TACKLING CYBERSPACE THREATS – THE INTERNATIONAL APPROACH

LTC Grzegorz Pilarski, Ph.D. Eng.
War Studies University, Faculty of Military Studies, Cyberspace Security Branch

Abstract

The fact that NATO has acknowledged cyberspace as the fifth dimension of combat operations indicates that this problem issue is really topical and is pointing at the direction from which the possible threat can be expected. However, the issues of information communication technology (ICT) security on the national level have been tackled in numerous countries for many years. Technological advancement has resulted in making communication, and at the same time services rendered in cyberspace, an international domain. Thus, the aspects of cyberspace threats should be considered through the international prism. The above-presented approach has become an incentive for the author to take up research on international activities in terms of cyberspace defence and reaction to the already identified as well as future threats.

Keywords: cyberspace, cyber defence, cybercrime, information communication technology (ICT).

Introduction

What is cyberspace and the interrelated phenomena? This question as along with many others is presently top topic in many countries worldwide among politicians, scientists, media representatives and ordinary people. It is enough that the media presents information about some hacking activity and each of us starts thinking whether we can be personally affected by hacker attacks.

Information on cybercrimes committed by organised international criminal groups is getting more and more publicity. Thus, it can be assumed that the aspects connected with cybercrime should be overseen by state organisations in order to assure that common citizens can safely function in the cyber-environment. The case outwardly looks easy within the area of one country, since it is enough to implement an Act and it is expected that everyone should observe the law in force. However, it should be remembered that the activities of cyber-criminal groups do not accept territorial borders and they operate worldwide. Here the problems emerge in terms of certain normative acts which will be fully observed by many countries. Undoubtedly, this is a difficult and time-consuming process and the adopted course of activities is very often not in line with the up-to-date ways of fighting used by the criminals. Everything comes down to one thing: providing the country with 'the ability to protect or defend the use of cyberspace against cyber attacks'[1]. The quoted definition of cyber-defence sounds very simple and it seems that the world is able to deal with the problem. Still, the research conducted by the author indicates that the problem issue is still complex and difficult to tackle on the international scene. The author analysed the present state of affairs by asking a question: what initiatives have been undertaken in the field of counteracting cyberspace threats on the international scene? In the process of finding an answer to the presented question, the author will firstly focus on the terminological analysis pertaining to cyberspace, and then he will indicate the chosen initiatives which have been undertaken on the international scene in the scope of cyberspace security and cybercrime.

Cyberspace – terminological aspects

Against all appearances, the concept of cyberspace in not a new term and its history dates back to over 30 years ago. At the beginning, the concept cyberspace was used in science fiction novels. It is very probable that its forefather was

1 The USA National Institute of Standards and Technology (NIST) - NIST security glossary: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf - access February 2017.

William Gibson[2], who in 1982 in his novel entitled 'Burning Chrome' wrote that cyberspace is 'A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding into the distance...'

The above description ushered in the deliberation on the essence of cyberspace pointing to some basic environmental attributes of network such as: global range (extent), even indicating the so called non-space understood as the inability of telling the dimensions as it is in case of the real world, a giant space of data, joint use of varied resources, etc.

A further step was to make the concept, which was differently presented in different parts of the world, sanctioned by law. The definition elaborated by the United States Department of Defence defines cyberspace in the following way: 'A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)'[3]. Cyberspace resembles a nervous system – a control system of the state. It consists of a big number of interconnected computers, routers, servers, net active devices interconnected by optical fibres, which allow for the operation of a critical infrastructure.

The European Commission in the dictionary of concepts referring to the defence of EU cyberspace suggested the following definition of cyberspace: 'the virtual global and common domain within the information environment consisting of all interconnected and interdependent networks of global, organisational and national information infrastructure, based on the Internet and telecommunications networks, to be extended by other networks, computer systems and embedded processors, and also containing stand-alone systems and networks'. The subject of

2 William Gibson – American science fiction writer, forefather of the so called cyberpunk.

3 *Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff USA, February 2016, p. 58.

analysis is a physically non-existing but logically isolated space consisting of data, files, Internet websites, applications provided by ICT systems.

Another approach to the term was presented in 2011 by the Office of the Prime Minister of Great Britain in a document entitled: *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*[4]. The document provides the following definition of cyberspace: 'an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances'. An amendment to the concept was included in a document entitled: *National cyber security strategy 2016–2021*[5], defining cyberspace as 'the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, Internet-connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept".

