TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Department of Software Science

Tedel Baca 177281IVCM

CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF KOSOVO: A POLICY ANALYSIS ON THE PROTECTION OF ELECTRIC-ENERGY AND WATER-SUPPLY SECTORS

Master's Thesis

Supervisor: Mika Juha Kerttunen (D.Soc.Sc)
Senior Research Scientist
Co-Supervisor: Kristine Hovhannisyan (MSc.)
Cyber Security Researcher

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Tarkvarateaduse osakond

Tedel Baca 177281IVCM

KRIITILISE INFRASTRUKTUURI KAITSE KOSOVO VABARIIGIS: ELEKTRIENERGIA JA VEEVARUSTUS SEKTORITE KAITSMISE STRATEEGILINE ANALÜÜS

Magistritöö

Juhendaja: Mika Juha Kerttunen (D.Soc.Sc)
Vanemteadur

Kaasjuhendaja: Kristine Hovhannisyan (MSc.)
Küberturve teadur

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Tedel Baca

13.05.2021

Abstract

Critical Infrastructure Protection (CIP) is an important part of national strategies. The reliance of CI components on IT systems introduced the issue of cyber-attacks and cyber incident response on the CI environment. The attention on this topic was even more important, when the first ever cyber-weapon resulted in physical destruction of a CI environment. EU saw the importance of CIP and introduced the NIS Directive and ENISA guidelines. One of the main goals of these documents is to improve the CIP policies and their implementation mechanisms on EU MS. Because the EU guidance is thorough and one of the best guidance on developing and improving CIP policies, it can also be used from nations outside of the EU. This is even more relevant after the 2015 cyber-attack on the Ukrainian electrical power-grid systems. In addition, it is important for nations to learn from previous real-world CI cyber-attacks. Repeating mistakes from these cyber-attacks could result in devastating consequences such as electrical power interruption or the poisoning of water-supply systems.

The Republic of Kosovo already has some policies in place on the CIP such as the law on CI and its national cyber security strategy. In this thesis, the author developed a methodology consisting of two elements, a policy evaluation criteria and a semaphore model, to evaluate Kosovo's current CIP state of policy. The EU relevant CIP guidelines have been used to develop the evaluation criteria. Using a synthesis, the semaphore model is applied on Kosovo's CIP policy criteria by considering Kosovo's current CIP policies and OES environment on electric-energy and water-supply sectors. By observing this synthesis, the author identified weaknesses in Kosovo's current CIP state of affair and offered recommendations on its improvement.

The methodology can be used by CI policy makers of other countries to evaluate their respectable CIP state of affair. This thesis is written in English and is 80 pages long, including 6 chapters, 11 figures and 2 tables.

Keywords: Critical Infrastructure Protection, Operators of Essential Services, the Republic of Kosovo, European Union, Strategy, Guidelines, cyber-attack, cyber incident, cyber-awareness, threat landscape, electric-energy, water-supply.

Dedication

This thesis is dedicated to the memory of my beloved mother, Arijeta Shehu Baca, who passed away two years ago. Mother, thank you for making me who I am today. Without your unconditional love, support, and sacrifices throughout the years, I would not be able to be where I am today. Your kind heart and positive mind taught me to be strong even on the hardest days of my life.

I know that you wanted to be there when I defend my master's thesis. Even though you are not there physically, I know that your energy still surrounds me, and I would not be able to finalise this thesis without the legacy that you left. I am the most privileged son in the world that I had the opportunity to call you my mother, and I hope that the work that I have done in this thesis would have made you proud.

Acknowledgements

Thank you, Dr. Mika Kerttunen, for your guidance and supervision throughout this thesis. Without your mentorship and the clarifications on the doubts I had, I would not have the confidence which now I possess on my research skills. Your way of explaining and simplifying my complex thoughts has really helped me to build a methodological way of research thinking. Msc. Kristine Hovhannisyan, thank you for pushing me, so that I could write this thesis on the best of my abilities. Your ideas and contribution on my independent thought process, helped me expand the horizon on the ways this thesis should be written.

I would like to also thank my two colleagues throughout the studies, Joanna Rose Del Mar and Olesia Yaremenko. At one point in time, I thought to not finish my masters studies, but they pushed me to not give up and were there to motivate me until the finish line. Thank you, girls. In addition, thanks to all the other colleagues and friends who were part of this wonderful journey. We all learned something from each other.

Last but not least, I want to thank my family. Throughout my life, my sister Adea Baca always gave me the support which made me calmer and stronger. Even though she is my younger sister, I always had to learn from her attitude as she is a kind and strong human being. I am such a lucky brother to have a sister as Adea. Meanwhile my father Skender Baca always gives me visions on how to become a better person in the future. He is right when he taught me and never forgets to repeat, that discipline, honesty, and hard work are the qualities that are needed on achieving my goals. I also want to thank my aunt Nora Shehu. She always took care of me and my sister since we were kids. Her positiveness, kind words and love, always motivates us to be the best of ourselves. I hope that this thesis work will make them proud.

List of abbreviations and terms

ACL	Access Control List
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ARKEP	Regulatory Authority of Electronic and Postal Communication
CERT	Computer Emergency Response Team
CG	Cooperation Group
CI	Critical Infrastructure
CIA	Confidentiality, Integrity and Availability
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIS	Critical Information Systems
CMM	Cybersecurity Capacity Maturity Model for Nations
DCS	Distributed Control System
DDOS	Distributed Denial of Service
DOJ	Department of Justice
DSP	Digital Service Providers
EMS	Energy Management System
ENISA	European Union Agency for Network and Information Security
EU	European Union
GCSCC	Global Cyber Security Capacity Centre
GDPR	General Data Protection and Regulation
GPS	Global Positioning System
HE	Hydro-economic Enterprise
HST	Hardware Security Token
HMI	Human-Machine Interface
IANA	Internet Assigned Numbers Authority
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IoT	Internet of Things
IIoT	Industrial Internet of Things
IL	Iber-Lepenc
ILC	Iber-Lepenci Company
IP	Internet Protocol
IT	Information Technology
ISP	Internet Service Provider
ISSP	Information System Security Policy

KEDS	Kosovo Electricity Distribution and Supply Company J.S.C.
KEK	Kosovo Energy Corporation J.S.C.
KOSTT	Kosovo Transmission System, and Market Operator J.S.C.
MBR	Master Boot Record
MED	Ministry of Economic Development
MS	Member States
MIA	Ministry of Internal Affairs
MW	Megawatt
NCSS	National Cyber Security Strategy
NIS	Network and Information Security
NTP	Network Time Protocol
OT	Operational Technology
OES	Operators of Essential Services
OS	Operating System
OSP	Operator Security Plan
PLC	Programmable Logic Controller
PMUs	Power Measurement Units
RQ	Research Question
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIS	Safety Instrumented Systems
SOC	Security Operation Center
TLD	Top Level Domain
TTP	Tactics Techniques and Procedures
UN	United Nations
UNDP	The United Nations Development Programme
VPN	Virtual Private Network

Table of contents

Author's declaration of originality 3
Abstract 4
Dedication 5
Acknowledgements 6
List of abbreviations and terms 7
Table of contents 9
List of figures 11
List of tables 12
1 Introduction 13
1.1 Motivation 14
1.2 Problem Statement 14
1.3 Research Question 16
1.3.1 Limitations and key assumptions 16
1.4 Methodology 18
1.4.1 Kosovo's CIP Policy Evaluation Criteria 18
1.4.2 Semaphore Model and its Structure 20
1.4.3 Synthesis: Application of Semaphore Model on Kosovo's current CIP Policies 21
1.5 Literature Review 22
2 EU Guidance 32
2.1 NIS Directive 32
2.2 NIS Cooperation Group Reference Documents on OES 34
2.2.1 Security Measures for OES 35
2.2.2 Incident Response and Notification for OES 37
2.3 ENISA Guidelines on ICS/SCADA Components and Cyber-Threat Landscape. 41
2.3.1 ICS/SCADA Systems Communication Network Dependencies 41
2.3.2 Cyber Threat Landscape 44
3 Lessons-Learned from Real-World CI Cyber-Attacks 48
3.1 SANS Institute Report on 2015 Ukrainian Power-Grid Cyber-Attack 49

3.2 Black Hat USA Research Paper on 2017 TRITON Saudi-Arabian Petrochemical Facility Cyber-Attack 53
3.3 Summary of Lessons Learned from Real-World CI Cyber-Attacks 55
4 Kosovo's National State Affair 57
4.1 Current CIP Policies and Cyber security Capacities in the Republic of Kosovo 57
4.1.1 Kosovo National Cyber Security Strategy and Action Plan 2016-2019 57
4.1.2 Kosovo's Law on CI 59
4.1.3 Kosovo's Cyber security Capacities 61
4.2 Kosovo's OES Environment 65
4.2.1 Kosovo's Electric-Energy Generation, Distribution and Transmission Environment 66
4.2.2 Kosovo's Water Security and Canal Protection Project 70
5 Synthesis: Application of Semaphore Model on Kosovo's CIP Policies and Recommendations 73
5.1 Application of Semaphore Model on Kosovo's current CIP Policies 73
5.1.1 Criterion 1: Identification of OES 73
5.1.2 Criterion 2: Single Point of Contact 75
5.1.3 Criterion 3: Cyber Awareness 76
5.1.4 Criterion 4: Penalties 77
5.1.5 Criterion 5: Threat Landscape 78
5.1.6 Criterion 6: Protection Mechanisms 79
5.1.7 Criterion 7: Incident Response Capacities 82
5.2 Summary of Synthesis 83
5.3 Recommendations on Improving Kosovo's CIP policies 86
6 Conclusion 90
References 93

List of figures

Figure 1. Critical Infrastructure interdependencies with other sectors [31] 43
Figure 2. Top Cyber Threats 2019-2020 [32] 44
Figure 3. Malicious Microsoft Office document used in 2015 Ukrainian power-grid cyber-attack [101] 50
Figure 4. Summary of the 2015 Ukrainian power-grid cyber-attack using ICS Kill-Chain model [19] 51
Figure 5. Schematic view of TRITON dropper phase [20] 54
Figure 6. “Kosova B” power plant operational room [21] 67
Figure 7. KOSTT operational room [23] 68
Figure 8. KEDS operational room where HMI of SCADA is shown [25] 69
Figure 9. SCADA vendor shown from KEDS magazine [25] 69
Figure 10. Iber-Lepenc Canal schematic map [28] 71
Figure 11. Kosovo Water Security and Canal Protection Project - SCADA architecture diagram [28] 72

List of tables

Table 1. The structure of the Semaphore Model 21
Table 2. The matrix that visualises the summary of synthesis 83

1 Introduction

Critical Infrastructure (CI) has a major influence in our daily lives. With the introduction of the digital age, a rapid digitalization of CI started. The protection of CI and Industrial Control and Supervisory Control and Data Acquisition (ICS/SCADA) systems against cyber threats and vulnerabilities has become even more important than ever before. From water-supply systems to electrical power-grids, governments of different nations saw the necessity to have policies and laws for Critical Infrastructure Protection (CIP). This necessity would maintain the above-mentioned essential services in a safe, operational, and secure state. One of the first national policy which explicitly mentions CIP as a national necessity is that of President Clinton's Directive (NSC-63) in 1998 [1]. In this directive, the cyber systems and its protection measures are explicitly mentioned as part of CI. But when the 20th century started, as is shown from Hemsley and Fischer's report [2], cyber incidents against ICS/SCADA systems increased rapidly and more measures had to be taken from nation-states across the globe.

After the September 11 terrorist attacks in 2001, CIP became increasingly important, as now terrorists could use cyber means to create havoc in the western world by attacking CI systems [3]. In 2003 United States took measures against these threats with "Presidential Directive/Hspd-7" where identification and protection of CI against terrorist attacks was established as a national policy [4]. Meanwhile, European Union (EU) did not stay idle against these threats and the changing environment of cyber-space. In 2004, EU established its own Agency for Cyber security (ENISA) where one of its mission is to contribute to EU cyber policies [5]. Meanwhile, in October of the same year, the European Commission of the European Communities, issued a communication [6] related to CI. This communication explained the risks against CI, defined CI sectors in Europe, and gave guidelines for the improvement of CIP in EU. The communication was later advanced with the creation of European Programme for Critical Infrastructure Protection (EPCIP) which defined an overall framework for CIP in Europe [7].

1.1 Motivation

With the increase of cyber-attacks and threats on CI, the physical damage on CI environment was also a possibility by attacking ICS/SCADA systems and its network dependencies (e.g. Stuxnet [8]). On 6th of July 2016, European Parliament adopted the Directive on security of Network and Information Systems (NIS Directive) [9]. NIS Directive helped EU Member States (MS) to have a common framework to protect their IT and OT systems. This directive also improved the cooperation between EU MS on response measures against cyber incidents. The adoption of the NIS Directive by the European Parliament made it mandatory for the EU MS to implement this directive into their national legislation by 9th of May 2018. In addition, by 9th of November 2018, each EU MS had to identify, report, and list their Operators of Essential Services (OES).

Kosovo, a country with an aspiration to join EU, has already taken some measures to protect its cyber space and CI. At the end of 2015, Kosovo adopted its first National Cyber Security Strategy (NCSS) [10] and in 2018, it created the law on CI [11]. These measures are still not sufficient as the current Kosovo's law on CI nor NCSS are not up-to-date and have not been transposed to NIS Directive. In addition, Kosovo and its cyber security policies are still not evaluated with regards to its preparedness in a real-world CI cyber incident.

This thesis will fill this gap based on an observational policy analysis of EU guidelines and technical papers on real-world CI cyber incidents against Kosovo's current CIP policies.

Kosovo's CIP policies and their impact were never researched before. Therefore, the author will develop its own evaluation framework to assess Kosovo's CIP policies and their impact on Kosovo's current CIP national state affair. In addition, based on this assessment, the author will propose recommendations on how these CIP policies can be improved.

1.2 Problem Statement

Kosovo is a small country with an approximate population of 1.8 million [12]. Since its independence on 17th of February 2008, the Internet penetration increased rapidly, where the latest data show us that 96% of Kosovo's household are connected to the Internet [13].

On December of 2015, Kosovo published its cyber security strategy [10]. The strategy has a dedicated section for Critical Information Infrastructure Protection (CIIP) and categorizes CI sectors based on a European Commission Green Paper [14]. In this green paper, the division of CI sectors does not differ much from NIS Directive [15]. Kosovo also has a law on CI [11], which further expands the procedures on identification of national OES and the division of CI sectors.

With regards to its incident response mechanisms, Kosovo has a national Computer Emergency Response Team (CERT) named Kosovo National Cyber Security Unit (KOS-CERT). KOS-CERT, which does not have a clear specific mandate of its responsibilities, is tasked with technical incident response and raising awareness against any incident that happens in Kosovo. Because of its limited mandate as well as due to its personnel shortage [16], KOS-CERT needs to improve its operational capabilities in order to properly respond against a cyber incident in Kosovo. This is especially important if a cyber incident could potentially affect an OES sector which has a greater impact on daily lives of Kosovo's citizens. Examples of such cases would be a cyber-attack on electric-energy or water-supply sectors.

Financial sector, one of the OES sectors, was already attacked in Kosovo. As shown in "Sense" report, a Kosovo Non-Governmental Organization (NGO) [17], on 19th of April 2020, Banka Ekonomike, a local Kosovo bank, was hacked by DopplePaymer ransomware operators. This resulted on a dump of client(s) data, financial data, and bank employees information onto the dark web. This was one of the biggest hacks that happened in Kosovo, and the consequences for the bank and for the citizens/customers are still to be seen. Another consequence of this hack is that it breached Kosovo's Law on Protection of Personal Data [18].

This shows that even though it has its CIP policies in place, the Republic of Kosovo still has problems with its national CI incident response mechanism. Before joining the EU or NATO, it would be appropriate for the Republic of Kosovo to be operationally ready by having a proper implementation mechanism on its CIP policies. This could be fulfilled by improving Kosovo's CIP policies, as well as mechanisms on protection and incident response on its OES environment.

This thesis will evaluate Kosovo's national CIP policies against a potential future cyber-attack on its OES with an emphasis on electrical-energy and water-supply sectors. The evaluation will be done by an observational policy analysis of relevant EU guidelines on CIP, and lessons learned through real-world CI cyber incidents (such as the cyber-attack on Ukrainian power grid system [19] and the cyber-attack on Saudi-Arabian petrochemical plant [20]). An evaluation framework will be developed and used to evaluate the preparedness of Kosovo's policies on CIP and incident response. The policy analysis on OES protection and incident response will have in focus the EU NIS Directive and other ENISA guidelines regarding OES protection, threat landscape and incident response.

1.3 Research Question

Taking into consideration the current state of Kosovo's CIP policies, NIS Directive, ENISA guidelines on OES and incident response, as well as previously known real-world CI cyber incidents, this thesis poses the following research question: **Are the current CIP policies of the Republic of Kosovo well-prepared on the response measures against a cyber incident on Kosovo's electric-energy or water-supply CI sectors? Therefore, do Kosovo's CIP policies adhere to NIS Directive and ENISA guidelines on CI? Also, do these policies comply with the recommendations taken from the lessons-learned of previous real-world cyber-attacks on CI?**

The author will answer the research question by analysing the current state of Kosovo's CIP policies against NIS Directive and ENISA guidelines. This will include the preparedness of Kosovo's current CIP environment and policies for response against cyber incident(s) on its electric-energy and water-supply infrastructure.

1.3.1 Limitations and key assumptions

A major limitation of this thesis is that it is based on publicly available information, including materials with regards to the CI cyber capacities of Kosovo. This includes the information of currently implemented projects on electric-energy [21] [22] [23] [24] [25] [26] [27] and water-supply [28] CI sectors.

Another limitation that the author raises is that Kosovo has not experienced a real-world cyber-attack on its water-supply or electric-energy OES sectors. This means that the

author's policy analysis of Kosovo's CIP on water-supply and electric-energy sectors, is based upon the examination of Kosovo's CIP policies preparedness according to EU and professional guidance.

Key Assumptions:

1. There is a risk and likely threat towards Kosovo's OES based on the disadvantages of its implementation mechanisms on CIP policies and national incident response institution readiness.
2. Kosovo's national policies and guidelines on CIP are not up to date. Therefore, a proper national guidance and implementation mechanism on Kosovo's OES protection and incident response against the latest threats is missing.
3. European CIP guidelines are one of the best guides in the world on the matter of CIP. These guidelines give proper and detailed instructions to nations on improving or developing properly their CIP policies and implementation mechanisms. In addition, Kosovo is a country that aspires to join EU. This means that the organizational and protection mechanisms of OES are required to be aligned with European CIP guidelines. These facts make European CIP guidelines relevant and applicable to Kosovo's CIP policies.
4. Despite that an implementation mechanism of its CIP policies and a proper incident response mechanism on its OES is missing, Kosovo is capable to apply European CIP guidelines. This can be done by updating its current CIP policies and their implementation mechanisms, as well as improving its national incident response institutions.
5. Kosovo's NCSS and law on CI are the locations where Kosovo's CIP preparedness can be detected and improved. Therefore, improvements on Kosovo's NCSS and law on CI, are effective to improve Kosovo's CI preparedness on protection and incident response mechanisms of OES.
6. Tactics, Techniques and Procedures (TTP) of attackers on CI are similar [19] despite on which country the cyber-attacks are happening. Having a proper awareness raising and resilience policy on OES against these TTP's would help nations on avoiding, responding, and recovering quicker against potential future cyber incidents on their CI. Therefore, previous real-world CI cyber-attacks are relevant and offer guidance to Kosovo in order to become better prepared for the protection of its CI.

1.4 Methodology

In this section, the author will present the evaluation framework and its elements:

- **Element 1**: The criterion against which Kosovo's current CIP policies will be evaluated, why that criterion was chosen and how are they relevant to Kosovo's CIP policies.
- **Element 2**: The idea behind semaphore model and the structure of the model where details of the rating system are described (maturity levels are color-coded).
- **Synthesis**: The application of semaphore model (element 2) on Kosovo's CIP policy criteria (element 1) to evaluate Kosovo's current CIP state of policy. This is followed by the analysis and justification of each specific verdict.

1.4.1 Kosovo's CIP Policy Evaluation Criteria

In order to define the criterion based on which the Kosovo's CIP policies will be evaluated, the following documents have been studied and used to elaborate those criteria:

- The NIS Directive requirements [15] and the reference documents from NIS Cooperation Group (CG) [29] [30].
- ENISA guidelines on ICS/SCADA systems [31] and cyber threat landscape [32].

A more detailed analysis of these documents is available in chapter 2 and chapter 3.

By taking into account the requirements from the documents mentioned above, the following criteria were identified:

- **Criterion 1: Identification of OES** - Evaluates Kosovo's ability to identify its OES on its own territory as it is required by articles 5 and 6 of NIS Directive [15]. This criterion is important because, without knowing the organizations which provide essential services, Kosovo's relevant authorities would struggle to identify where CIP policies should be enforced.
- **Criterion 2: Single point of contact -** According to article 8 of NIS Directive [15], an EU MS is required to have an assigned single point of contact for a better and simpler response mechanism against a potential cyber-attack on OES. This requirement exists because of a better cooperation mechanism between EU MS, based on which, the address where the incidents need to be reported is clearly defined. For example, a potential cyber-attack targets Kosovo's OES and one or

more of Albania's OES is affected. In this case, it would be easier for Kosovo to know a single address in Albania where the incident needs to be reported. This would eliminate confusion between states, in this case Kosovo and Albania, on where the incident should be reported. This criterion will evaluate Kosovo's ability on assigning the single point of contact from CIP perspective by analysing Kosovo's CIP policies on this matter.

- **Criterion 3: Cyber awareness -** Most of CI cyber-attacks start in the same way as cyber-attacks on other sectors: by sending phishing emails or messages to the CI operators from where an initial foothold is established. This criterion will analyse Kosovo's policies with regards to Kosovo's preparedness on cyber awareness but with a focus on CI operators.
- **Criterion 4: Penalties -** Article 21 of NIS Directive [15] requires EU MS to impose penalties to OES who do not adhere to CIP policies of that EU MS. This is an important mechanism that helps to create a strict environment by imposing a penalty on a Kosovo OES who does not adhere to national CIP policies.
- **Criterion 5: Threat landscape -** In order to anticipate potential cyber-attack vectors and landscape on Kosovo's CI, it is crucial to have a proper identification of threat landscape. This would improve the protection and threat intelligence mechanisms. The exchange of threats and vulnerabilities between CI owners is crucial on CIP. Therefore, this criterion will evaluate Kosovo's policies related to the identification of the threat landscape and the mechanisms on which latest threats and vulnerabilities are shared between CI owners.
- **Criterion 6: Protection mechanisms -** Evaluates Kosovo's CIP policy requirements to its OES on having a proper protection mechanism. Even though a protection mechanism does not guarantee that a cyber incident will not happen, the impact of that incident will be less significant if a proper protection mechanism is implemented. An example would be that the propagation of a malware in an IT network would be harder to be distributed if proper network security perimeter is in place. Another example would be that if a proper password-policy is followed, it would be harder for the attackers to guess the password of an administrator in an IT network that is part of CI environment.
- **Criterion 7: Incident response capabilities -** Evaluates Kosovo's readiness to respond to a cyber incident against one or more of its OES. This criterion will also

evaluate Kosovo's national CERT (KOS-CERT) ability to respond against a potential CI incident.

