The 14th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 7th-8th 2019

THE VULNERABILITY OF CRITICAL INFRASTRUCTURE FROM THE PERSPECTIVE OF CYBER THREATS

Marin-Marian COMAN

"Nicolae Bălcescu" Land Forces Academy of Sibiu

Abstract:
Critical infrastructures (CIs) are the specific physical, non-physical, and cyber resources or assets and systems that provide reliable essential services, which are indispensable for day-by-day life of the population, social wellbeing, and economy. The broad spread and access to existing and new technologies, gadgets or tools based on information and communication technology (ICT) offer to modern societies an important variety of services necessary for current life of citizens and for controlling the well functioning of critical infrastructure sectors. The purpose of this paper is to provide a systematic view related to the vulnerability issues of critical infrastructure functioning in a continuous changing cyber environment from the perspective of emerging cyber threats. During cyber attacks, the normal running of critical infrastructures is affected and the critical infrastructure security programs have to identify and mitigate the cyber threats in order to counter them. The critical infrastructure interdependencies are taking also into account for having a relevant analysis and a broad picture of real effects of cyber attacks on critical infrastructures.

Key words: critical infrastructure protection, vulnerability, cyber threats, cyber security

1. Introduction

Nowadays, population's usual life is linked to many services that enable more and more their wellbeing. The delivering of these services in a continuous and reliable manner should be one of the overarching considerations when we bring into discussion actual globalization and its effects on countries' economy, citizens' life and communities all over the world. Usually, the critical infrastructures, which are facilities or assets that afford the emerging and sustainable development of the economic environment of every country, provide all those necessary essential services to population. The essential services are related to infrastructure sectors, such as transportation system, commercial sector, communications, information technology, emergency services, energy, financial services, food and agriculture, healthcare and public health, chemical and nuclear sectors, waste system, and water and wastewater systems. If the functioning of CIs would be disrupted or stopped, the population's usual life would be dramatically affected. In this respect, the critical infrastructure protection remains a big concern for all government institutions that are involved in the securing and protecting these special facilities.

The technological advance of society influences every person's life in some way or another and helps businesses and organizations saving time and cost of production in order to gain competitive advantage. Today, the industrial sectors are rely more and more on digital technology that creates an emerging technological environment which evolves in a fastest manner in every domain of activities. The advancement of technology and mainly digital technologies make the world a better place as time progresses. Today, the essential digital services, which were not possible in the past due to the lack of specific technologies, support people and contribute to the citizens' wellbeing. The internet, digital

mail, social media, electronic banking transactions, and e-commerce are just few examples of digital services that are used all over the world in an intense manner by many citizens. In this way, the world of businesses and countries' economies are evolving by having no any physical boundaries among digital transactions and communication (data and big data).

Digital technologies provide huge advantages and essential services to population but, in the same time, by using them could be a great challenge for all private or government institutions in securing and providing protection to computer networks and electronic devices that are connected through internet technologies. Due to the fact that the cyber environment has no boundaries and not so many regulations, when operating within cyberspace almost everyone (citizens, private and public organizations, or government institutions) could be unprotected and unsecured at a certain time. As a result, cyber security has never been more critical than nowadays. In the same manner, the critical infrastructures viewed as a special systems of systems, which are operating using cyber environment and run by public or private organizations for offering essential services to population, need maximum supervision, physical protection, and cyber security due to their vulnerability to certain cyber threats. From this perspective, risk assessments and analysis are mandatory in order to mitigate and remediate all critical infrastructure cyber vulnerabilities that could appear when operating in the cyber environment.

2. Critical infrastructure and the cyber environment perspective

Critical infrastructure is foundational for the prosperity and quality of life in any society. By definition, its destruction or disruption would cause severe damage and possibly loss of life. [1] In a big picture, CIs are those systems, which involve elements that are vital to the normal operations of the human society.

