Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania

Manuela Tvaronavičienė, Tomas Plėta, Silvia Della Casa, Juozas Latvys

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

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

CYBER SECURITY MANAGEMENT OF CRITICAL ENERGY INFRASTRUCTURE IN NATIONAL CYBERSECURITY STRATEGIES: CASES OF USA, UK, FRANCE, ESTONIA AND LITHUANIA*

Manuela Tvaronavičienė [1], Tomas Plėta [2], Silvia Della Casa [3], Juozas Latvys [4]

[1,2] Vilnius Gediminas Technical University Saulėtekio al. 11, LT-10223 Vilnius
[1]Daugavpils University, Parades Str. 1-421, Daugavpils, LV-5401, Latvia
[3,4] NATO Energy Security Center Of Excellence, Šilo g. 5a, 10322 Vilnius, Lithuania

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

Received 18 March 2020; accepted 10 July 2020; published 30 September 2020

Abstract. The progresses made in terms of cybersecurity in these past years have been huge, and the implementation of newer strategies has brought interesting results all over the globe. However, the full implementation of cybersecurity presents a challenge to a lot of countries, especially if considered the Critical Infrastructure Protection (CIP), which is still one of the areas with the most gaps in terms of cybersecurity. In this article, the first five countries by cybersecurity level according to the Global Cybersecurity Index (GCI) 2018, in order UK, USA, France, Estonia and Lithuania, will be evaluated for their solutions in terms of Critical Infrastructure Protection. The results will show the effective accuracy of the index and will shed light on the various approaches to Critical Infrastructure Protection.

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

Reference to this paper should be made as follows: Tvaronavičienė, M., Plėta, T., Della Casa, S., Latvys, J. 2020. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, 2(4), 802-.813. http://doi.org/10.9770/IRD.2020.2.4(6)

JEL Classifications: M15, Q48

* *This research is/was funded by the European Social Fund under the No 09.3.3-LMT-K-712 "Development of Competences of Scientists, other Researchers and Students through Practical Research Activities" measure.*

European Research Council
Established by the European Commission

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

1. Introduction

The introduction of the concept of cybersecurity has brought to a major development of the role and responsibility of a state towards its citizens. Since cyber-attacks have been regarded as a growing phenomenon, especially in advanced countries, many of them decided to implement newer strategies, which considered the cybersecurity of both private and public spheres. According to the International Telecommunication Union (ITU), by the end of 2018, 3.9 billion people were using the Internet (ITU, 2019), which means that the cyberspace is growing more and more wach year and needs to be protected. Many countries worldwide have published National Cybersecurity Strategies (NCSSs), which embodied the will of securing the cyberspace from cyber attacks and ransomware.

However, there seems to be an obstacle to the achievement of full cybersecurity, which is the protection in particular of Critical Energy Infrastructures (CEI). For "*critical infrastructures",* the definition can vary from country to country, but the general meaning can be traced back to "*services and facilities used by society which disruption or malfunction would generate negative consequences to the public"* (Izycki et al., 2019). While past attacks were focused mainly to IT (Information Technology) environments, the trend shows that cyber risks is now greater in the OT (Operational Technology) environment. Even though the risk is present and growing, many NCCs do not address specific plans which include Critical Infrastructure Protection (CIP) or recognize the need of an adequate framework for granting supply chain and aid during and after a cyber attack.

This article will attempt to examine the issue of the CIP as a gap in NCSSs, by analyzing and comparing five different NCSSs. The countries will be firstly chosen by picking the first five that are represented in the Global Cybersecurity Index (GCI) 2018, issued by the ITU. The list is made by evaluating the country's commitment and development into cybersecurity solutions. The ranking is made by evaluating five elements, all with the same weight in the calculation of the final grade: *legal*, so the existence of legal institutions or frameworks concerning cybersecurity, *technical*, the existence of such technical institutions and framework, *organizational*, meaning policy coordinating institutions, *capacity building*, existence of research & development and education and training programs, and *cooperation*, so in terms of partnerships and cooperative framework (ITU, 2019). The list of the Global Ranking of 2018 puts in the first five slots (in order): UK, USA, France, Lithuania and Estonia (ITU, 2019).