1.4.2 Semaphore Model and its Structure

Semaphore model is used as an evaluation tool against Kosovo's CIP policy criteria. The author decided to use the semaphore model because of its simplicity where the criteria can be classified properly into the three coloured ratings. In addition, it was author's point of view that the semaphore model is easier to be understood and followed through. The specific criterion and its evaluation are represented in a more comprehensive and simple way through the visualization of the semaphore model, rather than representing them by other methods such as wording or numbering. Therefore, it is simpler for the reader to understand a particular rating by clearly defining what each colour-code of the semaphore model represents. This semaphore model will also have a "symbol" section, from which, based on the shape of the symbol, colour-blind people can also understand the rating. The definitions of each of the colours and their ratings are as follows:

- **Red** – Kosovo has a plan on its CIP policies, but the plan does not adhere to the requirements that derive from NIS Directive and/or ENISA guidelines related to CIP. An implementation mechanism on the plan that adheres to NIS Directive and/or ENISA guidelines does not exist. The implementation of the plan is initiated.
- **Yellow –** Kosovo has a plan on its CIP policies which partially adheres to the requirements that derive from NIS Directive and/or ENISA guidelines related to CIP. An implementation mechanism is partially established with regards to the plan, where it partially fulfils the requirements deriving from NIS Directive and/or ENISA guidelines. The implementation state of the plan has started but it is partially completed.
- **Green –** Kosovo has a plan on its CIP policies which fully adheres to the requirements that derive from NIS Directive and/or ENISA guidelines related to CIP. An implementation mechanism is fully established on the plan and it fulfils all of the requirements that derive from NIS Directive and/or ENISA guidelines. The implementation state of the plan has been completed and it is fully established.

A summary of the semaphore model structure is shown below:

Table 1. The structure of the Semaphore Model

Level of Maturity Rating	Symbols	Plan	Implementation Mechanism	Implementation State
Red	●	Does not adhere to EU guidance requirements.	Does not exist.	Initiated.
Yellow	■	Partially adheres to EU guidance requirements.	Partially established and partially fulfils the requirements derived from EU guidance.	Started but partially completed.
Green	▲	Fully adheres to EU guidance requirements.	Fully established and fulfils all of the requirements derived from EU guidance.	Fully completed and fully established.

1.4.3 Synthesis: Application of Semaphore Model on Kosovo's current CIP Policies

In order to understand Kosovo's current CIP state of affair the following documents will be analysed in chapter 4:

- Kosovo's NCSS. [10]
- Kosovo's law on CI. [11]
- Cyber security capacity assessment on the Republic of Kosovo. [16]
- Relevant documents and information on Kosovo's electric-energy CI sector from: Kosovo Energic Corporation J.S.C. (KEK) website [21]; Kosovo's Transmission System, and Market Operator J.S.C. (KOSTT) including implemented projects [22] [23] and electric transmission development plan [24]; Kosovo Electricity

Distribution and Supply Company J.S.C. (KEDS) including magazines [25] [26] and electric distribution development plan [27].

- World Bank project on water security and canal protection for the Republic of Kosovo. [82]

In addition, the following real-world CI cyber-attacks will be analysed:

- SANS [19] and Black Hat [20] reports of real-world cyber-attacks on CI by taking into account the lessons learned from these cyber-attacks.

The real-world CI cyber-attacks will give context on how a CI cyber-attack works on a real-world scenario. In addition, the author will create a lessons-learned section derived from these real-world CI cyber incidents, where they will be applicable to Kosovo's CIP policies and OES environment.

By analysing the EU guidelines mentioned on section 1.5.1, as well as the above-mentioned documents on Kosovo's CIP and real-world CI cyber-attacks, the author will apply this analysis to the semaphore model. This will evaluate Kosovo's current CIP policies using the synthesis.

The synthesis is made of two elements:

1. Kosovo's CIP policy evaluation criterions that are explained in section 1.5.1.
2. Semaphore model and its structure explained in section 1.5.2.

By applying the semaphore model (element 2) onto Kosovo's CIP identified criterions (element 1), this synthesis will evaluate current CIP policy state of affair in the Republic of Kosovo. The synthesis will also be used by the author to answer the research question, as well as to come up with recommendations regarding the improvement of Kosovo's CIP policies.

The discussion of synthesis, which will justify the verdict for a specific criterion on Kosovo's CIP policies, will be done in chapter 5.

1.5 Literature Review

ICS/SCADA systems are one of the most important part of CI. Some of the functions of ICS/SCADA systems include:

- The monitoring and alerting of the status of CI components to check if they are in a healthy, operable state.
- Monitoring and controlling the levels of amount of water that is filled in vaults of water supply systems.
- Managing the state of electric circuits by opening/closing them in electric distribution systems or electrical power grids.
- Showing real-time data on human operators using HMI.

In the early days institutions and scientific community were more focused on protection of ICS/SCADA systems within the aspects of national disasters [33] or the economic ones [34]. Even though until 2010 there were incident reports against ICS/SCADA systems, the world still did not see any big impact in case of a cyber-attack against CI systems. This all changed when the first cyber weapon named "Stuxnet" was sophisticatedly launched against Iranian nuclear plant in Natanz [8] [35], that resulted in a significant damage on Iran's nuclear centrifuges [36]. With this cyber incident, the focus on CIP shifted more towards the cyber rather than physical means for securing ICS/SCADA systems. This cyber incident showed that the risk assessment between a natural disaster and a cyber-attack could not be the same [37]. This does not mean that physical protection of CI was left behind. In fact, it is still an important aspect of CIP. With the advancement in technology nowadays (e.g. the aerial drones and Artificial Intelligence (AI)), IT is also being integrated into physical protection of CI. In their paper, Zhang and Chandramouli [38] show a novel approach of detecting drones or humans nearby CI areas. They do this by using neural network deep-learning models where classification of the objects happens using video data obtained from the cameras that are monitoring the CI area. Meanwhile the author also observed that aerial technologies like Unmanned Aerial Vehicles (UAV) can save human lives during a disaster in CI area like fire hazard or oil leakage. This can be seen from Costea, Dumitrescu and Nemtanu research paper [39]. By using an algorithm which they developed, they show how UAV's as well as sensors in the ground that can beacon information to UAVs can save lives if something unusual is happening. These research papers show that the future CIP policies of Kosovo can rely on AI and drones to improve its protecting and monitoring mechanism of its OES physical environment. In addition, the evaluation method developed from the author can be used from these papers on evaluating the CIP policies of a country from physical security perspective.

As the author mentioned above, ICS/SCADA systems are now heavily depended on IT systems. Research community had already taken into consideration cyberspace as a threat vector since the beginning of 20th century [40] [41] [42]. Yet, with the rapid advancements in technology, TTPs as well as cyber tools are changing day by day and are being easily accessible (e.g. Dark Web). In their experimental research paper [43], Adepu and Kandasamy, use a simulation environment [44] and show how by using vulnerabilities such as Dropbear SSH [45], attackers can modify PLC code. This can cause power supply interruption that can result in electricity interruption even on major cities. Another research paper [46] analyses major security challenges that water treatment facilities face, and recommends automation on CI in order to respond more feasibly against well-known cyber incidents. Other experimental research papers which focus on cyber-attacks include simulation of attacks on energy management systems that are used as a power grid test case [47]. One example of a research paper which focuses solely on PLC attack is that of Tzokatziou and Maglaras where they use a Teensy microcontroller to simulate these attacks [48]. These academic papers show that the funding of experimenting with cyber-attacks on CI has decreased. This means that by having a proper funding, potential future attackers who target Kosovo's CI can test their attacks on a simulation environment, before going in a real-world cyber-attack scenario. In addition, as observed from [46], future Kosovo's CIP policies should include automation on CI, to better respond against known TTPs that can be used in future cyber incidents.

Research community has also contributed on protection measures against CI cyber-attacks. IEC 60870 is an ICS/SCADA systems set of communication protocols and standards which is used in power system automation [31]. Matousek and Rysavy [49] propose an IP flow based analysis of IEC 60870 protocol as a behavioural anomaly detection security method to detect and respond against cyber-attacks. Meanwhile, Hyder and Govindarasu [50] propose a game theory approach to simulate real-world attack scenarios with a focus on US power grids. This can help defenders of Kosovo's CI environment to understand how real-world attack scenarios play out and what measures need to be taken in order to improve the protection and incident response mechanisms on Kosovo's power grids. In their research paper, Zhou and Xu propose a kill chain model for ICS [51] which can be used by Kosovo's CI defenders to better understand attacker activities so that security resources can be allocated reasonably and that defenders can take effective security measures in time. In cyberspace SIEMs are an important tool to

analyse logs in order to better understand what happened during a cyber-attack, but sometimes they can be tampered in order to give us false information. Fournaris and Dimopoulos [52] come up with a solution on CI systems to verify the integrity of the CI hosts, by using Hardware Security Token (HST). HST's can also have log monitoring capabilities. There are also examples of academic literature where there is proposal for protection of ICS/SCADA systems by using IDS [53]. Unfortunately, as it will be seen from the real-world attack examples, using detection tools such as IDS or SIEM are not enough to defend Kosovo's CI systems.

Most of the research literature recommends that collaboration between nations regarding the latest cyber threats in ICS/SCADA systems and its network dependencies should be taken as a priority. If Kosovo has good collaboration with its neighbours, it will be easier to protect its OES that are dependent from these neighbours. Another recommendation is that human operators of CI should have a higher level of cyber-hygiene as well as awareness in order to counter these cyber threats. Automation should also be taken with higher priority from Kosovo's CI operators. Repetitive tasks such as responding to known incidents can be automated and save time for SOC team members to focus more on new incidents and TTPs rather than known ones. Most of the research literature mentioned above is experimental and does not apply to real-world cases. The evaluation methodology developed from the author can be used on the usage of these papers on real-world scenarios. This can be done by evaluating the CIP policies of a nation from the cyber-threats and recommendations mentioned above. The CIP policy criteria would be developed on these issues, and then the semaphore model is applied for evaluating the criteria.

Internet of Things (IoT) was a breakthrough innovation where nowadays our home equipment's are connected to the internet. Ericsson report [54] suggests that with the introduction of 5G, by the year of 2024, there will be 4.1 billion IoT cellular connections globally. The Industrial Internet of Things (IIoT) is the usage of IoT technology in ICS/SCADA systems where IIoT sensors offer real-time data to OT operators in industries such as oil and gas, manufacturing, or healthcare. Market valuation of IIoT in 2019 was 313.27 billion US Dollars [55], and the market forecast of IIoT by the year of 2025 is expected to reach 607.73 billion US Dollars. This shows that CI will be heavily dependent in the future on IIoT.

In their research paper, Maglaras and Kim [56] analyse real-world cyber-attacks in ICS/SCADA systems and their relations with IoT. They conclude that this new synergy brings new security challenges for ICS/SCADA systems, and propose a more defence in depth approach on future CI architectures. Meanwhile Boyes and Hallaq [57] propose a framework that analyse IoT nature and its uses in industrial systems. This analysis framework can be used later to identify vulnerabilities and threats against IIoT. Transportation is also one of OES sectors. IoT is also being integrated now more in transportation sector, which is best known by the term "smart transportation". Research has already been made with focus in this sector [58], where a case study of an attack on smart transportation is presented as well as countermeasures recommendations are proposed such as resilience of IoT-based system. Meanwhile there is also research of IoT based on legal regulations and national security of EU MS [59].

CHARIOT is a project [60] financed from EU Horizon 2020 programme [61], where the main contribution of it is the security and integrity of IIoT. Meanwhile Urquhart and McAuley in their paper [62] make a comparative analysis of NIS Directive and GDPR on technical and regulatory perspectives of IIoT with a focus on smart energy sector. They emphasize the risks that come with IIoT such as the shift from offline to online infrastructure or engaging with infrastructural complexities. It is their opinion that the requirements that derive from NIS Directive and GDPR regarding cloud can produce alternative architectures for IIoT. Meanwhile Rubio, Roman and Lopez research work [63] shows that traditional security equipment such as IDS are not enough for protection of IIoT, especially against Advanced Persistent Threats (APT). New approaches, such as machine learning techniques, should be taken where they propose a framework for correlation of anomalies in IIoT to help detect and respond to potential APT attacks on IIoT.

Even though IIoT will not be the theme of this thesis, it is critical to understand the impact of IIoT in the future. Kosovo's CI will potential implement IIoT infrastructure in the future on its OES. Future Kosovo's CIP policies should take IIoT protection seriously, because as it was seen from the above academic literatures, there are already attacks as well as recommendations on protection measures to be taken. In addition, the evaluation method developed from the author can be used from a nation to evaluate its CIP policies readiness against IIoT cyber-threats issues that the CI faces on IIoT. This can be done by creating the national criteria based on the recommendations that would derive from EU

guidance on the subject of IIoT. Meanwhile semaphore model would be used to evaluate these criteria.

It is critical for nations to keep their CI in a healthy state where interruption of essential services such as electric distribution and/or water supply should be kept at a minimum level. With the inclusion of IT infrastructure and the close relationship nowadays between IT and OT, cyber security in international community has become more important than ever before. There are already recommendations from research community that even though countries can be physically located in different continents, terminologies and regulatory frameworks on CIP should be aligned, coordinated and harmonized between nations [64]. A research on social and legal issues of Spain on CI is done by Iglesias [65]. In this paper, he analyses the relationship between CI, smart cities and state approaches to fight cyber-crime on CI, by making a comparable analysis between Spain, EU and US laws. Meanwhile Grosse and Olausson focus on Sweden in their research paper [66], by examining the Swedish planning system STYREL model [67]. STYREL is a part of Swedish crisis management system, where Grosse and Olausson find blind spots in the execution and design of STYREL strategy. They propose a better governance on processes, people, and technology so that actions of them are aligned to reach a preferred future state of STYREL planning.

Research on CI national legislations and policies shows that although these legislations and policies seem feasible and easy to follow, when it comes to applying them in real-world scenarios, obstacles can be seen on its way. This is also an issue for Kosovo, which will be more ellaborated in chapter 5. Therefore, recommendations for better collaboration and coordination between aspects of CIP such as processes, people, legislations, and technologies used in CI should be considered.

As CI operators develop their strategies and design documents on CI design, it is imperative to have a risk assessment plan before going into production. This will help the CI operators to better understand their infrastructure and identify the systems in their environment that can have the highest risk and biggest impact, on a potential cyber-attack. Cherdantseva and Burnap in their research work [68], describe 24 risk-assessment methods such as attack trees or quantitative cyber risk reduction estimation methodology for SCADA systems and its vulnerabilities. They conclude that even though the probability for a cyber-attack on SCADA systems is low compared to other systems, the

impact of this risk is substantial. This shows that proper cyber-security investment in Kosovo's SCADA systems should be considered. A paper which reviews risk-assessment on electric power grid is that of Baggot and Santos [37]. In this paper, they find a disproportion on studies of risk assessment on US electric power grid with an emphasis on cyber-attack and incident response against those focused on natural disaster recovery. By this disproportion on number of studies, authors conclude that US electric power grid is vulnerable against cyber-attacks. They propose better formulation on strategies on US electric power grid protection as well as greater coordination between different stakeholders. Additionally, they observe that disaster recovery preparation for cyber-attacks should be different from that of a natural disaster incident. These recommendations should also be taken into account to Kosovo's CIP policies. These research papers are mostly based on comparative analysis and they lack on a proper evaluation methodology. The evaluation methodology developed by the author could be used as an additional tool to make these studies more complete.

Stuxnet [8][35] shows that cyber-attacks against CI were a reality since 2010. As CI components are being connected to the internet, cyber-attacks are now a common threat to CI environment. This pushed the cyber-security community to focus more their research efforts on incident response against potential future cyber-attacks. Line, Tøndel and Jaatun [69] analyse the state of cyber incident response on small and large electric distribution system operators in Norway. They recommend better collaboration with IT suppliers on the matter of cyber threats and incident response in the energy sector. In addition, they also recommend the initiation and the maintaining of a dialog between small and large electric distribution system operators. Plėta, Tvaronavičienė and Casa [70] observe the pros and cons of different US frameworks and guidelines as well as Belgium's Cyber incident Security Incident Management Guide on Critical Energy Infrastructure. They find that there is not an optimal guideline which covers everything such as risk assessment or a proper incident management against a potential cyber-attack on energy infrastructure. Furthermore, they propose an international collaboration that should be available 24/7, which can respond against an ongoing cyber-attack on an organization that is part of the energy sector. These kind of collaborations in Balkan Peninsula can help Kosovo on the protection of its CI. In their paper, Slipachuk, Toliupa and Nakonechnyi analyse the integrated system of the national cyber security sector management in Ukraine [71]. They describe the functional components of this Ukrainian

system and conclude that the modern integrated management system is an effective tool on response measures against CI cyber-attacks in Ukraine. Meanwhile, Settanni and Skoptik [72], as part of ECOSSIAN group [73], focus on collaboration of different national SOC's in EU with regards to responding against a CI cyber incident. They present a model for national cross-organizational cyber incident management and come up with a system architecture for a national SOC by defining its components and dependencies.

Research has also been made towards NIS Directive. Holzleitner and Reichl [74] make a detailed overview of NIS Directive and how it will be implemented from EU MS into their national laws with an emphasis on the energy sector. They conclude that EU MS must take important independent steps to decide how their national laws will comply with the Directive as things such as penalties are not clearly defined.

Country-specific research literature and how NIS Directive will have an impact on national laws of countries also exists such as Katulic's analysis [75] of NIS Directive transposition into Croatian national laws. Meanwhile, Maglaras and Drivas analyse NIS Directive [76] from Greece's perspective where they focus on real world CI attacks. They observe Greece's needed policies and its obligation on implementing NIS Directive and securing its cyber space. Another analysis of NIS Directive on the case of Greece is of Antonia's thesis work [77]. He analysed NIS Directive with a focus on OES, but his case study analysis and recommendations were focused on Greece's aviation sector. Some of his recommendations include identifying the cyber threats on Greece's civil aviation sector and a better incident response mechanisms against those cyber threats. These recommendations would also be beneficial on the improvement of protection and incident response mechanism on Kosovo's aviation sector against potential cyber threats that may arise in this sector. The gap between current thesis and Antonia's is that he focuses in the aviation sector, whereas this thesis is focused on electric-energy and water-supply CI sectors. Meanwhile, Shukla, Johnson and Jones analyse in their research paper [78] the NIS Directive implementation in the UK. They come up with 10 recommendations for a better implementation of the NIS Directive in the UK which includes a more holistic security governance. In addition, they recommend the creation of a progressive roadmap on the improvement of OES and DSP cyber capabilities. In their analysis, Carrapico and Barrinha [79] define the EU as a critical global actor in cyber security field and how the NIS Directive helps the EU to achieve this reputation by facilitating cooperation between

EU MS. The gap in Carrapico and Barrinha research is in generalisation of the EU. Even though the EU is a union, different EU MS have different issues related to their respectable CIP policies. This thesis focuses on Kosovo's CIP policies and it has a more real-world implication.

Analysis has also been done with regards to NIS Directive and its implication on EU's General Data Protection Regulation (GDPR). Markopoulou, Papakonstantinou and Hert [80] analyse NIS Directive in relation to GDPR and EU data protection policies where they note the NIS Directive does not affect GDPR on its prevalence and effectiveness in EU. In her thesis, Peedu [81] analyses the implementation of NIS Directive in Estonia on the subject of GDPR implications and whether its implementation is transparent. It is Peedu's point of view that Estonia's Cyber security Act does not give a fair balance between transparency and secrecy.

A survey-based software system is proposed by Kamola, Jaskola and Amanowicz paper [82] on building a National Cyber security Platform by taking into consideration the NIS Directive. This software system could provide workflow information for security events regarding OES to establish metrics for IT security requirements and reporting incidents.

By interviewing 30 cyber security practitioners in the UK, Michalec and Linden research work [83] focuses on OT security topic with regards to NIS Directive. They find a practical skill gap on OT professionals where there is not a clear formulation of career trajectories and professional norms for OT security. Some of their suggestions include a need for more professional guidelines as well as education regarding OT security which would include awareness raising on CIP from OT security professionals. The evaluation method developed from the author can further evaluate this skill gap on OT professionals by creating a criterion on this issue and applying it on CIP policies using the semaphore model. This would show nations the real-world implications of this issue.

An analysis of EU threats and challenges in the context of NIS Directive is made from Söderholm thesis work [84]. Söderholm makes a high-level overview of previous cyber-attacks such as WannaCry and Not-Petya. She also makes an analysis of the EU challenges on cooperation such as EU MS variety of approaches on cyber-security, as well as reporting and confidentiality challenges that derive from NIS Directive. Some of her recommendations are a better cooperation mechanism between EU MS is needed in

implementing NIS Directive from political and security view, by harmonizing NIS Directive into their legislations; trust must be gained not just from one EU MS but from the whole EU as a critical cyber security actor in the world; there should be clear policies and guidelines in relation to confidentiality. If a CI cyber-attack happens in EU MS, confidentiality policies and guidelines need to make sure to avoid leakage of confidential information when it comes to reporting that CI incident EU-wide. The evaluation methodology developed from the author can evaluate the adherence of national CIP policies against the recommendations derived from Söderholm.

2 EU Guidance

As Kosovo's aspiration is to join the EU and adhere to EU's CIP requirements, the author decided that EU relevant guidelines and directives on CI should be taken as a baseline against which Kosovo's CIP will be evaluated. In addition, these guidelines provide clear and detailed instructions on nations regarding the improvement of their CIP policies.

In this chapter the following documents will be analysed:

- NIS Directive. [15]
- NIS CG reference documents on security measures [29] and incident notification [30] for OES.
- ENISA guidelines on ICS/SCADA network dependencies [31] and cyber-threat landscape. [32]

2.1 NIS Directive

In August of 2016, the first EU-wide legislation on security of network and information systems known as NIS Directive entered into force [9]. This directive required that by 9th of May 2018, each EU MS had to transpose NIS Directive into their national laws. In addition, each EU MS was obliged to identify their OES by 9th of November 2018 [15]. The NIS Directive assesses that the existing EU policy capabilities on cyber security built until its development were not sufficient enough. Furthermore, there was not any single EU policy or legislation which would create a common overall framework requirement on EU MS regarding the identification of OES and digital service providers (DSP) [15]. In addition, an effective cooperation mechanism between EU MS did not exist if a cyber incident happened in one of their OES. NIS Directive tried to fill this gap by creating a strong and unitary EU legislation that each EU MS required to adhere to.

The gaps mentioned above that were filled from NIS Directive are really important. By building a unitary guidance and mechanism on OES protection and incident response, the EU took steps to ensure that all of its MS have a baseline from where they can start and improve their CIP policies.

