Cyber effect and security management aspects in critical energy infrastructures

Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

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

CYBER EFFECT AND SECURITY MANAGEMENT ASPECTS IN CRITICAL ENERGY INFRASTRUCTURES *

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

[1,2] Vilnius Gediminas Technical University Saulėtekio al. 11, LT-10223 Vilnius
[2]General Jonas Zemaitis Military Academy of Lithuania, Šilo Šilo g. 5a, 10322 Vilnius, Lithuania
[3] NATO Energy Security Center of Excellence, Šilo g. 5a, 10322 Vilnius, Lithuania

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

Received 20 February 2020; accepted 10 May 2020; published 30 June 2020

Abstract. The purpose of the paper is to compare various types of management models that regulate the response to cyber threats to Critical Infrastructures. The development of an effective management model that regulates the response to cyber-attack against Critical Infrastructure is an important issue in security management. Many frameworks attempt to regulate the response that has to be done to recover and eradicate possible threats, but still, there is not a universal appliable model for all Critical Infrastructures. The paper will offer a comparison of various frameworks in an attempt of evaluating the features that a hypothetical model for response to Cyber Incidents to Critical Infrastructures. The focus is on Critical Energy Infrastructure, as their damage directly means damage to other critical infrastructures, given their extreme interconnectivity. After the analysis of five frameworks of responses to Cyber Incidents, an evaluation will be provided, along with a recommendation.

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. 2020**.** *Insights into Regional Development*, 2(2), 538-548. https://doi.org/10.9770/IRD.2020.2.2(3)

* *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

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

JEL Classifications: M15, Q48

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

1. Introduction

In our current society, many new issues are affecting the functioning of the sources of energy, which are fundamental for all Critical Infrastructures. With the convergence of IT and OT environments and the birth of IIoT, the security of industrial systems of the critical infrastructure was not adequately updated, hence currently many enterprises are facing cyber risks without any management strategy (Bhayani 2016). While the definition of the adequate modality can vary from one enterprise to another, there should be an effective management model that could offer adequate guidelines in preparing, responding, and reporting a cyber-attack, as well as defining the management roles necessary to handle the operations and the decisions. Frameworks and standards were developed for both IT and OT environments but, as aforementioned, the IIoT represents the overlap of both, hence the model that should be adopted for CI should be taking account of both.

The development of a management model tailored for cybersecurity of critical energy infrastructure can be challenging, considering the peculiarity of its nature and structure. The management strategies that are used as guidelines of response to cyber incidents can be of a different approach: the focus can be on the fool proofing phase before the attack, on the action needed during the extent of the attack or on the assessment and recovery after the incident. Critical energy infrastructures are subjects to extreme interconnectivity, as usually more than one type is implemented to sustain one country's energy flow. The interconnectivity, while being an effective instrument for more reliable energy production, can mean that damaging one source can bring heavy consequences to other infrastructures that are on its receiving end.

The following paper will attempt to analyze various cyber incident response management strategies. The majority of the documents are for governmental use, hence there will be a general approach to CI. However, the focus will be on Critical Energy Infrastructures (CEI), as their importance and functioning affect immensely the other types of CI. The goal of the paper is to highlight the procedures that are more suitable to be applied to CEI in the frameworks, ad then propose a possible cybersecurity model for CEIs. The analysis will be conducted by comparing the procedures and by choosing the more suitable for CEI, not focusing on technological aspect but on the framework regarding management strategies. The framework were chosen due to the number of organization that implemented it, theoretical approaches and date of publication.

2. Analysis of cyber incidents‘ management strategies

2.1. NERC Implementation Guidance for CIP-008-6 (2019)

The North American Electric Reliability Corporation (NERC), a not-for-profit international regulatory authority, introduced in January 2019 “Cyber Security – Incident Reporting and Response Planning” for ensuring the functioning of the power grid. The framework is called Reliability Standard CIP-008-6, it proposes the guidelines for reporting and reacting to cyber incidents in the power grid, and it is classified under the OT Standards & Frameworks (NERC 2019). The types of cyber incidents are classified in a color code that progresses from no reportable to urgently reportable, with Green as “non-reportable, events\activity, or determination not made”, Yellow as “Cyber Security Incident, reportable determination not made”, Orange as “is determined reportable attempt to compromise an Applicable System” and Red as “determined Reportable Cyber Security Incident”

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

(NERC 2019). To summarize, the response is based on a "reportable\not reportable" classification, which criteria, however, are chosen by the Registered Entities, meaning the electric company following the procedure. The classification system can be quite valuable for determining the adequate response to different kinds of cyber events, as the emergency level goes up there are different roles that are prepared for the response.

