Analysis of the critical infrastructure cyber security policy

Manuela Tvaronavičienė, Tomas Plėta, Christos P. Beretas, Lina Lelešienė

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

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

ANALYSIS OF THE CRITICAL INFRASTRUCTURE CYBER SECURITY POLICY

Manuela Tvaronavičienė [1], Tomas Plėta [2], Christos P. Beretas [3], Lina Lelešienė [4]

[1,2] Vilnius Gediminas Technical University Saulėtekio al. 11, LT-10223 Vilnius
[3]Innovative Knowledge Institute – Paris Graduate School 21 Boulevard Haussmann 75009 Paris, France
[4] Mykolas Romeris University Ateities st. 20, LT-08303 Vilnius, Lithuania

E-mails:[1] *Manuela.Taronaviciene@vilniustech.lt*; [2]*Tomas.Pleta@vilniustech.lt*; [3]*c_beretas@yahoo.com;* [4]*lelesiene.lina@gmail.com*

Received 15 January 2022; accepted 10 March 2022; published 30 March 2022

Abstract. Critical infrastructures are complex operating environments that often require special protection and security. A successful security strategy design should adhere to the principles of durability, integrity, and regularity. In the European Union, there is a strong interest in the security of critical infrastructures, especially those with interdependence. Given the fact that critical infrastructures play an essential role in a country's economy, it makes them even more vulnerable. The main aim of this article is to analyze the critical infrastructures' cyber security policy. The creation of a security strategy requires identification of the needs for equipment, mode of operation, and required security level. It has to establish rules for precise operation and handling of situations. The article tackles the issues of security strategy for critical infrastructures to protect sensitive areas and sectors. In addition, a cybersecurity policy as a countermeasure is discussed.

Keywords: industry; control systems; security; privacy; attack; management; energy

Reference to this paper should be made as follows: Tvaronavičienė, M., Plėta, T., Beretas, Ch.P., Lelešienė, L. 2022. Analysis of the critical infrastructure cyber security policy. *Insights into Regional Development*, 4(1), 26-39. http://doi.org/10.9770/IRD.2021.4.1(2)

JEL Classifications: O38

1. Introduction

Critical industrial infrastructures are under the name of critical because of their specificity in terms of the products and materials they produce (Brucherseifer et al., 2021). Critical infrastructures play a crucial role in a country's economy and actively contribute to the country's development by making the country more competitive. Critical infrastructures embrace information systems, industrial constructions, telecommunication networks, energy infrastructure, etc. The critical infrastructures are, as a rule, interdependent (Blokus, Dziula, 2019; Lin, Tai, Kong, Soon, 2019). The upgrade of the industrial tools in each infrastructure varies across different countries and by type of infrastructure. Critical infrastructures apply the latest technological equipment, while others may still use older technology, and, maybe several years older equipment. The different architectures of systems and the age of

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

some industrial production units sometimes create, depending on their configuration, a security hole in the infrastructure, something that should be identified, evaluated, and eliminated.

In critical infrastructures, there are industrial control systems (ICSs) which include the various types of control systems (such as the SCADA system). Here it has to be mentioned, that SCADA in some cases appears to be vulnerable too (Cifranic et al., 2020). Besides SCADA, there is the Distributed Control Systems (DCSs), and other types of control systems in critical infrastructure, such as the Programmable Logic Controllers (PLCs) found in all critical infrastructures.

Critical infrastructure industrial systems consist of interdependent control devices designed to produce an industrial product or perform a process. Critical infrastructure, by definition, includes industries and areas, both physical and virtual (Krutz, 2016; Dawson, Bacius, Vassilakos, 2021). Critical infrastructure systems can be configured to operate with **loops**, and there are two types of loops, namely, the **open-loop** and the **closed-loop**. In the open-loop, control systems and the output is controlled by the specified settings. In the closed-loop, control systems and the output affects the input in such a way as to maintain system performance at the desired levels. A critical infrastructure contains numerous control loops, human-machine interfaces (HMIs), and diagnostic and maintenance tools based on a range of protocols. Industrial control processes are commonly used to manage resources and materials.

Critical infrastructure industrial production systems have evolved by adding IT functionality to existing systems of limited capabilities through automation of control mechanisms. Recently, the complete control of the data is carried out using digital media, which has replaced analogous mechanical controls. This technological breakthrough brought in huge advances in industrial technology, thus, production increased, safety rules were tightened, operating costs were reduced, and smart devices were added to take to automated roles, an example is a **smart grid**. Undoubtedly, it's a huge technological breakthrough. Still, it has significantly increased the connectivity of these systems and the ability to connect to other critical infrastructures that may be located in different geographical areas. This carries within it an increased risk that some of these systems at some point will be susceptible to some degree to vulnerabilities, whether small or large, assessing the level of penetration into the system by exploiting the system from which an attacker would attack trying to breach a system of critical infrastructure (Plėta et al., 2020; Djenna, Harous, Saidouni, 2021). For example, the unexpected and unalarmed shutdown of one high-voltage power line in northern Ohio in 2004 resulted in up to two days of blackout to 50 million people, costing an estimated $6 billion and leading to 11 fatalities (Yao et al., 2020).

