Piotr Milik*

International legal regulations in the area of cybersecurity

Abstract

The article compares and analyses the acts of international law on the cybercrime. Firstly, the analysis of multilateral international agreements was made. Next, bilateral international agreements and legislative resolutions of international organizations were analysed. On that basis, conclusions concerning the range and forms of international cooperation in the field of cyber-security were formulated.

Key words: international cooperation, cybersecurity, threats, international agreements, security policy, international organisations, international law

* Dr hab. prof. nadzw. Piotr Milik, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: p.milik@akademia.mil.pl.

Convention on Cybercrime of November 23, 2001 (Budapest Convention) of the Council of Europe together with the additional protocol of January 28, 2003

The most important, binding document of the international rank, bringing together the largest number of countries, is the Convention of the European Council on cybercrime passed and submitted for signature on November 23, 2001 at an international conference in Budapest.

This is the first international agreement in the world comprehensively handling the issues of computer crime, defining offences against confidentiality, integrity and accessibility of the IT data and systems which defines computer fraud and counterfeiting, crimes related to child pornography, offences related to the infringement of copyright and related rights, as well as specifying the forms of liability and types of sanctions[1].

This document became effective on the first day of the month following the expiry of the three-month period from the date on which five countries, including three member States of the Council of Europe, expressed their consent to be bound by its provisions, that is, on July 1, 2004. As at December 9, 2018 the parties to the Convention were 62 countries. Despite its regional, European nature, this agreement is the most effective tool for the international protection of all entities that use computer technologies or to whom these technologies enable or facilitate the commitment of crimes. As practice shows, a number of states which are not members of the Council of Europe or parties to the Convention on Cybercrime treat it as a role model and repeat its decisions in their legal systems.

The Republic of Poland ratified the European Convention on Cybercrime on October 28, 2014[2]. It became effective in relation to Poland on June 1, 2015.

1 Konwencja stanowi owoc ponad czterech lat pracy ekspertów w ramach Rady Europy z udziałem przedstawicieli, takich państw jak Stany Zjednoczone, Kanada, Japonia czy Republika Południowej Afryki, które wprawdzie nie są członkami Rady Europy, ale wspólnie z krajami członkowskimi pragnęły podjąć działania pozwalające skuteczniej walczyć ze zjawiskiem cyberprzestępczości.

2 Dnia 8.07.2014 projekt ustawy o ratyfikacji europejskiej konwencji o cyberprzestępczości wpłynął do Sejmu – druk nr 2608; 15.07.2014 projekt skierowano do pierwszego czytania w komisjach, do Komisji Spraw Zagranicznych oraz Komisji Sprawiedliwości i Praw Człowieka; 28.08.2014 pierwsze czytanie w komisjach (sprawozdanie komisji druk nr 2703, sprawozdawca: Elżbieta Achinger); wniosek komisji: uchwalić projekt ustawy bez

The provisions of the Convention can be divided into the following main groups: 1) norms of substantive criminal law – containing definitions of terms defining the constituent elements of crimes (Article 1–13); four types of cybercrime are defined in this set of regulations: a) crimes against confidentiality, integrity and availability of IT data and systems, b) computer crime, c) crime related to the nature of the information contained, d) crime related to the infringement of copyright and related rights; 2) the norms of procedural criminal law – defining the procedures to be followed in matters relating to crime specified in the Convention and other crimes committed with the use of an IT system and collection of electronic evidence related to these crimes (Article 14–21); 3) regulations regarding jurisdiction over offences specified in the Convention (Article 22); 4) provisions on international cooperation in the field of extradition and mutual legal assistance and the exchange of information (Article 23–35); 5) final provisions (Article 36–48).

The Convention on Cybercrime was intended to supplement the existing multilateral or bilateral treaties or agreements concluded between states, including the provisions of the European Convention on Extradition Open for Signature in Paris on December 13, 1957, the European Convention on Mutual Legal Assistance in Criminal Matters Open for Signature in Strasbourg on April 20, 1959, the Additional Protocol to the European Convention on Mutual Legal Assistance in Criminal Matters, opened for signature in Strasbourg on March 17, 1978.

The Convention on Cybercrime was intended to supplement the existing multilateral or bilateral treaties or agreements concluded between states, including the provisions of the European Convention on Extradition Open for Signature in Paris on December 13, 1957, the European Convention on Mutual Legal Assistance in Criminal Matters Open for Signature in Strasbourg on April 20, 1959, the Additional Protocol to the European Convention on Mutual Legal Assistance in Criminal Matters, opened for signature in Strasbourg on March 17, 1978.

poprawek; 11.09.2014 drugie czytanie na posiedzeniu Sejmu; decyzja: niezwłocznie przystąpiono do trzeciego czytania; 2.09.2014 trzecie czytanie na posiedzeniu Sejmu; głosowanie: całość projektu ustawy; wynik: 438 za, 1 przeciw, 1 wstrzymał się; decyzja: uchwalono; 15.09.2014 ustawę przekazano prezydentowi i marszałkowi Senatu; 9.10.2014 stanowisko Senatu: nie wniósł poprawek; 13.10.2014 ustawę przekazano prezydentowi do podpisu; 28.10.2014 prezydent podpisał ustawę.

Despite positive acceptance by official factors, the Convention has been criticized by numerous commentators, mainly representing human rights NGOs or internet providers for too many, in their opinion, unclear regulations, not precisely interpretable regarding the rights of relevant services authorized to conduct electronic surveillance. Criticism also concerned the lack of consulting in the course of preparing a draft of the convention with independent experts. For these reasons several countries negotiating the text of the Convention refused to sign it (e.g. the Czech Republic or Ireland)[3]. Among the countries that have not signed the Convention is also Russia, where, as international reports indicate, the scale of cybercrime is among the highest in the world[4]. Russian President V. Putin officially refused to accede to the Convention, pointing out that the agreement "strikes at Russia's sovereignty"[5].