The NIS Directive has 7 chapters which are made of 27 articles. As this thesis is focused on OES protection and incident response, the following main points are taken into consideration which are relevant on Kosovo's case, where NIS Directive:

- Provides clear criteria's on how MS should identify their OES such as what is an OES, its dependencies and the impact of an incident on it (see Article 5 and 6).
- Clearly defines the designation of national competent authorities and single point of contact regarding the security of network and information systems, who are responsible to ensure cooperation among the MS authorities. This would include national law enforcement authorities and requires from EU MS to ensure that these authorities have the adequate resources to carry out their tasks (see Article 8).
- Creates an EU-wide Computer Security Incident Response (CSIRT) network from EU MS CSIRTs and CERT-EU. Some of these organizations main tasks are to collaborate and exchange information regarding CSIRTs capabilities or possible coordination on incident response (See Article 12). It also defines the requirements and tasks that CSIRTs should have such as high level of availability of communication services, business continuity, as well as a proper incident response mechanism. (Annex 1 of NIS Directive).
- Clearly defines security requirements and incident notification for OES where the significance of the impact of the incident is measured by the following parameters: (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident (see Article 14).
- Gives guidelines related to usage of European or internationally accepted standards and specifications in cyber security for the purpose of having a more convergent OES network in the EU (see Article 19).
- Defines that penalties should be established by MS, which will include OES sectors if they do not follow the policies and laws of MS that are coherent with NIS Directive (see Article 21). [15]

As it will be seen in chapter 5, the above-mentioned points are important for the Republic of Kosovo to develop and improve its CIP policies and the implementation mechanisms. By having clear guidance and requirements on its CI operators with regards to the protection of OES environment, Kosovo would build a comprehensive national

implementation mechanism on its CI operators. This would help Kosovo on improving the protection of its OES environment. In addition, by adhering to NIS Directive, Kosovo would also have a better institutional mechanism on detecting and reacting quicker against possible future cyber incidents against its CI.

Annex 2 of NIS Directive also divides the OES into several sectors:

1. **Energy sector** – Includes following subsectors: (a) Electricity; (b) Oil; (c) Gas.
2. **Transport sector** – Includes following subsectors: (a) Air transport; (b) Rail transport; (c) Water transport; (d) Road transport.
3. **Banking sector**.
4. **Financial market infrastructure sector**.
5. **Health sector** – Includes health care settings where hospitals and private clinics are part of this setting.
6. **Drinking water supply and distribution sector**.
7. **Digital infrastructure sector**. [15]

Because OES are also dependent on DSP, NIS Directive divides DSP as follows:

1. **Online marketplace**.
2. **Online search engine**.
3. **Cloud computing services.** [15]

2.2 NIS Cooperation Group Reference Documents on OES

NIS Directive is a good baseline document on OES, but it is not thorough enough on how the protection and incident response mechanisms to the OES should be developed and implemented. Therefore, NIS CG published two reference documents which complement NIS Directive on the focus of cyber security and incident response measures on OES that are:

- "Reference document on security measures for Operators of Essential Services". [29]

- "Reference document on Incident Notification for Operators of Essential Services". [30]

In this section the author will analyse these documents in detail in order to better understand them and how they can impact the future CIP policies in Kosovo.

2.2.1 Security Measures for OES

Even though security measures do not guarantee that incidents on OES will not happen, it is imperative for Kosovo's OES environment to have proper protection measures. This would make it harder for potential attackers to disrupt these essential services, especially for long periods of time. Resilience measures such as proper backup policies on Kosovo's CI owners/operators would help them quickly recover from a potential cyber incident. "Reference document on security measures for Operators of Essential Services" [29] recommends security measures on EU MS for their OES. These security measures take into account some general principles such as the effectiveness, proportionality and compatibility that should be applied on them. As this document says "Cyberthreats to critical infrastructures are now recognized as among the most serious threats to the EU, its Member States, the economy and the society" [29], it highlights the importance for the EU MS on having a baseline for cyber security measures with the above-mentioned general principles in mind. These cyber security measures are separated in the following domains:

1. **Governance and ecosystem**: The recommendations that this domain provides on OES include the identification of OES Critical Information Systems (CIS) as well as implementing a risk analysis approach on these CIS. This should be done by considering new threats, recently discovered weaknesses or any changes in the risk situation. Implementing and maintaining an up-to-date Information System Security Policy (ISSP), which would create strategic security objectives and describe security governance, is also recommended from this part of cyber security measure domain. In addition, auditing this ISSP periodically would check the effectiveness of it on the CIS. Security awareness raising program should also be included in ISSP to all the staff as well as security training programs for employees with CIS related responsibilities.
2. **Protection**: One of the issues that this domain tackles is that of preparing an OES CIS in the best way possible to avoid or minimize cyber incidents. This is tackled by recommending IT security architectural, administrative

and maintenance protection measures, as well as identity and access management ones. The architectural protection measures would include installing only essential IT services and functionalities as well as connecting only essential equipment's which are needed for the proper functioning and security of CIS; system segregations which would limit the propagation of IT security incidents within CIS or subsystems; traffic filtering by implementing ACLs or firewalls on the network path that these CIS are located. This would be done by forbidding unnecessary traffic flows and regularly updating ACL/firewall filtering rules such as allowing only necessary port numbers, network addresses or protocols; implementing and establishing procedures and a policy with regards to cryptography in order to protect confidentiality, integrity, and authenticity of information in OES CIS. The administrative IT security protection measures would cover the segregation of user accounts where specific user accounts for administration would be used, be restricted as much as possible and kept up to date. It is also recommended that hardware and software resources should be separated for administrators where only specific devices are segregated for administrative tasks. Identity and access management subsection tackles the problem of identifying the operators by setting unique accounts for users and having proper authentication measures such as multi-factor authentication and changing the default credentials. Access rights is another topic that this subdomain tackles where accesses are granted only where that access is strictly necessary to carry their on-duty tasks by implementing principles of least privilege. IT security maintenance subdomain deals with keeping and maintaining the CIS software and hardware updated by installing new versions. This should be done by considering precautions such as checking the origin and integrity of the software version before installing it. Maintenance of ICS is also another area which is covered by recommending to the operator, to take into account security requirements for ICS. The protection domain also covers physical and environment security measures where an example would be using access cards to access restricted areas and monitor them using cameras.

3. **Defense**: This domain recommends procedures on incident response measures. In order to be aware of an incident, CIS need to have detection capabilities such as Intrusion Detection System (IDS) into the CIS environment. The IDS's can analyse data flows between CIS and third-party information systems. Logging capabilities are also important. By implementing systems such as Security Information and Event Management (SIEM), events such as user authentication, modification to security rules or suspicious network flows related to CIS are recorded, correlated, and analysed. This would make it easier for a CI operator to understand how an incident took place and what techniques did the attacker use. Procedures for handling, responding to and analysing incidents that affect CIS are also included in this domain where these procedures should be in accordance with the organisation's ISSP. Updated contact details should also be provided to national competent authorities and it is encouraged to connect the incident management with the national CSIRTs.
4. **Resilience**: ISSP should be prepared for CIS continuity if an incident, especially the one derived from cyber-attacks which targets availability (e.g. Distributed Denial of Service (DDOS) attacks) hits a CIS. The operator should define strategic guidelines regarding disaster recovery management. This is done by maintaining a backup policy as well as organizing a crisis management team and a process in order to quickly recover from a potential severe IT security incident. [29]

By taking into account these measures into its CIP policies, Kosovo would have a better protection guidance and mechanism on its OES. This would be done by requiring its CI operators to have proper defensive (e.g. patching of ICS/SCADA systems) or resilience (e.g. backup policy) measures. The recommendations that derive from this document will be used as an evaluation method on the semaphore model against Kosovo's current CIP policies.

2.2.2 Incident Response and Notification for OES

NIS Directive clearly defines to EU MS guidelines and requirements on incident notification for OES. In order to determine the significance of the impact of an incident, EU MS can calculate this by taking into account the following parameters:

(a) the number of users affected by the disruption of the essential service.
(b) the duration of the incident.
(c) the geographical spread with regard to the area affected by the incident. [15]
As NIS Directive does not exactly show EU MS concrete steps on how to implement its recommendations for incident response notification process, NIS CG came up with the "Reference document on Incident Notification for Operators of Essential Services" [30]. The main goal of this document is to provide usable and non-binding recommendations to EU MS, in order to support their transposition process from their current CIP policies to NIS Directive. This document explains in detail the incident notification scheme for OES according to NIS Directive and the parameters used to measure the impact of the incidents.

In order to have a proper incident notification scheme some of the requirements as of this reference document on OES incident notification are:

1. **Providing proper justification for the new incident response policy**: The message of this policy should be coherent and easy to understand explaining why incident notification as well as following these notification procedures on OES are important. This can be done by explaining the importance of OES to relevant authorities such as the criticality of OES nowadays on societal and economic activities.
2. **Maintaining a permanent public-private dialogue**: Coordination between public and private stakeholders in a state is essential on handling the incident on OES in an appropriate manner where strengthening this cooperation will help on implementing a more effective and suitable policy.
3. **Build trust and provide incentives for reporting**: Creating a coordination framework on incident response between different stakeholders and providing periodic analysis on collected incidents would be some of the examples on incentives which would help to build trust inside an EU MS and showing the importance of incident collection. Even though penalties are not the best way to build trust, they should not be excluded as a mechanism if a stakeholder does not follow the incident reporting requirements on OES.
4. **Monitor, review and evaluate the overall implementation**: The incident response framework should be periodically reviewed and if necessary, updated, in order to respond to the latest cyber security threats. [30]

As Kosovo still have issues in its national incident response capacities, it is imperative to take into consideration the requirements mentioned above. For example, if a national incident response framework is developed from Kosovo but it is not regularly updated, it will not be useful on the aspects of quick reaction against new threats and TTP's on OES. Next step for EU MS, as described in NIS Directive on Article 14 points 3 to 7 [15], is to follow incident notification requirements for OES which are:

- **Assign competent authorities or CSIRT's to get OES incident notification**: EU MS should assign CSIRT's or competent authorities which are the point of contact in regard to getting notification for significant OES incidents.
- **Identifying OES**: This requirement is important for EU MS. By identifying their OES, it is easier to identify the incidents that affect solely a CI component, rather than including other information systems which are covered by that particular OES. This will make it quicker to determine and identify which OES got attacked and what potential impact can that have for societal life.
- **Significant incidents should be reported**: All significant incidents should be reported without any delay as they can affect the operational continuity of OES.
- **Cross border impact must be notified**: The CSIRT or competent authorities should inform other EU MS affected, if an incident has an impact on the continuity of a OES in that EU MS. Notifications should also be forwarded to other EU MS from a single point of contact in order to update the affected MS with the progress of the incident handling and response actions.
- **Determine significance**: As mentioned in the beginning of this chapter, the significance of the impact of the incident should be determined by calculating the number of users affected by it, the duration of incident and the geographical spread. This can also be extended by also checking other factors such as the dependency of other OES sectors on the service provided by the affected entity or the market share of the entity.
- **Follow-up notifications**: When circumstances allow it, OES shall be notified by CSIRT or competent authority, with relevant information which can support the effective handling of the incident.
- **Informing the public**: With the consultation between OES and CSIRT or competent authority, the public can be informed regarding the incident, especially

where public awareness is necessary in order to deal with an ongoing incident on OES or prevent a future one. [30]

This document defines an OES incident as "any event affecting the confidentiality, integrity, availability (CIA) or authenticity of networks and information systems, that has a significant impact on the continuity of the essential service itself" [30]. As Kosovo is still in the process of identifying its OES, it is essential that it includes a proper plan to also identify the network and information systems that these OES rely on. This would improve the protection and incident response mechanisms of Kosovo's OES.

This reference document on incident notification for OES also describes in detail the parameters that measure the impact of an incident and the three main ones that can be related to Kosovo are:

a) **The number of users affected by the disruption of the essential service**: The number of users in this case means how many affected natural persons and legal entities are affected from which the provision of the service has been concluded [30]. Let us assume that Kosovo will classify an incident in its electrical distribution system as a significant incident, if the number of users affected from that incident passes the 20% threshold of its entire population. For example, let us assume that a cyber-attack happens on Kosovo's Electrical Distribution System company (KEDS), which distributes electricity to all Kosovo's population. Let the author assume that the Kosovo's population as of now is 1.8 million [12]. If approximately 360.000 users are affected by this cyber-attack, this OES incident should be classified as a significant cyber incident. Therefore, proper incident response measures according to NIS Directive should be taken by the stakeholders in order to properly respond against this incident.
b) **The duration of the incident**: The duration of the incident means the time period on which an essential service offered by a OES is not available due to a disruption affecting its CIA or authenticity of the underlying computer system. The time can be measured starting from when the incident breach was identified or from the time that service degradation got noticed [30]. As Kosovo is a small country, the significance of the incident should be identified quickly as users can complain on electricity or water-supply sector outages. As it will be shown in a later section, Kosovo is going into a process of modernisation of its OES sector systems, so it is essential to be prepared in suspecting that a cyber incident might be affecting

those outages. A combination of number of users and duration of incident can also be used as a parameter to define the significance of an incident on OES.

c) **Geographical spread**: Lets assume that a cyber incident on the OES of one of the EU MS affects other EU MS essential services. The competent authority of the EU MS where the origin of the cyber incident on OES is, should notify the other affected EU MS without undue delay. This is important as users of other EU regions can be potentially affected from that particular cyber incident [30]. Just recently, Kosovo won electricity independence from Serbia and established with Albania a Kosovo-Albania energy bloc [85]. If Kosovo's electricity network system experiences a cyber-attack which affects Kosovo-Albania bloc, it will be essential for Kosovo to inform Albania through the right procedures as per NIS Directive recommendations. This would allow Albania to be updated on the latest development of incident response by the Kosovo counterpart against this cyber incident and be informed if its OES are still operationally capable.

As the author gave some examples on how Kosovo can use the recommendations provided by NIS CG document on incident notification of OES, this document and its recommendations will be taken into consideration on the evaluation of Kosovo's CIP policies.

2.3 ENISA Guidelines on ICS/SCADA Components and Cyber-Threat Landscape

In this section the author will analyse guidelines and relevant reports from ENISA on CI components and cyber threat landscape where the author will explain:

- ICS/SCADA systems communication network dependencies. [31]
- Cyber threat landscape with a focus on OES. [32]

2.3.1 ICS/SCADA Systems Communication Network Dependencies

ENISA published a guideline for ICS/SCADA systems network dependencies named "Communication network dependencies for ICS/SCADA Systems" [31]. This document explains in detail the ICS/SCADA systems network dependencies, the communication protocols that these systems use as well as gives recommendations on how to protect and maintain ICS/SCADA systems against three attack case scenarios.

ICS/SCADA systems usually interact with the following components:

- **Programmable Logic Controller (PLC)** – a device which carries out physical interaction with the other system components. One example of such device are the actuators.
- **Human-Machine Interface (HMI)** – presents the data to human operators by using a console cable which controls and monitors the status of the operations.
- **Data Concentrators** – Remote Terminal Unit (RTU) is one such example where devices in this category transmit the data obtained from the sensors to other system components.
- **Historian** – a high-capacity system which mimics SIEM systems where they collect, and store logs generated by sensors, alarms and other events which are generate from plant devices.
- **Communication infrastructure** – this includes tradition IT network equipment's such as routers, switches, or cables, which enables intercommunication between different devices of the system.
- **Distributed Control System (DCS) central server** – in charge of the data acquisition and control activities of the operations and processes which may include analytical instrumentation and monitoring. [31]

This document also shows us the potential impact of a cyber-attack on OES, by showing the interdependencies of different OES. The figure below showcases the CI interdependencies with other sectors:

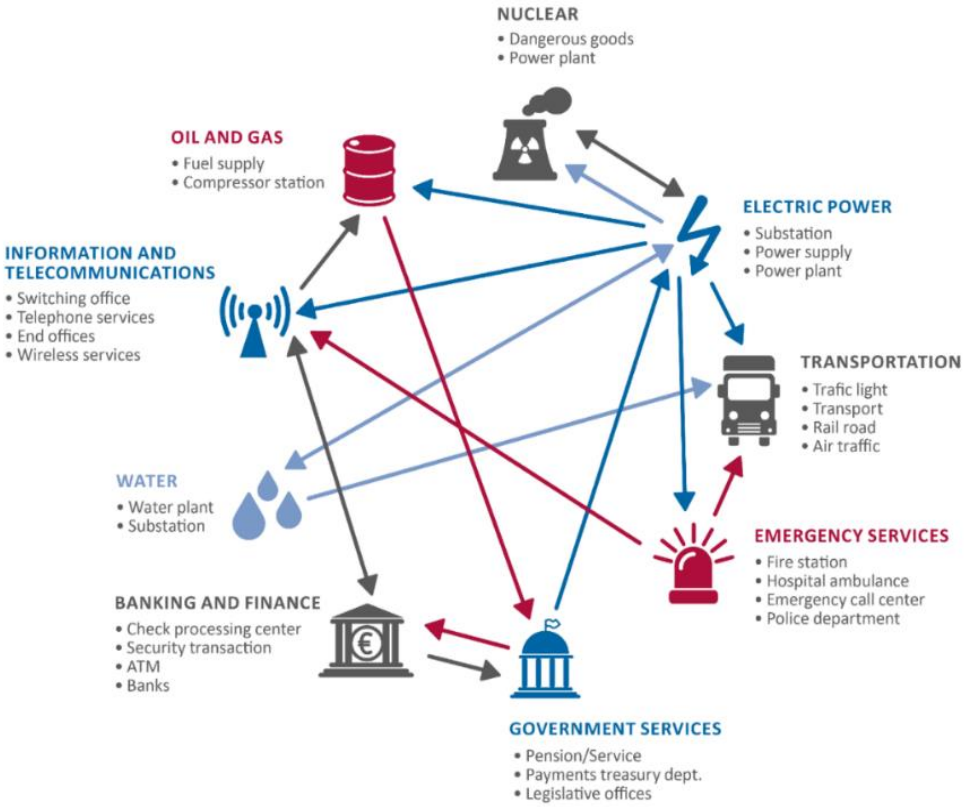

Figure 1. Critical Infrastructure interdependencies with other sectors [31]

By observing the above-mentioned figure, the author concludes that a devastating cyber-attack on an electric power plant/substation of an EU MS can result in leaving a water plant/substation without electricity. This can impact the operational status of the water plant, where attackers can take advantage of this cyber incident and poison the drinking water of general population.

This document also gives relevant recommendations on how to protect ICS/SCADA systems such as:

- Periodic device update of ICS/SCADA systems as part of main operation.
- Establishing ICS/SCADA security awareness and training campaign.
- Prioritizing security in the design phase of ICS/SCADA systems. [31]

These recommendations should be taken into account by Kosovo's CI operators. Taken from the above-mentioned observation, if a cyber-attack happens on Kosovo's electric-energy sector, the impact of this cyber incident can be distributed to other sectors, such as water-supply.

2.3.2 Cyber Threat Landscape

The connection to cyberspace from different devices expanded the threat landscape and the attack vectors, especially with the inclusion of IT devices in OES sectors. Just recently, ENISA updated their previous threat landscape analysis document [32] where the ranking of recent top threats is shown below:

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking:** ↗ Going up, — Same, ↙ Going down

Figure 2. Top Cyber Threats 2019-2020 [32]

From this list, the author notices interesting movements such as the phishing attack vector, where most of cyber-attacks start from [86]. As it will be seen later from the real-world CI attacks, this attack vector is relevant for OES as CI operators can open a malicious

email and infect the ICS/SCADA environment. This can have devastating consequences such as loss of data or even worse: physical destruction of the particular CI facility. Of course, this cannot happen without a malicious payload being executed, so as it can be seen from the list above, malware attacks are the biggest cyber threats. Another malware which can have impact in the future on OES are the file-less malwares [87] where instead of transferring and executing an executable file, the file-less malwares are injected into already installed and trusted software. This malware can gain persistence in the target environment through the registry or built-in task scheduler. This is harder to be detected by anti-malware engines and this type of malware can be really threatening to ICS/SCADA environment, as it can be triggered in specific timelines, and the attribution of a destruction in ICS/SCADA systems to a malware is harder. This type of malware, together with the increased relevance of phishing attacks, shows us that in the future cyber-hygiene will be relevant on preventing cyber incidents in OES environments as malwares are becoming more sophisticated on evading antiviruses.

Another attack vector on the threat landscape are the ransomware attacks. "Lockergoga" is a ransomware attack which can be delivered by phishing techniques and uses PsExec tool to pass some security checks as a semi-valid software [88] where once installed, it forces systems to change user account options and logs them off the system. Norsk Hydro, an aluminium company, was hit by this ransomware where its IT and OT systems were disrupted. The company did not give to the demand of the hackers to pay the ransom, and contacted Microsoft's cyber security team to help them restore their operations [89]. This is a good approach which should be taken into account by Kosovo's CI operators/owners, because the hackers are not required to give the keys to the victim to decrypt the data. But a ransomware attack like this can have devastating consequences on electrical power grid or water-supply systems of Kosovo. If a ransomware like this can infect the HMI of one of Kosovo's CI operator, it can disrupt the ability of that CI operator to have real-time data which can have devastating consequences to ICS/SCADA systems. This can be best shown on the ransomware attack against City Power in South Africa [90] from which energy supply critical services such as energy recharges were disrupted [91]. Therefore, it is crucial for OES sectors in Kosovo to have a better backup and recovery plan in order to be better prepared and be quicker on recovering the operational environment from a potential ransomware attack. Some of the recommendations from ENISA which are relevant to OES sectors are:

- Maintaining a reliable backup plan such as following the 3-2-1 rule (having at least three copies of the data, in two different formats, where one of those copies is saved somewhere off-site).
- Use network segmentation and access enforcement to ensure minimum exposure of data.
- Monitor access to the public infrastructure being used such as cloud environment.
- Have a Security Operation Centre (SOC) staffed by skilled cyber-security personnel within OES organisation or company. [88]

Another attack vector which is relevant for power grids and electrical distribution systems is a cyber-attack on the real-time data. ENISA paper on power sector dependency on time service [92] shows the dependencies and threats that can be as a result of a cyber-attack on time services in a power sector environment. Power stations use phasor measurement units (PMUs) to time-stamp measurements against a time source such as Network Time Protocol (NTP) or Global Positioning Systems (GPS) from where PMUs provide real-time information. As PMUs automate processes on power systems, a cyber-attack on one of its time-measurement dependencies (e.g., jamming the signal of GPS or hacking and modifying data of NTP server), it can lead to potential synchronization failures between different power substation devices. Another potential consequence can be the creation of monitoring errors between the Transmission/Distribution operator and the power stations by providing false real-time data. What is also of a concern in these cyber-attacks is that decisions and data analysis are performed in centralised systems such as HMIs which are unaware of the state of NTP servers or GPS receivers. This makes it even harder to spot a potential cyber-attack as there is no integrity check if NTP servers or GPS receivers are transmitting the real data to the CI operators or not. Some of the protection measures and security good practices against these cyber-attacks are:

- Security policies and procedures, governance models, training and awareness-raising should be applied to power sector as the dependency on IT systems is growing more.
- Close unnecessary ports in the network between PMUs and the ICS's to secure data streaming between them.
- Hide PMU IP addresses and when bidirectional connections are needed, employ the SSH protocol.

- Protect and implement a resilient NTP protocol by providing multiple paths between master and slave clocks.
- Implement firewall as well as access control lists (ACLs) to filter connections to NTP servers.
- Apply patching and updating procedures to software and devices. [92]

Kosovo's CI owners/operators should be aware of the risks and threats that can impact their systems. Protecting only their most critical ICS/SCADA systems is not the approach to be taken because, as seen from [92], attacks in NTP servers can impact these ICS/SCADA systems, where Kosovo's CI operators would not get real-time data. This would impact their ability to be updated on what is happening in their operational environment. An examples of this impact can be the loss of latest data on chemical levels of water shown to a Kosovo CI operator staff member on a water-supply company.