According to the above-mentioned, it implies a greater need for adaptability, durability, and safety. The Framework and the Reports are major steps towards a cyber-security national policy, they are restricted to those areas defined as critical infrastructure (Dawson, Bacius, Vassilakos, 2021). Critical infrastructure systems differ from IT systems, which means that a security policy that can be applied to an organization **cannot** be applied to critical infrastructures, but it can be used partially, as some key elements can be used in accordance with the creation of an individualized security policy of critical infrastructure systems. A general security policy **cannot** be applied to critical infrastructure, as detection and countermeasures differ significantly.

We should not forget that there are different risks and challenges in critical infrastructures that need different assessments and priorities (Coole, Corkill, Woodward, A. 2012; Gabrijelcic et al. 2022). A failure to implement a security policy can expose infrastructure to significant **internal and external** threats.

There is a separate strand of scientific literature and legal documents devoted to solving cyber security issues of critical infrastructure. Those sources could be conditionally grouped into the following sets embracing specific facets. One broad facet is related to risk assessment and threats (Bennett, 2018; Baig, Zeadally, 2019; Li, 2020). To that group, extreme events can be attributed (Urlainis et al. 2022). Some authors point to the wide range of

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

vulnerabilities brought by the Internet of things, and the Internet (Djenna, Harous, Saidouni, 2021). The risk and threats facet embraces the behavior of people, working with critical infrastructure (Kovacevic, Putnik, Toskovic, 2020). Another broad facet of cyber security issues is related to applied economic and legal principles (Loiko et al., 2020; Weiss, Biermann, 2021) applied for the management of critical infrastructure. Legal principles are reflected in the wide range of standards and guidelines, which is under constant development (e.g. IEEE Standards 2013, NIST, 2014; NIST, 2018; ISACA, 2018; NERC, 2019; Electric Reliability Corporation, n.d.). All those facets of cyber security issues result in the state of cyber security, or its resilience (Cernan et al., 2020; Rod et al., 2020). There are attempts of scientists to systemize the factors affecting the cyber security of critical infrastructure by building a theoretical model, which could be ultimately allowed us to see a bigger picture (e.g. Limba et al., 2017).

Despite all mentioned attempts by scientists and practicians, there are still many unanswered questions related to the formulation of cyber security policy elements. This gap triggers a research aim to articulate more clearly security strategy and cybersecurity policy in this specific area.

Failure of a security policy, therefore, poses a significant risk to the health and safety of infrastructure, equipment, and people in the infrastructure environment, causing serious damage to infrastructure facilities and disrupting the production process, as well as financial losses, as much as this implies the defamation of the state and the failure of the government to secure critical infrastructure in the country where the infrastructure is located.

The systems used in industrial plants in critical infrastructures have surpassed the older architectures. They are based on widely available interconnection technologies such as low-cost Ethernet and Internet Protocol (IP) devices. New architectures and increased interconnection capabilities significantly increase the chances of intrusion and vulnerability, which must be taken into account while designing the security policy to be implemented in critical infrastructure. Evaluation and countermeasures should be in place to identify security holes on time and to eliminate them. The higher the level of automation based on low-cost Ethernet and Internet Protocol (IP) devices, the greater the need to secure these systems against cyber-attacks. As mentioned above, there are no ready-made solutions for the protection and security of critical infrastructure systems. Each infrastructure should be evaluated differently; in no case should evaluations and safety proposals be overlooked for lack of difficulty in resolving decisions. The implementation of new security solutions should be considered as given, which will be adapted exclusively to the working environment and operation of the critical infrastructure. Critical infrastructures carry out complex processes that are constantly and uninterruptedly conducted, any interruptions of which would have disastrous consequences that might even affect other critical infrastructures, i.e. it is an immediate reaction to the problem, except of course the planned interruptions. The continuous inspections of the operations in infrastructure ensure a high level of rawness and availability of resources. A malfunction due to resource unavailability is capable of affecting production. It should be noted that these systems are not typical computers. Tips such as restarting to free up resources are unacceptable due to the adverse effects, as some systems run in parallel with other systems, in the event of a system's failure directly affecting the parallel systems with the result that perform a non-functional and highly complex operation of the infrastructure.

Cyber Security will grow even more together with an increase of the challenges for the security of critical infrastructures. Securing the function of critical infrastructures has become a policy priority worldwide as the potential for disasters given disruptions have been accentuated (Sonesson, Johansson, Cedergren, 2021). On the other hand, it will increase the critical infrastructures created with new standards and implement smart operational solutions that need particular analysis and protection. Electricity generation and management infrastructures face the most significant challenges, as all operations and services in all countries worldwide are based on energy. In addition, energy management systems use automated smart devices to immediately detect problem areas and immediately inform the control center. Artificial intelligence may, of course, significantly improve the situation. This technology allows for impending threats, process controls, and smart devices to be controlled and tracked in

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

real-time. Inspection robots can also be used alongside artificial intelligence. An inspection robot may inspect the equipment and take pictures according to a set schedule for creating logs that contain, precisely, the functions applied, event functions, equipment functions, and measurements. This article emphasizes the security of critical industrial infrastructure systems and countermeasures.