The Convention is supplemented by an Additional Protocol on the criminalization of racist or xenophobic acts committed by means of computer systems. It was adopted and open for signature on January 28, 2003 in Strasbourg and became effective on March 1, 2006. The Protocol defines racist and xenophobic material in cyberspace as any written material, image or other expression of thought or theory that incites, supports or stirs up hatred, discrimination or violence against any person or group of persons because of race, colour, national or ethnic origin, as well as religion, if it is used as an excuse for any of the above-mentioned behaviours. It calls on the states of the party to their criminalization and extends the scope of application of the 2001 Cybercrime Convention to them. Some states participating in the process of the negotiations, in particular the United States, has not agreed to the inclusion of the punish ability of racist or xenophobic acts in the Convention itself, citing the wide limits of freedom of expression in the USA guaranteed by the first amendment to the American constitution[6].

On January 29, 2015, the President of the Republic of Poland ratified the above-mentioned Protocol, thus subjecting Poland to its resolutions (it became effective on June 1, 2015; at that time, 24 countries were parties to

3 D. Cieślak, *Konwencja przeciw cyberprzestępczości*, www. computerworld.pl.

4 Raport o zagrożeniach bezpieczeństwa pochodzących z internetu 2011, http://ssl.certum. pl/certyfikaty/certy,informacje_ciekawostki_certyfikaty_SSL.dxml?MEDIA=pdf.

5 Putindefies Convention on Cybercrime, http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.

6 D. Głowacka, *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji*, http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf.

the Protocol); just like other countries, the parties are obliged to recognize in their internal legal order as criminal offences the acts of intentional and unlawful distribution or public disclosure in another manner of racist and xenophobic materials in a computer system. The Protocol thus expanded the catalogue of cybercrime formulated in the Council of Europe Convention against Cybercrime.

Both documents cited above constitute an important achievement in the area of harmonization of law and cooperation between states in combating computer crimes committed in cyberspace. Together, they establish a catalogue of computer crimes and set standards for their prosecution and punishment. An important achievement of the analysed documents is to identify areas sensitive to ICT networks such as child pornography, copyright and related rights, as well as racist and xenophobic content. Although the Convention and the Additional Protocol constitute documents of a regional and European reach, they undoubtedly constitute and will be a reference point for countries wishing to regulate prosecution and punishment of computer crimes in their internal legislation even without acceding to the indicated international agreements. The impact of the Convention and its Additional Protocol will undoubtedly contribute to the promotion and dissemination of the European values in the world, in particular human rights, such as respect for the right to information, privacy, confidentiality of correspondence, freedom of conscience and religion, and finally, human dignity. This is due to the fact that the negotiators creating the indicated documents on behalf of the countries in the Council of Europe tried on the one hand to develop effective instruments to fight cybercrime, but on the other hand, throughout the entire negotiation process, tried to take into account the necessity to respect fundamental human rights[7].

Finally, it should be emphasized that both the Council of Europe Convention against Cybercrime and the Additional Protocol thereto relate only to common crimes committed in cyberspace. On the other hand, they do not contain any regulations regarding terrorist activities in cyberspace, threatening the security of critical infrastructure of states, nor activities bearing the hallmarks of cybernetic military aggression provoking cyberwar.

7 Szerzej na temat zjawiska europeizacji prawa zob. M. Urbańczyk, *Protokół dodatkowy do Konwencji o cyberprzestępczości jako przykład europeizacji prawa karnego*, https://prawo.amu.edu.pl/__data/assets/pdf_file/0020/235145/12-DWS-Urbanczyk-M.,-Pro-tokol-dodatkowy-do-konwencji-o-cyberprzestepczosci.pdf.

The Council of Europe Convention on the Protection of Children against sexual exploitation and sexual abuse, drawn up in Lanzarote on October 25, 2007

The member states of the Council of Europe and other signatory countries to the Convention on the protection of children against sexual exploitation and sexual abuse set a goal to protect children (defined as persons under the age of 18), as closely and effectively as possible, against sexual abuse by adults, which has a destructive impact on the child's health and psychosocial development. The factor determining the countries to undertake work on the Convention was the worrying intensification of the phenomenon of sexual exploitation of children and their sexual abuse, which could be observed in particular in the ICT networks. This was undoubtedly associated with the increase in the use of information and telecommunications technologies by both children and perpetrators of crimes against them[8].

The main objectives of the Convention are to prevent and combat the sexual exploitation and sexual abuse of children, to protect the rights of children who are victims of sexual exploitation and to promote international cooperation against sexual exploitation of children. The objectives set out in this way do not focus solely on crime carried out via and by means of the ICT networks, but also include combating this type of increasing criminal activity.

Regarding the threats arising from the increasingly growing use of the internet by children, the States Parties to the Convention (including Poland[9]) have committed themselves to adopting necessary legislative measures to ensure that children, during their primary and secondary school education, receive information on the risks associated with the sexual abuse and protection measures against this threat. This information, in accordance with the commitment contained in the Convention, is to be transmitted within the framework of general knowledge of human sexuality and to emphasize risk

8 Zob. K. Badźmirowska-Masłowska, *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investement in the Common future*, Olsztyn 2013, s. 147–160.

9 Prezydent Rzeczypospolitej Polskiej ratyfikował Konwencję Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych 22 stycznia 2015 r.

situations, in particular situations related to the use of modern information and telecommunication technologies.

The convention signals two main problems related to the dynamic development of the ICT networks and the increase in the range of their impact. First of all, it has been noticed that the increasing availability of the internet, including for children using stationary or mobile communication devices, creates potential threats consisting in the direct recruitment of children by persons and criminal environments under the guise of innocent meetings or activities for the purposes of sexual exploitation, production of pornographic materials or even kidnapping and sale at the black market of human trafficking. Article 23 of the Convention defines the crime of the so-called solicitation of children for sexual purposes, consisting in a deliberate submission to a child by an adult through the information and telecommunication technologies of a proposal to meet for the purpose of committing any of the offences specified in the Convention against a child, in a situation when such a proposal is followed by the actual actions aimed at such a meeting.