3 Lessons-Learned from Real-World CI Cyber-Attacks

Documents such as guidelines and policies are a good start to tackle the problems that the CIP faces. But it is author's point of view that to have a more comprehensive evaluation on Kosovo's CIP policies, real-world cyber-attacks on CI would give a better insight on how the process of a CI cyber-attack develops. In addition, by taking these real-world cases as an additional "lessons-learned" sources, the evaluation on some of the Kosovo's CIP criteria such as the criterion on cyber awareness or protection mechanism would be more comprehensive.

With the introduction of ICS/SCADA systems, physical protection of CI was not the only concern for CI stakeholders. Technology gave many advantages to CI such as remote control of ICS/SCADA systems or even quicker reaction to different problems that can arise to CI operators by using modern technologies. But when the first cyber-weapon was introduced to the world called STUXNET and attacked one of CI sectors, the world saw that this technology can also be used by malicious actors to commit physical damage.

Just recently on February 5 of 2021, an unknown hacker attacked a water treatment facility in Oldsmar, Florida [93] [94] by using cyber means. The attacker had access to ICS of that water treatment facility and changed the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million. This could potentially have devastating effect on the city with a population of 15,000 people where if not noticed and stopped, it could harm people as water would be poisonous. This was a wake-up call where some senators even called that such cyber-attacks should be treated as a matter of national security [95]. The water treatment facility was using a remote-control software called TeamViewer [96]. The initial report show that the hacker intruded to the remote-control software because of poor cyber awareness, where he abused the credentials of remote access that were shared between employees of the water treatment facility [93]. Another concern was that of how the HMI application allowed such big values of sodium hydroxide, which shows us that misconfiguration of software that are part of ICS/SCADA systems can be a big concern. If there was a proper configuration mechanism of these software's, the CI sectors would have a better protection mechanism.

In order to better understand in detail how a cyber-attack on CI sector works and what lessons can be learned on it from a policy perspective, the author decided to focus on

world known respectable conferences and institutes. Therefore, the following cyber-attack reports on CI were analysed:

- SANS institute report on 2015 Ukrainian power-grid cyber-attack. [19]
- Black Hat USA 2018 research paper on 2017 Saudi-Arabian petrochemical facility cyber-attack named TRITON. [20]

The author decided to use these two reports based on the following criterions:

- The year when these attacks happened where the focus was on the most recent cyber-attacks on CI over the last 6 years.
- The impact that these cyber-attacks had on ICS/SCADA systems and CI sectors.
- The reputation of the respectable institutions and conferences that published these reports.
- The depth of explanation from the reports on TTP of how these CI cyber-attacks happened.

After the author analyses these reports, he will come up with a lessons-learned section that will be used as an additional evaluation method on the semaphore model against Kosovo's CIP policies.

3.1 SANS Institute Report on 2015 Ukrainian Power-Grid Cyber-Attack

The 2015 cyber-attack on Ukrainian power-grid system was one of the most devastating cyber-attacks that happened in the last couple of years. 225,000 customers were affected by a power-outage from three different distribution-level service territories and the cyber-attack lasted for hours [97].

SANS report [19], using the ICS kill chain model [98], makes a detailed analysis of this cyber-attack. This report shows that the 2015 cyber incident on Ukrainian power-grid is the first cyber incident which is publicly acknowledged to cause a power outage. Attackers used open-source information's such as detailed list on types of infrastructure such as RTU's that the electric companies were using. These type of information was posted online from the ICS vendor [99]. In addition, the Virtual Private Network (VPN) which was used to access the ICS from the business network, was also misconfigured where there was a lack of two-factor authentication. Misconfiguration was identified also

in the company's firewall which allowed attackers to remote admin out of the environment by developing remote access capability native to the system. The capability of the attackers to write custom malicious firmware and perform a long-term reconnaissance together with a highly synchronized multistage, multisite attack, clearly showed that the attackers had the time, resources and skills which threat actors such as hacktivists do not have. This can make authorities immediately suspect that the actor was an advanced persistent threat (APT) from a possible adversarial nation-state.

The initial foothold to IT networks of the electric companies was caused by spear-phishing emails, usage of BlackEnergy 3 malware [100] variants, as well as manipulation of Microsoft Office documents. An example of how the malicious Microsoft Office document looked is shown below:

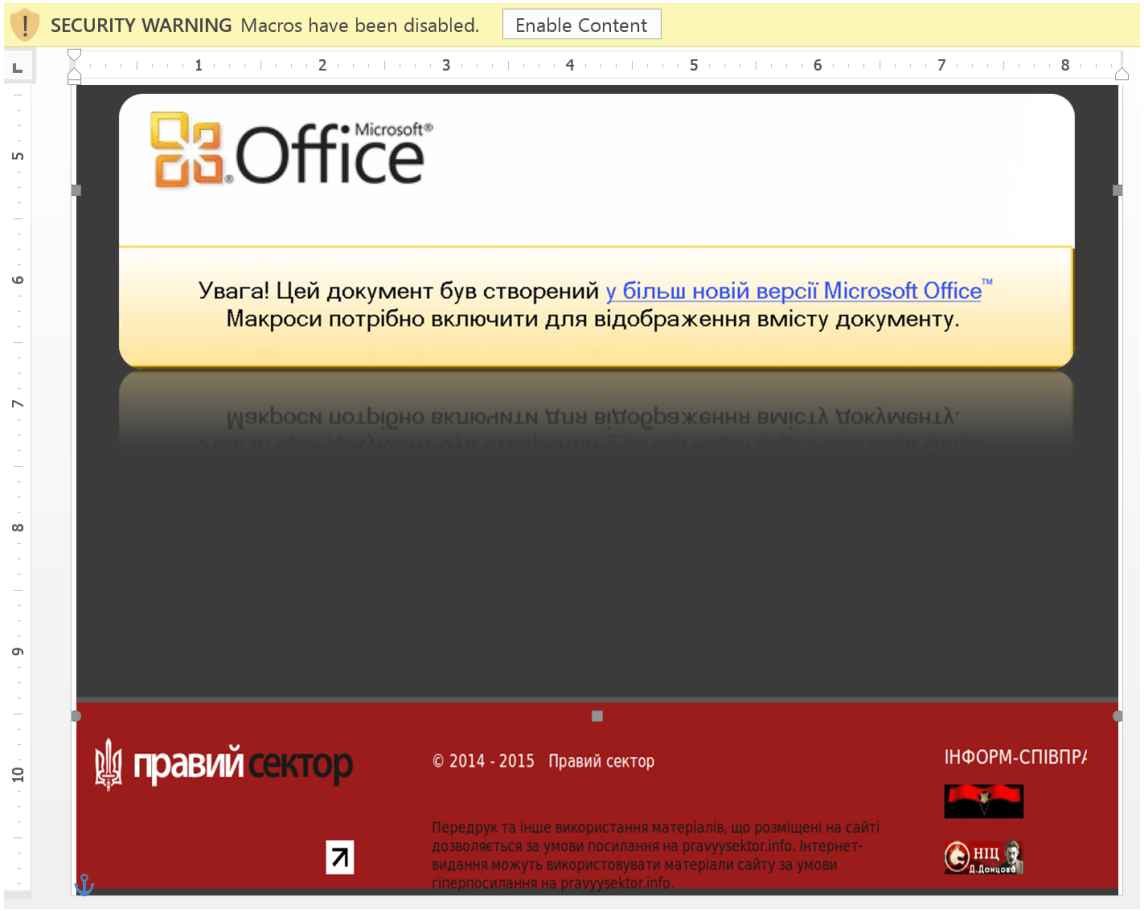

Figure 3. Malicious Microsoft Office document used in 2015 Ukrainian power-grid cyber-attack [101]

As seen above, the attachment was in Ukrainian language to look more legitimate to employees of the electric companies. This is an important information and a takeaway

point, as a similar spear-phishing campaign can happen to CI sector of Kosovo, where the attachments would potentially be in Albanian language.

Next step from attackers were to harvest credentials in order to pivot to other parts of the network to find and interact with HMI's of ICS/SCADA systems that the electric company was using. Once found, these HMI's were used to open circuit breakers of the electric company and cause the power outage. To clear their tracks, malicious actors used the KillDisk malware [102], which erases the master boot record (MBR) and system logs from the system.

As this thesis work is based on policy analysis, the author will not go into more details on the technical aspects of this attack. The following figure shows all the steps of the cyber-attack using the ICS kill-chain model:

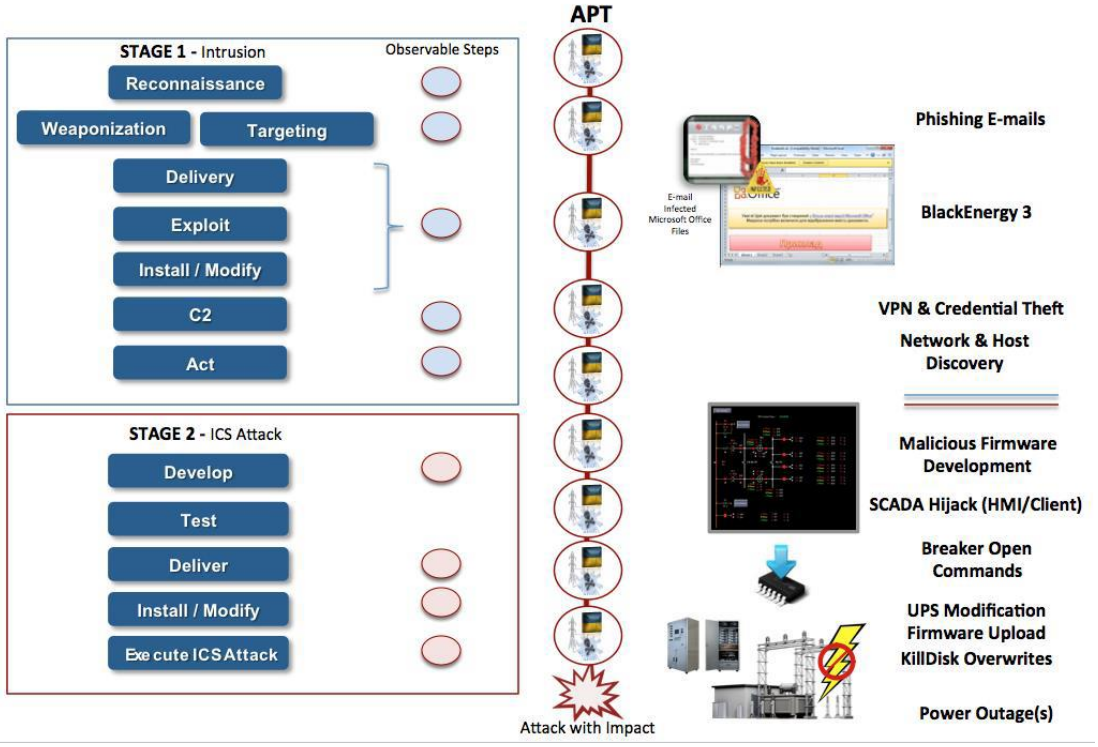

Figure 4. Summary of the 2015 Ukrainian power-grid cyber-attack using ICS Kill-Chain model [19]

The main recommendations from the SANS report on the 2015 Ukrainian power-grid cyber-attack are the following:

- **Architecture:** Measures such as: proper segmentation of network; ensuring logging is enabled both in IT and OT devices; having proper backup policy such as having backup of critical software including their MD5 and SHA256 digital

hash of installers for integrity purposes; are critical for the protection mechanism of ICS/SCADA and CI environment.

- **Passive Defense:** Implementing properly tuned firewalls between network segments; having a central logging and data aggregation point for forensic evidence; application whitelisting to limit the initial infection vectors for the adversary; enforcing password reset policies; are some of passive defensive measures that would help lessen the impact of a potential future cyber-attack on ICS/SCADA systems. In addition, these measures would mitigate possible consequences such as power outages.
- **Active Defense:** The planning and training of IT and OT personnel on incident response plans; training defenders on hunting odd communications leaving the network environment (e.g. blacklisting known malicious IP addresses); using backup and recovery tools; and last but not least, training defenders to use tools such as YARA rules to scan evidence collected; are some of active defensive measures that would help in responding properly against a potential cyber incident against ICS/SCADA systems in the future. Resilient operation plans are also important in order to survive a sophisticated cyber-attack and restore the system in acceptable time frames. [19]

Cyber-awareness is also one of the important lessons learned from this cyber-attack as the author noticed that the initial foothold was reached using spear-phishing email techniques. The report acknowledges that TTPs of this attack are employable around the world and the attack in Ukraine was not inherently specific to Ukrainian infrastructure. This shows that the recommended measures from this report are more overall and should be taken into account for the Kosovo CIP policies in the future.

It is worth mentioning that in 2020, U.S. Department of Justice (DOJ) charged six computer Russian hackers that were part of Russia's main intelligence agency GRU. One of the charges was related to the 2015 Ukrainian power-grid cyber-attack [103]. Even though Kosovo does not have the capabilities of the US, with proper mechanisms in place, Kosovo can anticipate from where the threats can come from and take proper measures on protecting its CI.

3.2 Black Hat USA Research Paper on 2017 TRITON Saudi-Arabian Petrochemical Facility Cyber-Attack

Kosovo has already projects on waste-water treatment facilities [104] [105] that are or being implemented. Even though the TRITON attack happened on one of the CI sectors that this thesis does not focus on (petrochemical sector), the relevance of this cyber-attack is in the ICS/SCADA system component that it was attacked, namely Safety Instrumented Systems (SIS) [20]. SIS are also used in waste-water treatment facilities [106], so this cyber-attack is also relevant to this thesis work. Additionally, the TTP's that this attack uses are relevant on the CI sectors that this thesis focuses on.

In 2017, Mandiant, a subsidiary of FireEye [107], reported that it responded to a cyber incident against a CI organization [108] where an attacker deployed a malware with the purpose to manipulate industrial safety systems. These systems, also known as SIS are a special type of PLC, that are designed to prevent industrial incidents such as operational failures which could cause damage, environmental harm or even loss of life [20]. This can be done after SIS in normal operational environment needs to shut down a process safety and predictably, if out-of-range operating conditions happen. These out-of-range operation conditions could lead to explosions, oil spills or even nuclear system meltdowns. The author can say with high confidence that SIS are the last line of automated defense in industrial facilities, and if someone is able to deploy malware on them, the damages can be devastating. This is why the TRITON attack was a wake-up call to CI community, as a malware that could corrupt a SIS could let a cyber-attack unnoticeable because of the focus on other components of ICS/SCADA systems. Later information showed that the TRITON attack targeted a Saudi-Arabian petrochemical facility [109] and FireEye with high confidence attributed this attack to Russia [110].

The TRITON attack reprogrammed the SIS of the Saudi Arabian petrochemical processing plant, which was a Triconex SIS from Schneider Electric. The SIS inadvertently shutdown after TRITON malware was deployed [108]. Thankfully, the petrochemical company noticed this and contacted Mandiant to investigate the incident before any physical damage could had happened.

The following files were used to implement this cyber-attack:

1. **trilogy.exe:** The initial foothold was most probably gained by delivering the payload using social engineering techniques where the CI engineer received or downloaded the legitimate dropper filename “trilogy.exe” (hence TRIconex LOGging filename). The purpose of the dropper file was to deliver the malicious payload to the target which was made of two separate binary files named: “inject.bin” and “imain.bin”.
2. **inject.bin:** The first part of malware payload which contained the 0-day exploit to execute the content of the file “imain.bin”.
3. **imain.bin:** This file contained the final code which allowed the attackers to gain remote full control access to the SIS device. [20]

The following figure shows a summary of how the attack happened:

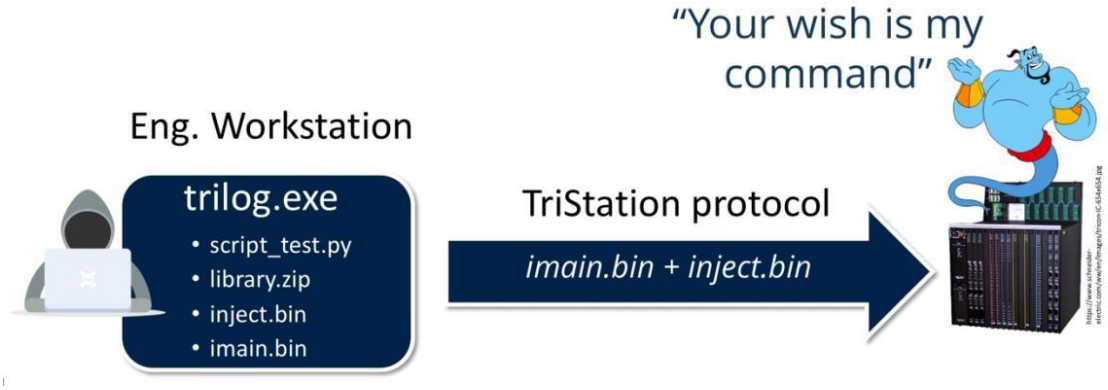

Figure 5. Schematic view of TRITON dropper phase [20]

The Black Hat research paper [20] show that the financial resources as well as effort and skills to create the TRITON malware are not that high and they even came up with two tools to detect the malware:

- **TriStation Protocol Plug-in for Wireshark:** A Wireshark [111] plug-in which passively detects TRITON activity in network communication that can be helpful to CI engineer to detect abnormal activity on TriStation communication.
- **Triconex Honeypot Tool:** Can be used by defense team to simulate SIS controllers so that they can be used as honeypot to detect reconnaissance scans and capture malicious payloads from possible future cyber-attacks. [20]

Some of the recommendations from this cyber-attack include:

- Network segmentation on SIS controllers where they should be segregated from process control and information system networks. [108]

- Monitor SIS such as the communication that happens with it and secure it against external cyber-attacks and make them more robust by developing built-in security for these important systems. [20]

3.3 Summary of Lessons Learned from Real-World CI Cyber-Attacks

As seen from the analysis of real-world CI cyber-attacks, it is the author's point of view that the TTP's that were used in the attacks mentioned above can also impact Kosovo's CI environment. Tactics such as spear-phishing campaigns can also be used as an initial-foothold by attackers on Kosovo's CI owners/operators. Therefore, the following aspects of lessons learned taken from real-world CI cyber-attacks should be taken into account when evaluating Kosovo's CIP policy using the semaphore model:

- **Cyber-awareness:** From all of the above-mentioned cyber-attacks, the author found that the attackers gained initial foothold by using social-engineering techniques against CI engineers or operators. It is critical to have a proper policy on training all of the CI engineers or operators on the potential threats and vulnerabilities that ICS/SCADA systems currently face from the cyber domain. In addition, a proper cyber-hygiene plan should be deployed so that the CI personnel does not fall a victim to a potential malicious spear-phishing campaign.
- **Architectural:** Network segmentation measures such as placing SIS or ICS/SCADA systems in a network area that has stricter security rules, would make it harder for an attacker to gain access on those systems. In addition, should one of the systems go down, proper backup policies would improve the resilience of these systems by providing continuity of service.
- **Misconfiguration mitigation:** The author observed from the Florida and Ukraine cyber incidents, that both of these cyber incidents had misconfiguration of remote access software, firewalls or even VPNs that can allow attackers to gain access to ICS/SCADA systems. Proper configuration, as well as patching plan, would make it harder for attackers to access critical ICS/SCADA systems or even SIS which as the author observed, can be manipulated, and have catastrophic consequences.
- **Incident response mechanism:** A proper incident response mechanism should be in place in order to react quicker against a potential cyber-attack. This would

include proper evidence collection mechanisms such as logging of events that SIS or ICS/SCADA systems produce. This evidence can be utilized, by training the defenders of these systems on the proper usage of tools such as YARA rules.

- **Cooperation with cyber-security community:** As the author observed from the Saudi-Arabian petrochemical attack, FireEye was contacted when the petrochemical plant operators found out that its SIS is not working in a normal operational state. It would be really helpful if a proper threat-intelligence mechanism would be in place with the cyber-security community, in order to have a quicker reaction on mitigating the potential future malwares on CI sectors.

4 Kosovo's National State Affair

In this chapter the author will analyse Kosovo's current CIP policies and cyber security capacities by analysing the following documents:

- Kosovo's National Cyber Security Strategy (NCSS). [10]
- Kosovo's law on CI. [11]
- World bank cyber security capacity assessment on the Republic of Kosovo. [16]

In addition, the author will analyse Kosovo's OES environment of electric transmission or distribution and water-supply sectors from the CIP perspective.

4.1 Current CIP Policies and Cyber security Capacities in the Republic of Kosovo

In this section, the author will have a thorough analysis of Kosovo's current CIP policies by analysing Kosovo's strategy on cyber security [10] and law on CI [11], as well as Kosovo's cyber security capacities based on a report by the World Bank [16].

4.1.1 Kosovo National Cyber Security Strategy and Action Plan 2016-2019

In December of 2015, Kosovo's Ministry of Internal Affairs (MIA) published Kosovo's strategy on cyber security [10]. This strategy was relevant from the year 2016 until 2019. Currently, there is a working group which is tasked for creating and implementing a new strategy for years 2020-2025 [112], but as of the time of this thesis work, the new national strategy was not published from Kosovo's MIA. Therefore, the author will take into account the current strategy which is in force today in Kosovo.

Kosovo's NCSS addresses the following cyber security topics:

1. CIIP.
2. Institutional development and capacity building.
3. Building public and private partnership.
4. Incident response.
5. International cooperation. [10]

The context and planning of the strategy is based on ENISA and strategies of EU MS. Because the focus of this thesis is on CIP and incident response against a potential cyber-

attack on Kosovo's OES, the author will analyse in more detail CIIP as well as incident response sections of the strategy. Meanwhile other sections that are related to CIP and incident response will be also analysed such as cyber-awareness section.

The strategy defines cyber threats by their motivation such as monetary gain where mostly hacktivism groups are the main threat, national security where cyber-attacks are mostly done by state sponsored actors or even terrorists.

The strategy authorizes Kosovo's MIA to hold the role of national cyber security coordinator. If it finds it necessary, Kosovo's MIA can also assign another authorized person whose role would be to guide, coordinate, monitor and report on the implementation of policies and actions which are related to the strategy.

Kosovo's NCSS clearly makes a separation of CI and CII where the main difference is that CII is divided as ICT systems that are as part of CI whereas CI also includes other OT services. It is worth to mention that the strategy divides CI sectors according to European Commission Green Paper for CIP [14] which matches with CI sectors from NIS Directive [15]. This was probably done because of the date the NIS Directive was published whereas Kosovo's strategy was published in December of 2015. Meanwhile CIIP, according to the strategy, should be viewed as cross-sector issue and its main aims are to keep the performance of CII into an acceptable minimum level of service. An additional aim is also to minimise the recovery time and damage in case of an attack, accident or a failure by defining procedures for CIP operators, owners and users. The importance of CI is also seen in the strategy where CIIP is considered as the main priority of cyber security after it could have severe consequence if it is destructed and disrupted. The strategy also defines how to identify CII assets and services based on ENISA's methodology [113]. Another important part of the strategy is the definition of procedures related to cooperation between public and private sectors.