2. Security policy analysis of the critical infrastructure

Critical infrastructure security is not just a countermeasure (counterattacking the hacker), but more like prevention measures. A security policy should protect facilities, processes, systems, production units, staff, integrity, confidentiality, and availability of information stored or transmitted in electronic form. It must anticipate and prevent any attack aimed at altering or limiting the functionality of the critical infrastructure. Staying on the same note, the statistics of cyber security for the past five years show a growing trend in the number of cyber-attacks against the systems of critical infrastructure as well in the detection of vulnerabilities and the gaps in the security of such systems (Bruzgiene, Jurgilas, 2021) (Fig. 1).

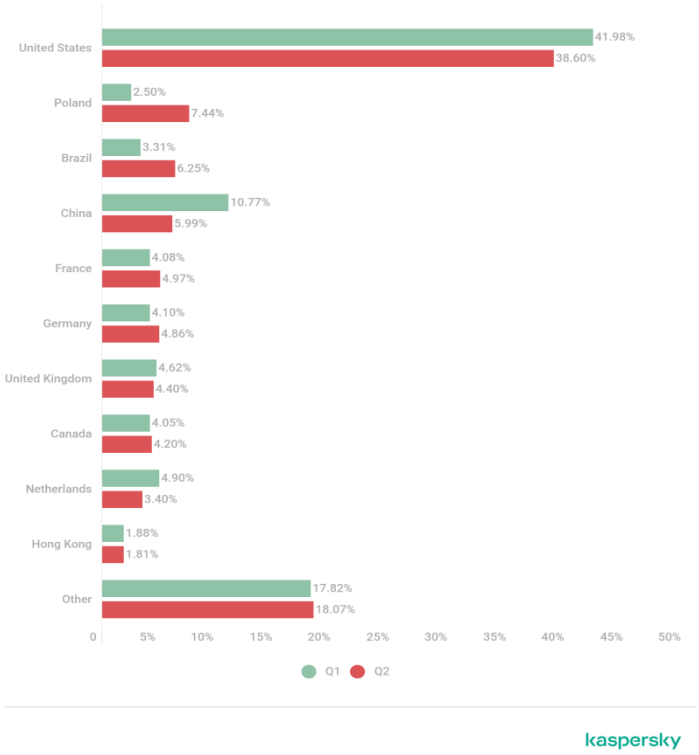

Fig. 1. Distribution of unique DDoS targets by country, Q1 and Q2 2021
Source: https://securelist.com/ddos-attacks-in-q2-2021/103424/

Creating an integrated security policy that offers realistic ways to detect, act, and respond to threats should take into account the following:

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

- *The country's legislation is governed by the operation and management of infrastructure, taking into account all the parameters of the legislation.*

- *Noting the assets of critical infrastructure, such an action may include the cost of industrial equipment and reimbursement of the expenses in the event of partial or total destruction.*

- *The physical analysis of infrastructure facilities is significant in creating a security policy.*

- *Finally, the risk analysis throughout the infrastructure territory, evaluation, and analysis of all parameters that can directly or indirectly affect the operation of the infrastructure*

To implement the right countermeasures (not in terms of counterattacking the hacker), there must be a security policy that has taken into account all the infrastructure units which identify in detail the risks, the impacts, the security methods, the ways of reaction, the safeguarding of the infrastructure property, and finally, the security of the staff, i.e. the human factor.

The main predictors of policy success appear to be (a) the nature of the cyber threat to firms' operations and (b) regulatory pressure on firms (Atkins, Lawson, 2020).

However, to have a comprehensive security policy, and therefore a comprehensive protection and countermeasures plan, requires a detailed evaluation of the industrial equipment and systems, not in the form of a cumulative assessment, but rather in the form of an analysis of the equipment in relation to the operational level.

Evaluation at different levels of assessment evaluation at this level will go a long way in identifying both targeted proposals, draft measures, and countermeasures. Based on the above analysis, the security policy produced will include risk assessments, presentation of hazards and vulnerabilities, and the manner how these vulnerabilities affect the smooth operation of the infrastructure, as well as the extent and countermeasures used on a case-by-case basis.

The security policy required by every critical infrastructure is not common to all infrastructures; each critical infrastructure has different needs and vulnerabilities, diverse operating modes, and different industrial equipment. A security policy should differentiate at the level of risk all entities within the infrastructure by defining how one entity contains another and to what extent, for example, in the event of malfunction or attack. For this reason, the importance of detailed analysis of all units mentioned above, but in the form of equipment analysis in relation to the level of operation, i.e. evaluation at different levels of evaluation, should be included in the main body of security policy planning.

A security policy is built on the organization chart of the critical infrastructure. A security policy including security measures and countermeasures cannot change the organization chart, bypass, or ignore sectors and entities. A security policy should describe and define the methods of implementation, technical measures that identify technical issues, security measures and methods, the description and definition of the security method, the means of communication, and the way how this will be ensured at the critical moment to protect the staff who needs to be trained based on the security policy when the attack is organized under the predetermined instructions without overruns.

In conclusion, someone could say that the proper analysis, design, and implementation of a security policy, that will include multi-level analysis of all entities in conjunction with the control, detection, and analysis of

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

vulnerabilities using models of forecasting future threats and defining the procedures and processes that will be adapted according to the circumstances, is a link for a very strong security policy.

