Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases

Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa, Konstantin Agafonov

▶ **To cite this version:**

Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa, Konstantin Agafonov. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 2020, 2 (3), pp.703 - 715. 10.9770/ird.2020.2.3(7) . hal-03271856

HAL Id: hal-03271856
https://hal.science/hal-03271856v1

Submitted on 27 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

Publisher
http://jssidoi.org/esc/home

CYBER-ATTACKS TO CRITICAL ENERGY INFRASTRUCTURE AND MANAGEMENT ISSUES: OVERVIEW OF SELECTED CASES*

Tomas Plėta [1], Manuela Tvaronavičienė [2], Silvia Della Casa [3], Konstantin Agafonov [4]

[1,2] Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223 Vilnius, Lithuania
[2] General Jonas Zemaitis Military Academy of Lithuania, Šilo 5a, LT-10322, Vilnius, Lithuania
[3] Daugavpils University, Parades Str. 1-421, Daugavpils, LV-5401,
[3] NATO Energy Security Center Of Excellence, Šilo g. 5a, LT-10322 Vilnius, Lithuania
[4] Mykolas Romeris University, Ateities g. 20, LT-08303 Vilnius, Lithuania

E-mails:[1] Tomas.Pleta@vgtu.lt; [2] Manuela.Taronaviciene@vgtu.lt; [3] Silvia.DellaCasa@enseccoe.org; [4] KA1979@gmail.com

Received 15 March 2020; accepted 15 July 2020; published 30 September 2020

Abstract. The purpose of the paper is to analyze the vulnerabilities of Critical Energy Infrastructures' systems in the event of cyber-attack. The global tendency of cyber-attacks puts Critical Energy Infrastructures on one of the first places for targets. Critical Infrastructure Protection (CIP) has become an increasingly relevant topic in the global industrial environment, as the consequences of cyber-attacks toward ICS can result in physical disruption and loss of human lives. The analysis presented in the paper will take into consideration three different case scenarios of cyber-attacks to Critical Energy Infrastructures, and will evaluate the outcomes and the tactics used by the organizations' response and recovery.

Keywords: critical infrastructure; management; cyber-attack; energy security; cybersecurity

Reference to this paper should be made as follows: Plėta, T., Tvaronavičienė, M., Della Casa, S., Agafonov, K. 2020. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. *Insights into Regional Development*, 2(3), 703-715. https://doi.org/10.9770/IRD.2020.2.3(7)

JEL Classifications: M15, Q48

Additional disciplines political sciences; information and communication; energetics and thermoenergetics; informatics

This research was partly supported by the project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

European Research Council
Established by the European Commission

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

1. Introduction

With the beginning of a new decade, the world in which we live is changing constantly, with continuous implementation of new types of technologies. The constant updating of new infrastructural possibilities has, on the one hand, the consequence of bringing more power onto our hands, but on the other, a world that is more and more "connected" can be subject to non-indifferent threats. The implementation of devices connected to the Internet of Things (IoT) is increasingly popular among the population, and it presents undeniable advantages as well for businesses. With IoT-based systems, there is the possibility of having more connected devices, and at the same time eliminating partially the need for human intervention for the control of the edge devices (Bhayani, 2016). However, with the possibility of faster and more precise information comes also a new set of expected threats to the software's security. The expected number of devices that by 2025 will be connected to the Internet is 75 billion (Resul Das, 2019), but the digital integration of industrial control systems will probably be more vulnerable to cyber-attacks. If we consider the number of "external attacks", such as hackers, the number has increased by 9 percent from 2017 to 2018 alone (Accenture Security, 2018).

The dependency that the Industrial Control Systems (ICS) are developing to the Internet of Things (IoT) connections is a big potential risk especially in terms of Critical Infrastructures (CI). Malicious forms of cyber-attacks have brought an increase of security breaches, increasing 11% from 2017 to 2018 and an outstanding 67% from 2013 (Accenture Security, 2019). The growing targets of cyber-attackers are part of the Operational Technology (OT) environments, such as water systems, energy plants, transportation, communication, critical manufacturing i.e. every type of CI. Critical Infrastructure Protection (CIP) has become an increasingly relevant topic in the global industrial environment, as the consequences of cyber-attacks toward ICS can result in physical disruption and loss of human lives. Each country has a different approach towards cyber threats in CI, and the increasing number of disrupting episodes brought to huge investments in cybersecurity strategies. The cybersecurity of many businesses is hardly adequate: the proposed techniques to secure vulnerable networks are many, from Blockchain technology to mechanical analogic "unhackable" components (Marszal, 2019). However, the main cause of cybersecurity breaches remains the human factor, source of 95% of network infection (Ahola, 2019), both unintentional errors to lack of proper action.