While the definition provided by the French Agence nationale de la sécurité des systèmes d'information (ANSSI) proposed in 2011 does not directly touch on the aspect connected with users, economic or social phenomena emphasising only the technical aspect indicating that cyberspace[6] means "the communication space created by the worldwide interconnection of digital data processing equipment".

Also, NATO presents the definition of cyberspace in a document 'Cybersecurity. A generic reference curriculum', defining the concept as 'the electronic Word created by interconnected networks of information technology and the information on those networks'[7].

4 *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, Cabinet Office, London, November 2011, p. 10.
5 *National cyber security strategy 2016-2021*, HM Government, 2016, p. 75.
6 *Information systems defence and security France's strategy*, February 2011, p. 21.
7 *Cybersecurity. A generic reference curriculum*, 1217-16 NATO Graphics & Printing, ISBN 978-92-845-0196-0, p. 63.

In Poland, the definition of cyberspace was placed in the amendment to the Act of 30th August 2011 on the state of war and the powers of the Commander-in-chief and the rules governing his subordination to the constitutional bodies of the Republic of Poland. In accordance with the document, cyberspace is defined as 'a space of processing and exchanging information created by the ICT systems, as defined in Article 3 point 3 of the Act of 17 February 2005[8] on the informatisation of entities performing public tasks (OJ No. 64, item 565, as amended), together with links between them and the relations with users; in accordance with Article 2 paragraph 1b of the Act of 29 August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces as well as the Commander's subordination to the constitutional authorities of the Republic of Poland (OJ No. 156, item 1301, as amended), Article 2 paragraph 1a of the Act of 21 June 2002 on the state of emergency (OJ No. 113, item 985, as amended) and Article 3 paragraph 1 point 4 of the Act of 18 April 2002 on the state of natural disaster (OJ No. 62, item 558, as amended)'.

On the basis of the Polish definition of cyberspace, it should be emphasised that the legislator implements the idea of one cyberspace as a digital space to process and exchange information which is formed from ICT systems interlinked with one another through the ICT network. The digital space is not only used for information exchange but it can also be used to assure processing, storing or reading information. Moreover, it is vital, as indicated by the legislator, to take into consideration relations between systems and mutual relations between users and systems stressing at the same time bilateral connections between operations in the space as well as those performed in the physical reality.

Taking into account the quoted definitions of cyberspace, it should not be forgotten that it is most of all used for communication taking into account the human and social factor. The essence of person's functioning in society is communication with its members, which holds out the prospect of the exchange of thoughts and of joint operation. The ability of interdisciplinary communication is the basis of

8 The document determines that the IT system – a group of IT devices and software cooperating with one another which assures the processing, storing, as well as sending and receiving data via ICT networks through a user's device proper for a given type of ICT network in accordance with the Act of 16th July 2004 – ICT law (Journal of laws of 2014, item 243 and 827).

contacts between people and the lack of such skill can result in loneliness, as well as in the feeling of dissatisfaction and helplessness which can be expressed by failures in private life.

American Initiatives

In the world of standardisation, the United States mostly prevails due to its dominant technical-economical standing. A special role is played by standards and criteria concerning the protection of information and the security of IT systems. The providers of services as a response to state orders have to comply with the standards implemented by the US Department of Defence as well as proper governmental agencies such as:

- National Institute of Standards and Technology (NIST) – elaborates standards connected with computer systems which are presented in different publications by the Federal Information Processing Standards (FIPS);
- National Security Agency / National Computer Security Centre (NSA/NCSC) elaborates standards connected with information protection.

In the field of international standardisation, there are also other associations and firms e.g.:

- American National Standards Institute (ANSI) American normalisation organisation cooperating with the International Organisation for Standardisation (ISO);
- RSA Data Security – a company that develops and improves the technique of public-key encryption;
- Institute of Electrical and Electronics Engineers (IEEE) vocational association which introduced, inter alia, the Standard for Interoperable Local Area Network and Metropolitan Area Network Security (SILS) standardising the rules governing the protection of the local and metropolitan networks according to the Open System Interconnection (OSI) model.