The security policy of critical infrastructure is not a study that should be intimidating, the security policy should be reverently followed, and its purpose is to describe, identify, state the objectives, possible vulnerabilities, security methods, countermeasures, the description of staff responsibilities, and methods of communication and organization. In addition to the description of the above contents of the security policy, the security policy itself is an operating agreement between the management and the staff, thus, achieving the avoidance of each other at a critical moment, as it is a commitment between the two parties. In critical infrastructure, as in any organization, it is necessary to monitor the security policy to comply with it properly and to assign improvements or changes.

The organization chart of the critical infrastructure should indicate the security department which will be responsible for the evaluation, changes, management of the systems according to the safety rules as they are reflected in the security policy, the security issues that will arise, the security issues that concern the operation of the infrastructure, such as issues of coordination, supervision, communications, administration, problematic system configuration, continuous recording of security issues, staff training, and finally, reporting on the performance of security policy, and proposals for its revision.

A security policy defines the duties of each visionary and the degree of their involvement by describing their responsibilities. It should be made clear and understandable that security, especially in critical infrastructure, is not selective and does not allow discounts, security concerns all critical infrastructure staff, describing in detail their main responsibilities and tasks for each job existing in the infrastructure, and how they must comply with the security policy from the top executives as far as the ordinary employee. The human factor plays an important role in the faithful observance of security policy, security methods, and the implementation of countermeasures (not in terms of counterattacking the hacker). The reason is that within an infrastructure, there are employees of different grades, there are employees who work at critical points, other employees use automation that can be more vulnerable than another sector, there are also employees who, according to the organization chart, have low involvement, which means that if there is an attack they cannot and will not be involved to a large extent. The number of responsibilities is the one that involves employees more than others. As it is easily perceived that in case of danger, some employees will be more involved, this involvement can be crucial, as they will be able to deal with situations which in no case should lead them to panic. They should react collectively and methodically according to the training given to them. For this reason, the employees of infrastructure should be included in risk categories, the creation of risk rules will help significantly in their training, as the front line staff is the ones who will carry all the weight of the attack, so it is very important in zero time, to be organized and to make methodical moves of countermeasures, so that there would be no risk to the infrastructure, but not affecting a colleague who works at lower risk levels.

Unfortunately, the economic factor directly affects both the quality of the security policy and the security policy itself. Financial constraint is responsible for the lack of analysis of infrastructure entities and the adoption of appropriate security policies that will secure the infrastructure against attacks both in the medium and long term. The economic factor has a direct impact on the staff training, lack of training, risks to both staff health, and the smooth and safe operation of the infrastructure. Staff training on systems management, security measures, countermeasures shall be implemented on a case-by-case basis and emergency strategy formulation. All of the above entities are critical and are set aside due to economic factors. Typically, the above entities are included in the infrastructure budget and specifically by the security directorate or are partially included in other departments' budgets related to an entity.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

Laws and regulations should develop the security policy. At first glance, everything is quite simple, but the legislation changes frequently, technologies do not standstill. Therefore, it is necessary to respond on time to all innovations and changes.

As mentioned in this article, cybersecurity philosophy in critical infrastructure is rather prevention, and not countermeasures (counterattacking the hacker). Countermeasures come as a second solution and damage mitigation measures, on the other hand of a successful attack, which means lack of preventive security measures, which equates to the incomplete analysis of all entities, misjudgment, error, or non-implementation of proposed security policies. Studies have shown that the successful implementation of a security policy, that has been properly established by partially evaluating all critical infrastructures entity by entity, may secure the infrastructure against attacks. It is possible to prevent potential intrusions and intercept intrusion attempts. The method usually described in security policies is "**4D**" (**Deter, Detect, Delay, Detain or Defend**), while if the plan includes recovery methods and countermeasures, then add "**2R**" (**Respond, Recover**). From the initial stage of tracking down critical infrastructure, the information produced by the would-be attacker must be negligible, which means that the attacker finds an armored system that is reluctant to provide anyone with basic information such as its architecture or operating system versions. All these attempts made by would-be intruders should be logged in to the infrastructure security systems, analyzed by the security department, and evaluated based on existing measures if an existing policy can repel the intruder, and what is possible could be added or modified.