The analysis would proceed by evaluating the strategies of Critical Infrastructure Protection of the first five countries by using the model that was developed by Limba T., Plėta T. et al., named the "*Cyber Security Management Model for Critical Infrastructure",* developed in 2017 (Limba, et al., 2017). The tiers are six, and each evaluates a specific feature needed for an adequate framework of management model for cybersecurity. *Legal regulation* evaluates the understanding of an organization of cybersecurity, its aims and the required planning; the second tier is for *risk management*, which evaluates the organization's ability to identify the growing risks and to develop adequate responses. Other important elements are *Security Culture*, which evaluates the level of undersanding of cybersecuirty for every member of the organization's staff, *Technology Management*, which concerns the knowledge of all of the organization's elements and their vulnerabilities and *Incident Management*, which considers whether the organizaiton has special planc regarding the incident consequence management (Limba, et al., 2017). After the evaluation, there will be a ranking which will establish the best and the worst strategy in terms of CEIP, and it would be possible to compare the results to the ones resulted from the GCI 2018. Furtherly, a new model will be proposed which could better ensure a high level of CEIP. In order to determine the level of preparation of NCSSs in terms of management models for Critical energy infrastructure protection, documents will be taken from official sources. However, the priority will be to consider documents

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

specifically dedicated to Critical Infrastructure Protection, in particular on management model and strategy. In the case of the country not having specific documents on CIP, the National Cyebrsecurity Strategies will be used.

2. Analysis of the National Cybersecurity strategies

The following chapter will offer an analysis of national cybersecurity approaches to the protection of critical infrastructures. As mentioned in the introduction, the model that will be used for the evaluation will be of Limba et al. (Limba, et al., 2017), called *Cyber Security Management Model for Critical Infrastructure.* The goal of the analysis it to show the existing gaps in the national strategies when it comes to protection of critical infrastructures (CIP). For this reason, the countries that were chosen supposedly to implement the best possible practices according to the Global Cybersecurity Index (GCI). The evaluations will assess the presence of frameworks dedicated to CEIP and of effective management strategies. If the country does not provide a specific document on CEIP management, the analysis will be conducted on the existing NCCS.

3. UK

According to the Global Cybersecurity Index (GCI), the United Kingdom is placed at the first place of the list, immediatey before the US (ITU, 2019). The choice to put the UK in the first place reflects a serious commitment of the country to invest in cybersecurity development. In the 2015 *National Security Strategy and Strategic Defence and Security Review* issued by the government (HM Government, 2015), it can be found a part dedicated to the *Critical National Infrastructure (CNI)* and *Energy security*. In the strategy, it is mentioned the will to ensure resilience of CNI to future threats such as power disruptions and such (HM Government, 2015). Moreover, the government founded the *Center for Protection of National Infrastructure*, which focuses on reducing the vulnerability of the national infrastructure, in particular on CIP (CPNI, 2020) along with the *National Cyber Security Centre* in 2016 (National Cyber Security Centre, 2020).

The analysis that was conducted on the UK approach to management aspects of Critical Infrastructure Protection revealed a peculiar situation. The main documents concerning the topic were the second and third report of the *Joint Committee on the National Security Strategy* on *Cyber Security Skills and the UK's Critical National Infrastructure* (Joint Committee on the National Security Strategy , 2018) (Joint Committee on the National Security Strategy, 2018). The documents confirm that, even though in 2016 the government published in 2016 the *National Cyber Security Strategy 2016-2021*, under the "Develop" section there are quoted *"the systemic issues at the heart of the cyber skills shortage"* (Joint Committee on the National Security Strategy, 2018). The issues that are recorded have to do with the lack of education and established carreers concerning the topic of cybersecurity (Joint Committee on the National Security Strategy, 2018), so that there are not enough English citizens who posses the needed skills and the abilioty to work in the Critical National Infrastructure sector (Joint Committee on the National Security Strategy, 2018). In the *third report*, as well, it is said that the Government's definition of Critical National Infrastructure it is too broad, and it does not help in identifying the types of Infrastructure that need the most protection (Joint Committee on the National Security Strategy, 2018).