The purpose of the paper is to consider techniques, viruses or attacks done against CIs, in particular of energy-related production. The analysis is conducted with the focus on types of frameworks developed for the response to cyber incidents in critical infrastructures. The latter will be evaluated in terms of prevention and solution applied after the end of the threat. This focus of the paper is due to the lack of effective comprehensive framework appliable to critical energy infrastructure protection, maybe because of its high complexity. An issue can be the lack of willingness to share information by a damaged company after the cyber-attack, as it may seem a sign of weakness for the company. Usually, the security breaches are possible because of obsolete or inefficient industrial infrastructures and, thereafter, they do not share vital information to maintain the reputation of the company. On the other, open access to data regarding new types of cyber-attacking techniques could be taken from hacking groups and used to damage other targets.

Examples of cyber-attacks in the next chapter will have a double function: firstly, they will help to highlight the usual critical elements of cyber emergencies, and then to assess the possible solution taken following that event. Even if there are plenty of proposed guidelines for cyber-attack management models, concerning critical energy infrastructures there is no clear classification of the degree of effectiveness of the attack, the degree of protection of the critical infrastructures or evaluation of the security system. The goal of this article is to highlight the variety

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

of vulnerabilities encountered in the event of cyber attacks in critical energy infrastructures and to verify if it is possible to formulate adequate criteria to compose a comprehensive cybersecurity strategy.

The methodology that will be used to conduct this reasearch will be of comparative approach: the phenomenon that will be analyzed will highlight the response and the cybersecurity level of critical energy infrastructures against cyber-attacks. The cases will be analyzed individually in order to determine the type of responses of the attacked organizations and their mistakes during and after the attack. Then the results will be classified in terms of type of mistake and the results will be compared in order to determine the most frequent mistakes in this type of infrastructures. However, before diving into the analysis it is important to understand in general the level of security in critical energy infrastructures.

2. Vulnerabilities in critical energy infrastructure

The possibility represented by the Internet of Things (IoT) was appealing at first for many businesses. For many, it meant safety and efficiency in the delivery of data, assisted decision-making and overall comfort. Before the updating of these systems, technology control was divided in Informational Technology (IT) and Operational Technology (OT) environments. IT is used mainly for systems that store, process and deliver information of an organization, while OT is for physical plant equipment, such as the aforementioned SCADA systems and embedded computer technologies (Inductive Automation, 2020). With the introduction of the IoT, however, the two environments started to converge, with industrial organizations introducing the Industrial Internet of Things (IIoT), a new kind of environment in which OT and IT coexist in the same environment. If OT technologies before were relegated to closed networks, with the IIoT the chances of being targeted for cyber-attack have risen to a critical point. If the convergence of OT and IT environments has been a rapid procedure, the same cannot be said for the development of an adequate response strategy for cyberattacks against industrial systems. Of these systems, Critical Infrastructures represent a major part, such as energy service sectors, dams, financial services, nuclear reaction sectors, agriculture, healthcare, communication, manufacturing, etc.

In the event of cyber-attacks, the role of the security manager of the attacked company is fundamental in ensuring the correct procedure for an efficient response. The work of the security manager can be divided into three major phases: before, during, and after the attack. For each phase, the common goal is to ensure a safe environment to exchange sensitive data, and to be able to restore the system is the latter is damaged due to external or internal factors. To develop an effective method to prevent cyber-security breaches there is the need to keep up-to-date firewalls and anti-virus in every device since outdated systems are most vulnerable to cyber-attacks (Ryder, 2019). Another necessary element onto which the company should rely on in the case of cyber-attack is the presence of efficient backup: many companies have not standardized cybersecurity risk meters; hence, they do not know its normal operating behavior (Israel, 2019). The majority of management strategies tend to reserve the same approach, minus some specifics, to every type of business: the distinction is usually made on “big vs small enterprise” type of model.

As aforementioned, the updating of ICS to the IoT has brought more vulnerabilities to cyber-attacks, as hackers developed different kinds of techniques to breach the systems’ security. Cyber-attacks to critical infrastructures can threaten human life as well as physical damage to the facilities, using multiple techniques at the same time (Resul Das, 2019). Attacks can be divided into five major groups, divided by the objective pursued by the attacker: *corruption of information, denial of service (DoS), disclosure of information, theft of resources* and *physical destruction* (Limba et al., 2017). However, the most used techniques for targeted cyber-attacks are *phishing*, sending multiple emails asking for sensitive information, and *ransomware*, with theft of sensitive data and the demand of a ransom in exchange for their restoration. Another example can be the deployment of *botnets* or the *subversion of the supply chain*, by attacking directly the equipment (CESG, 2015).

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

Cybersecurity in enterprises can present a challenge both in the implementation and in the case of cyber-attack event. It is important to remember that there is not a possible "one solution fits all" model for what concerns businesses, as each company or organization possesses different kinds of infrastructures and technical aspects. There are effective guidelines for the management of cyber incidents, however usually the attacked companies were caught unprepared in emergencies, both from the preparation of effective security measures and from immediate responses. The following chapter will try to depict the possible vulnerabilities of critical energy infrastructures, and to assess their possible consequences.

