University of Salford
A Greater Manchester University
University of Essex
ESSEX BUSINESS SCHOOL
International Centre for Entrepreneurship Research
The General Jonas Žemaitis Military Academy of Lithuania
Ministry of National Defence Republic of Lithuania
Vilnius Gediminas Technical University
RISEBA
Estonian Business School
NATO Energy Security Centre of Excellence
ENTREPRENEURSHIP AND SUSTAINABILITY CENTER
AVADA

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2018 March Volume 7 Number 3
http://doi.org/10.9770/jssi.2018.7.3(16)

THE MEANS TO SECURE CRITICAL ENERGY INFRASTRUCTURE IN THE CONTEXT OF HYBRID WARFARE: THE CASE OF UKRAINE

Tomas Plėta[1], Sergii Karasov[2], Tadas Jakštas[3]

[1,2,3]NATO Energy Security Centre of Excellence, Institution, Šilo g. 5A, LT-10322 Vilnius, Lithuania

E-mails: [1]tomas.pleta@enseccoe.org; [2]sergii.karasov@enseccoe.org; [3]tadas.jakstas@enseccoe.org

Received 15 October 2017; accepted 17 February 2018

Abstract. This article discusses the Ukrainian legislation on cybersecurity. The necessity of developing an efficient cybersecurity system was raised by the hybrid war conducted by Russia over the last few years, in which many critical infrastructure objects have been destroyed with serious consequences not only for the end consumers but also for the security of the state. Consequently, Ukraine has begun issuing a number of laws aiming at strengthening its cyber defense capabilities by establishing an efficient national cybersecurity system. The analysis has clearly shown that although important steps have already been taken in this direction, much still remains to be done to protect the Ukrainian critical infrastructure.

Keywords: cybersecurity, cybersecurity legislation, hybrid warfare, critical infrastructure protection, Ukraine

Reference to this paper should be made as follows: Plėta, T., Karasov, S., Jakštas, T. 2018. *The means to secure critical energy infrastructure in the context of hybrid warfare: the case of Ukraine, Journal of Security and Sustainability Issues* 7(3): 567–577. http://doi.org/10.9770/jssi.2018.7.3(16)

JEL Classifications: R00

1. Introduction

The rapid development of information technology is gradually transforming the world. An open and free cyberspace enhances people's freedom and opportunities and enriches the society. At the same time, the advantages of the modern digital world and the development of information technologies have created new threats to national and international security (Šišulák 2017). Indeed, the number and the power of cyberattacks is increasing. They are a new tool through which individuals, interest groups and sometimes states try to obtain private, technical, and institutional data and information. For this reason, a clear and efficient legislation on cybersecurity is essential. At the same time, it is necessary to distribute the activities and the tasks aiming at ensuring the cyber defense of the state to the bodies in charge of it in a very rational way.

Given this background, this article focuses on the efforts of Ukraine to establish an efficient legal framework that is able to ensure the cybersecurity of the state. This necessity essentially stems from the challenges coming from the hybrid war conducted by Russia against Ukraine in which cyber-attacks play a key role. This has made clear that the protection of the cyberspace is essential for the national interests. For this reason, the establishment of an efficient national cybersecurity system as part of Ukraine's national security strategy has recently become urgent (President of Ukraine, 2016).

Over the past three years, Ukraine has experienced several cyber threats in the context of the Russian hybrid war. Among them, the threats to the information and telecommunication systems to the industrial control ones and critical energy infrastructure (hereinafter - CEI) are particularly relevant. Two examples are the cyberattacks on CEI on December 23, 2015 and the latest large-scale cyberattack on June 27, 2017. These two examples clearly show that cyberspace is gradually becoming a separate sphere in which war can be conducted in addition to the traditional "Earth", "Air", and "Sea". Indeed, modern information and communication technologies can be used to carry out cyberterrorism. For instance, this can happen by interrupting the normal operation of the Supervisory Control and Data Acquisition (hereinafter - SCADA) systems that control the technological processes of CEI (President of Ukraine, 2016). According to the Energy Strategy of Ukraine until 2035, the creation of a state system for the protection of CEI including cybersecurity is one of the state's priorities in the energy sector (Cabinet of Ministers, 2017). In this context, the improvement of the legal framework on cybersecurity is essential. This would enable the institutions responsible for protecting CEI from cyberattacks to work more efficiently in order to coordinate the detection and response to threats in a timely manner. This will effectively ensure the uninterrupted operation of CEI, supply of energy resources to consumers and the stability of the whole energy complex of Ukraine.

In a hybrid war, such a task is even more relevant and important. The inability of the state to effectively and timely respond to cyberattacks could have serious consequences. Indeed, cyberattacks are a powerful means for affecting the safe and reliable operation of CEI and can even be combined with other means of influencing the work of such objects. This is exactly why an adequate legal regulation of the provisions on cybersecurity for an effective protection of CEI is a priority for Ukraine. Additionally, this is important for reforming and strengthening the defence and security sector.

