67 (final)).

¹⁰Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam of 13 April 2006 (C(2006) 57).

¹¹Recommendation of the Council on Protection of Critical Information Infrastructures of 30 April 2008 (C(2008)35).

¹²See more Radoniewicz (2019).

¹³S. Schjøberg, *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, <http://www.cybercrimelaw.net>, accessed on 10 October 2020, p. 17.

¹⁴Recommendation No. R(89)9 on Computer-Related Crime.

¹⁵See more in Radoniewicz (2016), pp. 158–160.

The aforementioned Convention on Cybercrime was the first, and only, international treaty on crimes committed via the Internet and other computer networks.

Work on the Convention, which took over 4 years to complete, was carried out with the participation of not only representatives of most Member States of the Council of Europe (including Poland) but also by U.S., Japanese and Canadian delegates (as observers), representatives of European institutions, and independent experts. Its main objective was to develop a legal framework to facilitate international crime prosecution. It proposed a range of solutions, which were innovative (at least at that time, given that the Convention was drawn up at the end of the previous century). Compared to some earlier documents adopted at the international level, it featured an extended list of criminal offences (including illegal access, illegal interception, system interference, acts involving hacking tools, computer-related forgery, computer-related fraud, offences related to child pornography,¹⁶ and offences related to infringements of copyright and related rights). Furthermore, it contained provisions on recognizing criminal liability depending on the stage of commitment, as well as aiding and abetting, and provisions on corporate liability (including also the liability of organizations without a legal personality). Several procedural solutions were also envisaged, including the preservation of data, search and seizure of stored computer data, real-time collection of traffic data, and the like.¹⁷

The obvious advantages of the Convention on Cybercrime include its open character, with countries not belonging to the Council of Europe being allowed to accede, and the fact that it contains optional clauses. The latter enable the Convention to be adopted with the exclusion of certain provisions, as a result of which on implementing the Convention the signatory countries, within their national laws, can reconcile the solutions it envisages with their own legal culture and tradition, and with the regulations already in force within their respective jurisdictions.¹⁸ Considering the above, by the first of January 2021, the Convention on Cybercrime had been signed by almost all Council of Europe Member States (more specifically, by 46 countries, with Russia being the only exception), and 44 of these had ratified it. Furthermore, the Convention was signed by 4 countries from outside Europe (Canada, Japan, the United States, and the Republic of South Africa, and the first three have already ratified it). Other 18 states (i.e., Australia, the Dominican Republic, Israel, Panama) acceded to it. It is also worth noting that several countries, including Egypt and Pakistan, while not signing the Convention on Cybercrime, used its provisions as a basis when developing their own domestic regulations.

¹⁶The Convention on Cybercrime only refers to one group in this category—offences related to child pornography. Initially, it was meant to additionally include offences driven by racism or xenophobia. Eventually, these were included in a separate Additional Protocol to the Convention on Cybercrime regarding the criminalisation of acts of a racist and xenophobic nature committed through computer systems of 28 January 2003. See further comments.

¹⁷Cf. Adamski (2001), pp. 9–11; Radoniewicz (2016), pp. 162–164; Tarnogórski (2009), pp. 207–210.

¹⁸Cf. Adamski (2001), pp. 9–17.

The Convention on Cybercrime entered into force on 1 July 2004 after it had already been ratified by five signatory countries. Although Poland was one of the first countries to sign the Convention (on 23 November 2001), it did not ratify its provisions until the 29th of January 2015. To date, two amendments have been made to the Criminal Code with a view to adjusting its content to the provisions of the Convention.¹⁹

The aforementioned Additional Protocol of 28 January 2003 to the Convention on Cybercrime²⁰ regarding the penalisation of offences motivated by racism or xenophobia, committed using computer systems (hereinafter the Protocol),²¹ is the only binding international law act developed within the Council of Europe which deals with the issues of crimes motivated by racism or xenophobia.

The fact that the provisions on crimes motivated by racism and xenophobia were included in a separate protocol, and not in the Convention on Cybercrime, resulted from the dissenting views expressed by delegates of the countries involved in its creation. Differences in the constitutional standards of free speech in individual countries substantially hindered a common standpoint. As a result, in order not to delay work on the Convention, it was decided that the provisions regarding such matters be included in a separate act.²²

1. Distributing, or otherwise making available, racist and xenophobic material to the public through a computer system (Article 3);
2. Threatening (persons or groups of persons) with the commission, through a computer system, of a serious criminal offence as defined under its domestic law, motivated by racism or xenophobia (Article 4);
3. Insulting publicly, through a computer system, persons or groups of persons, based on racist or xenophobic motives (Article 5);
4. Distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Court, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that party (e.g. the International Criminal Tribunals for the former Yugoslavia or Rwanda, or the International Criminal Court in Hague)—Article 6.