There are many approaches to define a CI, but these definitions slightly vary from one country to another or supranational entities, such as European Union:

- United States: "Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society." [2]

- European Union: "An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." [3]

- NATO: "Critical Infrastructure: Physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State’s security, economy, public health or safety, or the environment." [4]

Based on each country economic development level and own policy related to identification and classification of infrastructures as being critical, the list of critical infrastructure sectors comprises a different total number of CIs specific to every country. All critical infrastructures can be vulnerable to different threats that affect their normal functioning and the associated sort of risks can be related to natural hazards or man-made intentional or unintentional acts. As a result, every country have to issue own national strategy and a plan applied for critical infrastructure protection by taking into account the essential services provided to population, official international endorsed documents and assigned government institutions that are tasked to conduct specific activities during a certain intervention when an attack to a critical infrastructure occurs. Furthermore, the resilience of critical infrastructures is one of the paramount features that is related to their

qualities to reduce vulnerabilities, minimize the consequences of threats, accelerate response and recovery, and facilitates adaptation to a disruptive event. [5]

Besides the great commercial and economic advantages of making use of information and communications technology (ICT) through automation and digitalization in all industrial sectors and critical infrastructures, the wide spread and use of ICT also raises a lot of security vulnerabilities and emerging risks that could be easily exploited by all kind of attackers. The nowadays set up of cyber environment, the emerging technologies such as Internet of Things (IoT) or blockchain technology are used for operating the majority of digital resources and technical facilities, with implications in manning the critical infrastructures. From this perspective, with an increase in cyber threats, the special cyber security measures are paramount conditions for any government institution that is involved in securing and protecting a certain critical infrastructure. In the paperwork 'How to create a secure cyber environment', Don Hall has asserted, "the government entities are experiencing more cyber crime than ever before, with agencies twice as likely to experience a data breach than non-U.S. government organizations, according to the 2018 Thales Data Threat Report. The vast quantity of personal and confidential data that is gathered and stored by government makes it a prime target for cybercriminals, which both explains and exacerbates the issue." [6]

Taking in considerations all the above, the cyber resilience of critical infrastructures, viewed as an ability to resist, recover and evolve to improve own capabilities, when faced a certain cyber attack by making use of any of the information and communication technologies, must be appropriate and to function in a timely manner.

Public and private sector security partners have an enduring interest in assuring the availability of the infrastructure and promoting its resilience. The Information Technology (IT) Sector-Specific Plan (SSP) represents an unprecedented partnership and collaboration between the IT public and private sectors to address the complex challenges of critical infrastructure and key resources (CI/KR) protection. [7]

At the European Union level, the legal framework and regulations concerning cyber security and specific security agencies were set up. The European Union Agency for Network and Information Security (ENISA) was already established as being in charge with policies and strategies concerning cyber security domain. In 2013, the EU Cyber Security Strategy (CSS) was published detailing a series of actions to enhance the cyber resilience of IT systems, reducing cybercrime and strengthening the EU international cyber security policy and cyber defense. Then, the NIS Directive (Directive concerning measures for a high common level of security of network and information systems across the Union) as first piece of EU-wide legislation on cyber security that provides legal measures to boost the overall level of cyber security in the EU, was published in 2016. [8] The objective of the Directive is to achieve a high common level of security of network and information systems within the EU, by means of improved cyber security capabilities at national level, increased EU-level cooperation and risk management, incident reporting obligations for operators of essential services and digital service providers. The NIS Directive is a major milestone towards building cyber security resilience on the European level. [9]

Based on NIS Directive the "security and notification requirements should apply to *operators of essential services* and to *digital service providers* to promote a culture of risk management and ensure that the most serious incidents are reported." It is noticeable that the critical infrastructure operators were defined in the EU NIS Directive as operators of essential services meaning a public or private entities and comprising following type of services: energy (electricity, oil, gas), transport (air transport, rail transport, water transport, road transport), banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure. Related to digital service

providers, the NIS Directive also takes into account in the Annex III the following service types: online marketplace, online search engine, and cloud computing service.

