БЕЗБЕДНОСНИ ДИЈАЛОЗИ / SECURITY DIALOGUES

ISSN 1857-7172
eISSN 1857-8055
Година 11, Број 1, 2020/Vol. 11, No. 1, 2020

ISSN 1857-7172
eISSN 1857-8055
OPEN ACCESS
http:// sd.fzf.ukim.edu.mk

Издавач/Publisher

Филозофски факултет – Скопје/Faculty of Philosophy – Skopje
Институт за безбедност, одбрана и мир/Institute of security, defence and peace
Уредувачки одбор/Editorial board: тел. (+389) 2 3066 232, email sd@fzf.ukim.edu.mk

Компјутерска обработка:
МАР-САЖ

Печати:
МАР-САЖ

Тираж:
100 примероци

Ss. Cyril & Methodius University in Skopje, Faculty of Philosophy - Institute of Security, defence and peace has entered into an electronic licensing relationship with EBSCO Publishing, the world's most prolific aggregator of full text journals, magazines and other sources. The full text of Security Dialogues can be found on the following EBSCO Publishing's databases collections: International Security & Counter-Terrorism Reference Center.

CONTENTS

Original Scientific Articles

Review Articles

355.02:004]:340.13 – 355.02:004]:341.24 Review Article

LEGAL ASPECTS OF SECURITY IN CYBERSPACE

Biljana **KAROVSKA-ANDONOVSKA**, PhD
Military Academy "General Mihailo Apostolski" - Skopje
E-mail: biljana.k.andonovska@morm.gov.mk

Nenad **TANESKI**, PhD
Military Academy "General Mihailo Apostolski" - Skopje
E-mail: nenoreal@yahoo.com

Abstract: Cyber is a relatively new, virtual space, where intensive communication, business, banking, criminal, and military activities are in progress. Those activities create effects that national legal systems and the international legal order have never faced before. These features and capabilities of cyberspace open a number of substantive legal and security issues and dilemmas. Regulation of cyberspace with legal norms is one of the biggest challenges that modern states face. There is a widespread debate in various areas of law regarding the applicability of existing legal rules and standards in cyber space. At the same time, efforts to generate new rules specific to cyber space are being made, where existing rules cannot be properly applied. For certain topics opinions are divided and some issues remain open. This paper provides an analysis of the legal aspects of the functioning in cyberspace, as well as a review of the process of normative regulation in this space, with a special focus on European legal regulation. The paper emphasizes the spheres of law which, according to the authors' opinion, are most affected by the implications of cyber activities, and consequently show the most significant step forward in terms of creating a legal framework that forms the basis for security in cyberspace.

Keywords: cyberspace, legal aspects, cyber security, cybercrime, cyber warfare.

1. Introduction

The development of information and communication technologies has made significant changes in all spheres of social life. The functioning of modern societies and modern man today is subordinated to these technologies and almost dependent on them. This connection and dependence brings risks and threats to possible negative effects. With all its specific features, virtual cyber space is an ideal environment not only for communication and economic activities that make life and work easier, but also for criminal, terrorist and military actions.

Cyber threats began to attract attention in the late 90s of the 20th century. However, the problem began to be seriously treated when severe cyberattacks occurred in certain countries (for example, the cyberattack in Estonia in 2007 and a series of other attacks that followed, as

in Georgia in 2008 during the war with the Russian Federation, cyberattack with Stuxnet worm in 2010 on nuclear facilities in Iran, etc.). After these events, the global perception of cyber threats has changed dramatically. Political and ideologically motivated cyberattacks on critical infrastructure have been a wake-up call for security experts and have shown there is a price to pay for an advanced information society (Tikk, 2011). Through these developments the world has faced the fact that a cyberattack can paralyze entire systems in one state or in multiple countries simultaneously. Security incidents in cyberspace are expected to become much more prevalent in the future, due to the facts that more and more people are becoming "computer smart" all over the world; bad actors of many different types are becoming more and more aware of opportunities in cyberspace; connectivity is becoming more widespread and universal; more and more systems and infrastructures are shifting from mechanical/electrical control to electronic/software control; and human activities in cyberspace are expanding much faster than security efforts (Hundley and Anderson 1995/96). However, one of the biggest challenges related to security in cyberspace is the fact that from a legal point of view this space is still a matter that is not fully regulated. As a result, to all of these trends and dynamics political leaders, planners and operators face unusual challenge (Hadji-Janev 2016, p. 423). For these reasons, today a global debate takes place on the applicability of existing standards and rules in different areas of law in cyberspace. At the same time, efforts are being made in order to generate some new rules that are specific to cyber space. On certain topics the opinions are divided and some issues are still open.