In 2019, warnings that cyber threats pose a risk to public welfare, security, and prosperity were published in the National Intelligence Strategy Report of the United States. Those warnings were related to the fact that information technologies are inseparable from critical infrastructures and are widely used by society (Bruzgiene, Jurgilas, 2021). Prospective intruders who persistently attempt to invade a critical infrastructure system, properly implement security policy, adhere to measures, and write the correct security policy are the ones who will determine the successful avoidance of intrusion into the systems. An emergency delay plan should always be available, and this plan should be divided into **two phases**. The **first phase** is when a significant volume attack has been carried out, for example, **DDoS (**Fig. 2**)**, which may be large and cannot be dealt with existing security systems, this requires the application of mitigation methods; the **second phase** is when there is a partial breach of a system and delay methods should be applied which will prevent further break-in of intruders into the systems, a solution would be to use **Iron Box** and direct the attacker towards it. Partial breach of the network and intrusion into critical infrastructure systems **are not acceptable**. The above methods of delay are **temporary, and emergency solutions as in no case should potential intruders reach this point**. The implementation of delay methods denotes a lack of policy on the one hand because it signifies a breach of systems. On the other hand, the start of the implementation of the delay methods is equivalent to a period that can be crucial both for the plans, the industrial equipment, and the staff, and their protection of health and safety. Usually, when such attacks occur, the adequacy of security measures is judged. Regardless of the definition, CI entities are exposed to various types of threats related to human activities, natural disasters, and military, terrorist, or cyberspace attacks. Therefore, the ability to identify and predict threats toward CI entities and the capability to indicate how to proceed when they occur is nowadays a common subject of many research initiatives (Wisniewsk, 2020). For example, output from a recent evaluation of the European critical infrastructure protection directive (CIP directive) and the suggested new approach for the European program for critical infrastructure protection (EPCIP) suggests taking a resilience perspective as a means to enable more focus on cross-sector interdependencies (Sonesson, Johansson, Cedergren 2021).

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

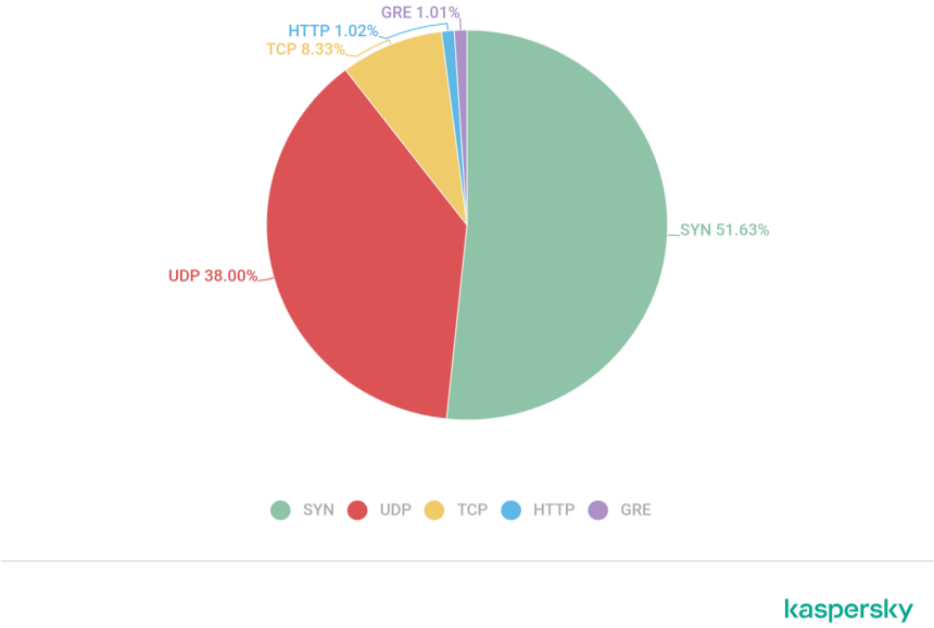

Fig. 2. Distribution of DDoS attacks by type, Q3 2021
Source: https://securelist.com/ddos-attacks-in-q3-2021/104796/

3. Methodology of security policy

The implemented critical infrastructure security policy, as mentioned in this article, should evaluate each sector as an entity, which means that the evaluation should not be uniform for all, it should take into account the criticality of each sector, it should implement the **layout policy of the six sectors** according to their criticality, as described below.

- **Sector 1:** *Security of the Perimeter of Critical Infrastructure.*
- **Sector 2**: *Indoor / Outdoor Entries.*
- **Sector 3**: *Shared Areas Within the Critical Infrastructure.*
- **Sector 4:** *Office Areas.*
- **Sector 5:** *Critical Industrial Sector / Systems Control.*
- **Sector 6:** *Very Critical Industrial Sector / Systems Control.*

Implementing security sectors in a security policy is very important because each industry has different security requirements. Besides, there is the possibility of implementing robust security policies between the sectors, especially the critical and very critical sectors. We should not overlook the fact that critical infrastructures are very expensive, and choosing the cost of the damage would be huge because those parts that have been damaged will have to be repaired or replaced. In addition, the social cost is huge as services, such as energy or fuel, will not

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

be provided to citizens. Power infrastructures are expensive to procure and complicated in their installation, hence, requires a comprehensive security provision for every potential threat, which could fail any unit, system or even cause cascade effects across the infrastructure (Abdulrahaman, Mohd, Raja, 2018).

Each of the above six sectors should form a safety belt that will be properly configured depending on the level of danger. Each industry will consist of complex security measures that include a combination of technical elements that will determine the seriousness of the sector they are applied to. In case of delay, rules will not involve the industry's security. Technical overlaps are **not acceptable** in critical infrastructures as overlap means the inability to apply the correct security rules, and in addition, overlaps hide security vulnerabilities. It is very important to have a secure security policy, especially in the very critical sectors of the infrastructure, so as not to jeopardize the smooth operation of the infrastructure. Nevertheless, to achieve security policy awareness effectively, it is necessary to use rich but compelling textual and visual material (Faizan, Dominic, Kashif, 2020). An important sector that needs high security is the control center, ranked as **sector 6**, which requires special attention and protection, from this point the controls are carried out in the industrial units of the infrastructure, a lack of security policy which would not taken into account security vulnerabilities, and implementation flaws would have a truly devastating effect in the event of an attack.