3.Digital transformation through artificial intelligence

Population standard of living has increased nowadays by owing to the application of technology, in special the application of digital technology, which led to what it is called today - the *digital transformation (DX)*. In a broad understanding, the digital transformation is related to integration of digital technology into all areas of business and industry sectors by changing the ways in how the economic activities are conducted. Even cultural interdependencies are boosted by digital technologies, social media as a service being a great example in this respect. The Agile Elephant Company defines DX as a "process of shifting your organization from a legacy approach to new ways of working and thinking using digital, social, mobile and emerging technologies. It involves a change in leadership, different thinking, the encouragement of innovation and new business models, incorporating digitization of assets and an increased use of technology to improve the experience of your organization's employees, customers, suppliers, partners and stakeholders". [10]

At the end of 2018, the Zymr Company considered the following digital technology trends as being relevant and important to digital transformation for the year 2019: cloud computing, internet of things (IoT), big data, Artificial Intelligence (AI), blockchain technology, 5G, e-commerce, enterprise resource planning (ERP) solutions.

The digital technology has boosted all industry sectors that result in very profitable businesses, which are growing very fast, resulting in creation of more employment opportunities for citizens all over the world. The globalization effects allow stakeholders and customers to stay connected through the means of digital technologies. Furthermore, in almost every industry sector the digital technology adoption plays a major role in managing the informational flux among the stakeholders and customers.

Implementation of digital technology into day-by-day life of the people influences our perception related to interaction human-computer type. AI plays a huge role in this perception. AI has the power to enhance customer service solutions such as messaging platforms, chatbots, and video for quick and error free customer support. AI has also a significant role in digital transformation potential, being a key element and a great enabler in digital businesses with an enormous potential for transforming everything around, from business operations to potential customers. AI changes the business models by helping to develop and advance in many industry sectors. There are many applications of using AI such as cognitive applications (Neural network, genetic algorithms, intelligent agents, fuzzy logic, learning and expert systems), robotics applications (visual perception, locomotion, navigation, and object detection), and natural interface applications (speech recognition, virtual reality/VR, image analysis, natural language processing, health monitoring).

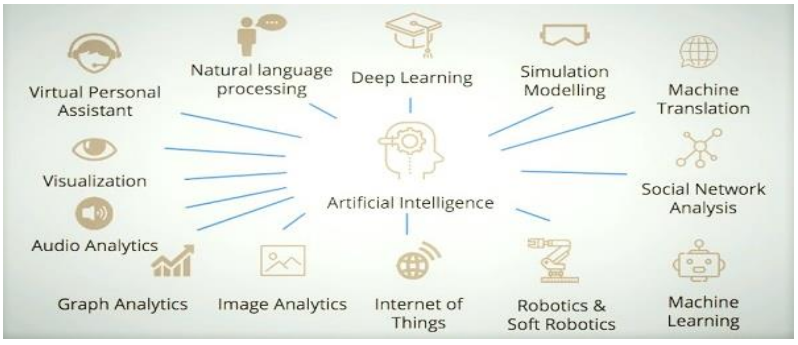

Fig.1 AI applications [11]

AI is already immersed into our life through the means of smart devices that are part of the internet of things (IoT). A good example of AI implementation is the use of smart phones by means of online applications and services for finding the fastest itinerary when we travel into a city or when we have to predict the best time to travel to a certain country.

IoT and AI are currently the buzzwords for every industry. IoT has improved the quality of life with its smart devices. AI has already proved its importance in all major business sectors like healthcare, education, automotive, agriculture, etc., to provide qualitative service. With the positive and overwhelming response to AI, researches are in progress to integrate it with IoT, to make it easier in decision making for some devices (smart home appliances, self-driving cars, etc) connected in IoT. [12]

4. Critical infrastructure - cyber threats and vulnerabilities

Besides reliable essential services provided to citizens, public or government sectors, the critical infrastructures have become also an integral part of cyber environment and they play a vital role in supporting many of our daily activities such as travel, water and power usage, telecommunications, financial banking transactions, and so on. From this perspective, the protection of critical infrastructures today is one of the most important areas of cyber security domain.

The damage or destruction of critical infrastructures by natural disasters, terrorism and criminal activities accomplished with the use of physical means or by using the cyberspace as a way to launch a cyber attack may have negative consequences for the national security of any country and for the wellbeing of its citizens.