Incident response section on this strategy defines the creation and functionalisation of national as well as other CERT/CSIRT-s in the Republic of Kosovo by emphasizing the necessary infrastructure as well as appropriately trained staffing personnel. It is also mandatory for Kosovo CERTs or CSIRTs to be listed in Trusted Introduced [114] and FIRST [115]. Since the creation and implementation of its strategy, Kosovo has created 6 different CERTs. As seen from ENISA CSIRTs inventory report for Kosovo [116],

none of the CERTs are member of FIRST, whereas 4 of them are listed in Trusted Introduced and 2, including national KOS-CERT are accredited in it.

Another aspect of the strategy which is important to mention is awareness raising. As the author noticed, most of cyber-attacks in CI, start from techniques such as spear-phishing campaigns. The strategy gives importance to this issue and encourages awareness measures such as information campaigns by promoting events such as "European Cyber Security Month". Additionally, adequate trainings for all stakeholders in an organization should be considered, who should have sufficient understanding of cyber domain as nowadays everything is being connected to the cyberspace.

Even though the strategy has some advanced requirements for its CIP and CERTs, as it will be seen in sections 4.1.3 and 4.2, Kosovo is still lacking in implementing most of these requirements. Taking that into account, Kosovo has still matured and has improved on many areas of cyber security capacity from previous years [117].

4.1.2 Kosovo's Law on CI

In 2018, the assembly of the Republic of Kosovo ratified the law on CI whose purpose is to "preserve and protect national and European critical infrastructure, protect citizens of the Republic of Kosovo, prevent incidents and minimize potential damage to critical infrastructure, general wealth, economic and social losses, ensure government stability, and enhance resiliency" [11]. This law clearly defines terms related to CIP and divides CI sectors which are based on common area of interest with the main goal of improving cooperation between different sector stakeholders. Two of these sectors are also energy and water sectors which this thesis is focused on.

Kosovo's law on CI clearly defines that Kosovo's MIA needs to lead the task of identifying and prioritizing CI located in Kosovo. This should be done in cooperation and consultation with other security, government, and non-government institutions as well as with private owners or operators and key international stakeholders. A risk analysis approach based on real global threats that could potentially disrupt or interrupt the operation of CI needs to be taken in order to identify the CI components. This risk analysis, as the law defines in paragraph 3 of Article 6, should be based on the following criteria:

- **Geographic scope** – This criterion is also in harmony with NIS Directive requirement where one of the parameters to calculate the impact of an incident on OES is the geographical spread of that incident. In this case, a risk assessment on one of Kosovo's OES will be based on the impact that a disruption on CIS of that OES can have.
- **Severity** – The severity of a potential disruption on CI is calculated based on the public impact which is the affected population number. This again is in harmony with one of the parameters of NIS Directive to assess the impact of an incident such as: public impact (number of population affected); economic impacts; environmental impacts; or public health consequences. [11]

Article 5 or European Critical Infrastructure (ECI) Directive [118], requires all EU MS to implement an Operator Security Plan (OSP) for all required CI operators or owners. OSP needs to identify CI assets and establish security solution for their protection by taking steps such as:

- Identification of CI important assets.
- Take a risk analysis approach on these CI assets based on major threat scenarios as well as potential vulnerabilities that exist on them. Additionally, the potential impact that a disruption of this CI asset can cause on the public, economic or environmental aspects should be taken into account. [118]

Kosovo's law on CI also requires that Kosovo's and European CI owners who are located in Kosovo, to develop and submit an OSP within 9 months after they get notified that their infrastructure is part of Kosovo's critical infrastructure. In addition to the ECI requirements mentioned above, the OSP should also include measures designed to prevent and protect CI assets from incidents or accidents and ensure business continuity and delivery of services is still available [11]. In addition, each CI sector of Kosovo needs to have a security coordinator who coordinates CIP activities within its own OES sector as well as a security liaison officer who shall be assigned by the operator/owner of CI. This officer's main task is to be the point of contact related to security issues between the CI operator and the relevant government authority. Article 21 of Kosovo's law in CI, states that a fine between 500 to 5000 euros can be imposed to a natural person or a person in charge who fails to implement the OSP according to the requirements mentioned above or if it fails to nominate a security liaison officer.

As the author will show in following sections, even though Kosovo's law on CI has some well-documented CIP measures, there is still a lot of work ahead to implement these measures in the Kosovo's OES environment.

4.1.3 Kosovo's Cyber security Capacities

In 2015, with an invitation from Kosovo's Ministry of Economic Development (MED) and through collaboration with the World Bank, the Global Cyber Security Capacity Centre (GCSCC) of University of Oxford, assessed the cyber security capacity in the Republic of Kosovo [119]. Later in 2019, taking this 2015 cyber security capacity report as a baseline, GCSCC and the World Bank again with the invitation of Kosovo's MED took another cyber security capacity review [16], in order to see the advancements and implementation from the previous report recommendations. In addition, the new report assessed the current cyber security environment in the Republic of Kosovo. Some of the stakeholders that participated in these reports were:

- Academia.
- Law enforcement agencies.
- Policy makers.
- IT officers from public sector.
- CI owners. [16]

This cyber security assessment report was done using the methodology of Cybersecurity Capacity Maturity Model for Nations (CMM) [120] which assesses a country's cyber security capacity maturity using the following five dimensions:

1. Cyber security Policy and Strategy.
2. Cyber Culture Society.
3. Cyber security Education, Training and Skills.
4. Legal and Regulatory Frameworks
5. Standards, Organisations and Technologies. [120]

These dimensions are made of number of factors that indicate how to enhance the cyber security maturity and uses a set of indicators for each factor that is used to assess cyber security maturity model along the following five maturity stages [121]:

- **Start-up stage**: No cyber security maturity exists where initial cyber security capacity building has been discussed but no concrete actions have been taken.

- **Formative stage**: There is evidence that some features of a cyber security aspect have been formulated and have begun to grow, but they might be disorganized and poorly defined even though they can be clearly demonstrated.
- **Established stage**: At this part of the stage the elements of a cyber security aspect are functional, defined, in place and working, but there is lack of consideration for allocation of relative resources.
- **Strategic stage**: There is a separation between which parts of a cyber security aspect are more important than other for the particular nation or organization where choices are made upon the nation or organization circumstances.
- **Dynamic stage**: This is the most advanced stage where there is a well-defined clear mechanism in place on altering strategy depending upon certain circumstances such as global conflict or the technology of the threat environment. In this part of the stage rapid decision-making is implemented and reallocation of resources is made in timely manners. [121]

In the Kosovo's cyber security capacity assessment review [16], the first dimension includes the factors that the author is most interested in: incident response and CIP. Meanwhile the author will also analyse some of other dimensions which are relevant to the two factors mentioned above.

In relation to Kosovo's NCSS implementation progress, this cyber security capacity report observes that there are improvements in training, international cooperation as well as cooperation between internal agencies. There are also some challenges where the risks, possible vulnerabilities and motivations of threat actors are not contextualised in their application to Kosovo and are described in general terms. The NCSS of the Republic of Kosovo is rated from the CMM stage maturity "Formative to Established" where steps such as independent evaluation of NCSS implementation as well as identification of lessons learned need to be taken to better understand how much of Kosovo's NCSS is implemented in the real-world.

KOS-CERT is Kosovo's official national cyber incident response unit, but which does not have an explicit mandate defining its responsibilities and duties and is setup under Regulatory Authority of Electronic and Postal Communication (ARKEP) of the Republic of Kosovo. ARKEP oversees network and electronic service providers and the reason why KOS-CERT is structurally integrated under ARKEP, it is because KOS-CERT

procedures and structures are based on the original model implemented by Lithuania. Lithuania's CERT, prior to its reorganisation in 2017, was setup under the Communications Regulatory Authority of Lithuania. The biggest challenge for KOS-CERT is the lack of staff, where, as of the time of this World Bank report, KOS-CERT was operated by only two staff members. This clearly shows that in a future coordinated cyber-attack, especially from a nation-state, KOS-CERT would not be able to respond timely because of its lack of staff and mandate. KOS-CERT tried to strengthen coordination and cooperation between different incident response team that come from both private and public sector in the Republic of Kosovo. Unfortunately, because of the low response rates from these organisations, there is still lack of cooperation between different stakeholders and KOS-CERT. Although KOS-CERT is structurally integrated to ARKEP, it has good cooperation with Internet Service Providers (ISPs).

KOS-CERT receives a low number of incident reports. This is not because there are no cyber incidents in the Republic of Kosovo, but as KOS-CERT analysed, it is because the insufficient capacities of relevant institutions to detect incidents. The incident can be reported on KOS-CERT's website but also by phone or email where submissions are registered in a ticketing system database, which operates without automated incident classification. Another problem with the cyber incident detection issues in the Republic of Kosovo is that of not receiving a Top-Level Domain (TLD) from the Internet Assigned Numbers Authority (IANA). This is because Kosovo is still not part of the UN, and by not having a TLD, Kosovo does not have its digital sovereignty. Internet Protocol (IP) addresses for devices physically located in Kosovo, are being listed as registered in Albania or Serbia. This clearly is a big issue as the incident reports from international partners concerning these IP addresses will be first directed to Albania or Serbia, and then it would be the decision of these countries if they would forward the incidents to Kosovo's relevant authorities. Even if these countries agree to forward the incident reports, there is still a slowdown of the receipt of time-sensitive incident reports, especially if these incidents can have impact in the citizens life such as an incident on one of OES sectors in the Republic of Kosovo.

Operators of potential CI, as the full identification of OES in the Republic of Kosovo has still not been made, reported a low use of internet-based technology and systems. In the event of an ICS failure, mechanical backup operations such as manual resets are designed as response steps to ensure continued delivery of service. Cyber security awareness and

measures from these operators are considered as lower priority where training is pursued based only in their own interest and initiatives. The budget of cyber security is also small in these potential CI, where if technical expertise arises, operators hire external contractors.

Some of the recommendations for incident response from the report are:

- Provide KOS-CERT with an appropriate staff count resources and a clear mandate which specifies roles and responsibilities.
- Incident-reporting requirements should be expanded to other sectors according to the legislation regarding identification and designation of CI systems and operators.
- A mechanism for information sharing between public and private sector should be established. [16]

Even though NIS Directive is still not transposed in its CI environment, Kosovo has a detailed and comprehensive law on CI. Unfortunately, there is a lot of work on implementing it in Kosovo's OES environment. As analysed from GCSCC, the timeline on identifying and analysing the risks of Kosovo's CI as defined in the law, have significantly deviated from the NCSS action plan timeline which was the end of 2016. Kosovo also was undertaking efforts to transpose the NIS Directive where a new law on cyber security was scheduled to be submitted to Kosovo's parliament for approval by the end of 2020. Unfortunately, because of current Kosovo's political crisis where two governments were brought down [122] during the year of 2020, there is still no indication that Kosovo identified its CI operators nor submitted the new law on cyber security for approval in the parliament.

Kosovo's electricity grid system is managed through a centralised SCADA system. Even though the "Energy Strategy of the Republic of Kosovo 2017-2026"[123] informs that sub-stations will be integrated into the central SCADA system, there is no reference to cyber security measures for protection to ensure resilience of the SCADA systems operations. Additionally, Kosovo's largest water company runs two SCADA systems that have been set by external Bulgarian contractors. Kosovo's local engineers and network administrators on site had minimal contact with contractors, and they are not trained to respond to an incident in case a cyber-attack hits these SCADA systems. This clearly shows that Kosovo lacks strategic implementation of its requirements that derive from its

NCSS and law on CI related to CIP. Lack of training of Kosovo's CI operators/owners staff; outsourcing the management of its ICS/SCADA systems to external contractors; as well as not clearly identifying its CI environment; makes this report rate the CIP, to the start-up stage maturity-level.

Some of the recommendations that derive from the GCSCC report related to Kosovo's CIP are:

- Cyber security and its requirements should be implemented in CI regulations as an integral component to strengthen the resilience of CI operators and systems.
- A mechanism for the exchange of vulnerability and threat information among CI owners and the government should be established.
- Responsibilities should be coordinated in relation to the transposition of NIS Directive in order to avoid any overlaps between the dedicated law on cyber security whose baseline will be the NIS Directive and the MIA efforts in implementing the Kosovo's law on CI. [16]

Cyber security awareness on CI operators as well as shortage of labour supply for skilled cyber security professionals are some of the other challenges that Kosovo faces. These can have an impact in developing a proper incident response mechanism against a potential cyber-attack on OES environment in the Republic of Kosovo.

4.2 Kosovo's OES Environment

Kosovo has taken steps on modernizing its CI environment. As this thesis is based on publicly available documentation, after some research, the author found relevant information for Kosovo's OES environment on the sectors of electric-energy and water-supply sectors. The following documents will be taken as a baseline to analyse Kosovo's OES environment on electrical-energy and water-supply sectors:

- Publicly-available information from Kosovo Energic Corporation J.S.C. (KEK) website. [21]
- Previously implemented projects [22] [23] from third-party companies as well as development plan of electric transmission [24] from Kosovo's Transmission System, and Market Operator J.S.C. (KOSTT).

- Magazines [25] [26] and development plan [27] of electric distribution from KEDS.
- World Bank project on water security and canal protection for the Republic of Kosovo. [28]

4.2.1 Kosovo's Electric-Energy Generation, Distribution and Transmission Environment

The Republic of Kosovo has three main companies responsible to generate, distribute and transmit electricity across its entire territory:

1. KEK - Main electric-energy corporation, where this corporation is 100% owned by the government of the Republic of Kosovo [124]. In 2013 the privatisation of electric distribution (KEDS) and transmission (KOSTT) was completed and now the main functions of this corporation are the production of coal and the generation of electric energy.
2. KOSTT - Manages the electrical transmission system in the Republic of Kosovo where its responsibility is to transmit electricity safely and reliably from generating units to the distribution system, 24 hours a day, 365 days a year. [125]
3. KEDS - Its main responsibility is to distribute, maintain and repair a stable electrical network of approximately 600,000 costumers spread throughout the territory of the Republic of Kosovo. [126]

KEK's division for electric energy generation consists of two main power plants: "Kosova A" and "Kosova B" [127]. "Kosova A" power plant started working and got in production on the year 1962 where it was made of 5 main blocks, from which currently only 3 of them are functional (A3, A4 and A5). Because that this power plant is old, there are plans to decommission it. The yearly generation from this power plant is around 1.500.000 megawatt (MW).

Meanwhile, "Kosova B" power-plant first started working on the year of 1982 where it is made of two units: B1 and B2 [21]. "Kosova B" power plant is fully functional, where its yearly availability rate can go up to 85%. This power plant, in contrast to "Kosova A", got and still gets investment since it was built, where both of its units are highly available even though they are more than 30 years old. The average electric generation from this power plant is around 3.750.000 MW [21]. This shows that from the main power plants

in the Republic of Kosovo, “Kosova B” power plant has more importance because Kosovo’s reliability on power generation from “Kosova B” power plant is higher. This makes “Kosova B”, the current main power plant of the Republic of Kosovo.

DCS-P320 [128] which is made from the French company “Alstom Power Service” is used as a command and control system in the “Kosova B” power plant [21]. The author can already assume from [128] that DCS-P320 uses the “Alspa” HMI to control the power-plant. This can also be confirmed from the following picture taken in “Kosova B” power plant:

Figure 6. “Kosova B” power plant operational room [21]

In addition, by zooming in the picture, on the right a lock screen of Microsoft Windows 7 can be seen, which makes the author say with high confidence that the Operating System (OS) being used in “Kosova B” power plant operational room is Windows 7. This, together with showing the specific software that is being used, in this case “Alspa” HMI, can be a cause of concern in the future, because this information is publicly available and threat actors can use this information to prepare a cyber-attack on “Kosova B” power plant. In addition, Windows 7 is an end-of-life OS [129], where future vulnerabilities on

this OS can be used by cyber-attackers to gain access on “Kosova B” power plant operational room.

In 2008 KOSTT gave a contract to KOMTEL and ALSTOM Grid [22] to implement its SCADA and Energy Management System (EMS). The project was successfully completed in 2011 where the assembling and mounting of SCADA/EMS systems on site as well as installation of RTU’s was done in 23 locations all over Kosovo. In 2014, the same companies were contracted from KOSTT to upgrade and update the SCADA/EMS systems [23]. A picture from the operational room is shown below, where it seems that the OS that is being used is that of Microsoft Windows XP:

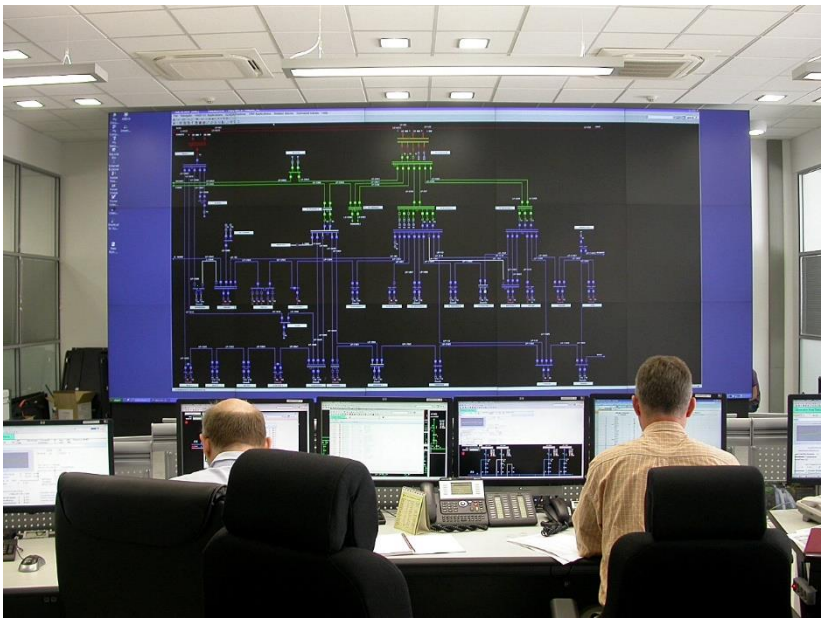

Figure 7. KOSTT operational room [23]

Microsoft Windows XP is an end-of-life OS since 2014 [130], which means it is not supported anymore from Microsoft including updates and patches, and it is really easy to exploit it.

It is worth mentioning as Kosovo together with Albania created a Kosovo-Albania energy bloc [85], that there was already an integration of SCADA/EMS systems of the respectable two countries [131].

In 2019, KOSTT came with a new document “Transmission development plan 2020-2029” [24], where one part of the plan is to upgrade the SCADA/EMS systems. Some of the expected SCADA/EMS upgrades, except the capacity upgrades, are to use the latest

Microsoft OS, as well as improve the security by replacing the existing firewall with more advanced firewall and related software (Project ID/029) [24].

In 2018, KEDS announced that it has started digitizing the electricity distribution network in Kosovo by enabling the SCADA system [132]. This SCADA system operates through the central office in the capital city of the Republic of Kosovo, Pristina. As of 2020, 29 substation were digitized by KEDS using the SCADA system [26], where some of these substations are located at the main cities of Kosovo. [27]

The figure below shows how the operational room of KEDS SCADA system looks:

Figure 8. KEDS operational room where HMI of SCADA is shown [25]

One concern from the KEDS magazines is showing what vendor is managing KEDS SCADA system. From the figure below, it can be clearly seen that in this case the vendor is “Siemens”:

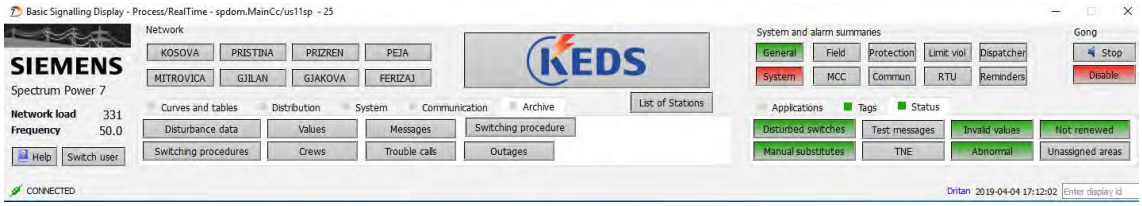

Figure 9. SCADA vendor shown from KEDS magazine [25]

As shown from real-world CI cyber-attack scenarios, this kind of open-source information such as the OS version being used, or the vendor of SCADA system can be used by attackers to target the specified SCADA system. There should be precautions when pictures are taken in the operational room as well as what information is shared in magazines of electric-distribution companies.

4.2.2 Kosovo's Water Security and Canal Protection Project

The Iber-Lepenc (IL) canal is a 49 kilometer, man-made hydraulic structure [133] that has various uses on supplying water to central Kosovo and it benefits approximately 500,000 people [134]. IL canal is managed by the Hydro-economic Enterprise (HE) "Iber-Lepenc" J.S.C. [135] otherwise known as Iber-Lepenci Company (ILC). It is worth mentioning that the Lepenc canal is not finished yet [135]. The status of ILC [136] describes the main functions of IL canal, some of which are:

1. Supply of raw water that is accumulated from "Ujman" lake to the following beneficiaries: (a) Industries such as KEK where the water is used on cooling power-plants "Kosova A" (during summer period) and "Kosova B" [133]; (b) Regional water-suppliers in Mitrovica and Prishtina; (c) Farmers.
2. Production and sale of electric energy.
3. Protection of hydro system objects.
4. Protection of water in hydro system objects from contamination. [136]

This shows that IL canal is Kosovo's main water-supply canal and of a critical importance to the Republic of Kosovo. A schematic map of IL canal is shown below:

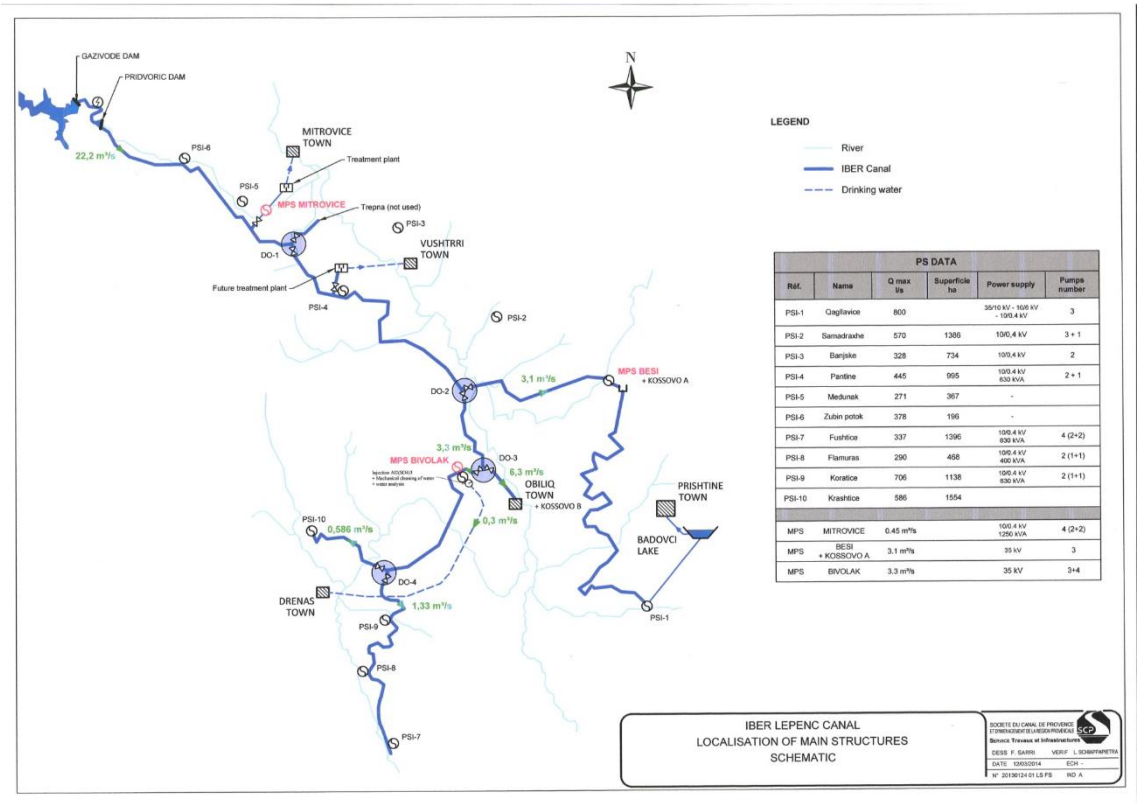

Figure 10. Iber-Lepenc Canal schematic map [28]

As Iber canal was built in 1970s, the canal is used for more than 40 years from which the concrete lining of the canal has been degrading, resulting in a significant (around 50%) seepage loss [134]. In addition, physical damage and pollution such as from landslides and mudslides, garbage and other debris, affected the quality of water in this canal. Therefore in 2017, Kosovo government signed with the World Bank the Letters of Agreements [137] for the "Kosovo Water Security and Canal Protection Project" [28]. The main aim of this project, which is being implemented by ILC and Kosovo's MED, is to restore Iber Canal to its original capacity [28] [137]. As of 24th of March 2021, 80.99% of the project is implemented [138].