In the analysis, it was difficult to find the requirements described in the Limba et al. model. *Legal regulation*, meaning the acknowledgement of the need of Critical Infrastructure Protection by official institutions (Limba et al., 2017), can be found in the *National Cyber Security Strategy 2016-2021* (HM Government, 2016). In the document, one of the objectives in the "Defend" section is "*protecting our Critical National Infrastructure and other priority sectors"* (HM Government, 2016). The Government declares that a reguatory framework is needed, but at the same time does not provide additional details about it. The UK government's has the *Cabinet Office's Civil Contingencies Secretariat (CCS)* held responsible for big emergencies including the ones involving Critical Infrastructures. The Cabinet office elects, a number designated *Lead Government Department (LGD)*, which guides the incident management and planning in emergencies of high classification (Civil Contingencies

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

Sectretariat, 2004). The 2004 document that was formed for describing the guidelines that LGDs have to follow to promote assistance, *The Lead Government Department and its role – Guidance and Best Practice* (Civil Contingencies Sectretariat, 2004) contains a bit of general parts of the elements of *good governance* and *risk management* according to the Limba model (Limba et al., 2017). The procedures and the planning processes are presented in the document, as well as the emergency operation checklists and the responsibilities; however, since the LGDs can intervene in varioius situation of emergency, the outline results to be too general to have an adequate overview on the correct procedures (Civil Contingencies Sectretariat, 2004). About the *security culture*, there are various documents that explain in general the different types of cyber attack that an organization can experience, such as *Common cyber attacks: reducing the impact* (CESG, 2016). The document presents basic knowledge on the different types of cyber attacks, but it focuses more on the procedures that a non-critical organization could follow (CESG, 2016). Concerning *technology management* and *Incident management*, there are no known solutions or specific documents from the govenrment that cocern Critical Infrastructures.

4. USA

The second country in the world for level of cybersecurity level, according to the GCI 2018, is the Unites States of America. In fact, the US government dedicated a Department of Homeland Security to cybersecurity, the *Cybersecurity and Infrastructure Security Agency (CISA*) which has a *National Infrastructure Protection Plan (NIPP)* (CISA, 2018), to form a dedicated and comprehensive strategy for CIP. The documents that were revised for the evaluation are many, since the NIPP website provides a lot of material available to anyone. Firstly it is necessary to say that there are multiple documents entirely dedicated to Critical Infrastructures: the website offers an extensive access to *core services and capabilities* of the CISA. Amongst the listed, the Department of Homeland Security has as a priority to conduct *assessments* on infrastructure and communities to help the organizations to make decisions, to provide and share *information* to both public and private sector (public-private partnerships are considered vital to the development of CIP). Another major focus in the *core services* is on *training and exercises* by collaborating on state, local, and tribal level and providing training on critical infrastructure security (CISA, 2018).

In order to conduct the analysis, the documents that will be taken into consideration will be eight. The most important is the *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience*, (Homeland Security, 2013), which outlines how the government and the private sector should behave in order to achieve CIP. The document represents an evolution of the preexisting version of the NIPP published in 2006, and provides the guidelines to achieve an *integrated and collaborative approach* to a secure and resilient critical infrastructure. The document is divided into *five sections: Vision, Mission and Goals*, which considers the guidelines for the critical infrastructure community, *Critical Infrastructure Environment*, which instead describes the policy, the risks and the partnership structure needed to achieve the community's goals, *Core Tenets*, describing the principles of the NIPP, *Collaborating to Manage risks*, which describes the framework for risk management activities, and finally the *Call to Action* to the entire critical infrastructure community (Homeland Security, 2013). There are as well three supplements of the NIPP 2013 that will be taken into consideration, such as the *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach* (Homeland Security, 2013), the *Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects* (Homeland Security, 2013) and the *Supplemental Tool: NPPD Resources to Support Vulnerability Assessments* (Homeland Security, 2013). In addition to the NIPP 2013 framework, which is appliable to all types of Critical Infrastructures, there are *Sector specifici plans* tailored for each type. Since that, as aforementioned, the focus on the article will be on Critical Energy Infrastructure (CEI), the two documents that will be considered for the analysis are the *Energy Sector-Specific Plan* (Homeland Security, 2015) and the *Energy Sector Cybersecurity Framework Implementation Guidance* (US Department of Energy, 2015). Ultimately, there will be mention as well of *NIST: Framework for*