2. The meaning of "cyberattack", "critical infrastructure", and "objects of the critical infrastructure" in the Ukrainian legislation on cybersecurity

The Ukrainian legislation contains a number of legal acts regulating the operation and protection of CEI. However, the terms "cyberattack", "critical infrastructure", "objects of critical infrastructure" have not been contemplated in the legislation until the Verkhovna Rada of Ukraine passed the Law "On the Basic Framework of Cybersecurity of Ukraine" on October 5, 2017. This law was signed on November 7, 2017 by the President of Ukraine and will come into force only six months after its publication. Before the adoption of this law, a clear definition of the concept did not exist in the legislation. Therefore, a large number of terms concerning cybersecurity-related issues was used. For example, the Law of Ukraine "On the Framework of National Security of Ukraine" contains terms such as "computer crime" and "computer terrorism", but the law does not define them (Verkhovna Rada, 2003). Another important legal act, the Law on the Fight against Terrorism, contains the expression "technological terrorism" instead of "computer terrorism" or "cyberterrorism". (Verkhovna Rada, 2003a). The "Doctrine of Information Security of Ukraine" refers to concepts like "computer crime", "cyberattack", "computer terrorism", but without any explanations or references (Verkhovna Rada, 2003a). The same applies to the Laws "On Information", "On the State Service of Special Communication and Information Protection of Ukraine", "On the National Security Information", as well as to the Strategic Document "National Security Strategies of Ukraine" and to "Cybersecurity Strategies". Nevertheless, the Cabinet of Ministers of Ukraine has approved the procedure to draw up a list of information and telecommunication systems of the critical infrastructure objects with a decree on August 23, 2016 (Cabinet of Ministers of Ukraine, 2016a). Here, the term ***"cyberattack"*** means unauthorized actions taken with the use of information and communication technologies. These actions aim at violating the confidentiality, integrity and availability of the information contained in the telecommunication system, or at violating the smooth functioning of such a system.

The term ***"critical infrastructure"*** (hereinafter - CI) refers to the part of the infrastructure of the state that is of utmost importance for the economy, the industry, the functioning of the society and for the security of the population. The decommissioning or destruction of that infrastructure may have an impact on national security and defence as well as on the environment. Additionally, this may lead to significant financial losses and human casualties.

"Objects of critical infrastructure" refers to enterprises and institutions (regardless of ownership) operating in sectors (e.g. *energy*, chemical industry, transport, banks and finance, information technology and telecommunications, food supplies, health care, and utilities) that are strategically important for the functioning of the economy and the security of the state, society and population. Therefore, the governmental decree includes in the "objects of critical infrastructure" also the ones concerning the energy sector. Finally, it is worth noting that before these laws and decrees were issued, the existing legislation contained a number of terms related to cyber-attacks and cybersecurity without providing any definition.

3. Cyberattacks on critical infrastructures, consequences and reactions

In December 2015, Ukraine faced a major escalation in the seriousness of the Russian cyber-attacks on its CEI (Ukrainian National News, 2016). According to the US Department of Homeland Security, which reported on the case, the Russian cyber-attack on the Ukrainian CEI was one of the most successful cyberattacks on CEI in the world (US Department of Homeland Security, 2016).

Facts are the following. An unpredictable blackout of electric power occurred in several areas of Ukraine (Ivano-Frankivsk, Chernivtsi, Kyiv regions) on 23 December 2015, at about 4:30 in the morning. In that moment, a message appeared on the official website "Prykarpattiaoblenergo" (Ivano-Frankivsk region) about large-scale failures in the power supply system that occurred for unknown reasons (Ukrainian National News, 2016). Immediately after the attack, it was discovered that the reason for stopping the work of the control equipment was an external intrusion into the operation of the power grid monitoring and control systems.

Simultaneously, hackers struck a powerful blow to the computer networks of the energy company "Kyivoblenergo". The hackers managed to access the IT systems controlling the substations of the company by temporarily disrupting the electricity supply to end consumers (Butrimas, 2017). Generally speaking, the cyberattacks of this kind have the following characteristics:

- it usually takes several months to be discovered by the victim;
- once the hackers have accessed the system, they try to explore the target network and to acquire the information of the victim;
- malicious takeover of ADCS control combined with shutdown operations at substations;
- disabling of IT infrastructure elements (uninterruptible power supplies, modems, RTU, switches);
- destruction of information on servers and SCADA control systems[1];
- „Denial of Service DOS" style attack executed against the call Centre's capability to accept customer calls wishing to complain about the lost service;[2]
- using an earlier obtained remote access to administrator computers of ADCS in corporate networks of power companies or directly to ADCS servers;
- the attackers try to control the distribution substation switches by using the ADCS client software. This causes the disconnection of end consumers.