The main focus of the author in the "Kosovo Water Security and Canal Protection Project" will be in the components 2 and 3 of this project [28], which are related to the installation of an advanced SCADA system and the training of ILC staff on the proper usage of this SCADA system. The main purpose of the SCADA system will be to provide ILC staff a tool to monitor water levels more efficiently at Gazivoda lake and provide time series. This project estimates that the SCADA system and other electromechanical equipment would cost 800,000 euros. After some research in the internet, the author found that the SCADA system is implemented and maintained from two companies [139],

namely “Oskar-El” from Bulgaria [140] and “InterAdria” from Kosovo [141]. As of 5th of February 2021, six of Kosovo’s government staff were trained efficiently on using the SCADA system [142], which is a good result as the initial projection was to train five of Kosovo’s government staff [134].

An architectural diagram of the SCADA system that will be used in “Kosovo Water Security and Canal Protection Project” is shown below:

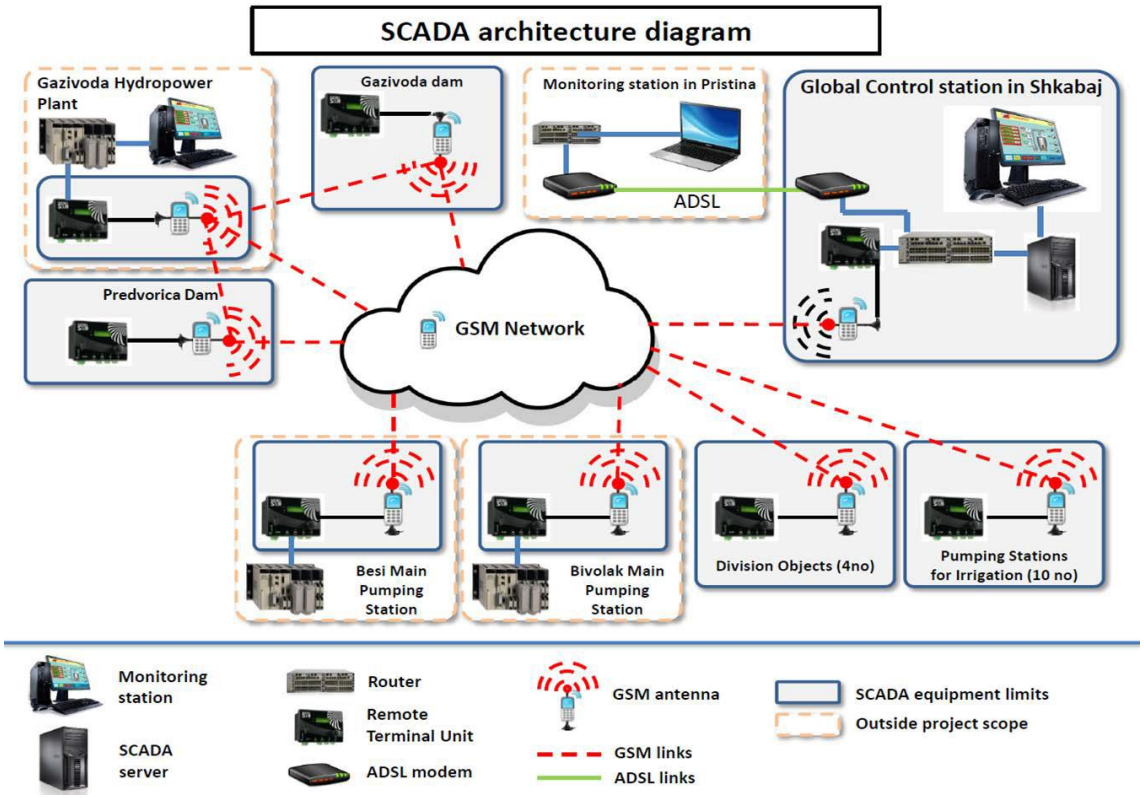

Figure 11. Kosovo Water Security and Canal Protection Project - SCADA architecture diagram [28]

An initial security concern in the above SCADA diagram is the communication standard that is being used between global control station and different dams, namely GSM. There are already different proofs on cyber-attacks against GSM communication standard [143] [144]. For example, as shown from the Check Point Researchers [145], potential attackers can take advantage of the GSM standard by only buying a 10 dollar GSM modem to start a SMS phishing campaign against ILC staff. This could be used as an initial attack vector to obtain access to the global control station in Shkabaj. The World Bank project on Kosovo’s water security and canal protection does not mention anywhere a cyber-awareness training to six Kosovo’s government staff that were trained on the usage of Iber canal SCADA system.

5 Synthesis: Application of Semaphore Model on Kosovo's CIP Policies and Recommendations

This chapter represents the evaluation of Kosovo's CIP policies using the semaphore model developed by the author and recommendations which would improve current and future CIP policies in the Republic of Kosovo. This chapter is made of the following sections:

- **Application of semaphore model on Kosovo's CIP policies**: The semaphore model (defined in section 1.5.2) is applied against Kosovo's current CIP criteria (defined in section 1.5.1).
- **Summary of synthesis:** Based on the findings from the discussion on section 5.1, the author presents a matrix on visualising the summary of these findings.
- **Recommendations on improving Kosovo's CIP policies:** In this section, author provides recommendations on improving current and future CIP policies in the Republic of Kosovo based on the findings discussed in section 5.1 and the matrix shown in section 5.2.

5.1 Application of Semaphore Model on Kosovo's current CIP Policies

In this chapter, the author applies the semaphore model defined in section 1.5.2 against the 7 Kosovo's CIP criterions defined on section 1.5.1.

5.1.1 Criterion 1: Identification of OES

When NIS Directive was transposed on the EU MS, one of its requirements was that all EU MS should identify their OES by 9th of November 2018 [15]. OES sectors are described on Annex 2 of NIS Directive.

Article 5 of NIS Directive gives the following criteria on the identification of OES, where, based on paragraph 4 of Article 4 (which defines an OES based on Annex 2), an OES should fill the following criteria:

a) An entity which provides a service that is essential for the maintenance of critical and/or economic activities.
b) The provision of that service depends on network and information systems.

c) An incident on that service could have significant disruptive effects on the provision of the service. [15]

Based on Article 6 (paragraph 1) of NIS Directive, these factors should be taken into account when determining the significance of a disruptive effect that could impact the services of an OES:

a) The number of users that rely on that OES.
b) The dependency from other sectors (defined in Annex 2 of NIS Directive) against the services provided from the OES.
c) The impact that incidents could have, in term of degree and duration as well as public safety or economic and societal activities.
d) The market share of the respectable OES.
e) The geographic spread with regard to the area that could be affected by an incident.
f) Based on the availability of alternative means for the provision of the services from OES, the importance of maintaining that service in a sufficient level. [15]

In addition, Article 5 of NIS Directive also requires EU MS to review and if needed, update the list of identified OES at least every two years.

Paragraph 1 of Article 4 in Kosovo's law on CI defines national critical infrastructure as "systems and assets, whether physical or virtual, so vital to the Republic of Kosovo that the disruption, incapacity, or destruction of such systems and assets would have a debilitating impact on security, economy, public health, or any combination of those" [11]. Even though Kosovo still did not transpose the NIS Directive, paragraph 2 of Article 5 in Kosovo's law on CI defines the sectors of CI. This makes the author conclude with high confidence that the CI sectors are in line with the OES sectors that are defined in Annex 2 of NIS Directive.

As explained in section 4.1.2 of this thesis, Kosovo's law on CI [11] also partially implements the disruptive effect parameters described in Article 6 of NIS Directive. Geographic scope and severity of different factors (number of population affected, economic impact, public health consequences) are defined in Article 6 (paragraph 3) of Kosovo's law on CI. These parameters are taken into account when a comprehensive risk analysis is made on Kosovo's OES, as described from Article 6 (paragraph 2) of Kosovo's law on CI.

Kosovo has taken some partial steps on identification of its OES from the documentation perspective such as Kosovo's law on CI. Unfortunately, there is still not a proper national mechanism from Kosovo's relevant authorities on implementing the requirements that derive from the law on CI. This was confirmed from few email exchanges taken place on March 2021, between the author and relevant Kosovar authorities with knowledge on this subject. From this discussion the author learned that Kosovo does not have a proper institutional mechanism on the identification of OES, and this is the reason why the Republic of Kosovo still did not identify its OES. Therefore, it is the author's evaluation and conclusion that the rating of this criterion is red.

5.1.2 Criterion 2: Single Point of Contact

Paragraphs 3 through 7 of NIS Directive's Article 8 [15], define the definitions and requirements for an EU MS to successfully assign a single point of contact. The main points taken from Article 8 of NIS Directive regarding the proper assignment and the duties of the single point of contact are:

- The role can be assigned to a single existing authority (paragraph 3).
- Should ensure cross-border cooperation between relevant EU MS authorities as well as national law enforcement and data protection authorities (paragraphs 4 and 6).
- In order to properly carry out the tasks assigned to them and fulfil the objectives of NIS Directive, adequate resources should be given to the single point of contact (paragraph 5). [15]

Section 5.2 of Kosovo's NCSS [10] assigns the role of National Cyber Security Coordinator to Kosovo's Minister of Internal Affairs or his/her authorized person. As described from this section, the main mandate and responsibilities of the National Cyber Security Coordinator are to coordinate, monitor, guide, and report on the implementation of policies and actions that are connected to Kosovo's NCSS. Meanwhile Kosovo Police is assigned as a 24/7 point of contact for international cooperation in the field of cybercrime.

Kosovo's law on CI describes contact point as "the central government authority responsible to communicate and exchange information on European critical infrastructure with competent authorities of the European Union and other countries" [11]. This role, as

shown in Article 4 (paragraph 3) of Kosovo's law on CI is assigned to Kosovo's MIA for both the Republic of Kosovo as well as collaboration with other European countries.

Even though it is author's point of view that there should be a separate institution in the Republic of Kosovo as a single point of contact which solely focuses on IT, such as is the case with Estonia [146], Kosovo clearly defined the single point of contact on the matters that are described by the NIS Directive and are relevant to CIP. Therefore, the author rates this criterion as green.

5.1.3 Criterion 3: Cyber Awareness

One of the requirements from NIS Directive, directed to EU MS, as described in point (d) of Article 7, is that the cyber security strategies of EU MS should address the issue of "education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems" [15]. This is especially important for CI owners/operators of respective countries, where the author found from the real-world scenarios, that a cyber-attacks on CI tend to start by using social-engineering and spear-phishing techniques (e.g. malicious Microsoft Office attachment in 2015 Ukrainian power-grid attack [101]). Chapter 1.1, "Human resource security" section (page 15) of NIS CG reference document on security measures of OES [29] recommends that security awareness raising program should be included to CI owners/operators.

The Republic of Kosovo has already taken steps on educating its population on the subject of cyber-awareness and cyber-hygiene. Chapter 3.2 of Kosovo's NCSS, under the "Vulnerabilities" section [10] acknowledges that awareness-raising is one of the biggest challenge among relevant personnel. In addition, section 6.2.3 of Kosovo's NCSS gives importance to promote the culture of cyber security across Kosovar society, by promoting events such as "European Cyber Security Month". Just last year, The United Nations Development Programme (UNDP) together with Kosovo's MIA launched the campaign named: "Be careful while on internet" [147] which organized several activities that were related to cyber-awareness towards Kosovo's population.

Meanwhile, Article 9 of Kosovo's law on CI [11] requires that OES in Kosovo should submit a OSP or equivalent plan to Kosovo's MIA 9 months after being notified on the OES designation. One of the measures that should be included in this OSP is awareness raising and training on information systems of OES (paragraph 4.1. of Article 9).

As shown from the above-mentioned discussion, even though Kosovo has taken measures on raising cyber-awareness against its population, there is not a proper mechanism on training Kosovo's CI operators staff against potential cyber-threats and vulnerabilities. This is shown from the World Bank cyber security capacity review report on the Republic of Kosovo [16] (section 1.2 page 35), where cyber security measures and related awareness are not taken as a priority concern to Kosovo's CI operators staff. Moreover, if a need for a specific technical expertise arises, these CI operators hire external contractors with necessary qualifications. In addition, training on cyber security is based only on CI operators staff own initiative. This should be a concern for Kosovo's future CIP measures and policies. As it is observed from real-world cyber-attack scenarios in chapter 3, attackers use phishing and social-engineering techniques against CI operators staff to gain initial foothold on ICS/SCADA systems. In addition, as shown from section 4.2, CI operators staff are not aware of the risks that can come up on publicizing in internet pictures of their operational rooms.

By taking into consideration all of the facts mentioned above, the author can conclude that Kosovo has taken some measures on raising awareness on its population against cyber-threats. Unfortunately, as there is a lack of proper awareness and training mechanism on Kosovo's CI operators staff, the risk and threat level on Kosovo's OES environment still remains high. Therefore, the author rates this criterion as red.

5.1.4 Criterion 4: Penalties

In order to ensure that EU MS implement the security measures defined in NIS Directive, Article 21 of NIS Directive [15] requires EU MS to lay down rules related to penalties in case those measures are not adopted from OES.

Article 21 (paragraph 1) of Kosovo's law on CI [11] defines the penalty measures where a fine from 25,000 to 40,000 euros can be imposed to a CI owner/operator if:

- An OSP is not developed according to article 9 of Kosovo's law on CI (paragraph 1.1).
- A Security Liaison Officer was not nominated according to Article 10 paragraph 4 and Article 14 of Kosovo's law on CI (paragraph 1.2). [11]

In addition, paragraphs 2 and 3 of Article 21 [11] require that a fine from 500 to 2000 euros shall be imposed to a natural person or person in charge if he or she commits an

offense as defined from above-mentioned paragraphs (1.1 and 1.2). Alternatively, a fine from 2000 to 5000 euros shall be imposed if that person carries out an individual business.

As there is a clearly defined mechanism on imposing penalty measures to Kosovo's OES if they do not comply to the security measures defined in Kosovo's law on CI, the author rates this criterion as green.

5.1.5 Criterion 5: Threat Landscape

Before any protection measures that can be taken, it is important to have an anticipation of the threat landscape against OES. By incorporating measures on threats such as where an attack can come from (e.g., spear-phishing because of lack of awareness from CI operators staff), these measures can help Kosovo's CI operators/owners to identify and mitigate the weak spots on their OES environment.

As seen from ENISA's 2020 threat landscape review [32], phishing attack is ranked as the third threat from which cyber-attacks can come from. Real-world CI cyber-attacks also showed us the relevance of the spear-phishing campaigns in gaining initial foothold on ICS/SCADA systems. After that, it is a matter of time before attackers can then plant malwares on these systems and control them. Meanwhile, ransomware attacks can also impact the availability of ICS/SCADA components such as HMI, from where CI operators cannot be updated on the latest data in their OES environment. This could cause health issues in the population of Kosovo such as the poisoning of water plants by not allowing CI operators to monitor the chemical levels on their water plants, and therefore, prohibiting them from the ability to take preventive measures. As shown from the TRITON attack [20], a proper cooperation mechanism between Kosovo's cyber security community and CI owners, would help Kosovo on its threat-intelligence capabilities from which the level of risks and threats on its OES would be lowered.

Page 11 of Kosovo's National Cyber Security Strategy (NCSS) [10] briefly mentions motivations that threat actors can use to attack Kosovo's cyberspace. Special attention is given to CI from which the strategy recognizes that OES environment is more frequently becoming a target of cyber-attacks. The strategy also recognizes that awareness raising also helps on shrinking the threat landscape against Kosovo's IT systems and the risks from cyber-attacks should not be underestimated.

Kosovo's law on CI (see Article 3 paragraph 1.14) defines risk analysis as "consideration of relevant threat scenarios in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure" [11] and requires Kosovo's CI owners to include the risk analysis in their OSP.

As shown from recommendation R1.21 (page 46) of the World Bank cyber security capacity review report on the Republic of Kosovo [16], the Republic of Kosovo has yet to establish a mechanism for the exchange of threat and vulnerability information between CI owners. Therefore, as a proper threat exchange mechanism does not exist nationally on Kosovo's CI owners and other relevant institutions, the author rates this criterion as red.

5.1.6 Criterion 6: Protection Mechanisms

Paragraph 1 in Article 14 of NIS Directive [15] requires EU MS to manage the risks posed to the security of their respective OES and relevant network and information systems, by taking appropriate and proportionate organisational and technical measures.

Meanwhile, as described in chapter 2 of NIS CG reference document on security measures for OES [29], some general principles should be taken into account when EU MS create their security measures on protecting OES. The security measures should be:

- **Effective:** Increase the cyber security of OES in relation to the current and foreseen threat landscape.
- **Tailored:** Avoiding unnecessary effort and duplication by having the most impact on OES cyber security.
- **Compatible:** Addressing basic and common security vulnerabilities of OES despite their sector.
- **Proportionate:** To the OES risks by avoiding unnecessary burden and prioritising only necessary security controls based on those risks.
- **Concrete:** Ensuring that the security measures are implementable by OES and contribute to the reinforcement of their cyber security.
- **Verifiable:** Ensuring that CI operators/owners are able to provide proof that the security policies are implemented effectively (e.g. security audit carried out by competent authority or a qualified auditor as described in paragraph 2, point (b) of NIS Directive's Article 15 [15]).

- **Inclusive:** Taking into account all security domains which may contribute on reinforcing the cyber security of OES, including physical security of information systems. [29]

Meanwhile, chapter 3 (part 2) of [29] also recommends architectural protection measures on OES such as system configuration and segregation, traffic filtering and cryptography. In addition, section 2.4 of the same chapter, also requires from CI operators to develop and implement a procedure for security maintenance that is in accordance with its ISSP. This includes the obligation on the operator to inform on any vulnerability and corrective security measures that concern CIS resources when it is installing any new version or corrective measure against that resource.

As seen from lessons-learned from real-world CI cyber-attacks described on section 3.3 of this thesis, protection measures such as proper configuration and patching mechanism of network and information systems that affect ICS/SCADA systems of an OES, are also important to be included in a proper protection mechanism. These measures, together with architectural measures such as network segmentation, would make it harder for an attacker to access ICS/SCADA systems.

It is in the author's point of view on emphasizing the fact that all of the protection measures mentioned above would have a really low impact on the improvement of cyber security of OES, if they do not have a proper implementation mechanism.

Article 3, Paragraph 1.12 of Kosovo's law on CI defines OSP as "a plan that identifies all of the owner/operator's critical infrastructure assets and establishes relevant security solutions for their protection" [11]. In addition, the description of security methods and procedures that need to be followed by the respectable CI owner or operator is also one of the main elements of OSP. Because the identification of OES was evaluated in criterion 1 by the author, the focus of this criterion will be in the second part of the OSP definition, namely establishing relevant security solutions on the protection of OES.

Article 9 of Kosovo's law on CI describes the measures that an OES located in Kosovo should take in order to properly implement its OSP. Paragraph 3 explains that these measures are designed to protect Kosovo's equivalent OES against potential accidents or incidents. Some of the measures that shall be included are:

- A proper risk analysis which takes into account different scenarios based on threats and vulnerability of each OES component as well as possible consequences in the event of operation disruptions on the CI (paragraph 3.2).
- Relevant dependencies and interdependencies (paragraph 3.4).
- Permanent security measures such as technical measures (installation of access control, protection, and prevention measures); awareness raising and training. (paragraph 4.1). [11]

In addition, paragraph 7 of article 9 also makes OSP or equivalent plans provided by owners/operators of Kosovo's CI a confidential document, by requiring from Kosovo's MIA to not disclose the relevant OSP to the public.

As shown from section 4.2, the author found many publicly available information on Kosovo's electric-energy and water-supply OES sectors. Pictures of operational rooms; usage of end-of-life OS; SCADA architecture diagrams; information on software, vendors and standards being used; are some of the concerns which Kosovo's CIP policies should take into account when implementing its protection mechanism, by prohibiting that this kind of information be publicly available. In addition, based on section 4.2.2 of this thesis, and section 1.3 (page 38) of the World Bank cyber security capacity review report on the Republic of Kosovo [16], the maintenance of two SCADA systems that Kosovo's largest water company use is outsourced to a Bulgarian contractor. This information makes the author assume that patching and configuration of these SCADA systems is also made from this contractor. This can have bad implications on implementing a proper protection mechanism on these systems, as in the case of any misconfiguration or vulnerability not being patched in time. This can result in cyber breach to the external contractor and these SCADA systems, where the respectable contractor can tend to hide that breach in order to save its reputation.

Even though there is proper documentation and planning on guiding Kosovo's OES on the required protection measures, such as how to implement properly an OSP, Kosovo still lacks behind in taking measures to have a full and proper protection mechanism on CI. Lack of protective measures such as prohibition of sensitive information being public; usage of latest operating systems (section 4.2); or leaving the maintenance of Kosovo's ICS/SCADA systems to its local CI operator staff; show that Kosovo still has to work on

the guidance derived from its CIP policies related to protective measures for OES. Therefore, the author rates this criterion as yellow.

5.1.7 Criterion 7: Incident Response Capacities

Article 4 (paragraph 7) of NIS Directive [15] defines the term "incident" as an event that can have an actual adverse effect on the security of network and information systems. An example of this would be a ransomware attack on the operational rooms of Kosovo's electric-energy sector (shown in section 4.2). Meanwhile paragraph 8 of the same article defines incident handling as "procedures supporting the detection, analysis and containment of an incident". These procedures should be properly and clearly defined, in order to have quicker reaction responses against possible cyber-attacks on Kosovo's OES sectors. The incident factor is also relevant when identifying OES. Article 5 (point c paragraph 2) of NIS Directive gives guidance to EU MS that disruptive effects on the services of OES should also be taken into account when identifying their respectable OES. This is also an important point for Kosovo because, as there is only one electric distribution company for the entire country (KEDS), an attack on KEDS would have significant impact on the daily lives of Kosovo's citizens. Article 14 of NIS Directive also gives guidance on incident notification procedures. Paragraph 3 of this article says that the OES are obliged, without undue delay, to notify competent authorities of impacted countries on incidents that are disrupting the continuity of their services. Meanwhile the significance of an incident, as shown in paragraph 4 of Article 14, is based on the duration, number of users affected and the geographic spread of the incident.