Due to the increase in the number of cyber threats witnessed in recent years, many countries and international organisations have started discussion on the future of cyberspace. According to the experts, many out of varied initiatives are of local or regional character; however, it is a must to take action of a global character in this

field. As an example of this kind of initiative, one can take the proposal of the United States in the scope of an international strategy for cyberspace[9]. In May 2011, the US administration officially presented the strategy, emphasising that beyond the issues of cyberspace security, it is necessary to face the issues pertaining to the development of the internet for the benefit of supporting freedom, democracy, and peace in the world. The document was prepared in consultation with eighteen American departments and it is not only a technical solution but it also describes the vision of the future cyberspace proposed by President Barack Obama.

The strategy is a kind of a 'road map' for American governmental institutions, whose common direction of operation is the construction and maintenance of an *open, interoperable, safe and reliant global network*[10]. It is the first global proposal of internet development. Due to the fact that no independent country or organisation is able to decide about the future and the security of cyberspace by itself, the United States have put forward an initiative to build an international 'cyber-coalition'. The vision of future cyberspace is based on seven priority areas[11]:

a. economy – activities connected with international standards of the free market and the protection of the intellectual property;
b. network protection – activities connected with the creation of international partnerships for the creation of consistent norms concerning cyberspace safety; the increase of security and the reliability of network; the creation of international systems of response to crisis situations;
c. law enforcement – activities connected with the creation of a consistent international policy for the fight with cybercrime in accordance with the existing conventions;
d. military cooperation – activities connected with the creation of new and strengthening of existing alliances in order to adjust the armed forces to new threats to the security of the military network;

9 Vide *International strategy for cyberspace* on: www.whitehouse.gov/sites/default/files/rss_viewer/ international_strategy_for_cyberspace.pdf
10 Ibidem, p. 5.
11 Vide M. Grzelak, *Międzynarodowa strategia USA dla cyberprzestrzeni*, kwartalnik Bezpieczeństwo Narodowe II-2011/18.

e. management of the global network – activities aiming at the support of openness and innovation in the internet through, inter alia, the creation of a safe and stable infrastructure;
f. international development – activities for the creation of global society responsible for the development of the cyberspace;
g. internet freedom – activities promoting the support of civil rights, the freedom of speech, protection of data and privacy as well as guaranteeing free flow of information on the internet.

The United States is to be the leader, thus particular areas of activities will be divided between US departments and agencies, which are to cooperate with overseas partners and the private sector.

The affairs directly connected with cyber security mostly refer to activities such as network protection, legislation and law enforcement as well as military cooperation.

In order to increase the safety of the global network, the United States intend to develop cooperation with other countries and organisations for the construction and protection of the critical infrastructure and the creation of norms for safe existence in cyberspace. Moreover, they are also going to develop abilities in the scope of monitoring, warning and response to computer incidents through the created procedures referring to the operation and exchange of information, as well as joint exercises with partners. The issue of core importance is legislation which should constitute the framework for activities in accordance with the letter of law which pertains to the prevention and consistent punishment of those who are found guilty of crimes in cyberspace.

In the United States, the repertory of standards referring to the storage of information and its protection is presented in the so called 'colourful books'. The most famous is the Orange Book, which represents Trusted Computer System Evaluation Criteria (TCSEC)[12].

This book was mainly intended to be useful for producers, as the guidelines specifying which means of protection, from the point of view of information

12 D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji,* Warsaw 2002, p. 430.

protection, should a product be equipped with, which category of protection does the product fall into, and it aimed at the creation of the basis for the determination of safety requirements in the products' specifications.

European initiatives

In Europe, there are several main standardisation organisations dealing with the preparation and the oversight of the process of uniting Europe in terms of normalisation. The organisations participate in the creation and development of regional and international standards of open systems defence. These are, inter alia:

- CEN (fran. *Comite European de Normalization*) deals with the unification of standards for information protection for the needs of ISO members;
- CENLEC (fran. *Comite European de Normalization Electrotechnic*) focuses on the cooperation with the European members of International Electrotechnical Commission (IEC);
- European Telecommunications Standards Institute (ETSI) prepares ICT standards supporting the European members of an international organisation, namely International Telecommunications Union Telecommunications Standardisation Sector (ITU-T);
- European Association for Standardising Information and Communication Systems (Ecma International) former European Computer Manufactures Organisation (ECMA) supports international ISO organisations, IEC as well as ITU-T providing designers with standardisation materials concerning problems in the scope of information protection and the safety of open systems;
- British Standards Institution (BSI) dealing with the problem issues concerning ICT security – the institution prepared the BS 7799 standard.