After the cyber-attack on Kyivoblenergo, some others followed. For instance, the "North" substation of 330 kV (NEC "Ukrenergo") was completely de-energized on 17 December 2016. This resulted in the outage of a load of 144.9 MW for the "Kyivenergo" Public Company (Kyiv City) and of 58 MW for another company, "Kyivoblenergo" (the Kiev region). A Kyiv pump-storage plant was also de-energized with a loss of in-house supply. One of the consequences of these cyber-attacks was that the automatic controlled systems were transferred to the local level control. According to some analysts, the attack was sophisticated but was not fully exploited (attackers had the power to do worse) and may have been just a "test" of a new capability (Butrimas, 2017).

---

[1] Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control the features in the industrial sector and energy transit infrastructure. The security of the SCADA system consists of four major elements: real-time monitoring, detection of anomalies, impact analysis and mitigation strategies. (Plėta et al, 2017)

[2] Denial-of-service (DoS) occurs when the access to the system is denied to authorized users. (Plėta et al, 2017)

Another large-scale cyberattack in Ukraine took place on June 27, 2017. Differently from the previous cyber-attack, this one was not directed against CEI but to the financial sector. In spite of this, this cyber-attack also damaged CEI. According to the reports from the Department of Cyber Police of the National Police, a virus attack on Ukrainian companies was launched against companies operating in the financial, media and mobile sectors among others through the M.E. doc. program, a software for records and document circulation. This software has a built-in update feature of approximately 333 kb in size. The investigation of the Cyber Police highlighted the three ways through which this kind of attack can occur: 1. Computers are infected and encrypted (therefore the system is completely compromised). Restoring the content of computers requires knowing the private key. Additionally, on the computer screen a message asking people to pay for a file in order to unlock the key appears; 2. Computers are infected and partially encrypted. The system initiates the encryption process, but external factors (e.g. power outages) stop the encryption process; 3. Computers are infected, but the encryption process of the MFT table does not initiate (Espreso TV, 2017a). Taking into account the danger of such cyberattacks, special equipment was purchased from NATO, which was transmitted to state bodies. Indeed, Ukraine actively cooperated with NATO, the United States and Great Britain to reduce the negative effects of these attacks (Espreso TV, 2017c).

4. The significance of critical infrastructure in the Cybersecurity Strategy of Ukraine

After the large-scale cyberattack on CEI on December 23, 2015, issuing a strategic document on defence and state cybersecurity on CEI became urgent. On January 27, 2016, the National Security and Defence Council of Ukraine (hereinafter - NSDC) adopted a decision "On the Cybersecurity Strategy of Ukraine" (hereinafter - the Strategy), which was put into effect by the Decree of the President of Ukraine March 15, 2016 (President of Ukraine, 2016). Its purpose is to create the necessary conditions for the secure functioning of the cyberspace and for its use in the interests of the individual, the society and the state. To achieve this purpose, it is necessary to:

- create of a national cyber security system;
- strengthening the capabilities of the security and defence sector to ensure an effective combat against *cyber-threats of military character, cyber-espionage, cyber-terrorism* and *cybercrime*, and deepening international cooperation in this area;
- providing the cyber defence of the state electronic information resources, the information required by the law to protect it, as well as the information infrastructure under the jurisdiction of Ukraine. The violation of its continuing functioning would have a negative impact on the state of NSDC (*critical information infrastructure)*.

This Strategy is based on the following: 1) the provisions of the *Convention on Cybercrime,* ratified by Law September 7, 2005 No. 2824-IV; 2) the Ukrainian legislation on national security: 3) the principles of national and foreign policy, the electronic communications, and the protection of the state information resources. The measures for the protection of these latter were adopted with the laws mentioned above and aim at contributing to the implementation of the Strategy of National Security of Ukraine by 2020, which was approved by the Decree of the President of Ukraine of May 26, 2015, No. 287 (President of Ukraine, 2016).

According to the Strategy, the Ministry of Defence, the State Service for Special Communications and Information Protection, the Security Service, the National Police, the National Bank, and the intelligence agencies are the main bodies of the national system of cybersecurity. Also, the strategy outlines the key points and the most important steps that need to be taken for an effective cyber defence of CI:

- issuing of laws aiming at regulating the national cybersecurity system;
- drawing up a list of CI objects;
- defining the requirements for an effective cyber defence of the CI objects;
- defining clear qualification requirements for certain categories of employees dealing with CI objects; the introduction of mandatory periodic attestation for such employees in order to verify their compliance with the specified requirements is also necessary;
- establishing the cooperation among the actors providing the cyber defence of CI; in this context, it is necessary to develop public-private partnerships to better prevent cyber threats, to efficiently respond to cyberattacks

and cyber incidents and to mitigate their consequences, in particular in crisis, emergency and military situations, during a special period of time;

- creating and implementing a mechanism for the exchange of information between public authorities, private sector and citizens regarding the threats to CI.

The discussion conducted here has made it clear that Ukraine has begun taking the necessary measures to build its cybersecurity legislation through the implementation of the Strategy on cyber defence of critical infrastructure.