The process of globalization has led to the emergence of regionally and globally distributed critical infrastructure networks, which are vulnerable to cascading disruptions and other specific phenomena. [13] The physical and virtual interconnections through networking among the critical infrastructures that are accomplished through the means of information and communication technology (computer networks working through WAN or internet environment) represent a way to manage the proper functioning of critical infrastructure systems and subsystems. At the same time, all these interconnections between critical infrastructures could imply real weaknesses and vulnerabilities from the perspective of cyber attacks resulting in a domino effect among critical infrastructure sectors.

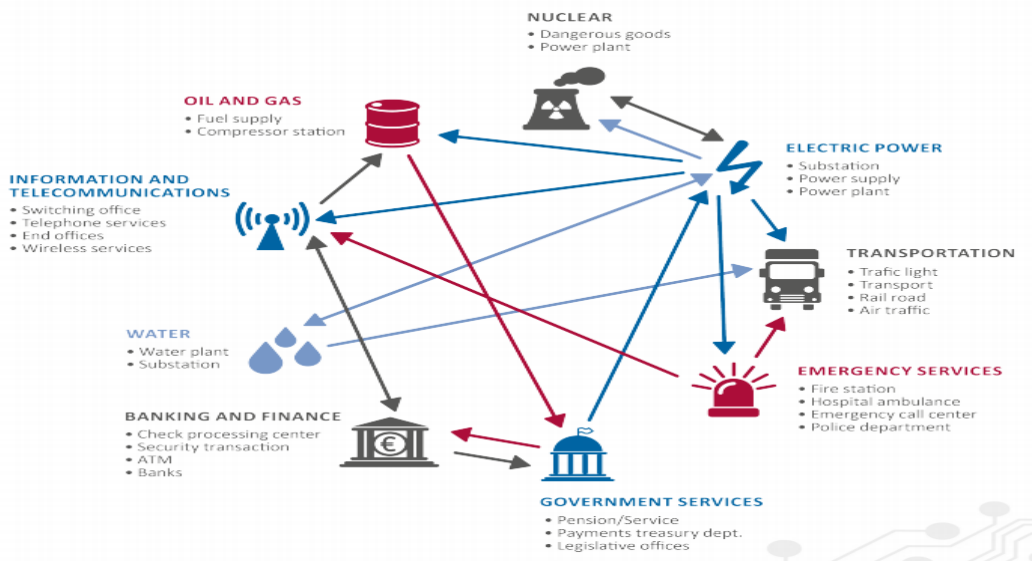

Fig.2 An interconnections' model of CI sectors (ENISA) [14]

THE VULNERABILITY OF CRITICAL INFRASTRUCTURE FROM THE PERSPECTIVE OF CYBER THREATS

As far as the digital technology is evolving, from the cyber security perspective, a comprehensive threat and vulnerability assessments are essential in order to secure the critical infrastructure sectors. Cyber threats on critical infrastructures differ from physical threats in nature by using information and communication technology (computers or other digital devices and means) in order to exploit all vulnerabilities of computer networks that are part of a certain critical infrastructure control system.

Vulnerabilities are weak points and security holes that may cause threats, and which are specific to an asset. Vulnerabilities do not cause any damage by themselves, but they may help threats to occur or cause damage. [15]

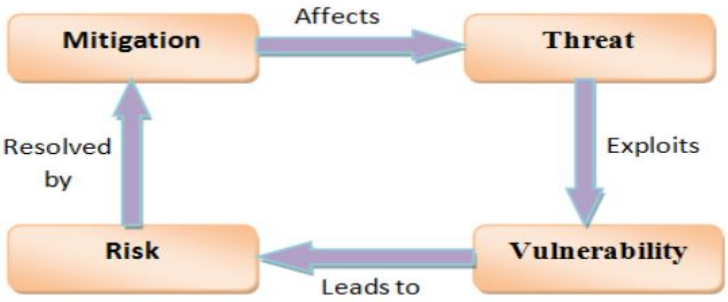

Fig.3 The relation between threats, vulnerabilities and risks [15]