The framework contains an example of the classification of cyber incidents with the NCCIC Cyber Incident Scoring System (NCISS), based on the National Institute of Standards and Technology (NIST) Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide, which will also be evaluated (CISA 2020). The infrastructure described in the framework is divided into the Corporate Zone and the SCADA zone. The Corporate zone consists of regular corporate assists and is the outer part of the infrastructure, protected by an Electronic Security Perimeter and an Electronic Access Control or Monitoring System (EACMS). The SCADA zone contains the core of the Industrial Control System (ICS) and is protected by other EACMS and a corporate firewall that protects the corporate assets from Internet intrusions. The NCISS aligns with the Cyber Incident Severity Schema (CISS), which has five levels of emergency, which ranges from white (level 0) to black (level 5), and is calculated by observing the preparation, the engagement, the presence and the effect (CISA 2020). Referring to the aforementioned infrastructure model, reportable incidents are attempts to compromise a system identified in the "Applicable Systems", and hence that is capable to breach from the corporate zone to the SCADA zone (NERC 2019).

In the process of identification, the first management role is the Incident Management Service Desk, which is responsible mainly for incident "ticketing" and "logging" (NERC 2019), meaning that it is responsible to assess the degree of the incident and, if necessary to assign the procedure to the responsible entity. The Incident Management Coordinator is responsible for the coordination of the activities and is consulted if the cyber event escalates, assisting the Service Desk to update the incident tickets with status and to communicate with the interested users. The E-ISAC/ NCCIC Reporting Coordinator is responsible for the coordination of regulatory reporting activities related to E-ISAC (Electricity Information Sharing and Analysis Center) and the NCCIC regulatory framework (NERC 2019). Finally, the Investigating Subject Matter Experts are responsible for the technical details related to the investigation of the incident. An appendix of the framework offers both the instructions to fill a Cyber Security Incident Reporting Form, which is a part of a correct approach, as it institutionalizes the reporting of the incidents and it makes it easier to classify the incident and having a faster response to it.

Overall, the NERC framework relies on the NIST guidelines; the introduction of the classification of Cyber Incidents based on a risk-assessment method could be a valid technique to develop in a general model. However, if the model will be referred to every type of CEI, it should consider more general elements of the infrastructure, as it may vary. The separation of the management role according to the incident's gravity is as well a good approach to the response to cyber incidents and should be included in the general guidelines for CEI. Registered Entities decide each of their criteria of classification of reportable\non reportable incidents, meaning that for CEI the approach should try to consider, for what is possible, a common set of emergency criteria. The management approach that emerges from this framework takes into consideration the risk-assessment method for the classification of Cyber Incidents and the "Lesson Learned" method, but the damage of a cyber-attack to CEI could not be quantifiable only in financial terms, but also in terms of loss of human lives and physical disruption. For this reason, the "Lesson Learned" approach is not recommended.

2.2. Computer Security Incident Handling Guide Special Publication 800-61 Revision 2 (2012)

The National Institute of Standards and Technology (NIST) offers standards and guidelines valid for governmental (US) Federal agencies, but not for national security systems (Cichonski 2012). The framework

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

comprehends and covers the procedures necessary for the implementation of an appropriate cybersecurity strategy for Computer Systems. Since the framework is widely used for Federal Agencies, it does not refer in particular to potential physical disruption or human life loss, and it may be in some ways unprepared to "newer" hacking strategies since it is from 2012. It is classified under IT Standards & Frameworks, and it offers a detailed procedure focused on incident response capabilities and incident handling. The reason for the chosen approach is due to the IT approach, which is related to governmental agencies and businesses, for which a cyber-attack could hardly resolve in the physical disruption.

In the framework, an extensive part is dedicated to the organization of a Computer Security Incident Response Capability (CSIRC) and offers a variety of team models. The major difference made in the framework is the division of the models between "large" or "small" enterprises, which confirms the dedicated approach to businesses and IT environments. While for small organizations it is advised a Central Incident Response Team, for larger agencies and organizations with "major computing resources at distant locations", Distributed Incident Response Teams are advised, meaning that all the groups should be coordinated by a single entity (Cichonski 2012). For both models, there should be a Coordinating Team, which provides advice to the other teams without having authority over them. Concerning the staffing of the Incident Response Teams, the agencies can pick one of three options; the first one is to form the team from employees, to be Partially Outsourced, or to be Fully Outsourced.