The aforementioned **sectors 5 and 6** are the heart of the infrastructure, for this reason, they need increased special security, there must be identification and development of security procedures that will be clear and efficient taking into account the procedures carried out in each sector, the origin and mission processes, staff carrying out the procedures in these areas, the level of staff training, the actions that staff can perform, it should also be taken into account how security mechanisms, delays, and countermeasures will work, whether they will work partially and automatically, or the human factor will be involved, as well as the reaction time will have to be determined. Staff working in areas **5 and 6** should be in addition to well-trained staff but should be aware of procedures for using computer resources in order not to be wasted unnecessarily so that when free resources are needed, there are no available ones. Moreover, in these **two sensitive sectors**, staff who have been involved in delinquent behavior in the past, who do not know what constitutes confidential information or who have been involved in sharing sensitive information, or have previously been found to be involved in sabotage **should not** be placed.

External collaborators invited by critical infrastructure executives to carry out projects should fully comply with the security policy, as well as carry out the necessary assessments if the external collaborators meet the system management and security criteria, particularly in **sectors 5 and 6,** as to their ability to perform the task for which they were called upon without affecting the safety of the critical infrastructure. Proper implementation of security policies is a prerequisite for achieving the desired level of security and is largely obtained by the correct use of equipment, forecast models, and the immediate use of countermeasures, where required. The staff's implementation of the security policy in a situation that continuously performs its role is the responsibility of the staff who uses it. Both responsibilities and cross-sectoral cooperation must be clearly described in the emergency management process as in the event of an attack.

The application of the **ISA 95** standard in industrial production will immediately highlight its benefits as there are many tools provided and many automated tools available to the infrastructure users. Implementing ISA 95 will **reduce costs, risk, errors and significantly increase safety** by preventing errors related to the management of production control systems. ISA 95 is a part of a multi-sectoral set of standards that defines the interfaces between the control and industrial sectors. The template complies with **IEC** regulations, and its purpose is to:

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

- *Defining control and construction fields.*
- *The organization of the data.*
- *Defining functions.*
- *The control interface with the functions of an infrastructure.*
- *Defining the information shared between systems.*

ISA 95 is an international standard for developing automated control systems interfaces developed by industrial system manufacturers and designed to be applied to the industry. The standard defines what information and with whom and which systems should interact. ISA 95 categorizes activities into categories defining the functions at the level of production, quality, maintenance, and inventory management. The human factor remains an important entity in critical infrastructure. Therefore, the human factor must be ranked within the infrastructure to distribute roles and responsibilities. Thus, an industrial unit should implement roles such as control, supervision, coordination, security, crisis management, response, incident collection, communication, and physical security. Hence, the roles are listed below.

- **Control team:** *Checks an industrial infrastructure whether it complies with operating standards and security, including proper process management, implementation of security measures, drafting security policy, Data recovery plan, conducting controls on infrastructure information systems, collection, and evaluation of security vulnerabilities, while any omissions are made in a report where they are then applied to the infrastructure.*
- **Supervision team:** *supervises the control team and all processes performed in an industrial unit. The team actively cooperates in departments for the industrial unit's smooth operation, elaborates studies and plans, sets safety standards, provides advice and practices, evaluates the criticality of systems, prepares improvement instructions, and plays an advisory role.*
- **Coordination Team:** *Hierarchically, receives and gives orders to other teams, works closely with the control team, collaborates with security and crisis management teams, and oversees overall operational management of the infrastructure.*
- **Security Team:** *is responsible for data security, information and process integrity, infrastructure upgrades, and security policies.*
- **Crisis Management Team:** *is responsible for the management and accountability of any crisis occurring within an infrastructure. It is responsible for crisis management, analyses the data up to now, supervises studies for future problems, and cooperates with the control team and the response team to neutralize any future threats.*
- **Response Team:** *consists of people who will face cyber-attacks and any other cyber threats that may damage the infrastructure. The team is also responsible for secure data recovery if needed.*
- **Incident Collection Team:** *operates as an incident logging center within the infrastructure. It collects the data, analyses it, and communicates it to the interested groups. In critical cases, it directly informs the competent group. Finally, it conducts statistical research of the requests.*

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

- **Communication Team:** *is responsible for internal and external communications and undertakes to inform citizens and competent bodies about anything in an infrastructure.*

- **Physical Security Team:** *It is the team that naturally guards critical infrastructure.*

Preventing an attack remains the primary choice. The use of countermeasures could be acceptable in applying countermeasures to changing settings and services on infrastructure during an attack, but this should not be confused with choosing countermeasures back to hackers. For example, it **would not be accepted** in the event of a distributed DDS attack being deployed to critical infrastructure, then the critical infrastructure being attacked back in the same way to hackers.