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

Improving Critical Infrastructure Cybersecurity (NIST, 2018) and and the *Critical Infrastructure Threat Information Sharing Framework* (Homeland Security, 2016).

Firstly, the field of *legal regulation* according to Limba et al. (Limba, et al., 2017) is broadly evaluated by the presence of security instructions to employees, information security officers, network administrators and standards (Limba, et al., 2017). The US documentation offers a broad choice of standards, but the most important is surely the *NIST: Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2018). The document has a complementary role, meaning that is accessible to every organization in order to enhance their cybersecurity level and to evaluate their performance (NIST, 2018). In terms of instruction to information security and network administrator another important document is the *Critical Infrastructure Threat Information Sharing Framework* (Homeland Security, 2016), which offers a list and contacts of all the entities participating in the *information-sharing process*, as well as the *Supplemental Tool: NPPD Resources to Support Vulnerability Assessments* (Homeland Security, 2013), which provides information on the Federal resouces that are available to the sector partners to identify and assess CI vulnerabilities.

For what concerns the aspect of *good governance*, the model refers to it also as *security planning* (Limba, et al., 2017), and the document which is the most useful in that sense surely is the *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience* (Homeland Security, 2013), which enlightens the policy and the environments in CIP. The documents offers an insight on the stucture of partnerships and the-ir fundamental role into the collaboration into building an effective regulation, as well as describing the National Partnership Structure, and the role of Infrastructure Partners and Stakeholders (Homeland Security, 2013). Instead for the aspect of *risk management*, which evaluates the presence of a contingency plan and is one of the main focus of the analysis, the document that is considered the most adequate is the *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach* (Homeland Security, 2013). In the document, it is described the *Critical Infrastructure Risk Management Framework*, which can be applied to all types of threats and hazards and is supported by the *Threat and Hazard Identification and Risk Assessment (THIRA).* As well the the *Energy Sector Cybersecurity Framework Implementation Guidance* (US Department of Energy, 2015) offers the *Energy Sector Cybersecurity Risk Management Approaches*, a list of possible approach s that can be implemented by any organization.

Concerning the *security culture*, meaning the presence of the security measures for all the employees (Limba, et al., 2017), can be evaluated as well in the *Critical Infrastructure Threat Information Sharing Framework* (Homeland Security, 2016), which offers as well a *Reference guide for critical infrastructure owners and operators* and general guidelines on the reporting of critical incidents, which as well reflect as well *incident management* (Limba et al.,2017). The *technology management* element (Limba et al., 2017) is overall about the organization's knowledge of their components and how they worked, and it can be found as a part of the aforementioned *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience,* (Homeland Security, 2013), which has as a priority the identification of the Infrastrucure.

5. France

According to the 2016 *French National Digital Security Strategy* (Government of France, 2015), one of the strategic objective of France in the field of cybersecurity is to gain "*fundamental interests, defence and security of state information systems and critical infrastrucrtures, major cybersecuirity crises"* (Government of France, 2015). Being in the third place in ranking in terms of cybersecurity index (ITU, 2019), France developed in terms of cybersecurity. In the document, it is explained the government's decision of partnering at the European level with the European agency ENISA (European Union Agency for Network and Information Security), and relying