Secondly, the widespread availability of the internet and the growing possibility of transmitting more and more data via this network creates a new market for illegal pornography. Article 20 of the Convention defines offences concerning child pornography as the intentional acts of producing, offering or sharing, distributing or transmitting child pornography, acquiring the same for oneself or for another person, as well as owning child pornography and knowingly acquiring access to child pornography through the information and telecommunication technologies.

It should be noted that these issues were also the subject of the optional Protocol to the Convention on the Rights of a Child on the sale of children, child prostitution and child pornography[10], adopted in New York on May 25, 2000, which, however, does not focus on the issue of committing such crimes by means of or via the internet. Nevertheless, the signatory countries of the Protocol have already expressed in the preamble their concern about the increasing availability of child pornography on the internet and other emerging technologies. In the rest of the document, however, we will not find a broader spectrum of threats to children's rights posed by the development of cyberspace, or a closer definition of computer crimes related to child trafficking, child prostitution or pornography. Rather, it should be assumed that

10 Dz.U. z 2007 r. nr 76, poz. 494.

violations of children's rights, as defined and described in the Convention, may also be committed by means of or via the internet, in particular, dissemination of child pornography.

The Agreement of the Commonwealth of Independent States on cooperation in combating computer crime signed in Minsk on June 1, 2001

The Agreement of the Commonwealth of Independent States (CIS) on cooperation in combating computer crime was signed in the capital of Belarus on June 1, 2001 by the then 12 member states of member states of the CIS (including Georgia, which withdrew from the Community in 2008); it was aimed at ensuring optimal effectiveness in the fight against crimes related to the computer information inside the CIS. Its member states agreed on the urgent need to intensify cooperation in this area and to this end a convention legal framework was established for cooperation between law enforcement and judicial authorities of the member states – parties to the Agreement.

The Minsk Agreement defines four types of computer crime: 1) illegal access to computer information protected by law, where such action causes destruction, blocking, modification or copying of information or disrupts the functioning of a computer, computer system or related networks; 2) creating, using or distributing malicious software; 3) violation of the regulations governing the use of computers, computer systems or networks related by a person who has access to those computers, systems or networks, as a result of destruction, blocking or modification of information about computers protected by law, when such violation causes significant damage or other serious consequences; 4) the illegal use of computer programs and databases protected by copyright or computer piracy, when such activity causes significant damage.

The agreement in question assumes a number of detailed forms of cooperation between the member states – parties to the Agreement, including exchange of information on crimes related to computer information, natural or legal persons participating in such crimes; ways and means of preventing, detecting and combating crimes related to computer information; means applied to commit crimes related to computer information; national laws and international agreements regulating matters related to prevention, detection, suppression, disclosure and prosecution of crimes related to computer information.

Agreement of the Shanghai Cooperation Organization on cooperation in the area of international information security, signed in Ekaterinburg on June 16, 2009

As we read in the preamble to the Shanghai Cooperation Organization Agreement[11] (SCO) on cooperation in the area of international information security, the governments of the member states of the Shanghai Cooperation Organization have noticed significant progress in the development and implementation of the latest information and communication technologies and ways of creating information in a global space. Governments of the SOW member states expressed their concern about the escalation of threats related to the possibility of using such technologies and means for purposes incompatible with the principles of peaceful coexistence of states. New information technologies can be used in both the civil and military sphere, raising the importance of international information security as one of the key elements of the international security system. The SCO member states expressed the conviction that further deepening of trust and development as well as cooperation of the parties in ensuring information security is an international imperative and necessity and is beneficial for their interests. In establishing an agreement on cooperation in the area of international information security, the member states – the parties to the agreement also took into account the important role in ensuring information security, human rights and fundamental freedoms. The preamble to the SCO Agreement on cooperation in the area of international information security also referred to the recommendations of the resolution of the UN General Assembly entitled *Achievementsin the area of computerization and telecommunications in the context of international security*, aimed at reducing threats to the international information security. The SCO member states as the main goal of signing the agreement on cooperation in the area of the international information security indicated a desire to secure international trade and exchange of

11 Szanghajska Organizacja Współpracy (SOW) – organizacja regionalna powstała w toku spotkań przedstawicieli dawnych republik radzieckich (Kazachstanu, Kirgistanu, Rosji, Tadżykistanu) i Chin, na których podjęto wysiłek uregulowania granic na obszarze Azji Centralnej po upadku Związku Radzieckiego. Wkrótce tematyka spotkań uległa rozszerzeniu o zagadnienia bezpieczeństwa regionalnego i rozbrojenia. Formalne powołanie do życia SOW miało miejsce 16 czerwca 2001 r. na szczycie w Szanghaju. W tym samym roku do Organizacji przystąpił Uzbekistan.

information and to create a secure area of information characteristic of the world, cooperation and harmony.

The agreement on cooperation in the area of international information security defines the main threats to the cybersecurity of the modern world; these are: 1) development and use of cybernetic weapons and preparation to carrying out an IT war; 2) cyberterrorism; 3) cybercrime; 4) use of a dominant position in the information sphere to the detriment of interests and security of other countries; 5) dissemination of information harmful to the socio-political, socio-economic, moral and cultural system of other countries; 6) security threats, stable functioning of global IT state and infrastructures, caused by natural causes and (or) by deliberate and intentional activities of the human being.

The Parties undertook to cooperate for the protection of information in the international digital sphere, being aware that such cooperation may contribute to social and economic development and will contribute to maintaining international security and stability, in accordance with the generally accepted principles and norms of the international law, including principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of non-interference and regional cooperation within the information resources of the parties.

The analysed agreement on cooperation in the area of international information security concluded between the member states of the Shanghai Cooperation Organization is not limited only to defining forms of common cybercrime, as do conventions on the security in cyberspace, signed under the auspices of the Council of Europe, but also refers to the issues related to the use of cyber weapons in the information warfare and cyberterrorism, thus broadly referring to the issues of international security.