¹⁹ Act of 18 March 2004 on amending the Criminal Code, the Code of Criminal Proceedings and the Code of Offences, Polish Journal of Laws No. 69, item 626 and the Act of 24 October 2008 on amending the Criminal Code and certain other acts, Polish Journal of Laws No. 214, item 1344.

²⁰ Convention on Cybercrime of the Council of Europe of 23 November 2001 (<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> Accessed on 1 September 2020).

²¹ Protocol of 28 January 2003 to the Convention on Cybercrime <https://rm.coe.int/168008160f>, accessed 1.12.2020.

²² Adamski (2001), p. 49.

The Protocol entered into force on 1 March 2006. In accordance with its Article 9 (1), it is open for signature by the states which have signed the Convention, which implies that it is also open to countries which are not members of the Council of Europe, both from Europe and outside of it. Such countries can accede to the Convention on Cybercrime provided that they participated in work on its development (as did the United States, Canada and Japan), or once they are invited to the Committee of Ministers or have obtained the consent from all the signatories.

Among other documents adopted by the Council of Europe, the subject-matter in question was also indirectly discussed in the following:

1. Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, done at Strasbourg on 28 January 1981;²³
2. Convention No. 201 on the Protection of Children against Sexual Exploitation and Sexual Abuse, on 25 October 2007;²⁴
3. Recommendation CM/R(99) 5 on the protection of privacy on the Internet of the 23rd of February 1999;²⁵
4. Recommendation CM/R(2009)1 electronic democracy (e-democracy) of the 18th of February 2009;²⁶
5. Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries.

4 Organisation for Security and co-Operation in Europe

Security of the data processed in computer systems has not formed the area of interest of the Organisation for Security and Co-operation in Europe (OSCE). However, this does not mean that cybersecurity issues are entirely neglected in OSCE activities. Examples testifying to the contrary include four decisions by the Committee of Ministers: two on combating the use of the Internet for terrorist purposes,²⁷ in which it was indicated that the use of the Internet by terrorist groups for such purposes as member recruitment, collection and transfer of funds, organisation of terrorist acts or propaganda, must be prevented. However, this must be

²³Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, done at Strasbourg on 28 January 1981 (<https://www.coe.int/en/web/data-protection/convention108-and-protocol>, accessed on 1.12.2020).

²⁴Convention No. 201 on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007 (<https://rm.coe.int/1680084822> accessed on 1.12.2020).

²⁵Recommendation CM/R(99)5 on the protection of privacy on the Internet of 23 February 1999 Recommendation Rec (99)5 on the Protection of Privacy on the Internet.

²⁶Recommendation CM/R(2009)1 electronic democracy (e-democracy) of 18 February 2009 Recommendation CM/Rec(2009)1 on Electronic Democracy (e-Democracy).

²⁷Ministerial Council Decision of 7 December 2004 No. 3/04 on combating the use of the Internet for terrorist purposes and Ministerial Council Decision of 7 December 2006 No. 7/06 on combating the use of the Internet for terrorist purposes.

done in observance of human rights, and in particular the right to privacy and the freedom of expression of opinions and views. This objective is to be facilitated by information exchange between the concerned parties and by establishing strategies for effectively combating this phenomenon. The other two decisions concern enhancing OSCE efforts to reduce the risks of conflict stemming from the use of information and communication technologies.²⁸

5 United Nations

First and foremost, it is worth noting that the United Nations initially attached importance mainly to preventing computer crime by referring to theoretical considerations and empirical studies conducted by criminologists in this field. In recent years, this approach has been changing gradually, as reflected in the so-called Salvador Declaration (see further comments).

Special attention to cybersecurity issues on the UN forum was paid for the first time at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held from 27 August to 7 September 1990 in Havana (such congresses regarding the prevention of crime are organised by the UN every 5 years, recently—i.e. since the Congress in Bangkok in 2005—as Congresses on Crime Prevention and Criminal Justice), and at the Symposium on the Prevention and Prosecution of Computer Crime, organised by the Foundation for Responsible Computing, which was an event accompanying the Congress. The discussions held at the Congress led to the General Assembly of the United Nations adopting, on the 14th of December 1990 at the initiative of Canadian representatives, Resolution 45/121 on Combating the Criminal misuse of Information Technologies.²⁹