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

on the CERT-EU (Computer Emergency Response Team of the European Union (EU) institutions, bodies and agencies) and to the NCIRC (Computer Incidence Response Capability) of the North Atlantic Treaty Organization (NATO) (Government of France, 2015). Hence, the approach of France is quite peculiar, as it bases on the international level rather than the national level. In terms of national organizations, France established in 2013 a regulatory framework for *Critical Infrastructures Information Protection (CIIP)* (ANSSI, 2020), the *"CIPP law"*. The framework identifies, in coordination with the *General Secretariat for National Defence and Security*, 12 sectors and 200 operators, defined as "*operator[s] whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation"*(ANSSI, 2020). The protection of CI is regardes as a priority, and the *National Cybersecurity Agency (ANSSI)* works with the government to nominate operators for each CI, which should be able to draw both *operator security plan (OSP)* and specific protection plans (Secretariat-General for National Defence and Security, 2017).

However, if we analyze the French approach, we can found gaps in the model proposed by Limba et al. (Limba et al., 2017). The *legal regulaton* is present, since the government is aware of the issue of Critical Infrastructures and hence is developing a solution, by putting their protection as one of the main objectives of their strategy, as aforementioned (Government of France, 2015). For what concerns *good governance*, the security planning is hardly markable as adequate, since the only security rules are common to every type of CI, and the processes are depending on the various operators and there is no mention of an effective common and comprehensive framework (ANSSI, 2020) (Limba et al., 2017). There are some measures in case of emergencies, during which the ANSSI receives information from the organization and provides assistance, but there are no mentions of plans or to effective regulations: the *incident management* could be considered as at a low level, but still present (ANSSI, 2020) (Limba et al., 2017). For what concerns the other elements in the model, France does not provide any more insights.

6. Estonia

Placed at the fourth place in the GCI 2018 (ITU, 2019), Estonia is seldom seen as the poster child of Europe's digitalization. The republic of Estonia is deeply invested in the cause of cybersecurity, however in their *Cybersecurity Strategy 2019-2022* one of the challenges marked in 2018 is "*Insufficient understanding of the impact of cyber threats, incidents and infrastructure interdependencies"* (Republic of Estonia, 2018). The republic passed in 2018 the *Cybersecurity Act*, which established requirements from businesses and institutions for preparing for a cyber threat (Republic of Estonia, 2018). In addition, the Minister of Entrepreneurship and Information Technology passed in 2018 the *Requirements for risk analysis of network and information systems and description of security measures*, established under the *Cyber Security Act* (Republic of Estonia, 2018). Following the 2007 cyber attacks in Tallinn, which brought distruption for the civilans for days, the government established the *Emergency Act* in 2009, which provides the legal basis for planning and crisis management (Government of Estonia, 2009): despite being passed in 2009, the act provides with guidelines for planning and risk assessment directed to *providers of vital services*, meaning Critical Infrastructure.It is important as well to mention the presence in Estonia of the *NATO Cooperative Cyber Defence Centre of Excellence*, which researches on cyber security expertise, and of the CERT-EE, established in 2006 and responsible for management of security incidents in .ee compiuter networks (Information System Authority, 2020) (CCDCOE, 2020).

The analysis accordind to the Limba model shows a better preparation for Critical Infrastructure protection than France, which is however put a rank above Estonia in the GCI. In terms of *legal regulation* (Limba et al. 2017), all the aforementioned documents mention the necessity to develop an effective cybersecurity for Critical Infrastructures, however in particular the *Cyber Security Act* enphasizes the necessity to maintain the functioning and maintenance of "*network and information systems essential for the functioning of societ and state"* (Republic of Estonia, 2018). The *Cyber Security Act* can be regarded, toghether with the regulation of *Requirements for risk analysis of network and information systems and description of security measures* can be part of the *good*

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

governance requirements , since it offers security planning over the risk analysis of Critical Infrastructures (Republic of Estonia, 2018). For what concerns *Risk management,* hence the presence of a contingency plan, the Estonian government offers an overview in the 2009 *Emergency Act,* in which are described the obligations of the *vital service providers* under law to perform risk assesments plan and continuous operation risk assessment (Government of Estonia, 2009). In the same *doument* there are the guidelines that the operators have to follow in the case of incident and disruption of critical services, which can be identified as part of the *incident management* tier (Limba et al., 2017) (Government of Estonia, 2009). *Security culture* and *technology management* have yet to be assessed for Estonia.