If we talk about the cybersecurity of power grids, the situation needs to be issued by keeping some key aspects in mind. Firstly, when talking about power grids, there is a need to divide the various types of energy infrastructures by the type of resource. Besides fossil fuels, the most extended power grid is issued by electricity coming from nuclear energy, geothermal energy, hydro turbines, combustion turbines, wind turbines, and solar direct (Blume, 2007). The vulnerability of power grids depends on their dynamic infrastructure systems that are usually multi-layered in their structure (Amin, 2010). Cyber-attacks targeting power grids require a higher level of urgency at a developing level, as the consequence of the hack of one of the parts of the systems brings potential risk to human life, environment, and businesses. In general, even though power grids are extremely complex and extended in their organization, the trend in the past few years has been of centralizing the control of electric power systems. As aforementioned, there have been several attacks against electric grids, which shows how easy it has become for hackers to gain control of the interfaces and send orders to the mechanical components, such as switches and connectors, and to halt the electricity flow in the plant, possibly causing blackouts or explosions (Kshetri, 2017).

The issues related to the electric power grids are a priority to each state's security, in a world increasingly dependent on the Internet and hence electricity such as in healthcare and businesses. Possible development of so-called "smart grids", grids with digital technology that allows two-way communication between the utility and the consumers, represented a big step in the development and the reliability of electricity. However, the digitalization of the grid has raised the vulnerability to cyber-attacks, as it blurred the lines between operational, informational and communication technologies (Oracle, 2012). The European Network and Information Security Agency (ENISA) differentiate the parts of ICS systems that support the smart grids and can be vulnerable to cyber-attack. The list differentiates *operational systems*, *classic IT systems*, *communication*, *networks and protocol* and *endpoints* (Egozcue, 2012). The interconnectivity brought by the digitalization of such systems assures efficiency and improve consumer service (Amin, 2002), but there are plenty of examples of attacks towards smart grids. In particular, to keep the security systems up-to-date, there is the periodical updating of security patches, but the issue is that sometimes it is not supplied to end-users, or are supplied but not applied for fear of affecting the software performance (Amin, 2010). One of the most significant components of smart grids is the Advanced Metering Infrastructure (AMI), which measures and gathers the information of the energy consumption to the households. The AMI usually consists of billions of low-cost commodities devices that are usually located in marginal positions, depending on the size of the grid (McLaughlin, 2010). If the Smart Meter (SM) is compromised by a cyber-attack, the hacker will be in control of the household power supply and use the SM as an entry point to further attacks to the system's network (Mahmud, 2015).

Many companies are using ICS, operated by a specialized assembly-like code on a programmable logic controller (PLC) that are usually not connected to the Internet (Falliere, 2011). The term ICSs systems can be used for several types of systems, such as DCS (Distributed Control Systems), SCADA (Supervisory Control and Data Acquisition), IAS (Industrial Automation System), IACS (Industrial Automation and Control System) and PLC (Programmable Logic Controller) (Drias, 2015). DCS is generally used for plants for process and generation, while SCADA systems regulate the distribution. The so-called "air-gapped" networks, as physically isolated from unsecured networks, are a common procedure for companies to enhance their resilience to external threats, such

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

as malicious codes. However, it is possible to infect any end device of the network by the introduction of a USB containing malicious code that could affect the whole system.

Most of the cyber-attacks are caused by the human factor, and the introduction of malicious codes in the system via USB\CD is a good example of it. It is a much-used technique for hackers to throw in the targeted company's parking lot or however near its facilities an infected USB card. As one of the employees will find it and, because of curiosity, will plug into the computer to see what is inside of it. A second option is to pay off an employee (or a former one) to plug in the USB. In both cases, however, it depends on the degree of security of the system: for what concerns the next step, or the control of the PLC, as a preventive measure, it can be needed a signature of driver files with a private key, unknown to external actors (Falliere, 2011). Yet in this scenario, the problem is mainly relying on the individual employee behavior, as he\she could agree to either steal or copy the signature in exchange for money. Another issue is the vulnerability of the network to malicious attacks: seldom hackers exploit the so-called zero-day vulnerabilities, meaning flaws in the system undetected from the programmers during the installation of the software. In general, there are many issues with the vulnerability of ICS of critical energy infrastructure in particular, since many companies do not possess an adequate plan of response to the event of a cyber-attack, and the staff is unprepared or unaware of the correct procedure.

3. Examples of cyber-attacks

In the following chapter, an analysis will be performed among cyber -attacks against Critical Energy Infrastructures (CEI). As aforementioned, Critical Infrastructures are being targeted for cyber-attacks, and the number has grown in the past years. The oldest on record is the Stuxnet malware, which in 2010 targeted Iranian uranium enrichment facilities (Kerr, 2010) before spreading to other countries. The 2012 Shamoon malware as well as disrupted the servers of Saudi Aramco, the biggest oil producer in the world located in Saud Arabia (Alshathry, 2017). Finally, the 2015 attack to the Ukraine power grid caused power outlets and was made appositely for the electric grid. These events, in particular, were chosen to represent the examples of critical energy infrastructures cyber-attack firstly because of the common target-type of critical energy infrastructure as well as highlighted substantial lacking in the organization and security of the attacked networks. The analysis will focus on the responses of the company\government during and after the attack, and to the determination of the "correct" procedure to follow in similar situations.