BS 7799 is one of the most popular standards in Europe, which at the same time constitutes international norms. The document is divided into two parts:

- the first one entitled '*Code of practice for Information Security Management*' includes definitions of control points out of ten key topics such as: security policy, security organisation, security vs personnel, management of computers as well as the computer network, control of access to the system, planning continuity of business processes, etc.;

– the second one entitled '*Specification for Information Security Management Systems*' includes a description how to implement the recommendations from the first part.

In Europe, similarly to America, certain criteria have been prepared for the assessment of the safety of products in many aspects starting from the design, up to the documentation and the preferred exploitation environment. The document was prepared in cooperation with Germany, France, Great Britain and the Netherlands and is known under the name Information Technology Security Evaluation Criteria (ITSEC). The criteria allow for the assessment of ICT systems, encryption devices from their first beginnings, namely the design phase, cost analysis, the level of security dependant on the weight of the protected information and the number of used measures.

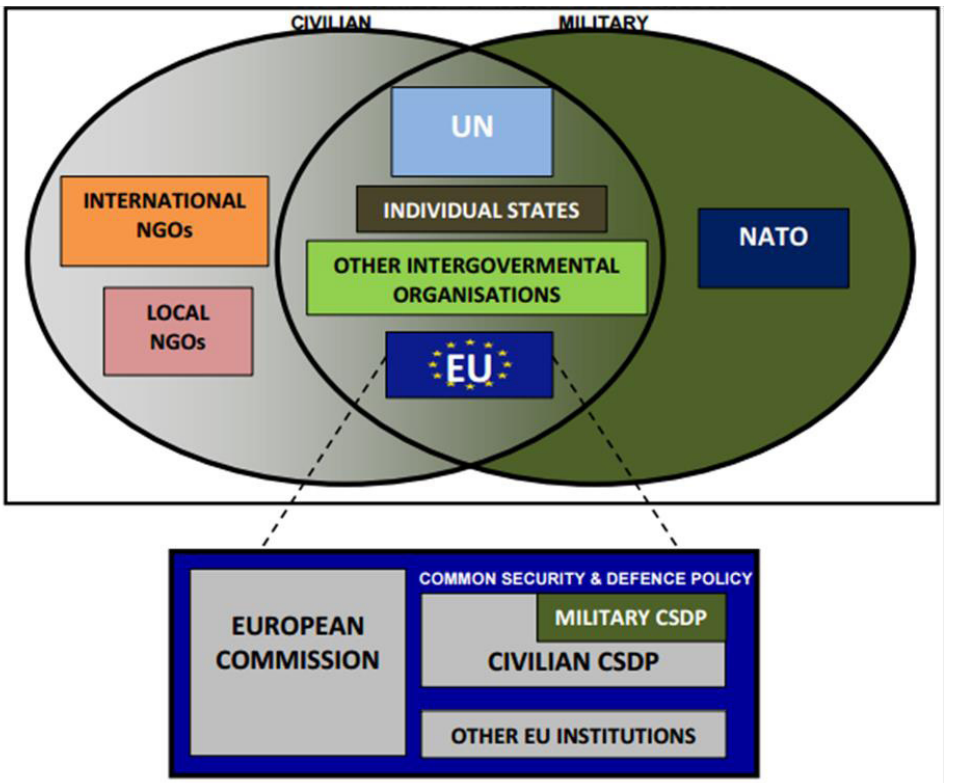
On the 7th of February 2013, the EU published a document entitled 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'. The document presents a complex approach to the issues of ICT security taking into consideration all EU member states. The strategy is a document which should be a pattern for member states to follow with the creation and implementation of national strategies in their own countries. The strategy is also a starting point for the elaboration of the concept of military operations in the EU, for example the division of civil-military roles in the process of cyberspace security management (Fig. 1.).

The figure above illustrates the roles played by civilian, military, and a mixture of both participants in a typical cyber management scenario.

The issues pertaining to computer crime became the focus of attention of The Council of Europe in the 1980s. The first initiative was connected with calling into being a team of 15 experts, called *Expert Committee*. The group of experts was tasked with dealing with the legal aspects of computer crime.

Another vital step was calling into being a committee of experts[13] named The Committee of Experts on Crime in Cyberspace – (PC-CY) by the European Committee on Crime Problems (CDPC). The first task of the committee was the commencement of work on an international project for the creation of cybercrime convention.