5. National Cybersecurity Coordination Centre

The National Cybersecurity Coordination Centre (hereinafter referred to as the Centre) was established by the Decree of the President of Ukraine June 7, 2016 (President of Ukraine, 2016b). The management body of the NSDC was established in accordance with the decision of the NSDC January 27, 2016 "on the Cybersecurity Strategy of Ukraine". It consists of the head, the secretary and other members of the Centre. The head of the Centre is also the secretary of the NSDC. The tasks of the Centre in the field of CI essentially consist in the analysis of the status of cyber security in the country and in the implementation of the legislation on cyber defence.

The Centre provides operational, informational and analytical support to the NSDC on cybersecurity issues. Also, the Centre develops and makes proposals to the NSDC in accordance with the established procedure. This concerns in particular the implementation of the measures necessary for the cyber defence of CI and the protection of the technological processes necessary for the well-functioning of the economy.[3] Additionally, the Centre deals with the improvement of the regulatory framework of cyber security, in particular the one concerning the responsibilities of the entities in charge of ensuring cyber security and the interaction between them.

Moreover, the Centre monitors the status of the development and of the implementation of the national standards and technical regulations for the application of information and communication technologies that are harmonized with the EU and NATO standards. It also carries out a control on the status of the implementation of the NSDC's decisions on cybersecurity issues, enacted by the decrees of the President of Ukraine. Additionally, it has the following rights:

to request and receive statistical data, information, and other material from the executive authorities;

- to use the information databases of the state bodies;
- to create expert and working groups;
- to address the Main Situation Centre of the NSDC, as well as the State Center for Cyber Defence and Counteraction to Cyber-threats of the State Service for Special Communications and Information Protection.

The establishment of the Centre is crucial to the creation of a functioning cybersecurity defense system. Indeed, it can be defined as one of the most important tools for the implementation of the cyber-security strategy of the state.

6. The Annual National Program of the Ukraine-NATO Commission in 2017

The Presidential Decree of April 8, 2017 approved the Annual National Program under the Ukraine-NATO Commission in 2017 (hereinafter – Program). Under this program, Ukraine has committed to carry out the main activities of NATO in accordance with the medium-term priority goals of the state in the various fields of activity. In particular, they include a plan to ensure cybersecurity and protect CI (President of Ukraine, 2017).

[3] "The real sector of the economy" is one of the national economy sectors, which includes the economic entities that directly create gross value added and form the gross domestic product and the national income. They also produce tangible and intangible goods and services that are not related to the financial sector of the economy. (Volot and Plisko, 2016)

The Annual National Program envisages the establishment of some important bodies in charge of strengthening the cybersecurity of the country. They are the following:

1) the Situational Centre for Cybersecurity whose task is identifying, preventing and neutralizing cybernetic actions against CI;

2) the State Centre for Cyber Defence and Counteraction to Cyber Threats, which ensures the operation of the Computer Emergency Response Team of Ukraine (CERT-UA) and serves as the technical coordinator of state bodies, local authorities, military units, enterprises, institutions and organizations irrespective of the form of ownership on issues of prevention, detection and elimination of the consequences of cyber incidents;

Additionally, the National Police runs a National Contact Point operating 24/7 for the response and exchange of urgent information on computer crimes. Its mid-term goal is to improve the national system of cyber security as a component of the information security system, its legal conceptual framework and practical mechanisms for counteracting the aggression of the state and /or state supported actors in the cyberspace. The priority tasks for the current year are the following:

- to ensure cooperation with NATO partners and the implementation of projects within the framework of the Ukraine-NATO Trust Fund on Cyber Security;
- to develop the expertise of the Situational Centre in the cyber security field;
- to continue improving the regulatory framework in the cyber security field.

The Program also envisages important measures aimed at ensuring the cyber defence of CI. Among them, it is worth mentioning the creation of an integrated security management system and response capability for cyber incidents aimed at detecting and preventing cyber threats to CI objects.

The cybersecurity institutions that are responsible for the implementation of security measures are the Security Service, the Administration of the State Service for Special Communications and Information Protection, the Ministry of Defence, the Ministry of Foreign Affairs, and other interested central executive authorities.

Taking into account that the implementation of the Program is still ongoing, it is too early to draw conclusions on its effectiveness. However, it is possible to state that the Ukraine-NATO cooperation within the framework of the Cybersecurity Trust Fund is productive and that the regulatory framework in the field of cybersecurity is gradually being implemented. For instance, on October 5, 2017, the Verkhovna Rada adopted the new Law "On the Basic Framework of Cybersecurity of Ukraine".

7. Response measures to cyber threats

As a consequence of the numerous cyber-attacks discussed above, the NSDC decided that the Cabinet of Ministers of Ukraine (hereinafter - CMU) should urgently issue legislative proposals regarding the determination of the requirements for the cyber defence of CI. These legislative proposals should also concern the rights and obligations of the main entities in charge of ensuring cybersecurity and of the owners (administrators) of CI. Additionally, they should define the mechanisms of information sharing between the owners of CI during the detection, prevention, and mitigation of cyberattacks.