The cases that were chosen for the analysis represent the most well-known events of cyber-attacks to critical energy infrastructure. The Stuxnet case traced back in 2010, was one of the first-ever recorded cyber-attacks that were appositely designed targeting specifically a nuclear plant, so one critical energy infrastructure. It is also interesting to consider how, despite almost a decade passing, the case did not report a confirmed culprit, and that there still is no current solution to the worm's effects. The second case, the Shamoon malware, was also particularly interesting because the company in question, Saudi Aramco, was targeted by cyber-attack both in 2012 and 2017, also with a similar pattern in both of the cases. The analysis will be conducted on the 2012 attack since it was the first occasion to observe the organization's response. About the Ukrainian case, it would be unfitting to perform an analysis of cyber-attacks and leave out the events happening in Ukraine in the last decade. The country was repeatedly targeted by cyber-attacks and other examples of hybrid warfare, mostly from Russian origin. The 2015 attack as well represents a case in which a cyber-attack caused physical disrupture that affected directly the Ukrainian citizens (power losses).

[1] The Stuxnet worm (2010*)*

The first attack that will be taken into the analysis is the Stuxnet worm, which was discovered in 2010. The worm aimed to possibly disrupt Iranian nuclear installations. The attack was conducted to the Iranian nuclear plant and

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

uranium enrichment site in Natanz, during a difficult period of tension between the US and Iran (Baezner, 2017). Although the official perpetrators of the attacks are still unknown and the virus managed to spread to approximately 100,000 infected hosts (Falliere, 2011), the virus presented some elements that put Iran as the targeted country. The worm, programmed to infect SCADA systems, in particular, PLCs organized in groups of 164 objects, and the cascades of the Natanz plant arranged in 164 centrifuges. The attack was conducted by an insider since the facility was using air-gapped software to carry out the production (Beazner, 2017).

The modality of attack following the implementation of malicious code can vary, as from a peripheral device the worm could either retrieve sensitive information, modify the supply chain by overriding ICS and at the same time to fool the plant operators into believing that the process is operating as usual (T. Ayral, 2016). However, to effectively gain PLC control, it is needed to now deeply its structure and functioning. The case of the 2010 worm Stuxnet represents a valid example of it, as the research before the attack allegedly took at least six months by a team of five to ten programmers, who developed the program to target exactly the PLCs of an Iranian nuclear plant and uranium enrichment facilities (Baezner, 2017). Thanks to the exploit of four zero-day vulnerabilities the hackers managed to gain control of the system and to spread the malicious worm to more than 10.000 hosts (Falliere, 2011).

In this case, the attack was made possible by an *insider*, meaning the introduction of external malicious codes that disrupted the system. For this reason, the main error that was made by the management system was first to *lack of testing* and *lack of communication*. The first represents the lack of adequate testing of the security responses, necessary to find the flaws of the systems via simulations, considering the zero/days vulnerabilities of the Microsoft Windows operating system used to spread the virus. The second concerns the behavior of the organization during and after the attack. Since the attack in itself was probably politically motivated, as it targeted Iranian uranium enrichment facilities, Iran did not denounce publicly the attacks' impact right away. After the Iranian officials admitted that some personal computers resulted infected with a computer virus, Iran abruptly stopped its production of enriched uranium for apparently no reason (Beazner, 2017). The latter is a usual mistake made by attacked organizations, as admitting to having been targeted and damaged from a cyber-attack affects their public image and so seldom the tendency is not to disclose any detail, making the eradication and recovery process even harder. In the case of Stuxnet, the physical damage was caused to the centrifuges controlled by the PLC. From the centrifuges used by the Natanz facility, ranging from 6000 to 9000 objects, 1000 had to be changed (De Falco, 2012).

The best practices advised contrasting this type of attack are targeting the management strategy of cyber incidents since the attack was made possible by the attackers' possession of digital certificates necessary for entering the system unnoticed (Beazner, 2017). Hence, the first thing to consider in building an effective security system is the creation of working groups that have to review the protocols and the overall security of SCADA systems. It is fundamental to introduce encryption and mutual authentication for every device connected to the system (De Falco, 2012). As aforementioned, it is fundamental also to apply strict rules for the management of digital certificates, such as the *storing of private keys* and the quality of the certificate.

Concerning this scenario, the main management mistakes concerned the communication techniques and the lack of testing of the system's flaws. The communication was uneven and unclear to national and supranational authorities, unacceptable behavior in CEI: transparency and collaboration are fundamental to ensure the readiness of response. The flaws of the system, in particular the zero-day vulnerabilities, allowed the hackers to infiltrate the malware and affect the functioning of the PLC. Continuous testing is required to discover potential weak spots of the system and to fix them without exposing the whole infrastructure at risk.