2. Legal aspects of cyber security

The term "Cyberspace" was first used by William Gibson in 1984 in his science-fiction novel "Neuromancer" as a term for denoting network connectivity and communication on computers. Cyberspace is not in itself a place; it is an activity, a complex type of mediated communication (Appazov 2014, p. 8). In other words, it is an intricate, multilayered communicative process that is sustained by a series of increasingly complicated technologies (Brenner 2002, p. 9). As such, cyberspace is a global information environment that includes individuals, groups and institutions that exchange information and data electronically through thousands of computers, fiber cables, servers, and routers. Due to the characteristics of cyberspace, the implications of the activities being undertaken in this space can be felt simultaneously in many countries, and each country is almost equally vulnerable in this context.

These features of cyberspace allow it to carry out specific processes and actions that create effects that national legal systems and the international legal order have never faced before. Cybersecurity often is conflated, particularly in legal circles, with data security. Although data security is an important part of cybersecurity, it is only one part because cybersecurity focuses not only on the protection of data, but also on the systems and networks of the public and private sector (Kosseff 2018). Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization

and user's assets. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise: availability; integrity, which may include authenticity and non-repudiation; and, confidentiality.[35]

In cyber security the assets that need to be protected can range from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure (von Solms and van Niekert 2013, p. 100). Attacks that have implications on national security test the existing national laws, the international legal framework and the basic international principles of jurisdiction, according to which each sovereign state regulates the activity and communications that take place on its territory. Furthermore, cyber attacks with national security implications test the limits of the existing legal framework for data protection, electronic communications and access to public information (Tikk 2011, p. 3).

Due to the fact that cyberspace is a unique space with no boundaries, it cannot be entirely regulated with traditional rules according to which the geographical territory or physical location is relevant. To be more precise, traditional rules related to the territory or related to the place of undertaking a particular activity, are necessarily determined in this context by the specifics of the cyber space. An additional problem and concern is the fact that there is no central entity under which the global Internet platform, as a system of interconnected computer networks, is managed. There is no one universal model for Internet content regulation. There are regulations related to the Internet which are usually country oriented and parts of the Internet are regulated under different approaches. Ultimately, each country's regulation of the Internet is driven not by technology or law but by the culture-in the broadest sense of the word-of the society (Hwa 2016). This certainly limits centralized control of the Internet by one entity.

3. Regulation of cyberspace with legal norms

The regulation of the cyberspace with legal norms is the starting point and assumption for building a secure cyber environment. In this regard, some logical and debatable questions arise: Is it possible to regulate this boundless space with legal norms at all? How to regulate behavior in a space that has no physical boundaries? Who should regulate the rules in cyberspace? Can cyberspace be controlled? Up to which level should behavior in the cyber space be regulated, without endangering certain human rights and democratic values? And finally, the question: Who should control the cyberspace and the activities in that space?

Cyberspace exists for many years now, and there has been significant progress in adapting national and international law in many areas related to cyber security which is a continuous effort over the years. One of the probably most significant and logical questions that arise in this context is the issue related to all previously mentioned questions and actually refers to jurisdiction in the cyberspace. Moreover, the answers to questions about the applicability of the basic

[35] See: Definition of cybersecurity, referring to ITU-T X.1205, Overview of cyber security, available at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

principles of International Public law in cyberspace (the principles of non-intervention, peaceful resolution of disputes, respect for human rights, reciprocity, etc.) largely depend on the answer to this question, as well as the answers to the questions of responsibility for committing unauthorized cyber activities, identification of responsibility, compensation for caused damage, etc. In spite of the belief that cyberspace cannot be regulated by legal norms or that it is beyond the reach of the law or the authorities of one state or the international community, Lessig (1999, p. 10), for example, considers that this belief about cyberspace is wrong, as well as the assumption that the nature of cyberspace is fixed and that there are no steps that can be taken in order to change its architecture. Namely, he thinks that cyberspace does not actually have nature and that cyber space does not actually have concrete architecture that cannot be changed. In his new edition of this book, Lessing explains that "Regulability" in the context of the Internet means the ability of the government to regulate the behavior of (at least) its citizens while on the Net. He also stressed that there is regulation of behavior on the Internet and in cyberspace, but that regulation is imposed primarily through code. The differences in the regulations effected through code distinguish different parts of the Internet and cyberspace. Some architectures of cyberspace are more regulable than others; some architectures enable better control than others. Therefore, whether a part of cyberspace-or the Internet generally-can be regulated turns on the nature of its code.