Within three months from the day the NSDC Decision enters into effect, the CMU and the Security Service of Ukraine have to prepare legislative proposals on the determination of restrictive measures regarding the use of the SCADA software and telecommunication equipment produced by the aggressor state entities. In this context, the implementation of the *Convention on Cybercrime*, ratified by the Law of Ukraine of September 7, 2005, No. 2824-IV, is of utmost importance. In particular, it contains the following provisions:

- it identifies the authorities in charge of defining the requirements for the owners of computer data (operators and telecommunication providers, other legal entities and individuals) for the urgent fixing and storage of computer data necessary for the disclosure of a crime over a period up to 90 days (with the possibility of prolongation to 3 years);
- it establishes the requirements for telecommunication operators and telecommunication providers in rela-

tion to the provision of the information necessary to identify service providers;

- it stipulates that the Court could impose a blocking (restriction) on telecommunication agencies providing information services;
- it establishes an effective mechanism for the use of electronic proofs in criminal proceedings, which can be collected during the investigation phase.

In addition, it is interesting to note that the NSDC will issue a protocol regulating the cooperation between the state institutions in charge of cyber security and the owners (administrators) of objects of CI during the detection, prevention, and the mitigation of cyberattacks and cyber incidents. Also, of the NSDC has planned to establish centres for the protection and the storage of state electronic information (President of Ukraine, 2016c). Here it is also worth mentioning the State Service for Special Communications and Information Protection (hereinafter - SSSCIP). It is in charge of monitoring the respect of the mandatory requirements of state bodies, enterprises, institutions and state organisations for the identification and authentication of the sources used to update softwares and for the checking of the reliability of such updates. SSSCIP also monitors the respect of the requirements for the official use of electronic digital signature for exchanging electronic documents (President of Ukraine, 2016c).

The successful implementation of the NSDC's decisions regarding the provision of cybersecurity of CI is directly proportional to the level of effectiveness of the response to cyber threats, their timely detection, prevention and localization in the case of cyberattacks on CI. One of the results of the NSDC's decisions is the adoption of the law "On the Basic Framework of Cybersecurity of Ukraine " by the Verkhovna Rada on October 5, 2017, which is the first law on the issue and which is discussed in detail in the next session.

8. Legal analysis of the new Law on the Basic Framework of Cybersecurity of Ukraine

During the 26 years of Ukraine's independence followed to the collapse of the Soviet Union, there was no single basic legal act regulating cybersecurity in Ukraine. This can be explained with the following reasons. Firstly, the necessity of a legal regulation of the response to cyber threats and cyberattacks on CEI as a public dangerous phenomenon arose during the hybrid war in Ukraine in 2014. On this occasion, CEI became a war target. A number of power stations was seized or destroyed. This led to disconnection from the United Energy System of Ukraine and damaged a number of transformer substations and electric power lines. In addition, the gas pipelines were destroyed with explosive devices. In most of these cases, the damage caused to CEI was carried out unintentionally during the combat operations (Sukhodolia, 2012). However, the need for an effective state response system in the context of the crisis in cyberspace became clear after the large-scale cyberattack at CEI on December 23, 2015 discussed above.

Secondly, the threats and attacks in the cyberspace are directly related to the rapid modern developments in the IT technology. The consequence is the development of malicious programs that are able to influence the industrial control systems (SCADA) used to monitor and control CEI.

Thirdly, cybercrimes and even the conduct of hybrid and full-scale wars using computer technology has become a "convenient" tool as the attackers can't be easily identified.

Fourthly, in recent years, Ukraine has become something similar to a "laboratory" for testing cyber weapons and attack methods for disturbing or degrading the uninterrupted operation of CEI. This was evident in the cases of the cyberattacks on part of Ukraine's power grid in December 2015 and again in December 2016 (Butrimas, 2017). Also, a process of norm-setting[4] aiming at facing cyber threats and attacks has only very recently begun.

[4] "A process of norm-setting" is an activity related to planning, development, examination, and adoption (publication) of a legal act. (Verkhovna Rada, 2003b)

On October 5, 2017, the Verkhovna Rada adopted the new Law of Ukraine "On the Basic Framework of Cybersecurity of Ukraine" (hereinafter - Law), which will come into force only six months after its publication (Verkhovna Rada, 2003b). This Law defines the legal and organizational framework for ensuring the protection of the vital interests of people, society and state, as well as the national interests of Ukraine in cyberspace, its main goals, directions and principles of state policy in the field of cybersecurity. Also, it defines the powers of state bodies, enterprises, institutions, organizations, persons and citizens working in this sector, and the main principles regulating the coordination of their responsibilities.