Cyber-physical systems as part of critical infrastructure comprise and integrate ICT parts and physical elements in order to improve usability, reliability, efficiency of the processes, etc. The Industrial Control Systems (ICS) are part of operating critical infrastructures and are widely used in Industrial and Power sectors such as energy, water, manufacturing and pharmaceuticals. Usually, they include Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA), and Distributed Control Systems (DCS). Besides an advantage related to critical infrastructure system operating, those kind of controlling elements introduce also a wide spectrum of cyber risks and an increase in vulnerabilities that are related to cyber attacks.

Cyber security is currently one of the main concerns for SCADA and ICS operators. In fact, SCADA systems collect the data and monitor the automation processes, which are visualized to the operators of the system via human-to-machine interfaces. [16]

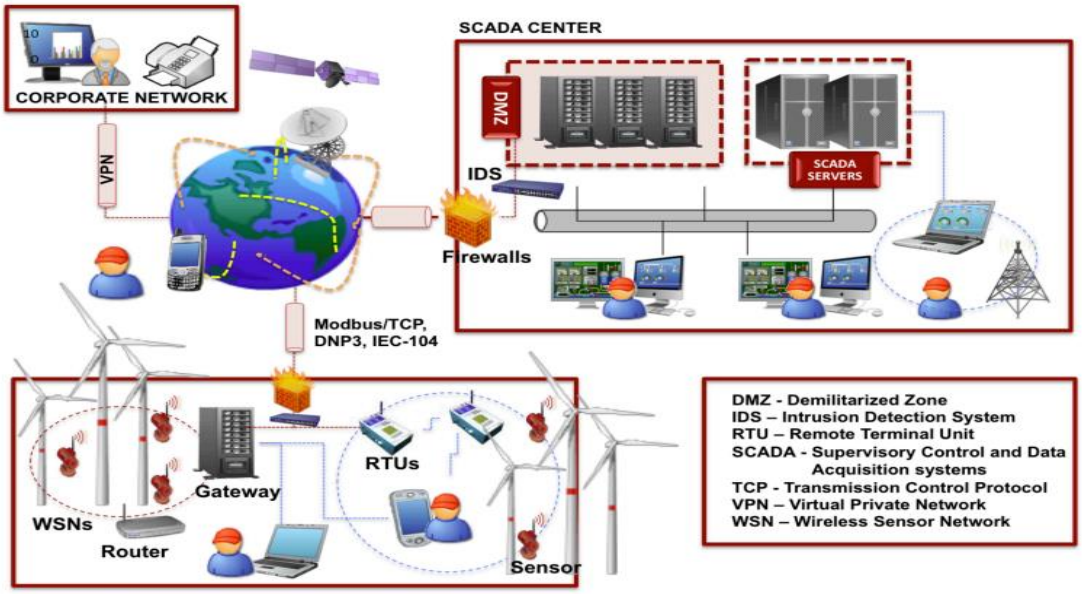

Fig.4 A general architecture of a SCADA network based on remote substations [17]

THE VULNERABILITY OF CRITICAL INFRASTRUCTURE FROM THE PERSPECTIVE OF CYBER THREATS

The ICS are vulnerable to cyber attacks from inside and outside the control system network based on their associated communications and operations' types. In fact, the vulnerabilities of critical infrastructures are increasing due to implementation of ordinary ICT which employs open digital technologies, universal operating systems (OS), or standardized specifications that are the subject to security risks similar to usual information and networking systems.