7. Lithuania

The last country to be part of the analysis is Lithuania, placed in the fifth place of the GCI (ITU, 2019). The resolution to the issue of cybersecurity is discussed in the 2018 *National Cyber Security Strategy* (Government of the Republic of Lithuania, 2018). Additionally, in September 2016 Lithuania launched its own *National Cyber Security Centre (NKSC),* which took on the information security incident investigation previously performed by the Communications Regulatory Authority of the Republic of Lithuania on January 2018 (National Cyber Security Centre, 2020). Concerning the protection of cyberspace, it is currently present the *Computer Emergency Response Team in Lithuania (CERT-LT),* which plays a key role in providing assistance to organizations and businesses (Government of the Republic of Lithuania, 2018). In the strategy however, it is mentioned that "[…] *on the national level, the security risk assessment culture and cyber security risk assessment are still fragmentary. There is a lack of analysis on cyber threats and gaps in security as well as full integration into activity risk assessment processes."* (Government of the Republic of Lithuania, 2018). There is a focus on the protection of Critical Information Infrastructure, but no sign of will if implementing a framework to protect CI. It is worth mentioning as well that in the capital Vilnius the *NATO Energy Security Centre of Excellence (ENSEC COE)* is collaborating with the government to research newer solutions to the issue of Critical Infrastructure Protection (NATO Energy Security Center of Excellence, 2020). Another important document that needs to be taken into consideration for the purposes of the analysis is the *National Cyber Incident Management Plan,* developed and implemented in 2018 (Government of the Republic of Lithuania, 2018).

According to the Limba model, the Lithuanian approach to the problem of Critical Infrastructure Protection seems unadequate, since that the documents taken into consideration were not either specifically drafted for Critical Infrastructures, or had mention of the issue as a separate goal. The *National Cyber Incident Management Plan* offers some insight to the general procedures of *risk management* and *incident management,* as it provides general guidelines on how to report and communicate to the authorities in case of a cyber incident (Government of the Republic of Lithuania, 2018) (Limba et al., 2017). There are general mentions to improve the cybersecurity of Critical Information Infrastructures in the *National Strategy* could be seen as an initial stage of *legal regulation* (Limba et al., 2017).

8. Evaluation and comparison

The previous part of the article provided an analysis of the first five countries for Cybersecurity Level according to the GCI 2018 (ITU, 2019). The model that was used provides six indicators, which are described in the table 1 below: each indicator can have a value that ranges from zero to five. *Zero* means that there is no mention of the indicator in the chosen documents, and there is no alternative seen in general cybersecurity approaches, and it ranges till the level *Five,* which indicates an adequate and comprehensive implementation of functioning regulations.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

Table 1. Indicators of Cybersecurity Level

	Legal Regulation	*Good Governance*	*Risk Management*	*Security Culture*	*Technology Management*	*Incident Management*
UK	*4*	*3*	*3*	*4*	*0*	*0*
USA	*5*	*5*	*4*	*4*	*4*	*4*
France	3	*2*	*0*	*0*	*0*	*2*
Estonia	4	*4*	*3*	*0*	*0*	*3*
Lithuania	*2*	*0*	*1*	*0*	*0*	*2*