13 Vide By decision CDPC/103/211196.



Source: Major General Maurice de LANGLOIS Andreas CAPSTACK, The role of the military in the EU's external action, IRSEM, 2014 No 23, ISBN 978-2-11-138614-3, p. 10.

Fig. 1. The role of the military in the EU's external action: implementing the comprehensive approach

In April 2001, after many meetings and negotiations in the international environment, the project of the European Council Convention on cybercrime (ETS/STE no. 185) was accepted. The convention on counter-fighting cybercrime was signed in Budapest by 30 member states and 4 states out of the EC who participated in the negotiation over the document – Canada, the USA, Japan, and South Africa. Numerous documents refer to the need for the implementation of regulations included in the EC Convention. Good examples of such documents include e.g. Internet Governance Strategy 2012-2015 or The protection of freedom of expression and information on the Internet and online media (Resolution 1877 - 2012).

International initiatives

Presently, the topic of cyber defence and cybercrime is commonly raised by many countries and organisations all over the world which have global influence on the security of cyberspace; the organisations include: the G8 Group (G7), the United Nations and the International Telecommunication Union. The author, in this part of the article, focused on the presentation of the world biggest organisation with response teams and security teams from all over the world in its ranks, namely FIRST[14] with its full name Forum of Incidents Response and Security Teams.

FIRST is a renowned world leader in the reaction to incidents in the scope of computer security. Membership of the organisation ensures that the response teams are the most effective in terms of ensuring security, providing access to the best practices, tools, and effective communication between trusted members of the teams.

The forum of teams consists of a network of particular teams of response to computer security incidents, which cooperate voluntarily in order to solve computer security problems as well as to prevent any attempts of breaching security. The teams represent governments, academic environments, the private sector, and other organisations interested in the problem of computer security.

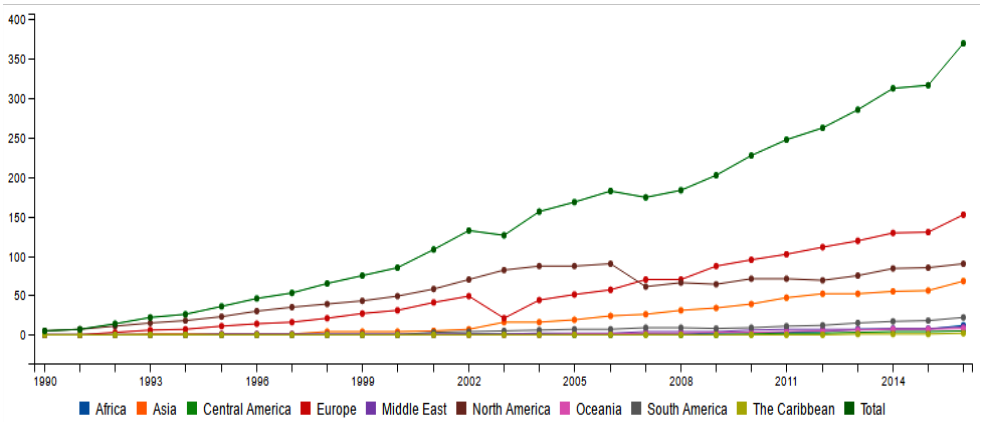
FIRST, as an international confederation of teams responding to incidents, mainly has the mission of:

- developing and sharing technical information, tools, methods, as well as best practices among the team members;
- encouraging and supporting the development of security, policy of products and services quality;
- developing and dissemination of the best practices of computer protection;
- supporting the creation and development of teams responding to incidents as well as members with organisations from all over the world;
- engaging teams and members in the promotion of knowledge, skills, and experience in the field of global cyberspace security.

14 Vide: www.first.org – access February 2017.

The first incident that exerted influence on the creation of FIRST took place in November 1988 and was the usage of an 'Internet worm called Morris', which paralysed the main areas of the internet. The reaction to the incident involved non-coordinated, often doubled efforts to solve the problem. Several weeks later DARPA[15] created the first Computer Emergency Response Team (CERT). During the ensuing two years, the next incident response teams were created, each with its own goal, financing system, and reporting scheme. Interaction between the teams posed a big problem in terms of language differences, time zones, as well as international standards and conventions.