As proposed by Hubbard and S. Schjøberg,³⁰ the subsequent resolutions adopted by the General Assembly of the United Nations can be divided into the following groups:

1. Resolutions 53/70 of 3 December 1998, 54/49 of 1 December 1999, 55/28 of the 20th of November 2000, 56/19 of the 29th of November 2001, 57/53 of the 22nd of November 2002, 58/32 of the 18th of December 2003, 59/61 of the 3rd of December 2004, 60/45 of the 8th of December 2005, 61/54 of the 6th of December 2006, 62/17 of the 5th of December 2007, 63/37 of the 2nd of

²⁸Decision No. 5/16 of 9 December 2016 on enhancing OSCE efforts to reduce the risks of conflict stemming from the use of information and communication technologies and Decision No. 5/17 of 8 December 2016 on enhancing OSCE efforts to reduce the risks of conflict stemming from the use of information and communication technologies.

²⁹Cf. Adamski (2000), pp. 9–10; Sieber (1998), pp. 162–163.

³⁰A.M. Hubbard, S. Schjøberg, *Harmonizing national legal approaches on cybercrime*, http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf, p. 6; accessed on 10.10.2020.

December 2008, 64/25 of the 2nd of December 2009, 65/41 of the 8th of December 2010, 66/24 of the 2nd of December 2011, 67/27 of the 3rd of December 2012, 68/243 of the 27th of December 2013, 69/28 of the 2nd of December 2014, 70/237 of the 23rd of December 2015, 71/28 of the 5th of December 2016, 73/27 of the 5th of December 2018, of 73/266 of the 22nd of December 2018, 74/28 of the 12th of December 2019, and 74/29 of the 12th of December 2019—all referred to as *Developments in the Field of Information and Telecommunications in the Context of International Security*, which contain rather general provisions, indicating the threats which may be posed by advancing IT, and recommending that countries adopt the guidelines periodically formulated in the information security reports drawn up by the Group of Government Experts on Information Security;

2. Resolutions 55/63 of the 4th of December 2000 and 56/121 of the 19th of December 2001 (both referred to as *Combating the Criminal Misuse of Information Technology*), in which more specific measures were indicated which should be taken at the international level, and implemented in national legal systems, with the aim of effectively preventing cybercrime. According to their authors, it was seen as indispensable to establish such legal regulations that would guarantee the protection of all aspects of computer data and system security (i.e. confidentiality, integrity and accessibility) from unauthorised impairment, and to ensure that criminal abuse is penalized in all countries. The need to take measures facilitating the cooperation between law enforcement authorities in the prosecution and penalization of perpetrators of computer misuse acts was also highlighted.
3. Resolutions 57/239 of the 20th of December 2002 (*Creation of a global culture of cybersecurity*), 58/199 of the 23rd of December 2003 (*Creation of a global culture of cybersecurity and the protection of critical information infrastructures*) and 64/211 of the 21st of December 2009 (*Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*), which all focused on the need to guarantee an increased security of computer systems and data processed in such systems. Resolution 57/239 focused mainly on the consequences of the interdependence between computer infrastructure and other sectors of the global infrastructures critical for public administration, while Resolution 64/211 encouraged Member States and international organizations, when developing strategies related to cybersecurity and the protection of critical infrastructures, to share their experience with other countries. In addition, the annex to the resolution featured guidelines intended to facilitate the creation of an effective system to ensure cybersecurity.³¹

At the aforementioned Eighth United Nations Congress, taking place in Havana in 1990, Resolution 45/121 on Combating the Criminal Misuse of Information Technologies was developed, together with the United Nations Manual on the

³¹Radoniewicz (2016), pp. 196–200.

Prevention and Control of Computer-Related Crime, which was published in 1994. In the declaration issued at the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders in Vienna,³² which was annexed to Resolution 55/59 of the General Assembly of 4 December 2000, computer crime was referred to in a very general manner (in Point 18 which dealt, *inter alia*, with the planned policy for issuing guidelines on the prevention of this phenomenon). In the declaration entitled *Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice*, annexed to Resolution 60/177 of the General Assembly of 16 December 2005 “Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice”,³³ ending the Eleventh Congress in Bangkok, attention was again paid to the significance of criminal law harmonisation, as a factor indispensable for the efficient fight with cybersecurity, and the instrumental roles of both by the UN and other international organisations were highlighted. In the so-called *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*, adopted at the Twelfth United Nations Congress in Salvador (12–19 April 2010), as the document concluding the event (annexed to Resolution 65/230 of the General Assembly of 21 December 2010), a recommendation was made for the UN Commission on Crime Prevention and Criminal Justice (CCPCJ), in cooperation with Member States, representatives of international communities and private sector entities, to develop draft versions of new solutions, both at the national and international levels, in response to the threat posed by cybercrime. At the Thirteenth United Nations Congress, which took place on 11–19 April 2015 in Doha (Al-Dauha), Qatar, attention was focused on the issue of integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges, and to promote the rule of law both at the national and international levels, also by involving society at large. As regards cybersecurity issues, the Congress participants once again stressed the need to take specific measures to establish a secure cyberspace. As regards preventing and combating Internet crime, emphasis was placed on such issues as identity theft, botnets, online recruitment for terrorist and human trafficking purposes, and the need to protect children. Furthermore, the significance of enhancing international cooperation as a condition precedent to ensuring cyberspace security was also stressed. The Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation,³⁴