From the results gathered from the analysis of the five countries, it is noticeable how the protection of Critical Infrastructure, despite being vital for the cybersecurity of a country, has yet to be developed even in the most developed countries in terms of cybersecurity. The US model currently represents the most comprehensive and adequate framework in terms of Critical Infrastructure Protection, as it offers higher marks compared to all the other countries, as seen in the analysis. It is interesting to see how much the evaluation shows a distancing between the USA and the rest of the countries taken in for the analysis, while according to ITU, the UK still has the first place for cybersecurity index (ITU, 2019). The table clearly shows the areas in which the countries possess gaps in the framework, and the countries that score the worst performance by having more zeros are Lithuania, at the last place of the GCI, and surprisingly France, which instead is placed above Estonia in the GCI. The areas that have resulted in getting the highest evaluations are *Legal regulation* and *Good Governance,* while the areas in which are regarded the more gaps are *security culture* and *technology management.* This shows how the weakest spot in the implementation of Critical Infrastructure Protection is the awareness and the training of the workers, fundamental for the development of newer solutions. In addition, beside the US it is seen a total lack of knowledge of the various components and parts of Critical Infrastructures, along with their functioning.

The analysis brought to light an average deep inadequacy concerning the protection of Critical Infrastructures, except the US approach. The model not only shows how the countries generally lack an adequate framework, but also how the general approach to cybersecurity can be apparently satisfactory, like the criteria used by the ITU to develop the GCI, but can be deceiving in evaluating the practical applications of the cybersecurity principles. The Limba model that was used in the analysis is adequate, but it could be highly improved. It should be implemented an international criteria which would consider more elements to be necessary for a country to develop. The model should also take into consideration a more hierarchical approach to the classification of Critical Infrastructure, by organizing a list in which the different types of Critical Infrastructure in the country could be evaluated in order of importance in case of attack or emergency, and to assure the supply-chain to the most important ones. This could help countries with a poorer state budget to prioritize their investment in Critical Infrastructure Protection. Another important issue that should be taken into consideration in developing a newer model should focus as well on the *planning,* as seldom it is unclear what it is to protect in Critical Infrastructure, and the previous analysis confirmed this vision with the lacks in *technology management.*

In order to develop a model with adequate criteria, the best standard that should be used to implement a newer approach is the *ISO/IEC 27002: Information Technology – Security Techniques – Code of practice for information security controls* (Technical Committee ISO/IEC JTC 1, 2013), which represents the best practices for implementing an effective model for Critical Infrastructure Protection.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

Bibliography

Government of the Republic of Lithuania. (2018). *National Cyber Incident Management Plan.* Vilnius: https://www.ird.lt/media/force_download/?url=/uploads/structure/docs/42166_cf30b855d9ac94e388b0d52cbf96ae86.pdf.

ANSSI. (2020). *FAQ: The French CIIP Framework.* Retrieved from ANSSI: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/#2-3

ANSSI. (2020). *The French CIIP Framework.* Retrieved from ANSSI: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

ANSSI. (2020). *The French CIPP Framework.* Retrieved from ANSSI: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

CCDCOE. (2020). *About us.* Retrieved from CCDCOE: https://ccdcoe.org/about-us/

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

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

CISA. (2018, November 21). *National Infrastructure Protection.* Tratto il giorno May 8, 2020 da https://www.cisa.gov/national-infrastructure-protection-plan

Civil Contingencies Sectretariat. (2004). *The Lead Government Department and its role – Guidance and Best Practice.* London: Cabinet Office. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61355/lead-government-departments-role.pdf

CPNI. (2020). *About* . Retrieved from Centre for the Protection of National Infrastructure: https://www.cpni.gov.uk/who-we-work

Government of Estonia. (2009). *Emergency Act.* Tallinn: Government of Estonia. Retrieved from https://www.riigiteataja.ee/en/eli/525062014011/consolide

Government of France. (2015). *French National Digital Security Strategy.* Paris: Government of France. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy

Government of the Republic of Lithuania. (2018). *Resolution on the approval of the National Cyber Security Strategy.* Vilnius: Government of the Republic of Lithuania.