For better understanding of ICT implementation on the industrial control systems that belong to certain critical infrastructures, on US Cybersecurity and Infrastructure Security Agency (CISA) website is portrayed and described a large-scale production system that utilize SCADA or DCS configuration with many computers, controllers and network communication components.(fig. 5)

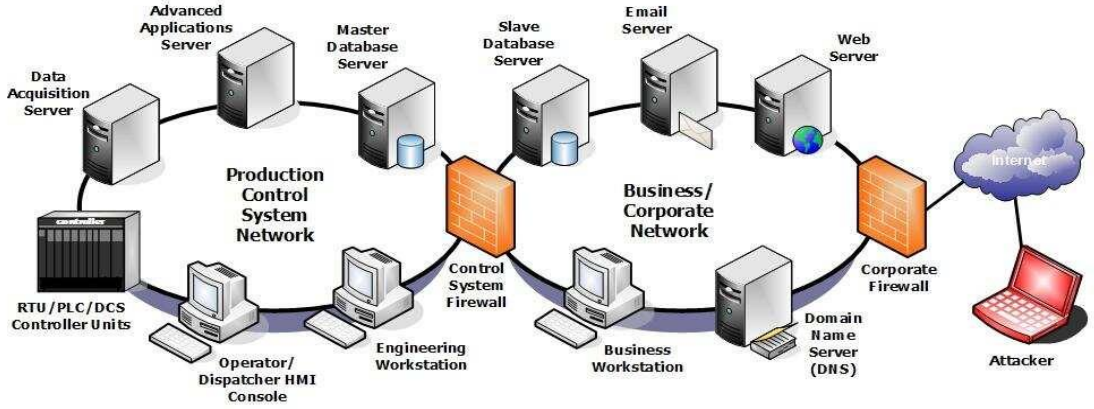

Fig.5 Typical two-firewall network architecture [18]

An attacker who wishes to assume control of a control system is faced with three challenges: gain access to the control system LAN; through discovery, gain understanding of the process; gain control of the process. [18]

All cyber attacks that affect the critical infrastructures, concern the critical infrastructures' operators, government institutions or private companies and service providers. They can be inflicted by the cybercriminals that are seeking financial gain or by some sort of hackers (black hats) that are operating under a certain state actors umbrella. In the year 2010, a well-known cyber attack was conducted in Iran. A malware named Stuxnet, which was susceptible of targeting SCADA systems, in special the programmable logic controllers (PLCs), was employed to Natanz uranium enrichment facility for destroying numerous centrifuges by causing them to burn themselves out. In fact, the first known successful cyber attack on a critical infrastructure system was conducted on December 2015 in Ukraine by using a malware called BlackEnergy3.

Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers. Most affected were consumers of «Prykarpattyaoblenergo» (servicing Ivano-Frankivsk Oblast): 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours. At the same time consumers of two other energy distribution companies, «Chernivtsioblenergo» (servicing Chernivtsi Oblast) and «Kyivoblenergo» (servicing Kyiv Oblast) were also affected by a cyber attack, but at a smaller scale. [19] The attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy 3 malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies. They demonstrated the capability to gain a foothold and harvest credentials and information to gain access to the Industrial Control System (ICS) network. [20]

5. Conclusions

Today, digital transformation is a reality of our modern society and it evolves very fast producing effects in all activity sectors. The information and communication technology, artificial intelligence or internet of things offer to all citizens, industrial sectors, and private or government institutions great opportunities by delivering essential services but in the same time, they could offer many possibilities to cybercriminals for launching cyber attacks within cyberspace.

The reliability on essential services provided by critical infrastructures, continuous operations, safety and security, maintenance and their protection represent national priorities for many countries around the world. The cyber attack on Ukraine power grid that disrupted the energy system has proved the real impact of cyber environment for proper functioning of all critical infrastructures that could be or not interconnected each other.

The disruption or shutting down of a certain critical infrastructure due to a cyber attack could have a domino effect leading to a failure of the associated essential services that are necessary for population wellbeing, for proper operating of the industrial sectors and government institutions, or could cause the stopping of business activities among private institutions. From this perspective, there is a need and a paramount condition to complete a cyber vulnerability assessment and analyses of all possible scenarios that imply the cyber attacks' effects for discovering of the patterns, ways and means used by cybercriminals in order to plan and assure real cyber security measures for a smooth and continuous functioning of all critical infrastructures.