³²The Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century); <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/562/93/PDF/N0056293.pdf?OpenElement>, accessed on 1 December 2020).

³³Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice; <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/498/22/PDF/N0549822.pdf?OpenElement>, Accessed on 1 December 2020).

³⁴The Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of

the provisions of which were adopted by acclamation on the first day of the Congress, was the concluding document of the Thirteenth United Nations Congress. It summarised the 60-year achievements of the UN congresses and activities in the field of preventing crime. It also marked an attempt at responding to contemporary challenges emerging in this respect. With a view to implementing the objectives envisaged in the Doha Declaration, the United Nations Office on Drugs and Crime, using Qatar's financial support, launched an ambitious programme with global coverage, aimed at supporting countries in crime prevention efforts, developing criminal justice, preventing corruption and promoting the rule of law. Next congress was scheduled on 20–27 April 2020, and was to take place in Kyoto (a city which hosted the Fourth United Nations Congress in 1970). However, due to the COVID-19 pandemic, it had to be rescheduled.

It is common knowledge that the speed of action is of utmost important in conducting criminal proceedings on cybercrime, considering that digital evidence is non-permanent (“perishable”). To accelerate and facilitate information exchange, *inter alia*, by more intensive cooperation with the private sector, a joint initiative has been launched by the Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Office on Drugs and Crime (UNODC), and the International Association of Prosecutors—Lawful Access to Digital Data Across Borders.

The UN Security Council also implements activities in the field of cybersecurity and fight against cybercrime. In Resolution 1373 (2001) of 27 September 2001, it called Member States to intensify the exchange of information on the ICT use by terrorist groups, and to block any terrorist recruitment attempts via the Internet. In Resolution 2129 (2013) of 17 September 2013, it stressed that the Internet and social media were increasingly used for facilitating various terrorist acts, including communication, abetting, recruitment, training, preparations, planning, financing, and information collection.

Recognising the need to engage the private sector in combating organised crime and terrorism, CTED has launched the Tech Against Terrorism initiative, its objective being to encourage private sector entities to take measures aimed at self-regulation and at counteracting the use of their platforms by terrorist groups.

In addition, Security Council Resolutions 2341 (2013) of 13 February 2017 imposed on CTED the obligation to verify Member States' efforts to protect critical infrastructures against terrorist attacks, and to identify threats and future challenges likely to emerge in this field.

6 The International Telecommunication Union

The International Telecommunication Union (ITU), with its seat in Geneva, is a United Nations specialised agency which is currently the most dynamically operating body in the field of ensuring cyberspace security by harmonising the legal orders in various countries, and by establishing international regulations. The ITU duties include standardising and regulating the telecommunications market, promoting international cooperation in the field of telecommunication, providing technical assistance to developing countries, and taking measures aimed at establishing a global telecommunication network combining multiple technologies.³⁵ The Plenipotentiary Conference composed of representatives of the ITU Member States is the chief political body of the Union. The Conference gathers every 4 years and sets the principal directions of the ITU policy, as well as elects members of the Council and defines the organisation's financial plans. The Council is entrusted with supervising the ongoing policies, strategies and activities of the Union in the periods between the consecutive Plenipotentiary Conferences. The General Secretary elected for a four-year term of office manages the General Secretariat, which is an office dealing with ITU resource and activity administration. The General Secretary is a legal representative of the Union.