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

[2] The Shamoon malware (2012)

The second type of attack that will be considered for the analysis in the case of the Shamoon malware of 2012, which targeted mainly Saudi Aramco, the largest oil production company of the entire world, centered in Saudi Arabia. Also known as *W32.Disttrack*, the malware consisted of three components, which affected an estimated 30,000 computers in the facilities of Saudi Aramco (Wuuest, 2014). The *dropper,* the main component, dropped components in the infected computer, copied and executed itself every time Windows was opened. The *wiper*, second component, is the destructive module which erased files from specific locations in the computer: after sending the information to the attacker, it overwrote the files with corrupted jpeg files. The final component was the *reporter,* which sent information back to the attacker's central computer (Mackenzie, 2012).

This type of attack, despite being associated with the target to the Stuxnet malware, represents an interesting case for cyber-attacks to energy infrastructures. The attack was probably brought out by an insider, someone who got access to users' credentials and gained access to the domain controller (Wuuest, 2014). Although it was compared to Stuxnet, the perpetrators were described as "skilled amateurs", because of the inferior level of competence and programming skills detected by the authorities (Bronk, 2013). The type of attack in consideration is *APT (Advanced Persistent Threat)*, meaning that the attackers have found the password hashes of the administrative accounts and gained the access to higher levels of the system (Alshathry, 2017).

The issues presented in this case are focused on the response of the organization to the cyber-attack. The issue that was mainly raised by the international authorities about the actual impact of the attack on the organization's system. The company declared shortly after the cyber-attack to have reduced its electronic systems from the outside to avoid further attacks. Saudi Aramco declared that, despite the wipe-out of data from the server, no physical disruption was recorded and the recovery of the company was complete (Alshathry, 2017). Nevertheless, the downtime of the organization's websites was recorded also after the declaration of complete recovery (Bronk, 2013).

The main issue represented by this attack is the *lack of communication*, so the behavior of the organization during and after the attack. The information regarding the attack was partial during and after the attack, considering that the infection spread beyond the initially targeted organization onto other companies, losing drilling and production data. The drilling procedures produce a huge quantity of data, which is sent to the Saudi Aramco database. The data was then centered and filtered and sent back manually twice a day. Perhaps because it was Ramadan, there were no backups for drilling and production data, and the filtered data got lost (Bronk, 2013). However, the company declared complete recovery almost immediately after the attack, in a way to assure other vendors and costumers that the damage was peripheral and contained. As aforementioned, this is a wrong approach in responding to cyber-attacks, especially in Critical Energy Infrastructure.

The main management problem identified in this scenario is the lack of security and lack of communication. The attack highlighted the lack of backups in the systems, which caused the websites and the data to be wiped out. In the management of cyber incidents, the solutions that are offered to mitigate the problem have to be implemented in the preparation phase. The most effective in this case is *redundancy,* an alternative response to a failing condition. In Critical Energy Infrastructure a failure in the system can resolve in physical damage, hence it is fundamental to ensure a homogenous process. *Redundancy* consists in the presence of a backup that is constantly updated to "mirror" the used components and, in case of the failure of the latter, immediately assumes control (ICS Engineering Inc., 2017). The implementation of this type of device should be mandatory in Critical Energy Infrastructures, as it makes the recovery from the attack a quicker process.

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

[3] Ukraine cyber-attacks (2015-16)

The last case scenario that will be considered for the paper's analysis will be the cyber-attack that took place in Ukraine in 2015-2016, targeting the Ukrainian power grid. The attack was due to an intruder in the company's computer and SCADA system (E-ISAC, 2016). On December 23, 2015, approximately 30 substations were disconnected from three hours, causing a power outage in three of its regional electricity distribution companies, Kyivoblenergo, Prykarpattyaoblenergo, and Chernivtsioblenergo, cutting out of power more than 200,000 costumers (FireEye, 2016). The perpetrators have been recognized as the *Sandworm Team*, a Russian hacker group that targeted NATO, European governments and ICSs in general (Park, 2017).

The attackers were highly skilled for the job, and the technical components used to conduct the attack were many. Firstly, *spear-phishing* was used to gain access to the business networks of the facilities (E-ISAC, 2016). The next phase was to implement the malware *BlackEnergy3*, the third variant of *BlackEnergy*, used by the Russian underground in *distributed denial-of-service* attacks (FireEye, 2016). The access then was used to steal the credentials from the business networks, including Virtual Private Networks (VPN) to enter the ICS network (E-ISAC, 2016). Then the attackers used existing remote access tools to issue commands from a remote station, and used a modified *KillDisk*, a hard drive eraser software, to erase the attacked organizations' systems. The power outages were caused by the *UPS systems* of the facilities, which usually provides emergency power to a load during electric fails, that impacted instead the connected load and caused the outage. The last part was to issue a *Distributed Denial of Service (DDoS)* attack to the call center so that costumers were not able to report the issue (E-ISAC, 2016).