HM Government. (2015). *National Security Strategy and Strategic Defence and Security Review 2015.* London: HM Government. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

HM Government. (2016). *National Cyber Security Strategy 2016-2021.* London: HM Government. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Homeland Security. (2013). *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience.* Washington DC: Homeland Security. Retrieved from https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Homeland Security. (2013). *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach.* Washington DC: Homeland Security. Retrieved from https://www.cisa.gov/publication/nipp-2013-ci-risk-management-approach

Homeland Security. (2013). *Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects.* Washington DC: Homeland Security. Retrieved from https://www.cisa.gov/publication/nipp-2013-resilience-ci-projects

Homeland Security. (2013). *Supplemental Tool: NPPD Resources to Support Vulnerability Assessments.* Washington DC: Homeland Security. Retrieved from https://www.cisa.gov/publication/nipp-2013-resilience-ci-projects

Homeland Security. (2015). *Energy Sector-Specific Plan.* Washington DC: Homeland Security. Retrieved from https://www.cisa.gov/publication/nipp-ssp-energy-2015

Homeland Security. (2016). *Critical Infrastructure Threat Information Sharing Framework.* Washington DC: Homeland Security. Retrieved from https://www.cisa.gov/publication/ci-threat-info-sharing-framework

Information System Authority. (2020, January 24). *CERT-EE.* Retrieved from Information System Authority: https://ria.ee/en/cyber-security/cert-ee.html

ITU. (2019). *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Izycki E., C. R. (2019). Protection of critical infrastructure in national cyber security strategies. Coimbra: European Conference on Cyber Warfare and Security. Retrieved from https://www.researchgate.net/publication/335760609_Protection_of_critical_infrastructure_in_national_cyber_security_strategies

Joint Committee on the National Security Strategy. (2018). *Cyber Security of the UK's Critical National Infrastructure: Third Report of Session 2017–19.* London: House of Lords & House of Commons. Retrieved from https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf

Joint Committee on the National Security Strategy. (2018). *Cyber Security Skills and the UK's Critical National Infrastructure: Second Report of Session 2017–19.* London: House of Lords & House of Commons. Retrieved from https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues, 4*(4), 559-573. https://doi.org/10.9770/jesi.2017.5.2(15)

National Cyber Security Centre. (2020). *National Cyber Security Centre.* Retrieved from National Cyber Security Centre: https://www.nksc.lt/en/

National Cyber Security Centre. (2020). *What we do* . Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

NATO Energy Security Center of Excellence. (2020). *About.* Retrieved from NATO Energy Security Center of Excellence: https://enseccoe.org/en/about/6

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

Republic of Estonia. (2018). *Cybersecurity Act.* Tallinn: Republic of Estonia. Retrieved from https://www.riigiteataja.ee/en/eli/523052018003/consolide

Republic of Estonia. (2018). *Cybersecurity Strategy 2019-2022.* Tallinn: Republic of Estonia. Retrieved from https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Republic of Estonia. (2018). *Requirements for risk analysis of network and information systems and description of security measures.* Tallinn. Retrieved from https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

Secretariat-General for National Defence and Security. (2017). *The Critical Infrastructure protection in France.* Paris: Government of France. Retrieved from http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

Technical Committee ISO/IEC JTC 1. (2013). *Information technology - Security techniques - Code if practice for information security controls.* Switzerland: ISO/IEC. Retrieved from https://www.iso.org/standard/62726.html

US Department of Energy. (2015). *Energy Sector Cybersecurity Framework Implementation Guidance.* Washington DC: US Department of Energy. Retrieved from https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

Acknowledgements

This research is/was funded by the European Social Fund under the No 09.3.3-LMT-K-712 "Development of Competences of Scientists, other Researchers and Students through Practical Research Activities" measure.

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 4 (December)
http://doi.org/10.9770/IRD.2020.2.4(6)

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

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

Silvia DELLA CASA is an MA student at the University of Bologna at the Interdisciplinary Research and Studies of Eastern Europe (MIREES) and 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

Juozas LATVYS is a PA officer at the NATO Energy Security Centre of Excellence (juozas.latvys@enseccoe.org). His main research interests are related to cyber security management of states critical energy infrastructure, state geopolitical aspects and its influence through strategic national resources, energy sector development and its impact on states economies.
ORCID ID: https://orcid.org/0000-0002-9284-677X

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