There is no doubt that the creation of the cyber rules is not impossible; however, it is certainly a complex process with many unknown elements. Additionally, this process is difficult because of the fact that information technology is developing extremely rapidly and the Law cannot follow this pace. Therefore, sometimes it seems easier to adapt the existing legal norms from different areas of law instead to create some new rules. Hence, regulation of relations in cyberspace with legal norms generally takes place in two ways: through the applicability of existing legal regulations, principles and adopted standards; and by finding consensual solutions where the existing rules cannot be properly applied. In doing so, it seeks to set a minimum legal framework specific to cyberspace.

The levels and sources of law relating to cyber security range from the soft (standards and best practices) to organizational (contracts and internal regulations) to national to international agreements and customary law, which inform the four key legal areas the law of network and information security (also referred to as cyber law or information-society law), dealing with, for example, data protection, e-commerce, electronic communications and access to information; criminal law (offences, investigation, cooperation); national-security law and possible restrictions to human rights and liberties resulting from national-security concerns; and the Law of Armed Conflict (Tikk 2011). According to the abovementioned, the following are certain basic approaches for regulation of cyber activities and sources of Law related to cyber security:

- National laws that regulate issues of cybercrime, personal data protection, intellectual property, communication and publication of information;
- International acts which regulate the issues relevant to cyber security;

- Established standards and good practices (Soft Law) as a voluntary and loose form of international regulation of certain issues related to the functioning and security of cyberspace;
- Organizational regulations (contracts and internal acts);
- he architecture of computers which is relate to information transfer in cyberspace;
- The Customary Law and moral norms that, relatively speaking, control the behavior of individuals in cyberspace in circumstances where laws will not manage to regulate certain activities the execution of which is enabled by the architecture of computers.

4. The role of the international organizations in creation of cyber secure environment at global and regional level

Cyber security and protection of critical information infrastructures are essential to each nation's security and economic well-being. Because of this, cyber security is a top priority for some of the relevant international organizations that are continuously actively addressing this issue. The legal, technical and institutional challenges posed by the issue of cyber security are global and far reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation (Gershe 2012). In this regard, on a global level, the UN adopted resolutions that treat the creation of a global culture for cyber security, the criminal misuse of information technology, the development of information technology and telecommunications in the context of cyber security, etc., as well as Action plan to combat cybercrime. The Global Cyber Security Agenda of the International Union of Telecommunications[36] is a global framework for dialogue and international co-operation for coordination of international response to the growing challenges of cyber security and for increasing trust and security in the information society. The Agenda is built on five strategic pillars (working areas): Legal measures; Technical and procedural measures; Organizational structures; Capacity building; International cooperation. According to this Agenda, the legal aspects should focus on the ways through which the state will handle with the legal challenges that are caused by criminal activities in an internationally compatible way. Furthermore, technical and procedural measures should focus on key measures for promotion and adoption of an approach aimed at improving security and risk management in cyberspace, including accreditation schemes, protocols and standards. Organizational structures refer to preventing, detecting, responding and managing cyber attacks, including the protection of critical information infrastructure systems. Capacity building should focus on developing strategies for capacity-building mechanisms aimed at raising awareness, transferring knowledge and strengthening cyber security. Finally, the international cooperation relates to cooperation, dialogue and coordination in dealing with cyber threats.

At the NATO level, cyber-security is adopted and adapted as central policy by the Heads of States and Governments, representing members of the Alliance. Private institutions/orga-

[36] https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

nizations that are leaders in creativity, innovation, and entrepreneurship in cyber-security and defense work along with NATO to create a resilient and robust protection mechanism against electronic threats (Efthymiopoulos 2019, p. 1). NATO strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application.

On a regional level it is important that in 2013 the European Union adopted a Cyber Security Strategy, which is the first comprehensive document on EU policy in this area, as well as an Action Plan on the safety of networks and cooperation of member states. Directives for electronic operation and for ensuring high level of security for networks and information systems have also been adopted. One of the major efforts within the framework of EU legislation aimed at enhancing the security of personal data in general, and in particular in computer databases is the Reform Package of Personal Data Protection documents adopted in 2016 and started to apply as of April 2018. The Reform Package includes the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Regulation (EU) 2016/679), as well as the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Directive (EU) 2016/680). The Regulation focuses on strengthening the rights of individuals, ensuring consistent implementation of rules, streamlining international data transfers and setting global data protection standards, while the Directive establishes a framework for the protection of personal data of persons involved in criminal proceedings.