The ITU conducts its activities in three principal fields which are supervised by separated structures, i.e. the radiocommunication sector (ITU-R), the standardisation sector (ITU-T) and the telecommunication development sector (ITU-D). ITU-T is in charge of examining and adopting guidelines pertaining to technical, operational and pricing issues, aimed at telecommunication standardisation globally. These are divided into series (each assigned a different letter of the alphabet), and feature separate and more detailed categories. The X series is entitled *Data networks, open system communications and security*, and it contains guidelines on general security, information and network security, application and service security, cyberspace security, the exchange of information on cybersecurity, and cloud computing security.³⁶ The World Telecommunication Standardization Assembly (WTSA), which gathers every 4 years, is a non-ITU institution. However, it sets the general direction of the activities of the standardisation (ITU-T) and radio communication (ITU-R) sectors. It is in charge of approving the list of technical topics related to telecommunications (referred to as queries) which can form the subject-matter of research and are submitted to the research groups operating within those sectors, which are established on an as-needed basis and comprise experts from various countries. These groups are in charge of drawing up *responses* which, in principle, take the form of a draft recommendation or a partial recommendation on a given issue, which is then subject to WTSA's approval. In addition, WTSA can adopt resolutions. For instance, the most recent WTSA, which gathered between 25 October and

³⁵See more in Kubicka (2007), pp. 127–128.

³⁶<https://www.itu.int/en/ITU-T/publications/Pages/structure.aspx#Z;>
1 September 2020.

accessed on

3 November 2016 in Hammamet, adopted Resolution 50 (Rev. Hammamet, 2016) on Cybersecurity, and Resolution 52 (Rev. Hammamet, 2016) on Countering and Combating Spam.³⁷

The Plenipotentiary Conference is yet another body issuing resolutions on the subject-matter discussed in this article, including Resolution 179 (Rev. Busan, 2014) of the Plenipotentiary Conference on ITU's role in child online protection, and Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference on definitions and terminology relating to building confidence and security in the use of ICT.

The executive body is the permanently operating secretariat with the Secretary General in the lead.

In 2001, the General Assembly of the United Nations passed Resolution 56/183 of 21 December 2001 on the World Summit on the Information Society (WSIS),³⁸ in which it approved the concept of conducting WSIS as proposed by ITU. The Summit was divided into two stages, the first of which took place on 10–12 December 2003 in Geneva, and the second on 16–18 November 2005 in Tunis.

The principal objectives of the first stage of WSIS included developing a shared viewpoint and adopting a statement expressing the political willingness to lay the foundations for “information society for all”, taking into consideration the diversified interests of all participants while also heralding the implementation of initial measures to attain this objective. The first stage resulted in adopting, on the 2nd of December 2003, the Geneva Declaration of Principles (*Building the Information Society: a global challenge in the new Millennium*) and the Geneva Plan of Action. The second stage of WSIS was aimed, in particular, at initiating the implementation process of the provisions of the Geneva Plan of Action, and at searching for solutions in such fields as Internet management and financial mechanisms on the Internet. On 18 November 2005, the Tunis Agenda on Information Society was announced, in which the role of international cooperation in combating cybercrime was stressed, entailing both collaboration between law enforcement authorities, and the establishing of dedicated legal frameworks by governments jointly with parties concerned (representatives of the IT industry and NGOs).³⁹

On 17 May 2007, the ITU Global Cybersecurity Agenda (GCA) was initiated. It acts as a framework for establishing international dialogue and cooperation to facilitate the coordination of global measures, serving as a response to the challenges related to combating cybercrime and building a secure information society. It is based on five strategic pillars (legal measures, technical and procedural measures, organisational structure, capacity-building, and international cooperation), its objective being to develop model cybercrime legislation that is interoperable with existing

³⁷https://www.itu.int/en/publications/ITU-T/pages/publications.aspx?lang=e&parent=T-RES&version_date=2016; accessed on 1 September 2020.

³⁸http://www.itu.int/wsisis/docs/background/resolutions/56_183_unga_2002.pdf, accessed on 1 September 2020.

³⁹Radoniewicz (2016), pp. 206–207.

national and regional legislative measures, and potentially applicable in the global context.⁴⁰

7 Group of Eight

At the meeting of representatives of the Justice and Home Affairs Ministries of the countries belonging to the Group of Eight,⁴¹ held on 10 December 1997 in Washington, a programme for combating computer crime, which was drawn up by the Subgroup on High-Tech Crime,⁴² was adopted featuring ten principles of combating cybercrime, together with a ten-point action plan.⁴³ The primary objectives included eliminating “hacker havens”, coordinating the prosecution of cybercrime regardless of where it was committed, as well as training and equipping law enforcement officers with adequate tools to combat high-tech crime.⁴⁴

The Ministerial Conference on Combating Transnational Organized Crimes which took place on 9–20 October 1999 in Moscow was dominated by such issues as financing terrorist activities, human trafficking or cybercrime. The last two issues were further discussed in annexes to the document⁴⁵ summarising the event. The

⁴⁰Radoniewicz (2016), pp. 207–208.