The NIST guidelines then proceed to describe the stages of the incident response process: it is divided into four major phases, Preparation, Detection & Analysis, Containment Eradication and Recovery, and Post-Incident Activity. In the phase of Preparation, the general procedure is for the response team to have a so-called jump kit at all times and ready to use. A jump kit is a portable case that contains materials that could be useful during the investigation, and that in the framework is divided into Communications and Facilities, Hardware and Software and Resources. It is also advised the presence of laptops and of spare workstations, servers, networking equipment that be used for restoration and tracing malware. Important tools that are also worth mentioning are cryptographic hashes of critical files: the US possesses a National Software Reference Library (NSRL), which maintains the record of hashes of various files that can be downloaded at any time for restoration and backup.

The Detection & Analysis phase provides a thorough description of the possible types of attack vectors that an organization can face during a cybersecurity attack, but most importantly, it offers an interesting approach in the classification of the intensity of the various cyber-attacks to the organizations. After the recommendations and the analysis of the incident, it is offered a system providing an Incident Prioritization system, which refers to three main categories, Functional Impact of the Incident, Information impact of the Incident and Recoverability from the Incident. It has four degrees of impact, none, when it does not affect the organization's ability to provide all services to all users, low, medium and high, where the organization is no longer able to provide some critical services to any users (Cichonski, 2012). The model is extremely detailed and could be useful for Critical Energy Infrastructure as well, but as the focus is more on IT environments, it puts focus on the information loss and not in terms of physical damage.

In the Containment Eradication & Recovery, NIST proposes that organizations should separate containment strategies that change for every major incident type, offering various criteria for determining the appropriate strategy. The last phase of Post-incident Activity focuses almost entirely on the "Lesson Learned" approach, by describing the structure of the meeting and the management of the incident data metrics (Cichonski, 2012). In addition to further recommendations, the framework offers an Incident Handling Checklist, as well as various scenarios in which are tested the responses to different types of threats. The presence of the latter is fundamental for adequate incident handling guidelines, and should, along with Critical Infrastructure specifications, be present in a hypothetical model.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

Overall, the NIST Cyber Incident Handling Guide offers a thoroughly detailed framework that considers an in-depth analysis of the phases necessary to build an effective response strategy for organizations belonging to IT environments. While many elements mentioned in the Guide could be effectively applied to the evaluation and strategy dedicated to Critical Energy Infrastructures, the guidelines propose the loss or theft of information as the worst possible scenario. For what concerns CEI, as aforementioned, cyber-attacks could resolve not only loss of money or information but with physical disruption and loss of human life. As well, the element of interdependency can represent a challenge for the formation of an adequate framework, a model framework for CEI should contain information loss prevention but should not stop the analysis to IT environment strategies.

2.3. Framework for Improving Critical Infrastructure Cybersecurity (2018)

The NIST: Framework for Improving Critical Infrastructure Cybersecurity is classified under the OT Standards & Frameworks, and relies upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with international stakeholders (NIST 2018). The document is defined as "technology neutral" as being constantly updated with global guidelines and standards for the technical aspects while maintaining its core. The common taxonomy of the framework for the organizations is to form a "Profile", which considers the current cybersecurity posture and the target state for cybersecurity and assesses the progress of the organization towards the goal (NIST 2018). Ultimately, the framework has a complementary role to other, previously established, cybersecurity programs in the organization and it is used solely to enhance the cybersecurity of Critical Infrastructures.

The framework is divided into three main parts: Framework Core, Framework Implementation Tiers and Framework Profile. The Core provides an interesting approach to the improvement of cybersecurity strategies: the goal is to provide an adequate method for managing and responding to cyber risks. The approach then is different from the previously seen frameworks, as it is not a set of actions to follow and check: this depends on the fact that the nature of the framework is not to be comprehensive but complementary; hence, the evaluation will be different. The core elements consist of Function, Categories, Subcategories and Informative References. The Functions serve in organizing the cybersecurity activities in phases in succession, Identify, Protect, Detect, Respond, and Recover (NIST 2018), while still aligning with existing methodologies in the organization. Each Function is divided into Categories, into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities, which are again divided in Subcategories, which divide each Category into specific outcomes of technical and\or management activities (NIST 2018).