In October 1989, as a result of an incident called 'WANK'[16], the need for better communication and coordination between CERT teams emerged. FIRST was created in 1990 as the answer to the problem. Since that moment, the organisation has evolved as the answer to the changing needs of particular response teams. Over the years, the number of FIRST members has increased. The tendency of the increase of interest in the membership in FIRST is depicted in Fig. 2.



Source: http://www.first.org/about/history - access February 2017.

Fig. 2. The tendency of the increase of FIRST members over years

15 DARPA - Defense Advanced Research Projects Agency – American governmental agency dealing with the development of military technology operating in the Department of Defence structures.

16 WANK - *Worms Against Nuclear Killers* – the worm had a vivid political envoi.

Alongwith the growth of the meaning of the internet to governmental organisations, the *Government Forum of Incident Response and Security Teams* (GRIST) was formed in 2003. The organisation consists of groups of technical experts and tactical response teams responsible for assuring security to the governmental IT systems. The GFIRST members cooperate with one another in the scope of the analysis of security violation incidents, as well as in terms of proactive and preventive security policy. GFIRST promotes full cooperation between federal agencies, including the defence department.

At the moment, FIRST is acknowledged on the international scene, specialising in fast propagation of information in the field of computer-related problems. Its most important task is to promote cooperation and coordination in the process of preventing incidents and at the same time to promote information exchange between CERT teams.

The Computer Emergency Response Team (CERT) entails expert teams, which deal with incidents breaching security in the internet network. The basic task of CERT is to oversee Internet traffic in 24/7 mode and to immediately take action in the event of any threats. CERT teams operate on the national level and they constitute expert subject in the field of cyber-security. The teams are partners for the government, industry, law enforcement institutions, and academic environment in order to elaborate advanced methods and technologies connected with counteracting sophisticated cyber threats on a large scale.

CERT specialists, who include scientists, programmers, analysts of security, and specialists of cyber intelligence, base their work on theoretical and empirical knowledge which allows the problems connected with security to be understood. Successive collections of information on incidents by teams all over the world allows the real situation of cyberspace security to be determined worldwide. Furthermore, the analysis of network traffic helps organisations to identify patterns which can indicate the attacks. Data bases with information concerning vulnerabilities in software security and malicious codes are used as the basis to prepare strategy and repair solutions in the scope of developer software.

CERT teams base their work on their own infrastructure, creating open-source tools to a series of operations i.e. discovering vulnerabilities, analysis of network traffic, etc. for the use of a wide circle of interested entities. The knowledge is

documented in different publications i.e. technical reports, articles, conference presentations, blogs and podcasts.

As for the pursuit for cybercrimes, CERT teams cooperate with enforcement agencies and intelligence services in order to ensure operational support. A wide spectrum of issues involves educational activities which aim at the perfection of the members of CERT teams and also at the support of interested subjects to improve cyberspace security in the field of their interest.
The main tasks of CERT teams include, inter alia:

- taking record of and administration of incidents breaching network safety;
- alerting users to direct threats;
- cooperation with other Incidents Response Team (IRT) in the framework of FIRST;
- running information-educational activities in the field of cyberspace security which has direct influence on the increase of internet users' awareness;
- posting up-to-date information on ICT security on the team's website;
- organising periodic topical conferences;
- running research and preparing reports on security in the region of CERT's operation;
- independent testing of products and solutions in the field of ICT security;
- works in the scope of creating patterns of dealing with and the record of incidents (classification and statistics);
- participation in national and international projects connected with ICT security.

The name CERT is a proprietary name, thus a group alternative to CERT can be the Computer Security Incident Response Team (CSIRT) as a team for computer security and response to incidents. The term CSIRT is mainly used in Europe instead of 'CERT', which is registered in the USA by the CERT Coordination Centre (CERT/CC). To refer to the same types of teams, the following varied names are used:

- Computer Emergency Response Team / Coordination Centre (CERT or CERT/CC);
- Computer Security Incident Response Team *(*CSIRT) team for computer security and response to incidents;
- Incident Response Team (IRT);

– Computer Incident Response Team (CIRT);
– Security Emergency Response Team (SERT) team for fast response to security threats.

CSIRT teams include experts in the field of IT security whose main task is to respond to incidents in the field of ICT security. The teams render services which are necessary to solve these types of problems and enable the users to restart they normal activity after their removal. In order to limit the risk and minimise the number of required reactions, most CSIRT teams also render prevention and education services to the users. They prepare newsletters concerning vulnerabilities in software and hardware security, and inform users about malicious codes and viruses making use of the weak points. Owing to that, the users can beef up and update their systems very fast.