⁴¹The Group of Seven (G7)/the Group of Eight (G8) is not an international organisation but a sort of a “semi-institution”—a political and economic forum involving the most influential countries in the world, including France, Japan, Canada, Germany, USA, the United Kingdom, Italy, representatives of the European Union, and Russia. Their leaders gather at annual political and economic summits. The first such gathering took place in 1975. The G7/G8’s main objectives include strengthening international cooperation, coordinating foreign policies of its Member States, and improving international commodity turnover. See Łoś-Nowak (2009), pp. 291–293.

⁴²On 15–17 June 1995, at the G8’s Summit in Halifax, a dedicated expert group was established, which was entrusted with designing solutions to improve the procedures related to combating organised crime. Its work resulted in formulating, in 1996, a set of Forty Recommendations which were adopted at the G8’s Summit in Lyon on 27–29 June 1996. The group was, therefore, named the G8’s Lyon Group for fighting international organised crime. Several subgroups were established within its framework, the activities of which involve diversified issues of combating crime, including the aforementioned Subgroup on High-Tech Crime established in 1997. Other subgroups focus on fighting human trafficking or on providing legal assistance. The principal duties of the G8’s Lyon Group related to criminal procedures, international cooperation and effective prosecution of computer crime. At the G8’s meeting held on 19 October 2001 in Rome, following the 11 September 2001 attacks, representatives of the Justice and Home Affairs Ministries decided that the G8’s Lyon Group be merged with the G8’s Rome Group dealing with fighting terrorism. Following that merger, the G8’s Lyon/Rome Group was formed.

⁴³Principles to combat against high-tech crime and Action Plan to combat against high-tech crime.

⁴⁴See also The Information Economy Report drawn up in 2005 at the UN Conference on Trade and Development, http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf, accessed on 1. September 2020.

⁴⁵Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime.

said document included basic principles to combat cybercrime, which were later restated in numerous international strategies dealing with this subject-matter.⁴⁶ The practical effect of the Conference was the expansion of the international network of 24/7 points of contact operating within the Group of Eight.⁴⁷ At the Conference in Paris, attention was once again drawn to the need to eliminate the so-called lawless digital heavens or Internet heavens, and to the role which the Convention on Cybercrime could play as an international agreement open also to those countries which are not members of the Council of Europe, thus potentially serving as a global regulation. At the G8 Government-Industry Workshop on Safety and Security in Cyberspace held in May 2001 in Tokyo, the issues of data retention and securing data for criminal proceedings were dealt with.

At the Washington meeting of representatives of the Justice and Home Affairs Ministries of the countries belonging to the Group of Eight, the continual development of (and amendments to) the national regulations on penalising computer misuse acts, in order to reflect the actual technological progress, was recognised as a condition precedent to effectively combating Internet misuse for terrorist and criminal purposes. Such an approach should accelerate international criminal proceedings on computer crime. With reference to the Convention on Cybercrime, it was pointed out that measures were taken to encourage countries to accede to that document.⁴⁸ At another meeting of representatives of the Justice and Home Affairs Ministries which was held in Sheffield (Great Britain) on 16–17 June 2005, Member States were recommended to develop regulations which would guarantee a prompt response to serious cyberthreats and network incidents.⁴⁹

At a meeting held in Moscow in 2006,⁵⁰ representatives of G8's Justice and Home Affairs Ministries and Prosecutors focused on the issues of terrorism and cybercrime. They stressed that these phenomena are inter-related, and the establishing of effective measures against cybercrime was, therefore, recognised as the condition precedent to effectively combating terrorist acts in the domain of modern technologies.⁵¹

⁴⁶Gercke (2011). p. 177.

⁴⁷The network of points of contact serving the purpose of information exchange for conducting proceedings in cybercrime cases, operating on a permanent (24/7) basis, parallel to the 24/7 network operating under the Convention on Cybercrime. See Adamski (2011), p. 179.

⁴⁸The statement by G8's Justice and Home Affairs Ministries of 11 May 2004, the Summit of G8's Justice and Home Affairs Ministries held in Washington on 10–11 May 2004, http://www.g8.utoronto.ca/justice/justice040511_comm.htm, accessed on 1 September 2020.

⁴⁹See General objectives adopted at the Summit of G8's Justice and Home Affairs Ministries on 16–17 June 2005, http://www.g8.utoronto.ca/justice/justice_uk2005.htm, accessed on September 2020.

⁵⁰The Summit of G8's Justice and Home Affairs Ministries and Prosecutors held in Moscow on 15–16 May 2006.