The core elements are defined as well, though it is specified that the goal is not to provide a serial path but to have general guidelines performed concurrently and continuously to address a dynamic security risk. The Identify function is defined as "Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities, which is fundamental for prioritizing the necessary improvement strategies. To Protect is to "Develop and implement appropriate safeguards to ensure delivery of critical services", a function that supports the ability to limit and contain the impact of a cyber event. To Respond is to "Develop and implement appropriate activities to take action regarding a detected cybersecurity incident", while to Recover is to "Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident." (NIST 2018).

The second part of the framework provides clarification on the use of Tiers in the framework: according to the definition offered by the framework, they describe a degree on sophistication in the already existing cybersecurity risk management practices of an organization. They are useful for determining the necessary modification of the cybersecurity strategy practices (NIST 2018). The Tiers are divided into four levels, Partial, Risk Informed, Repeatable and Adaptive. The method can be applied to the phases of the plan, design, build\buy, deploy, operate

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

and commission, and can be at any moment modified and updated (NIST 2018). It is worth mentioning that the frameworks provide an interesting approach that is focused on the specificities of Critical Infrastructures, by mentioning the importance of ensuring secure and constant communication among stakeholders in the supply chain, even though for CI they are especially complex and require multiple levels of organization (NIST 2018).

Overall, the NIST framework provides an interesting approach for the implementation of cybersecurity tactics compared to the previously analyzed documents. The peculiarity of its structure, however, provides it to be the main reference in the construction of an adequate framework. Some elements might be useful in developing a framework for CEI, as the approach is more complementary and takes account of the interconnectivity problem, though it does not offer a valid solution to it. Additionally, the implementation of Tiers as a determination of necessary cybersecurity improvements could be useful for CEI as an additional tool for determining the necessary implementation to improve their security.

2.4. Centre for Cyber Security Belgium: Cyber Security Incident Management Guide (2015)

The provided Cyber Incident Guide is offered as a National Cybersecurity guideline for the country of Belgium, developed by the Cyber Security Coalition to raise awareness among both citizens and organizations. The framework provides general guidelines for drafting a cybersecurity incident response plan and an incident response team. The first phase consists of Identify your assets and potential threat, so categorize and document the "vital" elements of the organization's structure to determine what to protect. The methodology of documentation is furtherly offered in the documents and proposes to determine a priority system for recovery, meaning to determine the order in which the systems will be reestablished (Darville 2015).

A very detailed part of the framework is dedicated to the creation of a Cyber Security Incident Response Team. For every role, are specified as well its responsibilities and necessary skills. The most important position is covered by the Cyber Security Incident Manager, whose responsibility is to keep the management of the cyber incident under control from the beginning to the end. The Management has the ultimate responsibility of deciding on how to proceed with the right resources at the moment of the cyber incident, so decide for example whether the internet connection should be shut down and when (Darville 2015). The ICT technical support staff has an eminent role in the team as well. The document then reserves an extensive part about the development of an effective contact list, which is, however, more targeted to SME and common businesses rather than CEI. A division is made among different stakeholders in internal (senior management, business managers, employees), external (media, customers, suppliers, and others) and official. The latter type of stakeholders is referred to with Belgian national organizations, such as the Privacy Commission and Cert.be, which are going to be later analyzed (Darville 2015).

The second part of the guide is dedicated to the detection and identification of potential cybersecurity incidents. The recommendations for preventing a cyber-attack are worth mentioning the protection of endpoint devices and the control of the logs to monitor unusual activity (Darville 2015). The third part is devoted instead to the strategies of containment of cybersecurity incidents, but there are some specificities on the SMEs approach. For example, the document proposes a "common strategic decision" that every organization potentially faces during a cyber-attack: the choice between disconnecting the system immediately to recover more quickly or to take the time to observe and collect the necessary evidence. Differently from the other analyzed frameworks, the guide does not offer a classification based on the level of intensity of the emergency. A further part is dedicated to detail on the communication during a cybersecurity incident. As aforementioned, the authorities that are mentioned are almost exclusively from Belgium. The framework ultimately offers an incident follow up and closure in a "lesson learned" approach which provides an evaluation of lesson learned and future actions, along with incident tracking and reporting. It is worth mentioning that in the Appendix is provided a table with the most common incident

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

types and how to neutralize them, a feature that could be useful for CEI employees: the most common types of incidents are briefly explained, along with a direction on the possible handling of the incident.

Overall the guide offers an exhaustive explanation of the appropriate procedures to follow in case of a cyber incident, although mostly focused on the procedures in SMEs and commercial businesses. The approach could be useful for CEI for some elements, such as the accurate description of the Incident Response Team. The division of the roles based on the responsibility is a good approach for a possible CEI model, as it would be easier for the business to raise awareness among the workers. Also, the appendix providing the solution for the most common incident could be really useful if available to all the workers. The excessive focus on the communication to external stakeholders, while being useful for SMEs, is not a CEI priority.