The Arab League Convention on combating information crime, signed in Cairo on December 21, 2010

In the preamble to the Convention on combating IT crime, we read that the states associated in the League of Arab States also noted the need to strengthen cooperation between them in order to combat IT crimes threatening their security and vital interests and the security of their societies. By joining the Convention, the Arab states expressed their conviction on the necessity of

adopting common criminal policy should in order to protect their societies against IT crimes. They referred to high religious and moral standards and principles, especially Islamic Sharia law, and the cultural heritage of the Arab people, which rejects all forms of crime. Finally, at the end of the preamble, reference was made to the need to respect relevant international human rights agreements binding the Arab countries.

The main purpose of the Convention is to increase and strengthen cooperation of Arab states in the fight against IT crime, identify and reduce such threats, which is to contribute to the protection of the security and interests of Arab states and the security of their citizens.

The League of Arab States Convention on combating the IT crime contains a catalogue of defined computer crimes, which include: the crime of illegal access, the crime of illegal data transfer, the crime against data integrity, the crime of misuse of information by means of IT, the crime of data falsification, the crime of fraud, crimes related to the production and distribution of pornography, crimes against privacy committed with the use of IT means, crime of terrorism committed with the use of IT means, crimes related to organized crime committed with the use of IT means, crime against copyright and related rights, illegal use of electronic payment tools.

It is clear from the above catalogue that the subject of interest of the signatory states of the Convention was mainly common computer crime, defined in detail in the types of individual offences. Nevertheless, it is noteworthy that, in addition to common crimes, the Convention also defined cyberterrorism.

It included the acts of spreading and supporting the ideas and principles of terrorist groups; financing and training for the purpose of carrying out terrorist operations; facilitating communication between terrorist organizations; dissemination of methods of producing explosives, in particular, to be used in terrorist operations; promoting religious fanaticism and attacking religion and beliefs.

The African Union Convention on cybersecurity and protection of personal data adopted in Malabo, June 27, 2014

The aim of the African Union countries making efforts to harmonize the laws and activities in the area of cybersecurity was to establish a legal framework for secure activities in cyberspace, including ensuring the protection of personal data of citizens of the African Union Member States at a regional level, and thus, contributing to the establishment# of an information society in this area.

The purpose of the Convention is also to establish in each state being a party to it mechanisms capable of combating violations of privacy generated as a result of illegal collection of personal data, their processing, transmission, storage and use. The Convention, proposing certain institutional solutions to secure mobility in cyberspace, at the same time constructs guarantees to respect the fundamental rights and freedoms of individuals, the rights of local communities and the interests of enterprises. It can be said that the Convention is trying to imitate and duplicate internationally recognized best practices.

At the beginning, the main obstacles to the development of e-commerce in Africa were defined, which first of all result from the lack of cybersecurity. They included the lack of: 1) regulations on the electronic signature and reliability of the transmitted electronic data; 2) the legal regulation of such issues as the protection of consumers, intellectual property, personal data and the information systems; 3) application of the IT techniques in the commercial and administrative activities; 4) e-commerce tax regulations. The first chapter of the Convention is devoted to the electronic trade. In accordance with the objectives set out in the preamble, the Convention seeks to introduce guarantees that protect the certainty of trade and to eliminate the possibility of fraud and abuse. Among other things the scope of liability of entrepreneurs operating in cyberspace, the scope of permitted electronic advertising and the forms of internet contracts (forms of legal transactions) were regulated. The second chapter regulates the issues related to the protection of personal data in connection with their collection and processing in electronic data sets. Chapter three contains the basic principles of cybersecurity, which the member states – parties to the Convention have committed to comply with, and the regulations on combating computer crime, and a wide catalogue of acts constituting computer crime. The last, fourth chapter contains the final provisions.

Bilateral international agreements

We will not find many documents in the category of the binding legal acts, which are bilateral international agreements regarding cooperation of states in the fight against cybercrime and other threats arising from the dynamic development of cyberspace. Such agreements, as a rule, are not concluded in bilateral relations, because only multilateral, regional or – optimally – common cooperation between states gives the opportunity to effectively combat threats resulting from irresponsible and criminal use of the internet. Bilateral cooperation between states in the prosecution of computer crimes has so far been implemented based on existing legal aid agreements. Nevertheless, we can point to a number of examples showing bilateral initiatives aimed at improving security in cyberspace.

The first example is the agreement concluded between the United States and Australia under the Pacific Security Pact (ANZUS). In 1951, at a conference in San Francisco, Australia, New Zealand and the United States concluded a Security Agreement (Pacific Security Pact) regarding military defence in the Pacific Ocean, named after the first letters appearing in the names of the countries – ANZUS (Australia, New Zealand, United States). The treaty was originally an alliance of three countries built on bilateral agreements – on the one hand the United States and Australia, on the other hand Australia and New Zealand as well as the USA and New Zealand (until 1987). Starting from 1985, New Zealand suspended its activities in the ANZUS pact, under which representatives of the USA and Australia met. In 2011, a new clause was added to the Pacific Security Pact stating that it will also apply to cyberspace.

New Zealand and the United Kingdom are currently working on an agreement on cooperation in the combat against cybercrime. Both countries have expressed their intention to share intelligence, conduct joint research and generate development in the area of combating online crime. To this end, they decided to prepare joint strategic goals.

In 2013, the United Kingdom and India declared their willingness to sign an agreement on cyberspace security aimed at improving the protection of personal rights and enabling an increase in the amount data from the United Kingdom stored on Indian servers.

The United States and Canada have also taken some steps in bilateral relations, establishing cooperation on combating cross-border computer crime as part of the Beyond the Border Program.