Section 2.1 (point 5) of reference document on incident notification for OES [30] also recommends to EU MS to periodically review, and if necessary, improve their incident response mechanisms. This point is really important for Kosovo, as when Kosovo develops an incident response mechanism, it should also take into account the review of its incident response mechanism in order to make it relevant to latest cyber risks and threats.

Section 6.4 in Kosovo's cyber security strategy [10] mentions that in order for a CERT/CSIRT to be operationally capable and properly mitigate and respond an incident, the following requirements should be met from Kosovo's CERT/CSIRT's:

- A necessary infrastructure.

- Staffing of CERT/CSIRT with an appropriately trained personnel. [10]

Unfortunately, as seen from section D1.2 of the World Bank report on Kosovo's cyber security capacity assessment [16], Kosovo's national CERT (KOS-CERT) has a severe personnel shortage which is operated by a staff of two. Therefore, because of this capacity disadvantage, the unit receives a relatively low number of direct incident reports. In addition, as Kosovo is not part of UN, and therefore of IANA, a TLD does not exist for the Republic of Kosovo. This means that a national digital sovereignty is missing, and all IP addresses of network and information systems located in Kosovo point either to Albania or Serbia. If one of these systems experiences an incident, it is a matter of Serbia or Albania if they report the incident to Kosovo. This does not differ for Kosovo's CI environment. Because a TLD is missing for Kosovo, we can take into account the following scenario: if an ICS/SCADA system located in Kosovo experiences a cyber incident, even if there is a proper monitoring mechanism on cyber-attacks happening in Kosovo, KOS-CERT cannot verify that the ICS/SCADA system is located in Kosovo, as its IP address location will point either to Albania or Serbia.

The lack of digital sovereignty and staffing of KOS-CERT has a direct impact for Kosovo's incident response capabilities to mitigate and react quick against potential incidents on its CI. This shows that a correct implementation mechanism of Kosovo's policies on incident response does not exist. Therefore, the author rates this criterion as red.

5.2 Summary of Synthesis

The following matrix summarises the findings of synthesis, which were discussed in section 5.1:

Table 2. The matrix that visualises the summary of synthesis

Criterion	**Requirements of EU Guidelines on CIP**	**Author's findings on Kosovo's CIP policies and implementation mechanisms**	**Rating**
Identification of OES	NIS Directive [15] requires that all national OES should be identified.	Law on CI [11] defines what is an OES and how to identify them but based on conversations with Kosovo's relevant authorities, a	●

		proper institutional mechanism on identifying Kosovo's OES is missing.	
Single Point of Contact	NIS Directive requires this role which can be assigned to a single authority and the role should be clearly defined.	Law on CI clearly defines the role of single point of contact and assigns it to Kosovo's MIA.	▲
Cyber Awareness	NIS CG reference document on security measures of OES [29] recommends awareness raising program to CI operators staff.	As shown from the World Bank cyber security capacity assessment report on Kosovo [16], an institutional mechanism on raising awareness to CI operators on threats or risks derived from cyberspace does not exist. In addition, publicizing pictures of Kosovo's CI operational rooms (section 4.2) on the Internet shows another lack of awareness from CI operators staff.	●
Penalties	NIS Directive requires imposing penalties to OES who do not adhere to national CIP policies.	Law on CI clearly defines penalties to OES who do not adhere to Kosovo's CIP policies which range from 25,000 to 40,000 euros to CI owners/operators.	▲
Threat Landscape	ENISA threat landscape guideline [32] emphasize the importance of cooperation mechanisms between relevant institution regarding threat landscape, that needs to be	As the World Bank cyber security capacity assessment report on Kosovo shows, a proper threat exchange sharing mechanism between CI owners and relevant authorities does not exist.	●

	included in policies of relevant nations.		
Protection Mechanism	NIS Directive requires nations to manage the risks posed to the security of their respective OES network and information systems that are being used in their operations. This is done by taking appropriate and proportionate organisational and technical measures. NIS CG reference document on security measures of OES explain in detail these measures such as patching and updating of systems, system segregation and traffic filtering.	Law on CI requires from Kosovo's OES to submit a security plan, which is comprehensive and detailed on protection measures. Unfortunately, there is lack of implementing these security plans properly from OES sectors. As shown in section 4.2, electric-energy sector of Kosovo still uses end-of-life operating systems, and there are no restrictions such as prohibition on taking pictures of CI operational rooms and uploading them in Internet. Usage of vulnerable communication protocols (GSM) in Kosovo's CI water-supply sector [28] shows also another concern which can be used by potential cyber-attackers. In addition, the maintenance of some of its SCADA systems in the water-supply sector is outsourced to foreign countries [139], which can impact in the implementation of the protection measures. An example of this impact can be that the local water-supply staff does not know if the SCADA systems have been updated or have the latest patch against a potential vulnerability.	■

Incident Response Capabilities	NIS Directive requires nations to notify competent authorities, without undue delay, on incidents that are having impact on continuity of their services. The reference document on incident notification for OES [30] also recommends to periodically review, and if necessary, improve the incident response mechanisms of the respectable nations.	One of the requirements for Kosovo's CERT/CSIRT's, as shown from Kosovo's cyber security strategy [10], is to have a proper and trained staff. Unfortunately, the implementation of this requirement is not being done from Kosovo's national CERT (KOS-CERT). Because of the lack of staff, hence capacity disadvantage, KOS-CERT receives a relatively low number of direct incident reports [16]. Another factor that weakens Kosovo's incident response capabilities is the lack of digital sovereignty, where Kosovo still does not own a Top-Level Domain (TLD) and all IP addresses of IT systems located in Kosovo, are registered and geo-located either in Albania or Serbia.	●

5.3 Recommendations on Improving Kosovo's CIP policies

Based on synthesis findings discussed in section 5.1 and matrix shown in section 5.2, the author recommends to Kosovo's relevant authorities on CIP, the inclusion of the following measures related to the improvement of current CIP policies as well as developing future ones:

- **Implementing a proper institutional mechanism on identification of OES:** Author found that the Republic of Kosovo does not currently have a proper institutional mechanism that identifies its OES. The CIP policies of the Republic of Kosovo cannot help on protection and incident response of Kosovo's OES if relevant Kosovo authorities do not have a list of organizations that fall in the

category of CI. Therefore, the Republic of Kosovo should create and functionalise as soon as possible a proper institutional mechanism which identifies the OES located in Kosovo. This can help CI owners/operators to focus on other requirements such as OSP derived from law on CI [11] whereas the relevant Kosovo's institutions can monitor the protection and incident response measures of relevant CI owners/operators.

- **Making cyber-awareness raising trainings/programs mandatory to CI operators staff:** Kosovo's cyber security strategy [10] and law on CI [11] correctly describe the importance of awareness raising on protecting Kosovo's network and information systems. Unfortunately, the author, as shown in section 4.2 of this thesis, found that Kosovo's CI staff does not have proper awareness on the risks and threats that can derive by publicizing pictures of CI operational rooms on the internet. By zooming in the pictures, author found end-of-life operating systems being used in electric-energy sector [21] [23], as well as vendors being used in this sectors SCADA systems [25]. In addition, as seen from the World Bank cyber security capacity assessment report on Kosovo [16], CI operators staff are not required to go through awareness raising programs/trainings. As shown from the real-world cyber-attacks in CI environment of Ukraine [19], Florida [93] or Saudi-Arabia [20], all of these cyber-attacks started with tricking the respectable CI staff on opening malicious emails from where attackers gained initial foothold. The information seen in section 4.2 should also raise concern to Kosovo's relevant authorities, as they can be used from potential threat actors on attacking Kosovo's CI. This shows that current as well as future CIP policies, should require that cyber-awareness trainings/programs should be mandatory for Kosovo's CI operators staff.
- **Development of a proper threat-exchange mechanism between CI owners and Kosovo's relevant institutions:** Identification of threat landscape helps on anticipating from where cyber-attacks can come from which can help on improving the national incident response mechanism of Kosovo. Unfortunately, as seen from the World Bank report on cyber security capacity assessment of Kosovo [16], a threat-exchange mechanism between Kosovo's CI owners and relevant institutions does not exist. In an example where Kosovo's national CERT (KOS-CERT) anticipates an immediate threat to Kosovo's CI, the lack of this mechanism can have severe consequences such as CI owners not being informed

in time in relation to that particular threat and taking precaution measures on mitigating it. Kosovo's relevant authorities should include this threat-exchange mechanism as mandatory on the future laws of cyber security.

- **Requiring CI owners/operators to follow best-practice protection measures on OES derived from EU guidelines:** Kosovo's current CI owners/operators do not follow best-practices in relation to protecting its ICS/SCADA systems. Usage of end-of-life operating systems [21] [23] or vulnerable communication protocols such as GSM [28] on electric-energy and water-supply OES sectors, can make it easier for attackers to gain initial foothold of these OES sectors ICS/SCADA systems. By making Kosovo's CIP policies to take into consideration protective measures such as: regularly patching and updating network and information systems that Kosovo's ICS/SCADA systems depend on; having a proper backup policy on the data of ICS/SCADA systems; or taking defensive measures such as traffic filtering, as described from the NIS CG reference document on security measures of OES [29], can help Kosovo to have a better ecosystem of protection on the systems that OES rely on.
- **Developing and maintaining a proper national incident response mechanism:** The World Bank report on cyber security capacity assessment of Kosovo [16] shows that Kosovo's national CERT (KOS-CERT) has lack of staff capacity, which directly impacts the numbers of incidents being reported to this institution. Additionally, because of political problems, the Republic of Kosovo is still not part of UN. This affects its incident report capacities as it is not a member of IANA and hence does not have digital sovereignty. If an information or network system that is part of ICS/SCADA systems located in Kosovo gets attacked, the first country that will be notified about this is either Albania or Serbia. Therefore, it is the responsibility of these countries to report the incident to Kosovo's relevant authorities. Kosovo should solve these issues by improving the capacities of KOS-CERT and also trying to find a workaround to be a member of IANA organization so that it has its own Top-Level Domain (TLD). In addition, KOS-CERT should have a clear mandate on reporting and monitoring cyber incidents that affect Kosovo's OES. Current and future CIP policies should focus in above-mentioned points as well as developing a better inter-institutional cooperation mechanism on notification and responding processes against potential future cyber incidents in Kosovo's OES. This can be done, by taking the NIS Directive [15] and the

reference document on incident notification for OES [30] as a guidance on properly developing and maintaining Kosovo's incident response mechanism.

6 Conclusion

In this thesis, Kosovo's CIP policies were evaluated against EU guidelines using a list of policy evaluation criteria on Kosovo's CIP and a semaphore model, which were both developed by the author. The structure of the semaphore model and its rating system were based on the requirements that derive from EU guidelines. These guidelines were analysed, and they provide clearly defined instructions that can help nations on improving their CIP policies and implementation mechanisms. In addition, technical papers on real-world CI cyber-attacks were analysed. From these previous real-world CI cyber-attacks, a lessons learned section was created by the author, which complemented the EU guidelines. These real-world CI cyber-attacks showed the process and impact of a successful cyber-attack from a real-world standpoint. Therefore, it is important for Kosovo on fulfilling the lessons learned derived from these cyber-attacks. This analysis was followed by the synthesis, where the author applied the semaphore model on Kosovo's CIP policy criteria by taking into account Kosovo's current CIP policies and OES environment on electric-energy and water-supply sectors.

Using the findings from the synthesis, the author found many gaps on Kosovo's CIP policies adherence to NIS Directive and ENISA guidelines. Kosovo is still missing a proper institutional mechanism on the identification of the OES located in its territory. This goes against one of the main requirements of the NIS Directive which requires from EU MS to identify all of the OES located in their territory. As seen from the real-world CI cyber-attacks, all of these attacks started with phishing techniques against the target CI operators staff to gain initial foothold on their ICS/SCADA systems. The lack of a proper and compulsory awareness program on Kosovo's CI operator staff, makes it easier for potential cyber-attackers that target Kosovo's OES environment to gain initial foothold on those ICS/SCADA systems. The lack of awareness from CI operator's staff is also observed on the impact that it can have on the protection mechanisms. The author found publicly available information on Kosovo's electric-energy and water-supply sectors CI components such as the operating systems being used or the communication protocols. These type of information make it easier for attackers to develop their TTPs as they are already aware on what operating systems or communication protocols are being used in Kosovo's OES environment. This increases the possibility that the cyber-attack will be successful. From this research, the author also found that Kosovo's national CERT

(KOS-CERT) has a lack of staff which impedes its ability to properly respond against future cyber incidents in the Republic of Kosovo. Additionally, the lack of a proper threat-exchange mechanism between CI owners and Kosovo's relevant institutions as well as the lack of Kosovo's digital sovereignty, would impede Kosovo's ability to quickly identify a cyber-incident on its OES environment. This would result in a slow incident response mechanism by which attackers can already erase their tracks. As seen from ENISA guidelines and real-world CI attacks, this can have a big impact on Kosovo's citizens where there could be electricity interruptions or even poisoning of their water-supply systems. Therefore, based on the author's observations of the facts mentioned above, Kosovo's current CIP policies are not prepared on properly responding against a cyber incident on Kosovo's electric-energy or water-supply CI sectors.

In order to improve Kosovo's current CIP state of affair in properly responding against a potential cyber incident on Kosovo's OES environment, the author offered some recommendations. First and foremost, Kosovo should have already implemented a proper institutional mechanism on identifying its OES. This would help Kosovo's relevant incident response institutions such as KOS-CERT to quickly identify on which OES the cyber-attack happened and measure the scope of this cyber incident. In addition, by knowing the details of the respectable OES, KOS-CERT can measure the impact that this cyber incident can have, and quickly inform other relevant authorities, which then should ensure alternate plans on the continuity of the essential service. This brings us to the other recommendation by the author, where Kosovo's relevant institutions should improve their threat-exchange cooperation mechanisms. By having a proper threat anticipation, KOS-CERT and relevant authorities can already know what CI component of OES was attacked and how to respond against it. This brings us to another point where Kosovo's CI operator staff should already have proper training on cyber-awareness and protection measures on OES. Even though cyber incidents cannot fully be mitigated, the impact of the cyber incident would be lower if Kosovo's CI operator staff would had already implemented some measures on their CI environment. By taking into account these recommendations on current and future CIP policies, the relevant authorities in the Republic of Kosovo would help on increasing Kosovo's CI resiliency, as well as the preparation to respond against a cyber incident on Kosovo's OES environment successfully and quickly.

As the EU guidelines provide clear instructions to nations on developing or improving their CIP policies and implementation mechanisms, the semaphore model that the author

created in this thesis can be used by CI policy makers of other countries to evaluate their respectable CIP state of affair.

References

[1] The White House, “PRESIDENTIAL DECISION DIRECTIVE/NSC-63,” 1998. https://fas.org/irp/offdocs/pdd/pdd-63.htm.

[2] K. E. Hemsley and D. R. E. Fisher, “History of Industrial Control System Cyber Incidents,” *INL/CON-18-44411-Revision-2*, no. December, pp. 1–37, 2018, doi: https://doi.org/10.2172/1505628.

[3] United Nations Office of Counter Terrorism, “The protection of critical infrastructures against terrorist attacks: Compendium of good practices,” 2018. https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf.

[4] The White House, “Presidential Directive/Hspd-7,” 2003. https://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html.

[5] ENISA, “About ENISA - The European Union Agency for Cybersecurity.” https://www.enisa.europa.eu/about-enisa.

[6] Commission of the European Communities, “Critical Infrastructure Protection in the fight against terrorism,” *Communication from the Commision to the Council and the European Parliament*, 2004. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004DC0702.

[7] Commission of the European Communities, “European Programme for Critical Infrastructure Protection,” *Communication from the Commision to the Council and the European Parliament*, 2006. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786.

[8] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Secur. Priv.*, vol. 9, no. 3, pp. 49–51, 2011, doi: 10.1109/MSP.2011.67.

[9] European Commission, “Directive on Security of Network and Information Systems,” 2016. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2422 (accessed Oct. 04, 2020).

[10] Kosovo’s Ministry of Internal Affairs, “Kosovo National Cyber Security Strategy and Action Plan 2016-2019,” 2015. [Online]. Available: http://www.kryeministri-ks.net/repository/docs/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_per_publikim_1202.pdf.

[11] Assembly of Republic of Kosovo, “LAW No. 06/L –014 ON CRITICAL INFRASTRUCTURE,” *OFFICIAL GAZETTE OF THE REPUBLIC OF KOSOVO*, 2018. https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=16313

(accessed Oct. 06, 2020).

[12] The World Bank, “Population, total - Kosovo,” 2019. https://data.worldbank.org/indicator/SP.POP.TOTL?end=2019&locations=XK&start=2019&view=bar.

[13] STIKK - Kosovo ICT Association, “Internet Penetration and Usage in Kosovo National Quantitative Survey October 2019,” 2019. [Online]. Available: https://stikk.org/wp-content/uploads/2019/11/STIKK_IK_Report_Internet_Penetration_V3-final-1.pdf.

[14] The European Commission, “Green Paper on a European programme for critical infrastructure protection,” 2005. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576 (accessed Oct. 08, 2020).

[15] European Parliament and Council of European Union, “NIS Directive,” *Official Journal of the European Union*, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=en (accessed Oct. 08, 2020).

[16] Global Cyber Security Capacity Centre, “CYBERSECURITY CAPACITY REVIEW: Republic of Kosovo,” 2020. Accessed: Oct. 08, 2020. [Online]. Available: https://mzhe-ks.net/repository/docs/Cybersecurity_Capacity_Assessment_for_the_Republic_of_Kosovo_2019.pdf.

[17] Sense Cyber Research Center, “A Look Inside Banka Ekonomike’s Data Breach,” 2020. https://sense.co.com/2020/05/01/banka-ekonomike-rks-breach/ (accessed Oct. 08, 2020).

[18] Assembly of Republic of Kosovo, “LAW NO. 06/L –082 ON PROTECTION OF PERSONAL DATA,” *Off. Gaz. Repub. KOSOVO*, p. 52, 2019, [Online]. Available: https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=18616.

[19] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” *Electr. Inf. Shar. Anal. Cent.*, p. 36, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[20] A. Di Pinto, Y. Dragoni, and A. Carcano, “TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, Its Communications and Its OT Payload,” *Black Hat USA*, 2018.

[21] Kosovo Energy Corporation J.S.C., “Power plant ‘Kosova B,’” *Kosovo Energy Corporation J.S.C.*, 2021. http://kek-energy.com/kek/termocentrali-kosova-b/ (accessed Apr. 06, 2021).

[22] KOMTEL, “Design and Installation of SCADA System in KOSTT,” 2011. http://www.komtelpe.com/komtel/en/electrical-engineering/energy/transmission/design-and-installation-of-scada-system-in-kostt/ (accessed Mar. 25, 2021).

[23] KOMTEL, “Upgrade and Update of KOSTT SCADA EMS System,” 2014. http://www.komtelpe.com/komtel/en/electrical-engineering/energy/transmission/upgrade-and-update-of-kostt-scada-ems-system/ (accessed Mar. 25, 2021).

[24] KOSTT, “Transmission Development Plan 2020-2029,” Pristina, 2019.

[25] KEDS, “Energy 2019,” *KEDS*, no. 36, Pristina, Aug. 2019.

[26] KEDS, “Energy 2020,” *KEDS*, no. 39, Pristina, Dec. 2020.

[27] KEDS, “Development Plan of Distribution System Operator 2019-2028,” 2019. https://www.ero-ks.org/2019/Tregu/Plani Zhvillimor i OSSH_2019-2028_eng.pdf (accessed Mar. 25, 2021).

[28] The World Bank, “REPUBLIC OF KOSOVO: Water Security and Canal Protection Project,” 2016. http://documents1.worldbank.org/curated/en/115821473965587777/pdf/PAD-disclosable-version-P133829-2016-09-09-09132016.pdf (accessed Nov. 25, 2020).

[29] NIS Cooperation Group, “Reference document on security measures for Operators of Essential Services. CG Publication 01/2018,” 2018. https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (accessed Nov. 20, 2020).

[30] NIS Cooperation Group, “Reference document on Incident Notification for Operators of Essential Services,” 2018. https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf (accessed Nov. 25, 2020).

[31] ENISA, “Communication network dependencies for ICS/SCADA Systems,” 2017. [Online]. Available: file:///C:/Users/anaso/Downloads/WP2016 1-2 1 Annual Threat Landscape Report.pdf.

[32] ENISA, “ENISA Threat Landscape: The year in review,” *ENISA*, 2020. https://www.enisa.europa.eu/publications/year-in-review (accessed Nov. 25, 2020).

[33] P. Hoffman, W. Bryan, and a Lippert, “Comparing the Impacts of the 2005 and 2008 Hurricanes on US Energy Infrastructure,” *... Energy Reliab. US Dep. Energy, ...*, no. February, 2009, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Comparing+the+Impacts+of+the+2005+and+2008+Hurricanes+on+U.S.+Energy+Infrastructure#0%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Comparing+the+Impacts+of+the+2005+and+2008.

[34] J. R. Santos, L. C. Herrera, K. D. S. Yu, S. A. T. Pagsuyoin, and R. R. Tan, “State of the Art in Risk Analysis of Workforce Criticality Influencing Disaster Preparedness for Interdependent Systems,” *Risk Anal.*, vol. 34, no. 6, pp. 1056–

1068, 2014, doi: 10.1111/risa.12183.

[35] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” *Survival (Lond).*, vol. 53, no. 1, pp. 23–40, 2011, doi: 10.1080/00396338.2011.555586.

[36] W. J. Broad, J. Markoff, and D. E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *The New York Times*, 2011. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

[37] S. S. Baggott and J. R. Santos, “A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid,” *Risk Anal.*, vol. 0, no. 0, 2020, doi: 10.1111/risa.13511.

[38] X. Zhang, K. Chandramouli, D. Gabrijelcic, T. Zahariadis, G. Giunta, and I. J. Stefan, “NEW-AGE THREAT OF DRONES AND HUMAN INTRUSION Queen Mary University of London ; † Venaka Media Limited ;,” pp. 3–6, 2020.

[39] I. Costea, C. Dumitrescu, and F. Nemtanu, “Advanced Terrestrial and Aerial Monitoring and Inspection System for Critical Infrastructures,” *Proc. 10th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2018*, pp. 2018–2021, 2019, doi: 10.1109/ECAI.2018.8679079.

[40] P. Oman and E. O. Schweitzer, “Concerns About Intrusions Into Remotely Accessible Substation Controllers and Scada Systems,” *Power*, vol. 20, no. November 2000, pp. 1–16, 2000, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.20.6519&rep=rep1&type=pdf.

[41] R. Carlson, “Sandia SCADA Program High-Security SCADA LDRD Final Report,” *Prod.Sandia.Gov*, no. April, 2002, [Online]. Available: http://prod.sandia.gov/techlib/access-control.cgi/2002/020729.pdf.