From the management perspective, the mistakes that led to the attack can be traced both in the phase of preparation against cyber-attacks and the phase during the attacks. The opportunities that the hackers exploited in this case were many, from the availability of open-source information on the type of ICS system that was used in the facilities and the lack of *two-factor authentication* in the VPNs (E-ISAC, 2016). Moreover, the media indicated that the facilities did not possess any capability of network security monitoring, with no one able to manually monitor the ICS network (E-ISAC, 2016). Firstly, it is necessary to enhance networking security monitoring capability, as the attack managed to gain control of the system also because of the lack of controls on its access points (FireEye, 2016). Moreover, implementing measures such as *Area of Responsibility (AoR)* limitations, meaning that only one operator could control some components of the system, could limit the possibility of the hackers to gain the control of the *HMI (Human Machine Interface)* (E-ISAC, 2016). Finally, the implementation of *two-factor authentication*, *blockchain technology* or *application whitelisting* could improve the secure management of access into the system.

4. Observations and recommendations

In the following chapter, there will be a comparison of the results that were shown in the analysis of the cases of cyber-attacks. As seen in the introduction, the expected results that will emerge from the comparison will be hopefully useful in determining the more vulnerable areas in cybersecurity. The model that was chosen to determine the criteria of comparison and to evaluate the common mistakes and areas of interest will be the one adopted by Limba et al. in *Cyber Security Management Model for Critical Infrastructure* (Limba et al., 2017). According to the article, the criteria which determine a cybersecurity management model are six: first, the *legal regulation*, which concerns the legal proceedings and aspects achieved by the organization in terms of legislation acts such as security instructions, information security officials, etc. (Limba et al., 2017). Then, *governance* concerns the understanding of the need for minimizing the impact of cyber incidents into the organizations and

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

risk management instead analyzes the growing risks around the organization (Limba et al., 2017). *Cyber Hygiene* is important for every organization as well, meaning that security must be understandable for every member of the organization (Limba et al., 2017). Finally *Technology management and Incident Management:* the first is about the knowledge about each component controlled by IT, while the second is more about the legal dimension, concerning special plans that need to be applied in case an incident occurs (Limba et al., 2017). It follows a summarization of the cases analyzed in the article and the aforementioned categories. The x marks the presence of a lack in the concerned area, and the cases are in the order in which they were presented in the paper (see Table 1).

Table 1. Identified gaps in cybersecurity model dimensions

	Governance	**Law and information**	**Cyber hygiene**	**Risk Management**	**Technology Management**	**Incident Management**
Case [1]	**x**			**x**		
Case [2]		**x**	**x**			**x**
Case [3]	**x**		**x**			

Sources: estimated by authors; used model (Limba et al., 2017)

The first analyzed cyber-attack in the article, Stuxnet, presents an interesting case for what concerns the gaps in the organization's cybersecurity model (Natanz nuclear plant). As mentioned in the analysis, the organization dealt with *a lack of communication* and a *lack of security*, but it can be tailored to the model presented in the table. As the table shows, the Stuxnet case (*Case [1])* presents gaps in *governance* and *risk management.* As said in the previous paragraph, to have *good governance* is fundamental to ensure proper cybersecurity, and that means as well that each project of activity planned in the organization must be reviewed from a security perspective (Limba et al.,2017). The Stuxnet case showed the vulnerabilities of the system of the Natanz power plant, and the organization seemed to not to worry about cyber vulnerabilities. The same type of gaps was as well recorded in *Case [3]* (Ukraine 2015 attack), because in that case the cyber-attack was conducted thanks to spear-phishing emails, implying that the system was not protected enough. About the *risk management* gap recorded in the Stuxnet case, it implies that the lack of security and testing provided multiple zero-days vulnerabilities that were then used by the hackers to introduce malicious codes into the system (Falliere, 2011).

The *Case [2],* as the Shamoon malware, recorded a *lack of communication,* as mentioned in the previous analysis. As the table indicates the gaps in cybersecurity model dimensions, this case was classified under *law and information, cyber hygiene* and *incident management.* The malware disrupted the system of the Saudi Aramco oil plant and wiped away the filtered data from many computers (Mackenzie, 2012), but the lack of backups for drilling and production data worsened the damages. Besides the lack of a built-in (not manual) backup system, there was no personnel checking on the missing filtered data, hence a gap in *cyber hygiene* (Mackenzie, 2012). The Ukrainian case as well presented a gap in *cyber hygiene,* since the method of spear-phishing was used to gain control of the business networks of the facilities (E-ISAC, 2016). For what concerns the *incident management,* the Shamoon malware was badly handled in terms of communication with the authorities since the organization passed just a part of the information (Bronk, 2013).

In conclusion, both the *governance* and *cyber hygiene* present the most targeted dimensions of cybersecurity gaps, since they are both presents in two cases out of the analyzed three. However, it is important to mention that, even with the provided model of identification of cybersecurity model dimensions, six categories are still not enough to cover all the aspects that are typical of critical energy infrastructure. The peculiarity of the latter depends on the

ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

interconnectivity and on the overlap of IT and OT environments necessary to have full coverage of the system. There are still no calculations that offer adequate criteria to measure the impact of cybersecurity measures on critical energy infrastructure, but this analysis can be taken as an example of the multitude of elements to take into consideration.