For several years dialogue in the area of security in cyberspace has also been conducted by the United States and China through their think tanks. Since 2009 bilateral talks on cooperation in the area of cybersecurity have been conducted by the Chinese Institute of Contemporary International Relations and the Centre for Strategic and International Studies of the United States. Six formal meetings of the representatives of these organizations have been held so far. However, for years the parties have not achieved significant rapprochement.

Admittedly, some shared views have been established on the issues such as the threat from 'third parties', non-state entities (e.g. terrorist groups) and views on cooperation in the combat against IT crimes such as computer fraud and child pornography.

However, there are still some disputed areas. For example, China has offered to conclude a no first use agreement ("I will not take the first step in cyberwar") between cybernetic powers and to prohibit cyberattacks for purely civilian purposes. Meanwhile, the United States have indicated that the borderline between civil and military purposes is vague today, but the concept of protecting civilians can be found in the Geneva and Hague Conventions, which according to Americans should be respected by all states in cyberspace. In addition, the parties attempted to determine what behaviours could be considered as cyberattack or cyberwar. It has been agreed so far that the scale of cybernetic acts justifying their recognition as cyberattack should be extensive, but the duration and effects of cyberspace activities which could be considered as cyberattack have still not been determined. It should also be noted that despite the ongoing dialogue between the two powers regarding cybersecurity, a number of cyberattacks in the territory of the United States carried out from Chinese servers have recently beenreported. However, the Chinese officials denied the allegations that these attacks were allegedly inspired by the Chinese authorities. Bilateral talks on security in cyberspace are also conducted by the representatives of China and France within the Joint Working Committee on Computerization and Communication[12].

12 Zob. na ten temat: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf.

In May 2015, Russia and China signed a memorandum which stipulates that both countries will not conduct cyberattacks against each other and that they will also jointly thwart the emergence of technologies that can potentially "destabilize the internal political and socio-economic atmosphere", "disturb public order" or "interfere in the internal affairs of the state." In addition, Beijing and Moscow have agreed on closer cooperation in the combat against cybercrime and on intensification of joint efforts to improve protection of critical information infrastructure in both countries. For China, this is the next step to promote its concept of sovereignty on the internet in direct opposition to the idea of the West – the internet freedom. The leadership of the Chinese Communist Party sees the Western idea of the internet freedom as synonymous with Western "cyberhegemony"[13].

In November 2010, in Lisbon, the United States and the European Union also established a Working Group for Cybersecurity and Cybercrime in order to develop a cooperation program and action plan, including developing a common approach to various problems of the internet crime and online security. The working group was tasked with developing a model of cooperation and good practices in combating critical cyber incidents and a model of public-private partnership, i.e. cooperation between governmental institutions and industry representatives in ensuring online security and combating cybercrime.

The group's task was also to examine the impact of the Council of Europe Convention on Cybercrime and to encourage the Member States of the European Union and of the Councilof Europe to its quick ratification. Although so far, the working group has not been able to present any results of its work, its goals seem specific and achievable[14].

13 Zob. F.S. Gady, *Have China and Russia Agreed Not to Attack Each Other in Cyberspace?*, http://thediplo-mat.com/2015/05/have-china-and-russia-agreed-not-to-attack-each-other-in-cyberspace/.

14 W. Kraft, C. Streit, *Ideas on the Establishment of an International Court for Cyber Crime*, World Council for Law Firms and Justice (WCLF) 2011, s. 4.

Directive of the Economic Community of West African States[15] on the combat against cybercrime adopted in Abuja on August 19, 2011

Information and communication technologies (ICT), as a manifestation of the modern information revolution, shape the globalization process to the greatest extent. Recognizing their potential to accelerate economic integration in Africa, and thus increase the level of prosperity and acceleration of social transformation, the Ministers of Communication and Information Technology of African countries met in May 2008 under the auspices of the African Union (AU) and adopted a document entitled Framework Reference for Harmonization of Policies in the area of information and communication technologies. The initiative became necessary, taking into account the progressive development in the electronic communications sector and the current tendencies of liberalization of policy in it. Coordination of policies in the area of information and communication technologies throughout Africa has become necessary because the policies, laws and practices implemented in each of the countries individually may be an obstacle in the development of competitive regional markets. The document adopted in 2008 by the ministers of the African communication and information department was one of the first steps to regulate and harmonize the fight against cybercrime in the African area.

A year later, in 2009, work on the relevant directive began in the forum of the Economic Community of West African States. On August 19, 2011, at the Summit in Abuja, at the 66th ordinary session of the Council of Ministers of the Economic Community of West African States, after consulting the ECOWAS Parliamentary Assembly, a document entitled the Directive on the fight against cybercrime of ECOWAS was adopted, binding on the ECOWAS member states which were obliged to implement directives to their internal legal systems by means of appropriate legislation no later than by January 1, 2014.

15 ECOWAS (Economic Community of West African States) – organizacja regionalna skupiająca 15 państw położonych w subsaharyjskiej części Afryki Zachodniej, powstała na mocy traktatu z Lagos podpisanego 28 maja 1975 r. Głównym celem ECOWAS jest promowanie integracji ekonomicznej krajów członkowskich.

The Directive contains three main areas of regulation: the area of substantive criminal law, the area of procedural law and the area of judicial cooperation. However, the main focus was on the definitions of a computer crime. Experience shows that harmonization of substantive criminal law provisions is, in principle, easier than harmonization of procedural law or implementation of international cooperation. Consequently, the focus was on harmonizing substantive criminal law.

Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communication sector of July 12, 2002

In July 2002, the European Parliament and the Council adopted a directive on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[16].

The extensive introduction preceding the actual content of the directive contained a number of interesting observations regarding, for example, the protection of data transferred via the electronic network: "(...) Protection against unauthorized access to messages requires appropriate measures to be taken to ensure the protection of confidentiality of communications, including both the content and data related to such messages, by means of public communications networks and publicly available electronic communications services. The national legislation in some Member States prohibits only intentional unauthorised access to communications".

"Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications may be recorded for the purpose of providing evidence of commercial transactions. Directive 95/46/EC applies to such processing. Parties to which the communication refers should be informed on the record, its purpose and period of storage prior to the commencement of the record. The recorded communication should be erased as soon as possible and in any

16 Dyrektywa Parlamentu Europejskiego i Rady w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej z dnia 12 lipca 2002 r., CELEX nr 32002L0058.

case by the end of the period during which the transaction can be lawfully challenged at the latest".

"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private zone of the users subject to protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. The so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may intrude upon privacy of these users in a significant way. The use of such devices should be allowed only for legitimate purposes, after previous notification of the users concerned.

"However, such devices, for instance the so-called "cookies", can be a legitimate and useful tool, for example in analysing the effectiveness of website design and advertising, and in verifying the identity of the users engaged in on-line transactions. In the case where such tools, for example cookies, are intended for legally permissible purposes, such as facilitating the provision of services to the information society, their use should be allowed, provided that users receive clear and accurate information in accordance with Directive 95/46/EC on the purpose of cookies or similar tool to ensure that users remain acquainted with the information placed on the terminal used by them. The users should have the opportunity to refuse to have cookies or similar device stored on their terminal.

This is particularly important in the case where the users other than the original user have access to the terminals and thereby, to any data containing privacy-sensitive information stored on such equipment. Information and the right of refusal may be offered once for various tools installed on the user's terminal equipment during the same connection and may include any further use of these tools that may be made of such tools during the subsequent connections. The methods of providing information, offering the right of refusal or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of cookies or a similar device, if it is used for a legitimate purpose".

This directive also devotes space to a spam regulation. Unordered advertising materials are discussed in Article 13 of the Directive entitled Unordered communications. This article states in clause 1 that the use of automated calling systems without human intervention (automatic calling machines), fax machines or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have expressed their consent to such use beforehand. Paragraph 2 stipulates that in the case where a natural or legal person receives detailed electronic contact details from their clients for the purposes of electronic mail in the context of the sale of a product or service, the same natural or legal person may use these detailed electronic contact details for the purposes of placing on the market their own similar products or services, provided that the customers have been clearly and explicitly informed of the possibility of objecting to such use of electronic contact details in a simple manner and free of charge. In paragraph 3, Article 13 obliges the EU Member States to take appropriate measures to ensure that free of charge, unordered communications for direct marketing purposes will not be allowed without the consent of subscribers. Clause 4 states that in any case the practice of sending electronic mail for the purposes of direct marketing, disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid current address to which the recipient may send a request to stop such communications, should be prohibited. Paragraph 5 of the quoted article states that the provisions of paragraphs 1 and 3 should apply to subscribers who are natural persons. At the same time, the EU Member States became obliged to ensure conditions in which legitimate interests of subscribers other than natural persons, with regard to intrusive communications, also receive adequate protection.

In January 2004, the European Commission presented a communication on spam, which outlined activities to be taken to complement the directive discussed above[17]. The communication stressed the need to undertake action by various entities in the scope of informing, self-regulation, technical solutions, cooperation and law enforcement.

17 Komunikat Komisji skierowany do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie niezamówionej informacji reklamowej spam z dnia 22 stycznia 2004 r., CELEX nr 52004DC0028.

Regulation No. 526/2013 of the European Parliament and of the EU Council of May 21, 2013 on the European Network and Information Security Agency (ENISA) and the repealing Regulation (EC) No. 460/2004[18]

The European Network and Information Security Agency (ENISA) was established by a regulation of the European Parliament and of the Council[19] to provide expertise to stimulate cooperation between the public and private sectors and to provide substantive assistance to the European Commission and the EU Member States. ENISA is to provide support and basis for solving problems of the growing threat to the security of electronic communications. According to the Polish website devoted to ENISA's activities – www.enisa.pl – this agency operates openly, acting as an independent centre gathering the knowledge of the best experts in the area of information security from the EU member states. In the intentions of the European Union, the Agency is to strengthen the capacity of the EU economy to counteract and respond to the IT security threats.

Directive of the European Parliament and of the Council on attacks against information systems of August 12, 2013[20]

In February 2005, the Council of the European Union, carrying out the tasks imposed on it in the Treaty on the European Union (TEU), adopted a framework decision on attacks against information systems[21]. It was then the most important document adopted under the third pillar of the European Union attempting to tackle the growing phenomenon of cybercrime. As the text of the Framework Decision itself stated, it was conceived as a supplement to the

18 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 r., nr CELEX 32013R0526.

19 Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Europejską Agencję Bezpieczeństwa Sieci i Informacji z dnia 10 marca 2004 r., nr CELEX 32004R0460.

20 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/ WSiSW, nr CELEX 32013L0040.

21 Decyzja Ramowa Rady w sprawie ataków na systemy informatyczne z dnia 24 lutego 2005 r., nr CELEX 3200F0222.

work completed by international organizations, in particular the Council of Europe, in the scope of approximation of the criminal law or G8 in the scope of cross-border cooperation in the area of crime with the use of advanced technology. The Framework Decision of the Council was to establish a unified approach in the European Union to the discussed issue. The intention of the decision makers was probably, among other things, to use the procedures and principles of the EU law to discipline the EU Member States, which as members of the Council of Europe signed the Council of Europe Convention on Cybercrime but delayed its ratification.

The framework decision was to provide an additional incentive for these countries to adjust their internal legal orders to the standards ensuring adequate international cooperation.

A. Adamski rightly notes that "the global nature of the internet creates a situation in which the use of a computer in the territory of one country may violate a criminal prohibition in force in another country. The perpetrator of such a violation, however, is not subject to criminal liability if he operates in a country whose legal system does not provide for the punish ability of hacking[22], dissemination of computer viruses or other IT abuse"[23].

According to the above quote, computer criminals may remain unpunished if their activity took place in the territory of a country that does not provide for such crimes in its law. Such countries are referred to as "hackers' paradise". The most notorious of this kind was the case of two young programmers from the Philippines who in 2000 infected hundreds of thousands of email systems worldwide with a virus called 'I love you'. Both pranksters remained unpunished because they did not violate any provision of the law in force binding in the Philippines. So, they did not hear any charges.