On the other hand, in 2001, the Council of Europe adopted the Convention on Cybercrime (2001), one of the significant legal acts aimed primarily at creating a common criminal policy for the protection of society from cybercrime, which will be discussed in the next part of this paper.

5. Cybercrime in the context of cyber security

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment (Gershe 2012). Cybercrime is a complex phenomenon that takes place in the electronic environment. This complexity arises from the fact that this type of crime covers activities that are etymologically diverse, which in turn creates difficulties in their definition. Basically, cybercrime is any activity in which computers or networks are a tool, a target or a place of criminal activity. Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems.[37] There is a wide range of acts that can be considered as cybercrime. In general, it is a crime that can consist of an attack on information systems, on-line frauds, forgery of content on the Internet, including material for children sex-

[37] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

ual abuse, incitement of racial hatred, incitement of terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Due to the specificity and transnational nature of cyber activities, a comprehensive approach is needed for dealing with the cybercrime. The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced (Gershe 2012). Over the few past decades, various solutions have been implemented not only at the national, but also at the regional levels. Due to the constant technological development and because of the changing methods and ways in which computer crimes are committed, this topic remains a great challenge. In this sense, the evident fragmentation of national criminal laws is still the biggest challenge. It is one of the main reasons for global vulnerability when it comes to cybercrime. According to Blake, many countries, especially developing countries do not have criminal laws that specially address cybercrime, neither do they have adequate capacity to enforce the laws (Blake 2017, p. 11). On the other side, according to UN, 138 countries (of which 95 are developing and transition economies) had enacted such legislation, but still, more than 30 countries had no cybercrime legislation in place.[38]

Fragmentation has imposed the need for harmonization of national legislation because of the unique legislative response to this global phenomenon. In this regard, creating a common criminal policy for the protection of society from cybercrime is the main purpose of the abovementioned Council of Europe's Convention on Cybercrime. The purpose of this Convention was to foster the creation of an effective legal framework through the adoption of appropriate legislation and fostering international cooperation that would constitute an essential part of national cyber security strategies as a vital element in countering this kind of crime. The Convention has supplemented the existing rules and contributed to the creation of a common criminal policy aimed at an effective criminal investigation by collecting evidence in electronic form and intensive international co-operation. The Convention sets out legislative and other measures that should be taken at the national level in order to criminalize acts such as unauthorized interception, unauthorized entry into the computer system, counterfeiting and computer-related fraud, acts related to child pornography, as well as acts related to violations of other related rights. In countries that have ratified this Convention, the incrimination of underground activities in cyberspace is conducted in two ways: through classical incriminations that are now committed via computer; or as new incriminations typical for computer crimes that have previously been incriminated. This process assumes the adaptation of national legislation to modern technologies, the identification of gaps in existing criminal legislation or the creation of new legislation. Regarding procedural criminal legislation, the Convention foresees the adoption of legislative and other measures that will enable the undertaking of special investigative actions and procedures, especially in order to obtain evidence in electronic form.

Two years upon the adoption of the Convention on Cybercrime, an Additional Protocol to this Convention was adopted, devoted to the incrimination of acts of racism and xenophobia

[38] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

committed through information systems. The aim of this Protocol is to complete the provisions of the Convention in order to criminalize this kind of acts.

6. Applicability of International Military and Humanitarian Law in Cyber Context

From a military point of view, cyber space is already perceived as the fifth dimension of warfare, along the mainland, water, air, and the cosmos. In general, cyber warfare refers to the disposal or use of computers and computer networks in the context of interstate conflict. The term "cyber war" was introduced by the security experts Arquilla, J. and Ronfeldt, D. in 1993 as a term which describe the "future of warfare" in the context of an IT-driven transformation of military systems. Cyber war could be defined as type of warfare which includes cyberattacks by one country in order to disrupt the vital computer systems of another, especially for strategic or military purposes. The issues that arise in this type of conflicts are moving in the direction of whether and which of the basic principles of International Law, as well as Military and Humanitarian Law as part of International Law, are applicable in the case of cyberattack or inter-state cyber conflict.