[42] A. Risley, J. Roberts, and P. LaDow, “Electronic security of real-time protection and SCADA communications,” *5th Annu. West. Power Deliv. Autom. Conf.*, 2003, [Online]. Available: http://www2.selinc.com/techpprs/6150.pdf.

[43] S. Adepu, N. K. Kandasamy, J. Zhou, and A. Mathur, “Attacks on smart grid: power supply interruption and malicious power generation,” *Int. J. Inf. Secur.*, vol. 19, no. 2, pp. 189–211, 2020, doi: 10.1007/s10207-019-00452-z.

[44] iTrust Centre for Research in Cyber Security, “Electric Power and Intelligent Control,” 2020. https://itrust.sutd.edu.sg/testbeds/electric-power-intelligent-control-epic/ (accessed Oct. 18, 2020).

[45] MITRE, “Dropbear SSH Vulnerabilities,” 2020. https://www.cvedetails.com/vulnerability-list/vendor_id-15806/Dropbear-Ssh-Project.html (accessed Oct. 18, 2020).

[46] S. Adepu, E. Kang, and A. P. Mathur, “Challenges in secure engineering of critical infrastructure systems,” *Proc. - 2019 34th IEEE/ACM Int. Conf. Autom. Softw. Eng. Work. ASEW 2019*, no. 1, pp. 61–64, 2019, doi:

10.1109/ASEW.2019.00030.

[47] K. Pan, A. Teixeira, C. D. Lopez, and P. Palensky, “Co-simulation for cyber security analysis: Data attacks against energy management system,” *2017 IEEE Int. Conf. Smart Grid Commun. SmartGridComm 2017*, vol. 2018-Janua, pp. 253–258, 2018, doi: 10.1109/SmartGridComm.2017.8340668.

[48] G. Tzokatziou, L. A. Maglaras, and H. Janicke, “Insecure by Design: Using Human Interface Devices to exploit SCADA systems,” *3rd Int. Symp. ICS SCADA Cyber Secur. Res. 2015*, no. June, 2015, doi: 10.14236/ewic/ics2015.13.

[49] P. Matoušek, O. Ryšavý, M. Grégr, and V. Havlena, “Flow based monitoring of ICS communication in the smart grid,” *J. Inf. Secur. Appl.*, vol. 54, 2020, doi: 10.1016/j.jisa.2020.102535.

[50] B. Hyder and M. Govindarasu, “Optimization of cybersecurity investment strategies in the smart grid using game-theory,” *2020 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2020*, pp. 1–5, 2020, doi: 10.1109/ISGT45199.2020.9087634.

[51] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, “Kill chain for industrial control system,” *MATEC Web Conf.*, vol. 173, pp. 1–5, 2018, doi: 10.1051/matecconf/201817301013.

[52] A. P. Fournaris, C. Dimopoulos, K. Lampropoulos, and O. Koufopavlou, “Anomaly detection trusted hardware sensors for critical infrastructure legacy devices,” *Sensors (Switzerland)*, vol. 20, no. 11, pp. 1–19, 2020, doi: 10.3390/s20113092.

[53] D. Krauß and C. Thomalla, “Ontology-based detection of cyber-attacks to SCADA-systems in critical infrastructures,” *2016 6th Int. Conf. Digit. Inf. Commun. Technol. Its Appl. DICTAP 2016*, pp. 70–73, 2016, doi: 10.1109/DICTAP.2016.7544003.

[54] Ericsson, “Ericsson Mobility Report: 5G uptake even faster than expected,” 2019. https://www.ericsson.com/en/press-releases/2019/6/ericsson-mobility-report-5g-uptake-even-faster-than-expected (accessed Oct. 24, 2020).

[55] Mordor Intelligence LLP, “Industrial Internet of Things (IIoT) Market - Growth, Trends, Forecasts (2020 - 2025),” 2020. https://www.reportlinker.com/p05954256/Industrial-Internet-of-Things-IIoT-Market-Growth-Trends-Forecasts.html?utm_source=GNW (accessed Oct. 24, 2020).

[56] L. A. Maglaras *et al.*, “Cyber security of critical infrastructures,” *ICT Express*, vol. 4, no. 1, pp. 42–45, 2018, doi: 10.1016/j.icte.2018.02.001.

[57] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (IIoT): An analysis framework,” *Comput. Ind.*, vol. 101, no. June, pp. 1–12, 2018, doi: 10.1016/j.compind.2018.04.015.

[58] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, “Secure Internet of

Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019, doi: 10.1109/ACCESS.2019.2920763.

[59] T. Limba, A. Stankevičius, and A. Andrulevičius, "Industry 4.0 and national security: The phenomenon of disruptive technology," *Entrep. Sustain. Issues*, vol. 6, no. 3, pp. 1528–1535, 2019, doi: 10.9770/jesi.2019.6.3(33).

[60] European Union's Horizon 2020 research and innovation programme, "CHARIOT - About," 2020. https://www.chariotproject.eu/about (accessed Oct. 25, 2020).

[61] K. Loupos *et al.*, "Cognition enabled IoT platform for industrial IoT safety, security and privacy-the CHARIOT project," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2019-Septe, 2019, doi: 10.1109/CAMAD.2019.8858488.

[62] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 450–466, 2018, doi: 10.1016/j.clsr.2017.12.004.

[63] J. E. Rubio, R. Roman, and J. Lopez, "Integration of a Threat Traceability Solution in the Industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 16, no. 10, pp. 6575–6583, 2020, doi: 10.1109/TII.2020.2976747.

[64] I. F. Mikhalevich and V. A. Trapeznikov, "Critical Infrastructure Security: Alignment of Views," *2019 Syst. Signals Gener. Process. F. Board Commun. SOSG 2019*, 2019, doi: 10.1109/SOSG.2019.8706821.

[65] A. T. Ledo Iglesias, "Analysis of social and legal issues on critical infrastructures in Spain," *2019 6th Int. Conf. eDemocracy eGovernment, ICEDEG 2019*, pp. 375–377, 2019, doi: 10.1109/ICEDEG.2019.8734451.

[66] C. Große and P. M. Olausson, "Blind spots in interaction between actors in Swedish planning for critical infrastructure protection," *Saf. Sci.*, vol. 118, no. April, pp. 424–434, 2019, doi: 10.1016/j.ssci.2019.05.049.

[67] P. M. Olausson, "Planning for resilience in the case of power shortage: The Swedish STYREL policy," *Cent. Eur. J. Public Policy*, vol. 13, no. 1, pp. 12–22, 2019, doi: 10.2478/cejpp-2019-0004.

[68] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016, doi: 10.1016/j.cose.2015.09.009.

[69] M. Bartnes Line, I. Anne Tøndel, and M. G. Jaatun, "Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations," *Int. J. Crit. Infrastruct. Prot.*, vol. 12, pp. 12–26, 2016, doi: 10.1016/j.ijcip.2015.12.003.

[70] T. Plėta, M. Tvaronavičienė, and S. Della Casa, "Cyber effect and security

management aspects in critical energy infrastructures," *Insights into Reg. Dev.*, vol. 2, no. 2, pp. 538–548, 2020, doi: 10.9770/ird.2020.2.2(3).

[71] L. Slipachuk, S. Toliupa, and V. Nakonechnyi, "The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine," *2019 3rd Int. Conf. Adv. Inf. Commun. Technol. AICT 2019 - Proc.*, pp. 451–454, 2019, doi: 10.1109/AIACT.2019.8847877.

[72] G. Settanni *et al.*, "A collaborative cyber incident management system for European interconnected critical infrastructures," *J. Inf. Secur. Appl.*, vol. 34, pp. 166–182, 2017, doi: 10.1016/j.jisa.2016.05.005.

[73] Transport Research and Innovation Monitoring and Information System (TRIMIS), "European Control System Security Incident Analysis Network (ECOSSIAN)," 2017. .

[74] M. T. Holzleitner and J. Reichl, "European provisions for cyber security in the smart grid - an overview of the NIS-directive," *Elektrotechnik und Informationstechnik*, vol. 134, no. 1, pp. 14–18, 2017, doi: 10.1007/s00502-017-0473-7.

[75] T. Katulic, "Transposition of EU network and information security directive into national law," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, pp. 1143–1148, 2018, doi: 10.23919/MIPRO.2018.8400208.

[76] L. Maglaras, G. Drivas, K. Noou, and S. Rallis, "NIS directive: The case of Greece," *ICST Trans. Secur. Saf.*, vol. 4, no. 14, p. 154769, 2018, doi: 10.4108/eai.15-5-2018.154769.

[77] N. Antonia, "The Directive on security of network and information systems (NIS Directive) from a practical view – Challenges for the Aviation Industry," International Hellenic University, 2018.

[78] M. Shukla, S. D. Johnson, and P. Jones, "Does the NIS implementation strategy effectively address cyber security risks in the UK?," *2019 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2019*, 2019, doi: 10.1109/CyberSecPODS.2019.8884963.

[79] H. Carrapico and A. Barrinha, "The EU as a Coherent (Cyber)Security Actor?," *J. Common Mark. Stud.*, vol. 55, no. 6, pp. 1254–1272, 2017, doi: 10.1111/jcms.12575.

[80] D. Markopoulou, V. Papakonstantinou, and P. de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation," *Comput. Law Secur. Rev.*, vol. 35, no. 6, p. 105336, 2019, doi: 10.1016/j.clsr.2019.06.007.

[81] L. Peedu, "Implementation of Network and Information Systems Security Directive 2016 / 1148 in Republic of Estonia : Balancing Transparency and Secrecy," Tallinn University of Technology - TalTech, 2018.

[82] M. Kamola, P. Jaskola, and M. Amanowicz, “Decision Support System for Identification and Security Management of Essential and Digital Services,” *2019 Int. Conf. Mil. Commun. Inf. Syst. ICMCIS 2019*, pp. 1–7, 2019, doi: 10.1109/ICMCIS.2019.8842769.

[83] O. A. Michalec, D. Van Der Linden, S. Milyaeva, and O. Michalec, “Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures This paper is included in the Proceedings of the Sixteenth Symposium on Usab,” *Soups*, 2020.

[84] A.-I. Söderholm, “Threats and Challenges Around European Cyber Security Cooperation in the Context of the European Union Directive on Security of Network and Information Systems,” University of Jyväskylä, 2018.

[85] S. Dragojlo, “Kosovo Electricity Grid Starts Operating Independently from Serbia,” *Balkan Insight*, 2020. https://balkaninsight.com/2020/12/15/kosovo-electricity-grid-starts-operating-independently-from-serbia/ (accessed Jan. 21, 2021).

[86] P. Bosco, “Breaking the Ice: Gaining Initial Access,” 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/bestprac/breaking-ice-gaining-initial-access-36220.

[87] ENISA, “ENISA Threat Landscape 2020 - Malware,” *ENISA*, 2020. https://www.enisa.europa.eu/publications/malware (accessed Dec. 08, 2020).

[88] ENISA, “ENISA Threat Landscape 2020 - Ransomware,” *ENISA*, 2020. https://www.enisa.europa.eu/publications/ransomware (accessed Dec. 08, 2020).

[89] Microsoft, “Hackers hit Norsk Hydro with ransomware. The company responded with transparency,” *Microsoft*, 2019. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ (accessed Jan. 18, 2021).

[90] ENISA, “ENISA Threat Landscape 2020 - Main Incidents in the EU and Worldwide,” *ENISA*, 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents (accessed Nov. 28, 2020).

[91] P. de Wet, “Here’s how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions,” *Business Insider*, 2019. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7 (accessed Jan. 19, 2021).

[92] G. Stergiopoulos, “Power Sector Dependency On Time Service,” *ENISA*, 2020. https://www.enisa.europa.eu/publications/power-sector-dependency/at_download/fullReport (accessed Jan. 19, 2021).

[93] S. Kardon, “Florida Water Treatment Plant Hit With Cyber Attack,” *Industrial Defender*, 2021. https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/ (accessed Mar. 23, 2021).

[94] F. Robles and N. Perlroth, "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," *New York Times*, 2021. https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html (accessed Mar. 23, 2021).

[95] M. Rubio, "Tweet from Senator Marco Rubio on Florida City's Water Supply Cyber-Attack," *Twitter*, 2021. https://twitter.com/marcorubio/status/1358909642185859077?s=20 (accessed Mar. 23, 2021).

[96] TeamViewer, "TeamViewer," *TeamViewer*, 2021. https://www.teamviewer.com/en/products/teamviewer/ (accessed Mar. 23, 2021).

[97] U.S. CISA, "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure," *U.S. CISA*, 2018. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 (accessed Mar. 24, 2021).

[98] M. Assante and R. M. Lee, "The Industrial Control System Cyber Kill Chain," *SANS Institute*, 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297 (accessed Mar. 24, 2021).

[99] Galician Computer Company, "Public Information from ICS Vendor," 2015. http://galcomcomp.com/index.php/ru/nashi-proekty/15-proekt3-material-ru (accessed Mar. 24, 2021).

[100] MITRE, "Software: BlackEnergy 3," *MITRE*, 2020. https://collaborate.mitre.org/attackics/index.php/Software/S0004 (accessed Mar. 24, 2021).

[101] SecureList, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," *SecureList*, 2016. https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/ (accessed Mar. 24, 2021).

[102] MITRE, "Software: KillDisk," *MITRE*, 2021. https://collaborate.mitre.org/attackics/index.php/Software/S0016 (accessed Mar. 24, 2021).

[103] U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," *U.S. Department of Justice*, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (accessed Mar. 24, 2021).

[104] S. Xhafa and S. Spahiu, "Water recycling- waste water treatment plant at Badovc," *Environmental Science & Technology 2018*, 2018. https://www.imedpub.com/proceedings/water-recycling-waste-water-treatment-plant-at-badovc-1667.html (accessed Apr. 05, 2021).

[105] European Investment Bank, "Kosovo*: EIB invests €11 million for wastewater treatment in Gjilan/Gnjilane," 2020. https://www.eib.org/en/press/all/2020-133-

eib-invests-eur11-million-for-wastewater-treatment-in-gjilangnjilane-kosovo (accessed Apr. 05, 2021).

[106] Instrumentation Tools, "SIS – Safety Instrumented System Example," *Instrumentation Tools*, 2020. https://instrumentationtools.com/sis-example-water-treatment-oxygen-purge-system/ (accessed Apr. 05, 2021).

[107] FireEye, "Mandiant," *FireEye*, 2021. https://www.fireeye.com/mandiant.html (accessed Mar. 24, 2021).

[108] J. Blake, D. Caban, and M. Krotofil, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," *FireEye*, 2017. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (accessed Mar. 24, 2021).

[109] R. McMillan, "New Type of Cyberattack Targets Factory Safety Systems," *The Wall Street Journal*, 2018. https://www.wsj.com/articles/hack-at-saudi-petrochemical-plant-compromised-a-safety-shut-off-system-1516301692 (accessed Mar. 24, 2021).

[110] FireEye Intelligence, "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," *FireEye*, 2018. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html (accessed Mar. 24, 2021).

[111] Wireshark, "About Wireshark," *Wireshark*, 2021. https://www.wireshark.org/ (accessed Mar. 24, 2021).

[112] Kosovo's Ministry of Internal Affairs, "It has been held the meeting of the working group for the National Cyber Security Strategy and Action Plan 2020-2025," *Kosovo's Ministry of Internal Affairs*, 2020. https://mpb.rks-gov.net/f/57/505/U-mbajt-takimi-i-grupit-punues-për-Strategjinë-Shtetërore-të-Sigurisë-Kibernetike-dhe-Planin-e-Veprimit-2020-2025 (accessed Jan. 25, 2021).

[113] R. Mattioli, C. Levy-Bencheton, and European Union. European Network and Information Security Agency., "Methodologies for the identification of critical information infrastructure assets and services : guidelines for charting electronic data communication networks.," ENISA, 2014. [Online]. Available: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis.

[114] TF-CSIRT Trusted Introducer, "Services for Security and Incident Response Teams," 2019. https://www.trusted-introducer.org/index.html (accessed Jan. 25, 2021).

[115] FIRST, "About FIRST," 2020. https://www.first.org/about/ (accessed Jan. 25, 2021).

[116] ENISA, "CSIRTs by Country - Interactive Map - Kosovo," 2021. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-

country-interactive-map#country=Kosovo* (accessed Jan. 25, 2021).

[117] The World Bank, “Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment,” 2020. https://www.worldbank.org/en/news/press-release/2020/06/29/kosovo-has-undertaken-critical-steps-in-cybersecurity.

[118] Commission of the European Communities, “ECI Directive,” 2006. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/national-security/eci-directive (accessed Jan. 25, 2021).

[119] Global Cyber Security Capacity Centre, “Cybersecurity Capacity Assessment of the Republic of Kosovo,” 2015. [Online]. Available: https://www.combattingcybercrime.org/files/virtual-library/national-laws/cybersecurity-capacity-assessment-of-the-republic-of-kosovo.pdf.

[120] Global Cyber Security Capacity Centre (GCSCC) University of Oxford, “Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition,” 2017. https://cybilportal.org/tools/cybersecurity-capacity-maturity-model-for-nations-cmm-revised-edition/ (accessed Oct. 08, 2020).

[121] Global Cyber Security Capacity Centre (GCSCC) University of Oxford, “Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition,” 2016. doi: 10.2139/ssrn.3657116.

[122] Reuters Staff, “Kosovo’s highest court rules parliamentary vote electing government was illegal,” *Reuters*, 2020. https://www.reuters.com/article/us-kosovo-court-ruling-government-idUSKBN28V2SU (accessed Jan. 26, 2021).

[123] Kosovo’s Ministry of Economic Development, “Energy Strategy of the Republic of Kosovo 2017-2026.,” 2017. Accessed: Nov. 25, 2020. [Online]. Available: https://mzhe-ks.net/repository/docs/Kosovo_Energy_Strategy_2017_-_26.pdf.

[124] Kosovo Energy Corporation J.S.C., “KEK Profile,” *Kosovo Energy Corporation J.S.C.*, 2021. http://kek-energy.com/kek/profili-i-kek-ut/ (accessed Apr. 06, 2021).

[125] KOSTT, “KOSTT - About,” 2021. https://www.kostt.com/Home/About (accessed Mar. 25, 2021).

[126] KEDS, “KEDS - About Us,” 2021. https://www.keds-energy.com/eng/about-us/keds-profile/ (accessed Mar. 25, 2021).

[127] Kosovo Energy Corporation J.S.C., “Power plant ‘Kosova A,’” *Kosovo Energy Corporation J.S.C.*, 2021. http://kek-energy.com/kek/termocentrali-kosova-a/ (accessed Apr. 06, 2021).

[128] ICSS, “About Alspa P320.” https://www.icss.biz/about-alspa-p320/ (accessed Apr. 06, 2021).

[129] Microsoft, “Support for Windows 7 has ended,” *Microsoft*, 2021.

https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support (accessed Apr. 06, 2021).

[130] Microsoft, “Support for Windows XP ended,” *Microsoft*, 2021. https://www.microsoft.com/en-ww/microsoft-365/windows/end-of-windows-xp-support (accessed Apr. 06, 2021).

[131] KOMTEL, “Integration of Interconnection Kosovo – Albania,” 2016. http://www.komtelpe.com/komtel/en/electrical-engineering/energy/transmission/integration-of-interconnection-kosovo-albania/ (accessed Mar. 26, 2021).

[132] KEDS, “KEDS starts with the digitalization of the network,” 2018. https://www.keds-energy.com/eng/news/keds-starts-with-the-digitalization-of-the-ne-605/ (accessed Mar. 26, 2021).

[133] Government of Kosovo, “FEASIBILITY STUDY FOR PROTECTION OF IBER LEPENC CANAL KOSOVO,” 2016. [Online]. Available: http://iber-lepenc.org/repository/docs/ESIAF_and_ESMF_WSCP_project_Feb2016_ENG_WITH_PUBLIC_CONSULTATIONS_REPORT_2007.pdf.

[134] F. Hadja, “WATER SECURITY AND CANAL PROTECTION PROJECT REPUBLIC OF KOSOVO: CONSULTANCY SERVICES FOR DESIGN & IMPLEMENTATION SERVICES,” Pristina, 2018.

[135] Hydro-Economic Enterprise “Iber-Lepenc” J.S.C., “Enterprises History,” 2014. http://www.iber-lepenc.org/?page=2,12 (accessed Apr. 06, 2021).

[136] Hydro-economic Enterprise “Iber-Lepenc” J.S.C., “Status of Hydro-economic Enterprise ‘Iber-Lepenc’ J.S.C.,” Pristina, 2020. [Online]. Available: http://www.iber-lepenc.org/repository/docs/Statuti_i_Nd_rmarrjes_2020.pdf.

[137] The World Bank, “World Bank and Kosovo Sign Project to Support Water Security in Kosovo,” *The World Bank*, 2017. https://www.worldbank.org/en/news/press-release/2017/01/27/world-bank-and-kosovo-sign-project-to-support-water-security-in-kosovo (accessed Apr. 07, 2021).

[138] The World Bank, “Kosovo Water Security and Canal Protection Project: Development Tracker,” *U.K. Foreign, Commonwealth and Development Office*, 2021. https://devtracker.fcdo.gov.uk/projects/44000-P133829 (accessed Apr. 07, 2021).

[139] Oskar-El, “Design of installation and start-up of SCADA system for site: Iber Canal, Kosovo.,” 2021. https://oskar-el.com/jv-interadria-and-oskar-el~600.html? (accessed Apr. 11, 2021).

[140] Oskar-El, “About us,” 2021. https://oskar-el.com/en/company.html (accessed Apr. 11, 2021).

[141] Dun & Bradstreet, “InterAdria L.L.C.,” 2021. https://www.dnb.com/business-directory/company-

profiles.interadria_llc.c6c558ad8061289d5a6b5083d468268b.html (accessed Apr. 11, 2021).

[142] The World Bank, “Kosovo Water Security and Canal Protection Project,” *The World Bank*, 2021. https://projects.worldbank.org/en/projects-operations/project-detail/P133829?lang=en (accessed Apr. 07, 2021).

[143] G. Cattaneo, G. De Maio, P. Faruolo, and U. F. Petrillo, “A Review of Security Attacks on the GSM Standard,” in *Information and Communication Technology*, 2013, pp. 507–512.

[144] L. H. Newman, “Hackers Could Decrypt Your GSM Phone Calls,” *Wired*, 2019. https://www.wired.com/story/gsm-decrypt-calls/ (accessed Apr. 07, 2021).

[145] A. Skrobov and S. Makkaveev, “Advanced SMS Phishing Attacks Against Modern Android-based Smartphones,” *Check Point Research*, 2019. https://research.checkpoint.com/2019/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/ (accessed Apr. 07, 2021).

[146] The European Commission, “Implementation of the NIS Directive in Estonia,” 2019. https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-estonia (accessed Apr. 11, 2021).

[147] Kosovo’s Ministry of Internal Affairs, “October, the Cyber Security Awareness Month - ‘Be careful while on Internet,’” 2020. https://mpb.rks-gov.net/f/57/484/Muaji-Tetor,-muaji-i-ndergjegjesimit-per-siguri-kibernetike--“Kujdes-ne-internet%22 (accessed Apr. 11, 2021).