The new law defines *critically important infrastructure objects* as enterprises, institutions and organizations, regardless of ownership, whose activities are directly related to technological processes and/or the provision of services of major importance to the economy and industry, and to the functioning of the society. The interruption of these activities may have a negative impact on the state of national security and defence of Ukraine and on the environment, and may cause property damage and/or endanger human life and health. *The law stipulates that the control system of the technological processes* is an automated or automatic system that is a set of equipment, means, complexes and systems of processing, transmission and reception and is designed for organizational management and / or control of the technological processes (*including industrial*, electronic, communication equipment, other technical and technological means) regardless of whether the system has access to the Internet and / or other global data networks (Verkhovna Rada, 2003b).

The law distinguishes the notion of *incident of cybersecurity* from the one of *cyberattack*. *An incident of cybersecurity* is an event or a series of adverse events of a non-intentional nature (natural, technical, or technological) and/or those that could have been generated by a cyberattack and that constitute a security threat to electronic communications systems and to systems management of technological processes. In so doing, these events jeopardise the correct functioning of such systems (by provoking a disruption and/or by blocking the system and/or through the unauthorized resource management) and threaten the security of the electronic information resources. *A cyberattack* is a targeted (intentional) action in the cyberspace that is carried out with the help of electronic communications (including information and communication technologies, software, hardware, other technical and technological means and equipment) and is aimed at achieving one or a combination of the following objectives: 1) violation of the confidentiality, integrity, availability of the electronic information resources processed (transmitted or stored) through communication and/or technological systems; 2) violation of safe, stable, reliable and correct functioning of the communication and/or technological systems; 3) use of the communication system, its resources and means of electronic communications (Verkhovna Rada, 2003b).

Furthermore, it is necessary to note that the law does not specify the meaning of some other types of cybercrimes such as ***cyber aggression*** and ***cyber-sabotage*** making the distinction among them quite vague when trying to refer to the Criminal Code of Ukraine. This makes difficult to determine the legality of an investigation on malicious cyber activities acts. Such an argument is confirmed by the provisions of Article 2 of the Law on the principles of the application of the rule of law. According to this Article, the application of the legislation in the field of cybersecurity shall be carried out in compliance with the principles of objectivity and legal certainty. As cyber aggression and cyber-sabotage are not well defined by the law, it is not possible to consider them as crimes and, consequently, to legally proceed. According to the Law, the CMU shall outline an appropriate procedure to draw up a list of CI objects, and to include them in the state register of CI objects. Currently, the list of critical infrastructure objects has not yet been approved, but this is a necessary step for the clear definition of CI objects that need to be protected in case of cyberattacks.

Furthermore, according to the law, the following bodies are in charge of ensuring the cyber-security of the country:

- the President of Ukraine, who coordinates the activities in the field of cyber security through the NSDC as an integral part of Ukraine's national security;
- the National Cybersecurity Coordination Centre (which is the working body of the NSDC) that monitors and coordinates the national security and defense activities in order to implement the cybersecurity strategy;

- the CMU that ensures the implementation of the state policy in the field of cybersecurity, and is in charge of ensuring the protection of people's rights and freedoms, as well as the national interests of Ukraine in the cyberspace, and the fight against cybercrime. It also organizes and provides the necessary forces, means and resources for the functioning of the national cybersecurity system. It defines the requirements of and ensures the functioning of the information security audit system related to the CI;
- the ministries and other central executive bodies;
- the regional state administrations;
- the local self-government bodies;
- the intelligence and counterintelligence agencies, and the bodies of operational and investigative activities;
- the Armed Forces, other military formations with formed in accordance with the law;
- National Bank;
- enterprises, institutions and organizations classified as objects of CI;
- private entities, citizens and associations of citizens who carry out activities and/or provide services related to the national information resources, electronic information services, electronic transactions, electronic communications, information security and cyber defence (Verkhovna Rada, 2003b).

The CMU is in charge of defining the requirements of an independent audit of information security. The legislation concerning this latter is issued on the basis of the international, the European Union and NATO standards with the mandatory involvement of the representatives of the main actors dealing with cybersecurity (e.g. scientific institutions, independent auditors, experts and public organisations working in the field of cybersecurity). Additionally, the owners and/or managers of enterprises, institutions and organizations have the following responsibilities: 1) providing the cyber defence of the communication and technological systems of CI; 2) protecting technological information in accordance with the legislation; 3) urgently informing the Government response team in case of incidents of cybersecurity; 4) organizing an independent information security audit on CI objects. In this context, the role of CERT-UA and of volunteer organisations for the information sharing is of utmost importance. The Verkhovna Rada is in charge of checking that the legislation on cybersecurity is observed during the implementation of the national measures adopted to ensure cybersecurity. The President and the CMU exert a control over the activity of the state bodies in charge of ensuring the national cybersecurity. These bodies submit periodical reports on the status of the implementation of the measures aiming at ensuring the cybersecurity of the state. These reports should include, in particular, information on the results of an independent audit of their activities. The Verkhovna Rada Committee is in charge of evaluating these reports.