5. Conclusions

The convergence on IT and OT technology brought to life a new concept of online systems, alongside multiple innovations in the management of Critical Infrastructures(CI). However, alongside the innovation comes a new concept of cybersecurity, as the protection of CI is becoming more difficult to achieve from both IT and OT perspective. The global tendency shows that the Critical Energy Infrastructures are due to be one of the main targets of cyber-attacks, hence the priority is both to increase their protection and to raise awareness on the general lack of preparation concerning the development of an effective cybersecurity strategy for critical energy infrastructures. The analysis of the paper showed three case scenarios that depicted different cyber-attacks to Critical Energy Infrastructures, analyzing the response of the organizations and the mistakes of the management in the preparation and the response.

As aforementioned, the human factor plays an important role in cybersecurity: it is one of the main causes of cyber-attack, both in lack of knowledge or in incorrect behavior. The analysis showed that in all of the cases of cyber-attacks, given the political nature of the conflict, information was not disclosed entirely, or was partially excluded from the reports. This type of error, alongside security issues, is the most dangerous to Critical Energy Infrastructures, as it not only compromises the integrity of the attacked organization but leaves out the possibility of studying the used worm or technique, so for the hackers potentially to replicate them somewhere else. To develop a correct response to cyber incidents, it is necessary to communicate and cooperate on a national and international level.

The model that was introduced in this article should shed some light on the issue of cybersecurity of Critical Infrastructure and should be aiming to measure adequately the cybersecurity level of an organization. As aforementioned, critical energy infrastructure require an additional level of preparation and complexity due to the merging of IT and OT environments. Moreover, in the comparison of the results, it merged a possible model to evaluate cybersecurity level of critical energy infrastructure, but the calculations and the described areas are far from being adequate.

References

Accenture Security. (2018). *Gaining ground on the cyber attacker: 2018 State of Cyber Resilience.* USA: Accenture Security. Retrieved from https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index

Accenture Security. (2019). *The Cost of Cybercrime.* Traverse City, Michigan: Ponemon Institute. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Ahola, M. (2019, October 18). *The Role of Human Error in Successful Cyber Security Breaches.* Retrieved from usecure: https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches

Alshathry. (2017, February). Cyber Attack on Saudi Aramco. *International Journal of Management of Information Technology, 11*(5), p. 3037. doi:https://doi.org/10.24297/ijmit.v11i5.5613

Amin, M. (2002). Security challenges for the electricity infrastructure. *Computer, 35*(SUPPL.), 8-10. doi:https://doi.org/10.1109/MC.2002.989920

Amin, S. M. (2010, Spring). Securing the Electricity Grid. *The Bridge: Linking Engineering and Society, 40*(1), 13-19. Retrieved from http://massoud-amin.umn.edu/publications/Securing-the-Electricity-Grid.pdf

Ayral T., O. J. (2016, July). *Minimize industrial cyber security risk in plants in 12 steps.* Retrieved from Hydrocarbon Processing: https://www.hydrocarbonprocessing.com/magazine/2016/july-2016/process-control-and-instrumentation/minimize-industrial-cyber-security-risk-in-plants-in-12-steps

Beazner M., R. P. (2017). *CSS Cyber Defence Hotspot Analysis: Stuxnet.* Zurich: Center for Security Studies (CSS), ETH Zurich. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

Bhayani M., P. M. (2016). Internet of Things (IoT): In a Way of Smart World. In B. Y. Satapathy S., *Proceedings of the International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing* (Vol. 438). Singapore: Springer.

Blume, S. W. (2007). *Electric Power System Basics.* (I. o. Engineers, A cura di) Wyley and Sons, INC.

Bronk C., T.-R. E. (2013). *Hack or Attack? Shamoon and the evolution of Cyber Conflict.* SSRN. doi:http://dx.doi.org/10.2139/ssrn.2270860

CESG. (2016). *Common Cyber Attacks: Reducing The Impact.* London: CESG. Retrieved from https://www.ncsc.gov.uk/static-assets/documents/common_cyber_attacks_ncsc.pdf

Chesla, A. (2012, October 25). *Cyber War Rooms: Why IT Needs New Expertise To Combat Today's Cyberattacks.* Retrieved from Security Week: https://www.securityweek.com/cyber-war-rooms-why-it-needs-new-expertise-combat-todays-cyberattacks

Darville C., D. B. (2015). *Cyber Security Incident Management Guide.* (C. f. Belgium, A cura di) Belgium: Cyber Security Coalition. Retrieved from https://b-ok.cc/book/3704644/d3244d

Das R., Z. G. (2019). Analysis of Cyber-Attacks in IoT-based Critical infrastructures. *International Journal of information Security, 8*(4), 122-133. Retrieved from http://www.ijiss.org/ijiss/index.php/ijiss/article/view/490/pdf_80

De Falco, M. (2012). *Stuxnet Facts Report: A Technical and Strategic Analysis.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Dragos. (2017). *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations.* Hanover: Gragos.Inc. Retrieved from https://www.key4biz.it/wp-content/uploads/2017/06/CrashOverride-01.pdf