22 ##Hacking to w języku informatyków czyn polegający na penetrowaniu systemów komputerowych, gromadzeniu wiedzy o systemach i o tym, w jaki sposób działają. Podana definicja wykazuje wyłącznie pozytywne konotacje słowa hacking. Oprócz powyższego w języku informatyków występuje również pojęcie crackingu, czyli technicznie działalności zbliżonej do hackingu, ale różniącej się intencją przestępczą – niszczenia danych bądź ich nielegalnego pozyskiwania i wykorzystywania. Dla prawodawcy, podobnie jak dla szerokiej opinii publicznej powyższe rozróżnienie nie istnieje, to właśnie haker pozostaje synonimem komputerowego przestępcy, szerzej zob. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

23 A. Adamski, *Rządowy projekt dostosowania polskiego Kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości*, www.cert.pl.

The conclusions of the Council of November 27–28, 2008 indicated that the Commission together with the Member States should develop a new strategy taking into account the content of the 2001 Council of Europe Convention on Cybercrime, as this Convention sets the legal framework for combating cybercrime, including attacks on information systems. The new directive should be based on this Convention. Possibly fastest completion of the ratification process The Convention should be considered a priority by all Member States.

The Framework Decision of the Council on attacks on information systems of February 24, 2005 was effective until it was repealed by the new EU regulation – Directive of the European Parliament and of the Council of August 12, 2013 concerning attacks on information systems. After eight years of validity of the framework decision, a decision was made to replace it with an act of the rank of a directive adopted by the Council together with the European Parliament, which undoubtedly raised the importance of matters regulated in such a manner in the EU legal order.

The motive to resume work within the European Union on the issue of attacks on information networks and systems was the statement that both within the Union and globally the threat of attacks on information systems, and especially attacks carried out as part of organized crime, is increasingly growing. The Directive also expressed concerns about the possibility of attacks of a terrorist or political nature directed at information systems as part of the critical infrastructure of the Member States and the Union.

According to the authors of the directive this poses a threat to the achievement of a safer information society and of the space of freedom, security, and justice, and therefore, requires a response at the Union level and improved cooperation and coordination at the international level.

Another reason was the existence and deepening of the tendency to increasingly more dangerous and repeated large-scale attacks against information systems often crucial for the Member States or specific functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called 'botnets', which involves several stages of a criminal act, where each stage individually may pose a serious risk to the public interest. This Directive aims, inter alia, at introducing criminal penalties for the creation of botnets, namely, the activities consisting in acquiring remote control over a significant number of computers by infecting them with malicious software through targeted cyberattacks. Then, the infectedbotnet computer network can be launched

without the knowledge of computer users to initiate large-scale cyberattacks which can usually cause serious damage.

It has also been noticed that the information systems are a key element of political, social and economic relations in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union are vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of the information systems should form part of an effective and comprehensive framework of preventive measures accompanying criminal law responses to cybercrime.

The objectives of the new directive highlighted the approximation of the criminal law of the Member States in the scope of attacks on information systems by establishing minimum rules on the definition of crimes and appropriate penalties, and improving cooperation between competent authorities, including police and other specialized law enforcement agencies in the Member States, as well as relevant specialized agencies and the Union bodies such as EUROJUST, EUROPOL and its European Cybercrime Centre and the European Network and Information Security Agency (ENISA).

It was also stressed that significant gaps and differences in the Member States' laws and criminal procedures in the area of attacks against information systems may hamper the fight against organised crime and terrorism and may complicate effective police and judicial cooperation in this area. The transnational and cross-border nature of modern information systems gives attacks against such systems a cross-border dimension, thus underlining the urgent need for further action to approximate criminal law in this area.

It is noteworthy that this directive not only refers to common computer crimes, but also includes potential terrorist attacks against critical infrastructure of the Member States. Compared to the previous EU regulations more emphasis was put on these types of threats.

Summary

Ensuring cyberspace security is nowadays a key challenge for the globalizing world. The development of communication techniques and tools: communication satellites, optical fibres, mobile telephony and internet, referred to as the information revolution, creates new civilization opportunities for societies and state economies, but at the same time creates new, previously unknown

fields for potential abuses. In order to implement harmonious, sustainable development of the world economy, but also to ensure peace and security in the world, it became necessary to identify these new threats related to cyberwar, cyberterrorism and, finally, common computer crime. This is not possible without universal, close cooperation of all sovereign entities and their organizations on the international stage. It is also necessary to engage and make aware of the existence of cybernetic threats to societies, in particular, the societies of developed countries, which fulfil their life needs on a daily basis via the internet and using modern technologies and devices. Awareness of threats at society level and harmonization of law at an international level are a necessity.

For over two decades, countries have been making efforts to identify cyber threats and harmonize legislation and cooperate in combating them. Despite this, there is still no global, universal agreement defining the basic threats in cyberspace, and there is no agreement as to which of them should be described as crimes. Although most countries and a number of regional organizations have introduced the provisions and framework of legal cooperation necessary to combat cybercrime over the past 20 years, and thus some harmonization of material and procedural norms can be seen, legal differences remain significant. There are many reasons why this is so. Firstly, a criminal act alone can result in negative consequences with varying degrees of intensity in different countries. In particular, hacker attacks can be carried out from so-called developing countries, third world countries, in which criminal legislation is not keeping pace with the globally developing technical civilization, against highly developed, industrialized and largely computerized countries. The negative effects of such attacks will then be felt by rich, high tech Western societies. On the other hand, they will not be noticed by the societies of the countries from whose territories such attacks were carried out. In such a situation, there may be a lack of understanding on the part of developing countries and societies, and justified irritation on the part of industrialized countries and societies. Secondly, the approach to law enforcement and the scope of civil liberties in various countries is disputed.