2.5. Security PHA Review for Consequence-Based Cybersecurity (2019)

The last text to be analyzed will be the Security PHA Review for Consequence-Based Cybersecurity written in 2019, which represents an exception compared to the other documents taken into consideration. While not being implemented on a national level, the framework offers a uniquely innovative approach for the response to cyber incidents in Industrial Control Systems (ICS). The manual developed by the International Society of Automation (ISA) concerns the OT environment and has an overall technical approach to the improvement of cybersecurity. It is usually implemented in wet process industries (chemical, oil refining, and petrochemical), and it proposes a different approach to the assessment of an industry's cybersecurity level. The proposed method is the PHA method, or "Possible Hazard Scenario" method, which consists in the evaluation of the cybersecurity level based not on the safeguards that should be used but on what accident scenario the safeguard presents against (Marszal 2019). The basic methodology described uses the following steps: generate potential scenarios and brainstorm about the possible outcomes of the scenario. With this method, every safeguard is tested in the situation in which assumingly it does not operate (Marszal 2019). Then all the scenarios are ordered by the likelihood of it happening, and finally, there is a recommendation on how to improve the overall situation. The scenarios are then implemented according to their security level, a qualitative measure that expresses the amount of mitigation of cyberattack risk necessary (Marszal 2019).

An interesting approach is furthermore used in this document, as the scenarios are classified as "hackable" or "non-hackable". If the action needs a virtual command for it to be pursued, it is hackable, while if the action needed is manual it is non-hackable. Hence, if for every virtual action performed by the ICS it will be implemented a physical, non-hackable safeguard, the risk of cyber-attack would be highly diminished (Marszal 2019). As aforementioned, the documents present a big part of technical aspects concerning the types of non-hackable safeguards appliable to the ICS. However, it will not be considered in-depth for the analysis. Even though the system is applied to a relatively restricted field of ICS, the brainstorming approach would be ideal for CEI, as it is focused on prevention rather than a "lesson learned" approach. As the previous analysis tried to identify and analyze the various approached of the preexisting frameworks, the following part will summarize the elements that were found useful for a hypothetical framework.

3. Recommendations for a possible framework and conclusions

The article proposed to develop a possible solution to the lack of regulation of CEI by analyzing various frameworks that offered a different approach. While not being able to develop a precise degree of accuracy or to classify the framework for "best application", it is, however, possible to highlight the best solutions to the issues in CEI. To develop an effective cybersecurity model, the structure that will be taken into consideration will be the one described by Limba & Pleta (Limba et al. 2017). The dimensions of a good cybersecurity model are firstly

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

legal regulation, meaning that there are legal proceedings and requirements about cybersecurity, good governance, which means that the main aims of cybersecurity need to be understood (including the fact that some risks could never be excluded) (Limba et al. 2017). However, the most important dimensions taken into the analysis will be risk management, security culture, as the organization is "as vulnerable as the people working there", technology management and incident management (Limba et al. 2017).

As mentioned before, one problem that is usually part of the CEI cyber-attacks is the lack of awareness or training of the employees. Following the model, the dimension taken into consideration is the security culture. In the case of a cyber incident, the document that better addressed the awareness issue is the Cyber Security Incident Management Guide. In a possible framework for CEI, the training part of the document should use the same approach of the Guide, as it offers a general tone that can be understood by the employees. Along with the distribution of the appendix of the most common cyber incidents and how to resolve them, the document as well offers a clarification on the formation of the Cyber Incident Response Team (Darville 2015) based on responsibility. The latter explains the roles necessary for each organization to form an adequate Cyber Incident Response Team, clarifying the tasks that each part of the team should fulfill. For these reasons, the document's approach to awareness and training is the best.

For what concerns the risk management, it is described as the ability to properly identify risks ad ensuring that they are being taken care of by specialists (Limba et al. 2017). The document that provided the most adequate guidelines for a hypothetical CEI framework is the NERC Implementation Guidance for CIP-008-6. As mentioned in the previous chapter, the framework contains an example of the classification of cyber incidents with the NCCIC Cyber Incident Scoring System (NCISS) (NERC 2019). The classification of possible cyber incidents is done with the intent of dividing different situations by the level of emergency and ensuring a comprehensive response assessment. Additionally, the implementation of a standard form to be filled for it to be classified is a method that could be useful in emergencies. However, in the NERC document, the criteria of emergencies were depending on the Registered Entity, which could not be the best approach for CEI, as it would need more general criteria that are appliable to every type of CEI.