Having a special team for IT security in an organisation facilitates the process of minimising the scope of serious incidents and counteracting them, as well as the protection of valuable assets. Other benefits include:
– centralised coordination of activities pertaining to the IT security within an organisation;
– centralised and specialised service and response to incidents in the scope of IT security;
– availability of expert knowledge, necessary to support users and help them in fast re-start of normal operation after the security-related incident took place;
– safeguarding legal issues and evidence in case of a trial;
– staying current with the development of situation in the field of security;
– stimulating cooperation in the scope of IT security within users' societies (awareness building).

Conclusions

At the time of information technology development as well as the increasing role of the internet globally, a lot of subjects which play a vital role on the international scene took the initiative for the benefit of cyberspace protection. At the beginning, the organisations operated in the scope of their own interest. However, new challenges from the criminal world and the growth of the territorial

area of cybercrime's influence indicated that there was a need for joint activity of organisations working for the benefit of cyberspace protection. International cooperation on cyberspace security footing is developing each year, but it is still not stable enough to effectively fight cybercrime. Reports and research carried out by expert teams in the field of ICT security indicate that there is a need for international cooperation in the scope of exchanging information on incidents of ICT security breaching. A network of CERT teams on the territory of the whole world is a good way to fight with cyber threats of the contemporary world. Still a question emerges as to whether additional solutions should be employed, solutions such as accepting legal mechanisms on international grounds that would regulate which cyber threats should be subject to pursuit and punishment. It seems to be a good solution to elaborate and accept strategies which would standardise the area of cyberspace security. However, the process is difficult to carry out and implement, due to the fact that standards and norms accepted by different countries very often rule out each other out. On the basis of the presented information, one can conclude that the issue of cyberspace security is a really vital topic on the international scene. Different institutions, most of all the governmental ones, are interested in the increase of ICT security contributing at the same time to an effective protection of their own data. Let us take as the example, inter alia, the agreement of 2016 between the European Commission and The European Cyber Security Organisation (ECSO) regarding innovative solutions in the field of cyberspace security. Another very important fact is the acknowledgment at the NATO summit in Warsaw that cyberspace next to land, sea, airspace and aerospace is another area of combat operations. The step taken by NATO member states will result in the intensification of operation on the international scene, and cooperation with industry and the academic world in one case, namely the security of cyberspace for all citizens.

On the basis of the research carried out in the scope of international initiatives for the benefit of the protection of cyberspace, the author concludes that the activities presently in this scope within a given country of territory are not enough to effectively fight international cybercrime; however, mental progress is visible among international actors and it might shortly lead to a change in the present state of affairs in order to try to be one step ahead of the cyber-criminal.

Bibliography

Cybersecurity. A generic reference curriculum, 1217-16 NATO Graphics & Printing, ISBN 978-92-845-0196-0.

Cyberspace protection policy of the Republic of Poland, Warsaw, 25 June 2013.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji,* Warszawa, 2002.

Department of Defense Dictionary of Military and Associated Terms, Joint Chiefs of Staff USA, February 2016.

EU Concept on Cyber Defence for EU-led Military Operations and Missions, Brussels, 14 November 2016.

Grzelak M., *Międzynarodowa strategia USA dla cyberprzestrzeni*, kwartalnik Bezpieczeństwo Narodowe II-2011/18.

Information systems defence and security France's strategy, February 2011.

Major General M. de LANGLOIS A. CAPSTACK, The role of the military in the EU's external action, IRSEM, 2014 No 23, ISBN 978-2-11-138614-3.

Kissel R., *Glossary of Key Information Security Terms*, National Institute of Standards and Technology, May 2013.

National cyber security strategy 2016-2021, HM Government, 2016, p. 75.

Pilarski G., *Ochrona informacji w sieciach komputerowych*, AON, Warszawa 2004.

The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, Cabinet Office, London, November 2011.

Ustawa z dnia 16 lipca 2004 r. - *Prawo telekomunikacyjne* (Dz. U. Nr 171, poz. 1800, z późn. zm.).

https://www.ecs-org.eu/ - access February 2017.

http://www.nato.int/ - access February 2017.

http://www.first.org/ - access February 2017.

https://www.cybsecurity.org/ - access February 2017.

http://www.cert.gov.pl/- access February 2017.