It should be emphasized that, like the other countries, Ukraine has its own procedures to protect critical infrastructure. Indeed, a consensual model to protect critical infrastructure does not exist. Here, it can be argued that an efficient cyber security management of the communication and technology systems ensuring the well-functioning of CI should include the following elements: 1) legal regulation of enterprises at the local level; 2) a good governance aiming at reducing the probability of cyber incidents and cyberattacks; 3) a risk management including risk identification and contingency planning; 4) a cybersecurity awareness training for the staff of companies and enterprises 5) an efficient technology management, 6) an efficient incident management, including special plans for managing the consequences of the incidents (Plėta et al, 2017). Nevertheless, it should be stressed here that a well-functioning cybersecurity system is ensured by a combination of various elements. One of them is the organizational and technical model of cybersecurity, which ensures a secure access of the state authorities to Internet, an antivirus protection of the national information resources, and an efficient cyber defence of CI. This model includes a vulnerability detection and response system to cyber incidents and cyberattacks, computer interaction response teams as well as cyber-threat response scenarios, measures to counteract such threats, programs and methods of conducting cyber exercises (Verkhovna Rada, 2003b).

Additionally, in order to protect CI it is essential to strengthen the crucial role played by the public-private partnerships. The reason is that infrastructures are usually owned by the private sectors, but the public one shares the responsibility of protecting them because the well-functioning of CI is in the national interest. However, a problem is that the private sector is not so much inclined to share information about specific attacks even

though such information could significantly contribute to the strengthening of cybersecurity. The reason is that it is unlikely for the private sector to share the information about the cyber security attacks and the vulnerabilities that they have identified in their infrastructure because this information can ruin their reputation and make their business partners rethink the attractiveness of collaboration (Plėta et al, 2017).

Conclusion

Ukraine began developing its legislation on cybersecurity as a response to the cyber-attacks of the last years that have showed how important protecting critical infrastructure is and the gaps of the legislation in this field. For this reason, Ukraine has passed a number of laws and decrees in order to regulate its cybersecurity system aiming at strengthening the capacity of the state to efficiently and timely respond to cyber-attacks and to mitigate cyber-threats. A good example is the law " On the Basic Framework of Cybersecurity of Ukraine", adopted by the Verkhovna Rada of Ukraine on October 5, 2017, which will come into force only six months after its publication, as stated above. Additionally, some bodies ad hoc have been established such as the NSDC, which is necessary for an efficient cybersecurity system in Ukraine.

However, these are just some steps towards the establishment of an efficient legislation system. More efforts are still needed to make Ukraine able to face cyber-attacks and threats not only at the national level but also at the international one. In this context, strengthening the cooperation with NATO would be crucial as information sharing would be of utmost importance to increase and improve the competences on the cybersecurity-related issues of the state bodies and energy companies in Ukraine.

References

Butrimas, V. 2017. Cyber-attack on Ukraine's CEI (2015) Case Study. *Energy Security Awareness Course* Tbilisi

Cabinet of the Ministers. 2017. Order of the Cabinet of Ministers of Ukraine of August 18, 2017 No. 605-p on Approval of the Energy Strategy of Ukraine for the period up to 2035. Retrieved from http://zakon2.rada.gov.ua/laws/show/605-2017-%D1%80

Espreso TV. 2017, June 27. Computer virus is spreading in Ukraine, which has already paralyzed the work of public and private companies. Retrieved from https://espreso.tv/news/2017/06/27/kogo_atakuvav_virus_vymagach_petyaa_spysok_usikh_kompaniy

Espreso TV. 2017a, July 3. The Cyber Police made recommendations for the restoration of partially encrypted data that has suffered from cyberattack Petya Retrieved from https://espreso.tv/news/2017/07/03/ctalo_vidomo_yak_quotozhyvytyquot_kompyuter_pislya_ataky_petyaa

Espreso TV. 2017b, June 27. Hacker attack on Ukraine was carried out through the program for reporting and document circulation M.E.doc. Retrieved from https://espreso.tv/news/2017/06/27/u_kiberpoliciyi_nazvaly_programu_cherez_yaku_atakuvaly_ukrayinu

Espreso TV. 2017c, June 29. NATO will provide Ukraine with equipment and technology for protection against hacker attacks in excess of a million EURO. Retrieved from https://espreso.tv/news/2017/06/29/nato_nadast_ukrayini_obladnannya_dlya_zakhystu_vid_kiberatak

Espreso TV. 2017d, July 6. The group of hackers who created the Petya.A virus, contacted users of the American Motherboard resource, giving details of the Petya virus. Retrieved from https://espreso.tv/news/2017/07/06/rozrobnyky_virusu_petyaa_zrobyly_pershu_zayavu

NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Terms and definitions.* Retrieved from https://ccdcoe.org/cyber-definitions.html

Plėta, T., Limba, T., Agafonov, K., Damkus, M. (2017). Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability. *Entrepreneurship and Sustainability Issues* 4(4): 559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