Egozcue E., R. D. (2012). Annex II. Security aspects of the smart grid. In D. H. E. Egozcue, *Smart Grid Security: Recommendations for Europe and Member States.* European Network and Information Security Agency (ENISA). Retrieved from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case.* Washington: SANS ICS. Retrieved from http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Falliere N., M. L. (2011). *W32.Stuxnet Dossier.* Cupertino, CA: Symantec Security Response. Retrieved from https://css.csail.mit.edu/6.858/2014/readings/stuxnet.pdf

FireEye. (2016). *Cyber Attacks on the Ukrainian Grid: What you should know.* Milpitas, CA: FireEye. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf

ICS Engineering Inc. (2017). *Types of Redundancy.* Retrieved from ICS Engineering Inc.: http://www.icsenggroup.com/types-of-redundancy.shtml

Inductive Automation. (2020, February 28). IIoT: Combining the Best of OT and IT. *Industrial Ethernet Book , 95\14*. USA: IEB Media GdR. Retrieved from https://iebmedia.com/index.php?id=11673&parentid=63&themeid=255&hft=95&showdetail=true&bb=1

Israel, M. (2019, April). No More Dangling from Rooftops: Integrating Cybersecurity. *Advancing Automation Cybersecurity into the Connected Plant Transformation, XV*, p. 5-9.

Kerr P., R. J. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* Washington: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/natsec/R41524.pdf

Kshetri N., V. J. (2017). Hacking Power Grids: A Current Problem. *IEEE Security & Privacy*, 91-95. doi:10.1109/MC.2017.4451203

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

Mackenzie, H. (2012, October 25). *Shamoon Malware and SCADA Security – What are the Impacts?* Retrieved from Tofino Security: https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-–-what-are-impacts

Mahmud R., V. R. (2015). A survey on smart grid metering infrastructures: Threats and solutions. *2015 IEEE International Conference on Electro/Information Technology (EIT)* (p. 386–391). IEEE.

McLaughlin S., P. D. (2010). Energy Theft in the Advanced Metering Infrastructure. *International Conference on Critical Information Infrastructures Security* (p. 176-187). Berlin: Springer-Verlag Berlin Heidelberg. doi:10.1007/978-3-642-14379-3_15

NATO. (2020, March 17). *Cyber Defence.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/topics_78170.htm

OpUtils. (2020, February 21). *Rogue Device Detection Software*. Retrieved from ManageEngine: https://www.manageengine.com/products/oputils/rogue-detection-tool.html?lhs

Oracle. (2012). *Mitigating Cyber-Security Risk of Smart-Grid AMI.* Oracle. Retrieved from www.oracle.com/us/technologies/bpm/mitigate-cyber-security-risk-1533517.pdf

Park D., S. J. (2017, October 11). *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.* Retrieved from The Henry M. Jackson School of International Studies: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#/

Ryder R., M. A. (2019). *Cyber Crisis Management.* New Delhi: Bloomsbury India.

Wuuest, C. (2014, January 13). Targeted Attacks Against the Energy Sector. *Security Response*. Retrieved from https://bluekarmasecurity.net/wp-content/uploads/2014/09/Symantec_Targeted-Attacks-Against-the-Energy-Sector_whitepaper.pdf

Z. Drias, A. S. (2015). Analysis of Cyber Security for Industrial Control Systems. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC 2015)* (p. 83-91). Shanghai, China: IEEE.

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 3 (September)
http://doi.org/10.9770/IRD.2020.2.3(7)

Acknowledgements

This research was partly supported by the project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

Tomas PLĖTA is a Communications and Information System Security Officer / Head of Division at the NATO Energy security Center of Excellence and PhD student at Vilnius Gediminas Technical University. His PhD topic related to cyber security management for critical energy infrastructure. His research interests also include information and data security, data protection and Industrial control system cybersecurity.
ORCID ID: https://orcid.org/0000-0002-5376-6873

Manuela TVARONAVIČIENĖ is professor at Vilnius Gediminas Technical University and Jonas Zemaitis Military Academy of Lithuania. She is national head of several international projects, financed by European Commission, author of numerous papers, editor of a book, published by Elsevier. Her research interests embrace wide range of topics in area of sustainable development and security issues.
ORCID ID: https://orcid.org/0000-0002-9667-3730

Silvia DELLA CASA is an intern in the NATO Energy Security Centre of Excellence (ENSEC COE) in Vilnius (e-mail: slv.dellacasa@gmail.com). Her MA paper topic is related to cyber security management and energy security management. Her research interests also include hybrid warfare and cyber security issues.
ORCID ID: https://orcid.org/0000-0003-3231-8323

Konstantin AGAFONOV is a PhD student at the Mykolas Romeris University (e-mail: ka1979@gmail.com). His PhD topic is related to cyber security management for e-voting systems. His research interests also include information and data security, data protection and cyber security issues.
ORCID ID: https://orcid.org/0000-0002-8962-0083

Make your research more visible, join the Twitter account of INSIGHTS INTO REGIONAL DEVELOPMENT:
@IntoInsights

Copyright © 2020 by author(s) and VsI Entrepreneurship and Sustainability Center
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access