⁵¹See the press conference of representatives of G8's Justice and Home Affairs Ministries, <http://www.g8.utoronto.ca/justice/justice2006.htm>, Accessed on 1 September 2020.

At the conference of G8's Justice and Home Affairs Ministries held on 23–25 May 2007 in Munich, the attendees undertook to work on the penalisation, also through domestic measures, of computer misuse acts committed via the Internet for terrorist purposes.⁵²

On 7–9 July 2008, at the summit of G8 Member States in Hokkaido Tokyo, Japan, a report drawn up by the Rome/Lyon Group was presented,⁵³ which once again outlined the various ways of exploiting new technologies by terrorist groups. A further extension of the network of 24/7 points of contact was also recommended, including in particular the extension of its coverage (at that time, the network covered around 50 countries).

At the 2009 meeting of G8's Justice and Home Affairs Ministries and Prosecutors, which was held on 29–30 May 2009 in Rome, the report prepared by the G8's Lyon/Rome Group for the UN Commission on Crime Prevention and Criminal Justice (CCPCJ) was discussed.⁵⁴ In the statement⁵⁵ containing a summary of the Summit, attention was drawn to the technological progress and new forms of Internet misuse, such as the criminal misuse of social networks, encryption services, VoIP services, the Domain Name System, and other new and evolving criminal attacks on information systems.

At the Summit in Muskoka, Canada, held on 25–26 June 2010, cybercrime was only mentioned in the context of Internet misuse by terrorists. Attention was drawn both to the problem of networks being put under terrorist threat, and their misuse by terrorists for communication purposes⁵⁶ (i.e. for disseminating ideologies, recruiting new members, training terrorists or coordinating terrorist activities).⁵⁷

On 24–25 May 2011, Paris was home to the e-G8 Forum *The Internet: Accelerating Growth*, in which Internet-related issues were discussed in attendance of representatives of scientific circles and enterprises operating in the widely understood IT industry (e.g. Microsoft, HTC, Google, Facebook, Alcatel, France Telecom, Eutelsat).⁵⁸ The Conference immediately preceded the G8 Summit scheduled on 26–27 May 2011 in Deauville (France). It was attended by representatives of the e-G8 Forum participants who brought a special message to governments (*Message to Deauville*), which stressed the significance of the Internet as a major drive of both

⁵²Gercke (2011)p. 180.

⁵³<http://www.g8.utoronto.ca/summit/2008hokkaido/2008-crimereport.pdf>, accessed on 1 September 2020.

⁵⁴Cf. <http://www.cybercrimelaw.net/G8.html>, Accessed on 1 September 2020.

⁵⁵http://www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf, accessed on 1 September 2020.

⁵⁶See *Muskoka Declaration: Recovery and New Beginnings*, Point 42, <http://www.g7.utoronto.ca/summit/2010muskoka/communiqué.html#peace>, accessed on 1 September 2020.

⁵⁷Cf. The statement from the G8 Summit held in Heiligendamm on 8 June 2007 on combating terrorism, <http://www.g8.utoronto.ca/summit/2007heilgendamm/g8-2007-ct.html>, Accessed on 10 October 2020.

⁵⁸<http://www.g8.utoronto.ca/summit/2011deauville/eg8/index.html>, Accessed on 1 September 2020.

social and economic development and recognised it as an “engine for change” (with the Arab Spring as an example). Governments of the G8 Member States were called to provide an unconstrained, fast and secure Internet. Although the Message met with a full understanding, and even approval, of the addressees, it did not translate into any specific recommendations.⁵⁹ At the subsequent G8/G7 summits⁶⁰ (the 2012 Summit in Camp David, the 2013 Summit in Lough Erne, the 2014 Summit in Brussels, and the 2015 Summit in Schloss Elmau), the issues of cybercrime were not dealt with, while at the 2016 Summit in Ise-Shima (Japan, the 26th–27th of May 2016), cyberspace security was again one of the most important subjects of the debate. In the declaration⁶¹ adopted at that Summit, it was stressed that a secure cyberspace was one of the main contributors to economic growth and prosperity. An undertaking was, therefore, made to establish close cooperation against the malicious use of cyberspace both by state and non-state parties, including terrorist units. The existing international law was again recognised as applicable to states’ operations in cyberspace. An undertaking was made to protect and promote human rights on the Internet, and to support a multilateral approach to Internet management entailing a full and active involvement, *inter alia*, of governments, private sector entities, civic societies, technological communities and international organisations. The specific duties and roles of countries in the tele-information environment aimed at ensuring security, stability and prosperity were stressed. Finally, a promise was made to establish a new G7 working group for cyberspace, with a view to facilitating concerted measures to ensure security and stability in cyberspace.