Access (by physical or electronic means) to critical infrastructure installations is restricted to authorized users, processes, and devices by physical or electronic means. This requires appropriate "**Authentication**" mechanisms, and access control procedures. Systems and applications are installed, developed, and managed to take into account the security policy that must be fully complied with security requirements throughout their life cycle. The data necessary for essential services are protected from their possible loss by keeping backup copies in an appropriate format, which allows for their immediate recovery. For this purpose, applicable policies, procedures, and automated systems for making and maintaining back-ups mentioned in the security policy are applied. To ensure the resilience of the systems against threats, appropriate and proportionate security solutions are installed and used. In particular, technological solutions to detect, record, and analyze threats are encouraged to achieve a more realistic security policy against threats. The results of a successful attack can lead to huge financial costs, difficulty, the long time to return the industrial systems to operating conditions, the loss of secrets or national security information, etc. Cyberwarfare takes the form of an asymmetric war. It is, therefore, very difficult to locate the attackers and their source. It requires specialized and highly educated staff, and finally, while it requires relatively low cost, it brings huge financial consequences, for these reasons, the critical situation of a country should be obliged to implement the security policy which should be regularly updated using models of future threat forecasts.

Conclusions

This article was written to highlight the validity of the comprehensive and proper use of a security policy in critical infrastructures. The facts set out in this article were aimed at understanding how a security policy should determine both the elements of correct recording, forecasting, and countermeasures. Countermeasures do not mean counterattacking the attacker the same way the attacker attacked the infrastructure. On the one hand, the advancement of technology offers new security possibilities. On the other hand, modern computing power creates new applications with new opportunities that affect the infrastructure. This article emphasizes the need for the security of critical infrastructures to be divided into sectors, each sector having a different weight from the others, different needs, and different functions. By the method of division into sectors, the most detailed overhaul of the operational parts of the infrastructure is achieved, as well as the application of different enhanced security measures in critical industries that use critical industrial equipment about other sectors, such as the control center, provides operators with increased state awareness which translates into increased prevention or early detection of operational problems. When threats to critical infrastructure are rising, their security technology applications using sophisticated studies enable them to address threats in the best possible manner. The security policy of critical infrastructure should in no case be considered as a model that was designed and continues to be applied for years, especially in cases where it has not been tested in the form of an attack on critical infrastructure. The security policy should be reviewed regularly, including security measures, countermeasures, and user education. The evaluation of actions taken no later than six months after the initial or renewed version of the security policy should be extensively evaluated. The security policy should include instructions for reporting security

vulnerabilities detected by staff using the industrial systems. Finally, new research and proposals in the security policy of critical infrastructures can protect and improve security.

References

Abdulrahaman, O. O., Mohd, W. M., Raja, M. L. 2018. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, 5(3), 468-483. https://doi.org/10.1016/j.jesit.2018.01.001

Atkins, S., Lawson, Ch, 2020. An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure, *PAR*, https://doi.org/10.1111/puar.13322

Baig, Z., Zeadally, S. 2019. Cyber-Security Risk Assessment Framework for Critical Infrastructures. *Intelligent Automation and Soft Computing*, 25(1), 121-129.

Bennett, B. T. 2018. Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel, the 2nd Edition. Wiley.

Blokus, A., Dziula, P. 2019. Safety Analysis of Interdependent Critical Infrastructure Networks. *Transnav-International Journal on Marine Navigation and Safety of Sea Transportation*, 13(4), 781-787. http://doi.org/10.12716/1001.13.04.10

Brucherseifer, E., Winter, H., Mentges, A., Muhlhauser, M., Hellmann, M. 2021. Digital Twin conceptual framework for improving critical infrastructure resilience. *at-Automatisierungstechnik*, 69(12), 1062-1080. http://doi.org/10.1515/auto-2021-0104

Bruzgiene, R., Jurgilas, K. 2021. Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication. *Electronics*, 10(15), Article Number 1819 http://doi.org/10.3390/electronics10151819

Cernan, M., Muller, Z., Tlusty, J., Halaska, J. 2020. Critical Infrastructure and the Possibility of Increasing its Resilience in the Context of the Energy Sector. In Ed. (Muller, Z., Muller, M.) 21ST INTERNATIONAL SCIENTIFIC CONFERENCE ON ELECTRIC POWER ENGINEERING (EPE). Book Series International Scientific Conference on Electric Power Engineering, 505-509.

Cifranic, N., Hallman, R.A., Romero-Mariona, J., Souza, B., Calton, T., Coca, G. 2020. Decepti-SCADA: A cyber deception framework for active defense of networked critical infrastructures. *Internet of Things*, 12 Article Number 100320 http://doi.org/10.1016/j.iot.2020.100320

Coole, M., Corkill, J., Woodward, A. 2012. Defence-in-depth, protection in depth and security in-depth: A comparative analysis towards a common usage language. SRI Security Research Institute, Perth, Western Australia: Edith Cowan University.