The incident management dimension of a good possible cybersecurity strategy for CEI could follow the NIST Computer Security Incident Handling Guide approach. The framework offers an in-depth analysis of the procedures to implement before a cyber incident occurs. The development of a jump kit (Cichonski 2012) could be extremely useful if implemented in the CEI as a habit, so the time of response would be considerably lower. Moreover, the separate containment strategies that change for every major incident type are another element that could improve greatly the security level during a cyber-incident. Also using containment strategies, besides having the advantages of being tailored for every CEI, allows the response patterns to be classified according to a prioritization system. This could be effective if there would be a separate classification for cyber incidents and emergency levels, which would be general for every CEI and then modified with in-depth situations and framework for every type of CEI.

Lastly, for technology management, the most interesting approach was offered by the Security PHA Review for Consequence-Based Cybersecurity, as it offered the knowledge about each component that is controlled by IT can be vulnerable (Limba et al. 2017). As mentioned in the previous analysis, the scenario-based approach is the best one that can thoroughly analyze every single component of an ICS system. The approach should be found extremely useful for CEI, as well as the approach would offer a complete and comprehensive view on the likelihood of the various components to be attacked.

A possible classification of Cyber Incidents could be the one used in the NERC Implementation Guidance for CIP-008-6 and the NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide, known as CISA Cyber Incident Scoring System. Used by the US government agencies, the system includes weighted

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

arithmetic mean to produce a score from zero to 100 (CISA 2020) based on different categories. Each category has a weight, and each response score is multiplied by the category weight. The categories are Functional Impact, Observed Activity, Location of Observed Activity, Actor Characterization, Information Impact, Recoverability, Cross-Sector Dependency, and Potential Impact (CISA 2020). After the scoring of an incident, a priority level is assigned. The levels are Emergency (Black), Severe (Red), High (Orange), Medium (Yellow), Low (Green), Baseline. An interesting feature in the evaluation of the incident promoted by this system is that the final evaluation takes into account "Multiple Connected Incidents". The latter is, as aforementioned, a common issue in the evaluation of the emergency level of an attack against CEIs, making is the most accurate system currently available. Additionally, the Cyber Security Incident Management Guide mentions the Cert.be (federal Cyber Emergency Response Team) as an organization that supports and helps targeted organizations. The development of a similar organization is already present in countries like the US and Canada but could help if implemented on an intranational level. NATO has developed the NATO Computer Incident Response Capability (NCIRC) in Belgium but is still far from being used frequently by organizations/government in distress (NATO 2020).

In conclusion, the analysis presented in this paper offers interesting insights regarding the development of a management model for CEIs. Firstly, none of the framework that were analyzed were considered comprehensively adequate, although each of the document presented useful elements of analysis. The final structure of the hypothetical model gathers various theoretical approaches which, if considered part of a larger cyber security strategy model for CEIs, are more than adequate for the goal of the paper. The analysys of this paper demonstrated that it is possible to develop an effective model valid for all CEIs, however it is necessary to activate effective intranational organizations, available 24/7, which can offer support to organizations under cyber attacks.

References

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

CISA. (2020, February). *CISA Cyber Incident Scoring System*. Retrieved from Cybersecurity and Infrastructure Security Agency (CISA): https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System

CISA. (2020). *Cyber Incident Severity Schema.* USA: Cybersecurity and Infrastructure Security Agency (CISA). Retrieved from https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf

Marszal, J. M. (2019). *Security PHA Review for Consequence-Based Cybersecurity.* USA: International Society of Automation (ISA). https://open.spotify.com/track/3MRWIuuhlyA4ClGIFWhP1m

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)

Beazner M., P. R. (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., M. P. (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.

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

NERC. (2019). *Cyber Security – Incident Reporting and Response Planning: Implementation Guidance for CIP-008-6.* North American Electric Reliability Corporation. Retrieved from www.nerc.com/pa/comp/Reliability Standard Audits Worksheets DL/RSAW CIP-008-5_2015_v1.docx

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

Cichonski P., T. M. (2012). *NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide.* Washington: U.S. Department of Commerce. Retrieved 2012, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

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

European Research Council
Established by the European Commission

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 2 (June)
http://doi.org/10.9770/IRD.2020.2.2(3)

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 General 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. Her MA paper topic 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

Register for an ORCID ID:
https://orcid.org/register