References:

[1] Olga Bucovetchi, Alexandru Georgescu, Dorel Badea, and Radu D. Stanciu, *Agent-Based Modeling (ABM): Support for Emphasizing the Air Transport Infrastructure Dependence of Space Systems,* Sustainability-Open Access Journal, 2019, pg. 1, available online: https://www.mdpi.com/journal/sustainability (accessed on 26 September 2019)

[2] *Critical Infrastructure Security*, available online: https://www.dhs.gov/topic/critical-infrastructure-security (accessed on 26 September 2019)

[3] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,* available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (accessed on 27 September 2019)

[4] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, available online: http://csef.ru/media/articles/3990/3990.pdf or https://ccdcoe.org/research/tallinn-manual/ (accessed on 28 September 2019)

[5] David Rehak, Pavel Senovsky, and Simona Slivkova, *Resilience of Critical Infrastructure Elements and Its Main Factors,* Systems-Open Access Journal 2018, available online: https://www.mdpi.com/journal/systems (accessed on 28 September 2019)

[6] Don Hall, *How to create a secure cyber environment*, Systems-Open Access Journal 2018, available online: https://gcn.com/articles/2018/07/19/secure-agency-environment.aspx (accessed on 29 September 2019)

[7] *Information Technology, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* Homeland Security, 2007, available online: https://www.hsdl.org/?view&did=474327 (accessed on 03 October 2019)

[8] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,* EUR-Lex, 2016, available online: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (accessed on 30 September 2019)
[9] About the CSIRTs (Computer Security Incident Response Team) Network, available online: https://csirtsnetwork.eu/ (accessed on 30 September 2019)
[10] David Terrar, *What is Digital Transformation?*, 2015, available online: http://www.theagileelephant.com/what-is-digital-transformation/ (accessed on 01 October 2019)
[11] *Artificial intelligence applications*, available online: https://zitoc.com/artificial-intelligence-applications/ (accessed on 01 October 2019)
[12] *IoT Environment Compromising Cyber Security*, 2019, available online: https://www.cyberdefensemagazine.com/iot-environment-compromising-cyber-security/ (accessed on 03 October 2019)
[13] Olga Bucovetchi, Alexandru Georgescu, Dorel Badea, and Radu D. Stanciu, *Agent-Based Modeling (ABM): Support for Emphasizing the Air Transport Infrastructure Dependence of Space Systems,* Sustainability-Open Access Journal, 2019, pg. 1, available online: https://www.mdpi.com/journal/sustainability (accessed on 02 October 2019)
[14] Rossella Mattioli, CSIRTs relations team, ENISA, *Securing Europe's information society: bridging the gap between industry, security community and Member States*, 2019, available online: https://download.ernw-insight.de/troopers/tr18/slides/TR18_Keynote_Day_2.pdf (accessed on 02 October 2019)
[15] Marzieh Sameni Toosarvandani, Nasser Modiri, Mehdi Afzali, *The risk assessment and treatment approach in order to provide LAN security based on ISMS standard*, 2012, available online: https://www.researchgate.net/publication/272391570_Critical_infrastructure_protection_Requirements_and_challenges_for_the_21st_century (accessed on 03 October 2019)
[16] Leandros Maglaras, Mohamed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, Helge Janicke, Stylianos Rallis, *Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures*, 2018, available online: https://www.researchgate.net/publication/328077921_Threats_Countermeasures_and_Attribution_of_Cyber_Attacks_on_Critical_Infrastructures (accessed on 03 October 2019)
[17] Cristina Alcaraz, Sherali Zeadally, *Critical infrastructure protection: Requirements and challenges for the 21st century*, International Journal of Critical Infrastructure Protection, 2015, available online: httpshttps://www.researchgate.net/publication/272391570_Critical_infrastructure_protection_Requirements_and_challenges_for_the_21st_century (accessed on 03 October 2019)
[18] *Overview of Cyber Vulnerabilities*, available online: https://www.us-cert.gov/ics/content/overview-cyber-vulnerabilities (accessed on 03 October 2019)
[19] *December 2015 Ukraine power grid cyberattack*, available online: https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack (accessed on 03 October 2019)
[20] *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, 2016, available online: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf (accessed on 03 October 2019)