A group of legal experts hired at the initiative of the NATO Center for Excellence in Tallinn, offered answers to many of these issues in 2013 when the document titled as - Tallinn Manual for International Law Applicable for Cyber Warfare, was published. The Manual is a comprehensive but non-binding document that answers questions on sovereignty and jurisdiction in cyber space and questions of control of cyber infrastructure in the context of the application of the right to armed conflicts, means and methods of cyber warfare.[39] This document does not treat cyber activities below the "use of force" level, such as cybercrime, cyber spying, intellectual property, human rights. The document also contains answers to the questions related to humanitarian protection in cyber-attacks. The first rule set out in the Tallinn Manual refers to the sovereignty of states and it is limited to the fact that the state controls the cyber infrastructure and activities related to the infrastructure in its sovereign territory and, in doing so, the state has to establish effective control over cyber infrastructure located in its territory (Rule 1). Accordingly, cyber infrastructure is under the legal and regulatory control of the state, and each state should ensure the security of cyber infrastructure by providing capacity to deal with threats, overseeing electronic communications providers and the balanced development of information society in the interests of national security. In doing so, state sovereignty protects cyber infrastructure regardless of whether it belongs to the government or to private entities, and independently for which purpose it is set. Regarding jurisdiction, the Tallinn Manual emphasized that the state has jurisdiction over persons engaged in cyber activities on its territory and over cyber infrastructure located on its territory, as well as externally, in accordance with the rules of International Public Law (Rule 2). Regarding the responsibility of the state, the Tallinn Manual points out that when a cyberattack is made through an information system located in a particular state

[39] The Tallinn Manual does not reflect NATO views nor the views of the NATO Center for Excellence, but only the views of the experts involved in its creation.

territory, it can be considered that the state committed the attack. Moreover, the Tallinn Manual addresses the basic principles underlying modern International Law, which refer to the prohibition of the use of force and the rule of non-intervention. Namely, a state must not allow cyber infrastructure located in its territory or under its exclusive control to be used for an act against another state that would cause damage to persons or objects under the territorial sovereignty of that state. Each state should refrain cyber operations that pose the threat of the use of force against the territorial integrity or political independence of a sovereign state or operations that do not conform to the goals of the UN. Individual or collective self-defense is justified if the cyberattack according to its scale and effects is at the level of a military attack, and if it really happened or cannot be avoided. Self-defense principles must respect the principles of necessity and proportionality. Assessment is made according to the severity and intensity, the military character, the involvement of the state and the consequences (victims and material damage). According to the Tallinn Manual, this right is also applied in facing a cyberattack by non-state actors, such as terrorists or rebel groups, IT companies and Internet providers. The UN must be informed immediately of the measures of self-defense that have undertaken. If the UN Security Council determines that a cyberattack is a threat to peace, violation of peace or aggression, it will approve the application of non-violent measures. However, if the Council assesses that such measures are not adequate, it will decide to apply measures using force, including appropriate cyber measures.

In 2017, an updated and significantly expanded second edition of the Tallinn Manual was published, which provided a comprehensive analysis of the applicability of International Law in cyberspace. As such, the 2017 edition covers a full spectrum of international law applicable to cyber operations ranging from peacetime legal regimes to the law of armed conflict, covering a wide array of International Law principles and regimes that regulate events in cyberspace. Some pertain to general international law, such as the principle of sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialized regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law, are examined in the context of cyber operations.

From the abovementioned, it can be concluded that the purpose of the Tallinn Manuals is to clarify some of the complex issues that are related to cyber operations, especially those related to the right to the use of military force, i.e. right to go to war (ius ad bellum) and to right to conduct in war (ius in bello). Although Tallinn Manuals are unofficial documents, these documents are very important project and are considered as a solid basis for the further creation of international documents that would regulate these issues with binding norms. Such a thing is not impossible in perspective, but it would be a long and complex process. Even the creators of the Tallinn Manuals fail to reach a consensus for some of the issues, and for certain questions they state that they should be dealt with on a case-by-case basis.

Conclusion

The existence of cyberspace and activities in that space have strong implications in many different areas of Law, mostly expressed regarding the cybercrime; the jurisdiction of states in cyber space; the protection of right to privacy and personal data; regarding rules and restrictions in cyber warfare; as well as in electronic communications, electronic commerce, industrial property, access to information. There is some agreement that countries should regulate the issues related to the use of cyberspace in the national framework, but at the same time, to create standards that are applicable internationally, because cyberspace as a cross-border category affects all countries. This is particularly important because of the fact that there is no country that could provide a secure cyber environment on its own and that each state is almost equally vulnerable in that context. For these reasons, security in cyberspace remains a central topic not only nationally, but also globally.