What is unlawful in one country is considered as an obvious exercise of freedom in another. Therefore, approximation and harmonization of the approach to law is necessary if international investigations carried out by national prosecutors are to be effective. However, this postulate is not easy to implement due to the significant development and cultural differences of contemporary states and their societies.

Despite the lack of an international agreement of a universal scope, there are regional conventions and bilateral agreements based on which cooperation in the area of combating cybercrime is implemented. The Council of Europe Convention on Cybercrime of 2001 remains the most important regional agreement.

Other documents, such as the Commonwealth of Independent States on cooperation in combating offences relating to computer information of 2001, the Agreement of the Shanghai Cooperation Organization on Cooperation in the Field of Assuring International Information Security of 2009, the Convention of the League of Arab States on Combating IT Crime of 2010 or the African Union Convention on Cybersecurity and Protection of Personal Data of 2014 have smaller range of impact. Nevertheless, they are an important element of the harmonization of law regarding prosecution and punishment of acts that violate the freedom and security of cyberspace.

In addition to the above-mentioned regional international agreements devoted entirely to combating threats in cyberspace, there are also bilateral initiatives implemented between states, also in the form of bilateral international agreements devoted to these threats. Unfortunately, these are individual initiatives which cannot significantly affect the increase in the level of cybersecurity. Cooperation between law enforcement agencies of different countries can and is being implemented based on traditional instruments not solely devoted to computer crime, i.e. based on cooperation and legal assistance agreements. The main limitation of this method of cooperation results from the fact that most of the legal aid treaties currently in force in bilateral relations between states are based on the principle of "double criminality", i.e. only if the act is illegal in both countries, legal assistance may be provided. For this, universal harmonization of regulations is required. At this point we return to the starting point, i.e. to the statement about the political, economic and cultural diversity of the modern world.

An important element in the landscape of activities aiming at improving security in cyberspace is the regulatory and operational activity of regional international organizations equipped with the statutory competence to legislate directly or through an institution mandatory implementation of resolutions into the legal orders of the Member States. The European Union, which brings together rich, highly developed Western countries, takes the lead in this category.

The above considerations refer primarily to cooperation between states in combating common computer crime, which is in fact the most common and

burdensome phenomenon in the modern computerized world. There are no regulations in the form of an international agreement, whether universal, regional or even bilateral, which would comprehensively address the issue of cyberwar and cyberterrorism.

Although there are some references in the documents analysed in this work to the issues of combating international cyberterrorism and a mention of the use of ICT in activities supporting military aggression, there is no comprehensive regulation of these problems at the international level.

The most widely discussed issue of new information technologies that can be applied in both the civil and military sphere, raising the importance of international information security as one of the key elements of the international security system, was addressed in the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security of 2009.

It is a pioneering international agreement relating to the issue of development and use of cyberweapons and preparation and conduct of an information warfare or the use of a dominant position in the information space to the detriment of the interests and security of other countries.

Noteworthy is the initiative generated within the United Nations, specifically within the United Nations Office on Drugs and Crime# (UNODC), in 2010 an international group of experts in the field of internet crime – UNODC – was established. The group of experts has been charged with the task of considering the possibility of developing effective methods to combat internet crime. The experts were tasked with analysing the existing judicial mechanisms, proposing their possible strengthening or proposing new national and international judicial measures or other effective measures against internet crime. The following legal issues were considered on the agenda of the first (and so far, only) meeting of the group: harmonization of legislation, substantive criminal law, procedural instruments, international cooperation in law enforcement, protection of electronic evidence, liability of internet service providers. Out-of-court measures and strategies, including technical investigative capabilities and defence strategies in the private sector against internet crime, have also been included. At this meeting, a list of issues was prepared and the scope and level of detail at which they should be considered by a group of experts was discussed. However, no specific proposals for action were made. Creation of international court for cybercrime did not appear at the time on the extensive agenda.

Bibliography

Literature

Adamski A., *Rządowy projekt dostosowania polskiego Kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości*, www.cert.pl.

Badźmirowska-Masłowska K., *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investement in the Common future*, Olsztyn 2013.

Cieślak D., *Konwencja przeciw cyberprzestępczości*, www. computerworld.pl.

Gady F.S., *Have China and Russia Agreed Not to Attack Each Other in Cyberspace?*, http://thediplo-mat.com/2015/05/have-china-and-russia-agreed-not-to-attack-each-other-in-cyberspace/.

Głowacka D., *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji*, http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf.

Kraft W., Streit C., *Ideas on the Establishment of an International Court for Cyber Crime*, World Council for Law Firms and Justice (WCLF) 2011.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Legal acts

Decyzja Ramowa Rady w sprawie ataków na systemy informatyczne z dnia 24 lutego 2005 r., nr CELEX 3200F0222.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/ WSiSW, nr CELEX 32013L0040.

Dyrektywa Parlamentu Europejskiego i Rady w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej z dnia 12 lipca 2002 r., nr CELEX 32002L0058.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 r., nr CELEX 32013R0526.

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Europejską Agencję Bezpieczeństwa Sieci i Informacji z dnia 10 marca 2004 r., nr CELEX 32004R0460.

Międzynarodowe regulacje prawne w dziedzinie cyberbezpieczeństwa

Streszczenie

Artykuł dokonuje zestawienia i analizy aktów prawa międzynarodowego poświęconych problematyce cyberbezpieczeństwa. W pierwszej kolejności dokonano analizy wielostronnych umów międzynarodowych. Następnie analizie poddano dwustronne umowy międzynarodowe oraz uchwały o charakterze prawotwórczym organizacji międzynarodowych. Na tej podstawie sformułowano wnioski dotyczące zakresu i form współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa.

Słowa kluczowe: współpraca międzynarodowa, cyberbezpieczeństwo, zagrożenia, umowy międzynarodowe, polityka bezpieczeństwa, organizacje międzynarodowe, prawo międzynarodowe