Dawson, M., Bacius, R., Vassilakos, A. 2021. Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy Review*, XXVI, 1(101), https://doi.org/10.2478/raft-2021-0011

Djenna, A., Harous, S., Saidouni, D.E. 2021. Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences-Basel*, 11(10), Article Number 4580 http://doi.org/10.3390/app11104580

Dong, S.J., Malecha, M., Farahmand, H., Mostafavi, A., Berke, P.R., Woodruff, S.C. 2021. Integrated infrastructure-plan analysis for resilience enhancement of post-hazards access to critical facilities. *Cities*, 117 Article Number 103318 http://doi.org/10.1016/j.cities.2021.103318

Electric Reliability Corporation. Retrieved from www.nerc.com/pa/comp/Reliability Standard Audits Worksheets DL/RSAW CIP-008-5 2015 v1.docx

Faizan, A. R., Dominic, P.D.D., Kashif, A. 2020. Organizational Governance, Social Bonds and Information Security Policy Compliance: A Perspective towards Oil and Gas Employees, *Sustainability*, 12(20), 8576 https://doi.org/10.3390/su12208576

Gabrijelcic, D., Caleta, D., Zahariadis, T., Santori, F., De Santis, C., Gasparini, T. 2022. Part III: Securing Critical Infrastructures of the Energy Sector: Security Challenges for the Critical Infrastructures of the Energy Sector. now publishers inc.

Boston - Delft http://doi.org/10.1561/9781680836875.ch13

IEEE Standards. 2013. *IEEE Cyber Security for the Smart Grid.* New York: IEEE Standards. Retrieved from https://ieeexplore.ieee.org/abstract/document/6613505?casa_token=wMK-pzZ6EdwAAAAA:4c4nRqlxSrEEYXLRsUo56fNrE1A_iCQotwioes8cBpp4_GHUmbSvd8FTwjKJaQXODRpQWVQ

ISACA. 2018. *COBIT® 2019 Framework: Governance and Management Objectives.* ISACA. Retrieved from https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19igio

Kovacevic, A., Putnik, N., Toskovic, O. 2020. Factors Related to Cyber Security Behavior. *Ieee Access*, 8, 125140-125148 http://doi.org/10.1109/ACCESS.2020.3007867

Krutz, R. L. 2016. Industrial Automation and Control System Security Principles. International Society of Automation; 2nd edition.

Li, J. H. 2020. Overview of Cyber Security Threats and Defense Technologies for Energy Critical Infrastructure. *Journal of Electronics & Information Technology*, 42(9), 2065-2081. http://doi.org/10.11999/JEIT191055

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)

Lin, J., Tai, K., Kong, R.T.L., Soon, S.M. 2019. Modelling critical infrastructure network interdependencies and failure. *International Journal of Critical Infrastructures*, 15(1), 1-23

Loiko, V., Khrapkina, V., Maliar, S., Rudenko, M. 2020. Economic and Legal Principles for Protecting Critical Infrastructure Protection. *Financial and Credit Activity-Problems of Theory and Practice*, 4(35), 426-437.

NERC. 2019. *Cyber Security – Incident Reporting and Response Planning: Implementation Guidance for CIP-008-6*. North American

NIST. 2014. *Guidelines for Smart Grid Cybersecurity.* Washington: NIST. http://dx.doi.org/10.6028/NIST.IR.7628r1

NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* Washington: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Plėta, T., Tvaronavičienė, M., & Casa, S. D. (2020). Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development*, *2*(2), 538-548. https://doi.org/10.9770/IRD.2020.2.2(3)

Rod, B., Lange, D., Theocharidou, M., Pursiainen, C. 2020. From Risk Management to Resilience Management in Critical Infrastructure. *Journal Of Management In Engineering*, 36(4), Article Number 04020039 http://doi.org/10.1061/(ASCE)ME.1943-5479.0000795

Securelist by Kaspersky https://securelist.com/ddos-attacks-in-q3-2021/104796/

Sonesson, T.R. Johansson, J., Cedergren, A. 2021. Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety Science*, 142 Article Number 105383 http://doi.org/10.1016/j.ssci.2021.105383

Urlainis, A., Ornai, D., Levy, R., Vilnay, O., Shohet, I.M. 2022. Loss and damage assessment in critical infrastructures due to extreme events. *Safety Science,* 147. Article Number 105587 http://doi.org/10.1016/j.ssci.2021.105587

Weiss, M., Biermann, F. 2021. Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform* http://doi.org/10.1080/17487870.2021.1905530

Wisniewsk, M. 2020. Methodology of situational management of critical infrastructure security. *Foundations of Management*, 12(1), 43-60. http://doi.org/10.2478/fman-2020-0004

Yao, X.J. Wei, H.H., Shohet, I.M., Skibniewski, M.J. 2020. Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation. *Applied Sciences*, 10(20), Article Number 7162 http://doi.org/10.3390/app10207162

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2022 Volume 4 Number 1 (March)
http://doi.org/10.9770/IRD.2022.4.1(2)

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

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 is 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

Christos P. BERETAS is PhD expert on cyber security. Head of Programme Master of Science in Cyber Security (2021-2022) in Innovative Knowledge Institute – Paris Graduate. His research interests also include information and data security, data protection, and industrial control system cybersecurity.
ORCID ID: https://orcid.org/0000-0001-9681-9456

Lina LELEŠIENĖ is a PhD student at the Mykolas Romeris University (e-mail: lelesiene.lina@gmail.com). Her PhD topic is related to cyber security management of e-health systems. Her research interests also included information security in banking, data protection, and cyber security issues.
ORCID ID: https://orcid.org/0000-0002-6822-9907