At the 2017 Summit in Taormina (Italy, 27 May 2017), attention was drawn to the fact that cyber attacks targeted at critical infrastructures worldwide highlighted the need to strengthen international cooperation aimed at ensuring cyberspace security as a condition precedent to economic growth and prosperity.⁶²

At the subsequent summits, taking place on 8–9 June 2018 in Charlevoix, Canada,⁶³ and on 24–26 August 2019 in Biarritz, France,⁶⁴ the issues of cybercrime and cybersecurity were barely touched upon. The 2020 Summit was planned to be held in March in Camp David. However, due to the COVID-19 pandemic, it was cancelled and a series of videoconferences were organised instead.

⁵⁹Gercke (2011), p 181.

⁶⁰In consequence of the events taking place in Ukraine in 2014, the G7 formula was restored, with Russia’s membership being “on suspension”. Thus, the 2014 Summit which was initially planned to be organised in Sochi was eventually held in Brussels (without Russia’s attendance).

⁶¹G7 Ise-Shima Leaders’ Declaration, <http://www.g8.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html>, Accessed on 1 December 2020.

⁶²Taormina Leaders’ Communiqué; <http://www.g8.utoronto.ca/summit/2017taormina/communiqu.html>, accessed on 1 December 2020.

⁶³The Charlevoix G7 Summit Communiqué, <http://www.g8.utoronto.ca/summit/2018charlevoix/index.html>, accessed on 1 December 2020.

⁶⁴G7 Biarritz Leaders’ Declaration; <http://www.g8.utoronto.ca/summit/2019biarritz/declaration-of-leaders.html>; accessed on 1 December 2020.

References

- Adamski A (2000) Prawo karne komputerowe, Warsaw
- Adamski A (2001) Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, Toruń
- Adamski A (2011) Cyberprzestępczość – rozwój regulacji prawnej w Europie. Doświadczenia krajowe na tle implementacji prawnych instrumentów zwalczania cyberprzestępczości, London, 11–12 November 2010). Prokuratura i Prawo 6
- Chałubińska-Jentkiewicz K (2019) Cyberodpowiedzialność, Toruń
- Gercke M (2011) Understanding Cybercrime: A Guide for Developing Countries. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf. Accessed 10 Oct 2020
- Hubbard AM, Schjølberg S. Harmonizing national legal approaches on cybercrime. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf. Accessed 10 Oct 2020
- Kubicka J (2007) International organizations – The United Nations Organization – its activity and reforms. Dąbrowa Górnicza
- Łoś-Nowak T (2009) (ed) Organizacje w stosunkach międzynarodowych. Istota – Mechanizmy działania – Zasięg, Warsaw
- Radoniewicz F (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warsaw
- Radoniewicz F (2019) In: Kitler W, Taczowska-Olszewska J, Radoniewicz F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw
- Schjølberg S. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, <http://www.cybercrimelaw.net>. Accessed 10 Oct 2020
- Sieber U (1998) Legal Aspects of Computer-Related Crime in the Information Society – Comcrime-Study, Würzburg
- Tarnogórski R (2009) Konwencja o cyberprzestępczości – międzynarodowa odpowiedź na przestępczość ery informacyjnej. In: Madej M, Terlikowski M (eds) Bezpieczeństwo teleinformatyczne państwa, Warsaw

Filip Radoniewicz PhD; legal advisor; adjunct in the Department of Cybersecurity Law and New Technologies at the Institute of Law, War Studies University, Warsaw; expert at the Academic Centre for Cybersecurity Policy, (War Studies University) and in the Ministry of Justice; he worked as an assistant judge (in the Fourth Criminal and Sixth Penitentiary Department of the Regional Court in Lublin); graduate of post-graduate studies: “European Union Law” at the Jagiellonian University, “Human Rights and Freedoms”, co-organized by the Institute of Legal Sciences of the Polish Academy of Sciences and the Helsinki Foundation for Human Rights, and “Computer Network Administration” at the Lublin University of Technology; author or co-author of approximately fifty publications, mainly in the field of broadly understood criminal law, new technology law and human rights. Selected publications: F. Radoniewicz (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym/Criminal liability for hacking and other offences against computer data and information systems/, Wolters Kluwer, Warszawa; Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz /Act on the National Cybersecurity System. Commentary/ (2019) ed. W. Kitler, J. Taczowska-Olszewska, F. Radoniewicz, CH. Beck, Warszawa.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.