President of Ukraine. 2016. Decree on the decision of the National Security and Defence Council of Ukraine of January 27, 2016. Retrieved from http://zakon2.rada.gov.ua/laws/show/96/2016

President of Ukraine. 2017. Decree on the Decision of the National Security and Defence Council of Ukraine of December 29, 2016. Retrieved from http://www.president.gov.ua/documents/472017-21374

Cabinet of Ministers of Ukraine. 2016a. Decree on Approval of the Procedure for Establishing the List of Information and Telecommunication Systems for the State's Critical Infrastructure Retrieved from http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF

President of Ukraine. 2016b. Decree on the National Cybersecurity Coordination Centre of June 7*, 2016,* No. 242/2016. Retrieved from http://zakon3.rada.gov.ua/laws/show/242/2016

President of Ukraine No.103 / 2017. (2017). Decree on Approval of the Annual National Program the Ukraine-NATO Commission for 2017. Retrieved from http://www.president.gov.ua/documents/1032017-21670
President of Ukraine. 2016c. Decree on the decision of the National Security and Defence Council of Ukraine of December 29, 2016. Retrieved from http://zakon5.rada.gov.ua/laws/show/32/2017

President of Ukraine. 2017a. Decision of the National Security and Defence Council of July 10, 2017 on the Status of Implementation of the Decision of the National Security and Defence Council of Ukraine of December 29, 2016. Retrieved from http://zakon3.rada.gov.ua/laws/show/n0006525-17

Šišulák, S. 2017. Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5(2): 297-314. https://doi.org/10.9770/jesi.2017.5.2(10)

Sukhodolia, O. 2012. Problems of protection of the energy infrastructure in a hybrid war. Analytical note n.23. *National Security Series*. Retrieved from http://www.niss.gov.ua/articles/1891/

Ukrainian National News. 2016. The first case of a successful cyberattack on energy objects has been registered in Ukraine. Retrieved from http://www.unn.com.ua/uk/news/1552689-minenergovugillya-pershiy-u-sviti-vipadok-vdaloyi-kiberataki-na-obyekti-energetiki-zareyestrovano-v-ukrayini

US Department of Homeland Security. (2016). Cyber-Attack Against Ukrainian Critical Infrastructure. Retrieved from https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Verkhovna Rada. 2003. The Law of Ukraine on the Fundamentals of National Security of Ukraine of 19.06.2003. Retrieved from http://zakon2.rada.gov.ua/laws/show/964-15

Verkhovna Rada. 2003a. The Law of Ukraine on Combating Terrorism, March 20, 2003 No. 638-IV. Retrieved from http://zakon3.rada.gov.ua/laws/show/638-15

Verkhovna Rada. 2003b. The Law of Ukraine on the Basic Framework of Cybersecurity of Ukraine of 05.10.2017. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657

Volot. I., Plisko, I. 2016. Real economy: essence, components and its significance in providing steady growth of state economy. *Scientific bulletin of Polissia.* volume 1(5). Retrieved form http://journals.uran.ua/nvp_chntu/article/view/73938

Acknowledgements

Special thanks to Colonel Gintaras Bagdonas, Vytautas Butrimas, Major Rimantas Šikas, and Renata Vaišvilienė for their helpful comments and inputs.

Tomas PLĖTA, is currently Head of Support Division/Communication and Information System Officer at NATO Energy Security Centre of Excellence (ENSEC COE). Before joining NATO ENSEC COE, he worked as IT Specialist first in the Lithuanian Army and later at the Lithuanian Ministry of Defense. He holds a Master's degree in Management and e-Business Administration and two bachelors in Informatics Engineering and in Computer Science respectively. He is an expert in cybersecurity on which he has published in international journals. Research interests: cybersecurity, cyber defense, energy infrastructure protection, energy infrastructure protection management, cybersecurity management.

ORCID ID: https://orcid.org/0000-0002-5376-6873

Sergii KARASOV is an intern at NATO Energy Security Centre of Excellence (ENSEC COE). Previously, he was an intern at the Local National Court of Ukraine where he was an assistant. He holds a bachelor's from the Yaroslav Mudryi National Law University. During his studies, he spent a period as an Erasmus student at the Faculty of Law of the Comenius University of Bratislava. He also holds a Master's degree in law from the same university. In 2016, he received the qualification of Military Legal Advisor and the rank of Lieutenant from the Military Law Faculty in 2016. He currently studies as a master student at the International Law Faculty (LL.M) of the Mykolas Romeris University. Research interests: cybersecurity legal regulation in Ukraine as well as in the international context, the legal regulation of critical energy infrastructure protection.

Tadas JAKŠTAS, PhD, is a subject matter expert at NATO ENSEC COE. Before joining NATO ENSEC COE, Tadas worked as a project manager at NATO Allied Command Transformation and the Council of the European Union. He holds a PhD degree in Government from the University of Essex and two Master's degrees in International Relations from Leiden University and the University of Southampton. Research interests: energy security, cyber security, and defence policy analysis.