Facing a series of cyberattacks that have the potential to hinder the functioning of the critical infrastructure in the countries where they have been carried out, has imposed the need to establish a minimum legal framework that will regulate permissible behavior in cyberspace and that will sanction illicit behavior in that space. In that sense, the efforts are aimed at identifying the existing legal norms and standards that can be adequately applied in cyberspace, i.e. to create new rules specific for cyberspace, where the existing ones cannot be applied.

The progress in this context, regionally, has been made in the field of cybercrime, particularly with the Council of Europe Convention on Cybercrime, through which the national legislation in European countries has been harmonized, both in the material as well as in the procedural Criminal Law. Also an important step is the adoption of the European reform package of acts in the sphere of personal data that harmonized the data protection legislation of the EU member states and the countries aspiring to join the EU. The Tallinn Manuals, as non-binding acts, also offer answers to complex issues related to cyber operations or cyberattacks in the context of inter-state conflict.

The results of the implementation of this legal framework remain to be seen over time, because the security of cyberspace as a strategic goal of one state and the international community as a whole, apart from the legal norms, requires fulfillment of other conditions and assumptions, especially commitment and coordination of all relevant stakeholders in society, both in the public and private sectors, raising public awareness of risks in cyberspace as well as intergovernmental coordination and cooperation.

References

1. Appazov, A. (2014) Legal Aspects of Cybersecurity, Faculty of Law University of Copenhagen, available at http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf
2. Arquilla, J. and Ronfeldt. D. (1993), "Cyberwar is Coming!", *Computer Strategy*, 12 (1) pp.141-165

3. Blake, D. (2017) Regulations and Compliance in Cyber Security, Literature Review, Vectors Institute
4. of Technology Capstone project, available at: https://www.academia.edu/35544835/LEGAL_REGULATIONS_AND_COMPLIANCE_IN_CYBER_SECURITY_LITERATURE_REVIEW
5. Brenner, S.W. (2002) "The Privacy Privilege: Law Enforcement, Technology and the Constitution",
6. *Journal of Technology Law & Policy*, 124-131.
7. Efthymiopoulos, M.P. (2019) "A cyber-security framework for development, defense and innovation at
8. NATO", *Journal of Innovation and Entrepreneurship* , 8:12.
9. Gerche. M. (2012) *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU,
10. available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
11. Hadji-Janev, M. (2016) *International legal Aspects of Protecting Civilians and Their Property in the*
12. *Future Cyber Conflict*, Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, IGI Global, USA
13. Kosseff, J. (2018) "Defining Cybersecurity Law", *Iowa Law Review* 103:985, p. 985-1031, available at:
14. https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/
15. Lessig, L. (2006) Code, version 2.0. Basic Books, New York, available at
16. http://codev2.cc/download+remix/Lessig-Codev2.pdf.
17. Peng Hwa, A. (2016) "How countries are regulated Internet content", available at:
18. https://web.archive.org/web/20160103124414/https://www.isoc.org/inet97/proceedings/B1/B1_3.HTM
19. Rossouw von Solms, Johan van Niekert (2013) "From information security to cyber security",
20. *Computers & Security*, 97-102, available at: https://profsandhu.com/cs5323_s18/Solms-Niekerk-2013.pdf
21. Tikk, E. (2011) Ten Rules for Cyber Security, NATO Cooperative Cyber Defense Centre of Excellance,
22. Tallin, available at: https://citizenlab.ca/cybernorms2011/rules.pdf
23. **Documents**
24. ETS 185 - Convention on Cybercrime, Council of Europe, Budapest, 23.XI.2001
25. Convention on cybercrime - Protocol on Xenophobia and Racism (2015)
26. Directive (EU) 2016/680 of The European Parliament and of The Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data
27. Regulation (EU) 2016/679 of The European Parliament and of The Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

28. Tallinn Manual on the International Law applicable to Cyber Warfare (2013) Cambridge University Press, available at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

On-line resources

29. https://ccdcoe.org/research/tallinn-manual/
30. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
31. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf
32. https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en
33. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx
34. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

ВО ОВОЈ БРОЈ: ŽARKO PUHOVSKI
BERNARD BOËNE
HAKAN WIBERG
BULENT GOKAY, LILY HAMOURTZIADOU
VASSILIS K. FOUSKAS, BULENT GOKAY
BILJANA VANKOVSKA, RADMILA NAKARADA
SRĐAN M. JOVANOVIĆ
BILJANA KAROVSKA-ANDONOVSKA, NENAD TANESKI