Journal of Universal Computer Science, vol. 25, no. 11 (2019), 1437-1457
submitted: 5/2/19, accepted: 26/7/19, appeared: 28/11/19 © J.UCS

Cyberattack Response Model for the Nuclear Regulator in Slovenia

Samo Tomažič
(Slovenian Nuclear Safety Administration, Ljubljana, Slovenia
samo.tomazic@gmail.com)

Igor Bernik
(Faculty of Criminal Justice and Security, University of Maribor, Ljubljana, Slovenia
igor.bernik@fvv.uni-mb.si)

Abstract: Cyberattacks targeting the nuclear sector are now a reality; they are becoming increasingly frequent and sophisticated, while the perpetrators are increasingly motivated. The key stakeholders in the nuclear sector, such as nuclear facility operators, nuclear regulators responsible for nuclear safety or nuclear security, technical support organisations and computer equipment suppliers, must take the necessary cybersecurity measures to prepare for potential cyberattacks and provide the highest possible level of response to such cyberattacks. This can only be achieved by adopting a systematic approach to cyberattack response. When conducting the research study presented herein, a descriptive method was applied to review the scientific literature, various standards, recommendations and guides, as well as to devise an inventory of publicly available sources. On the basis of such an analysis, individual questions were then formulated in order to compile a structured interview, which was conducted with international experts working at nuclear facilities, nuclear regulators, technical support organisations, computer equipment suppliers and other organisations responsible for providing cybersecurity in the nuclear sector. On the basis of their responses, researchers devised an innovative and comprehensive Cyberattack Response Model to be used by Slovenia's nuclear safety regulator and the regulator responsible for the physical protection of nuclear facilities and nuclear and radioactive materials.

Keywords: Nuclear Security, Regulator, Cybersecurity, Cyberattack, Response
Categories: H.3.1, H.3.2, H.3.3, H.3.7, H.5.1

1 Introduction

In a modern society, life without electricity can no longer be envisaged, since all of us are almost fully dependent on it. Our modern lifestyles are not relying only on electricity, but are also fully dependent on information technologies, connectivity and cyberspace. The increased connectivity on one hand and the vulnerability of the information and communication technology (ICT) on the other hand are the fundamental reasons why malicious acts performed in cyberspace have become ever more frequent in our everyday lives [see SI-CERT 2018]. Connectivity is an important factor, as it is closely related to the protection of both personal [see Markelj and Markelj 2016] and business data [see Vrhovec et al. 2015]. User privacy and the security of business information systems and data cannot be guaranteed without secure connections as well as need to defend [e. g. Mihelič and Vrhovec 2018].

Information security systems and analyses of potential failures [see Brezavšček 2015] guarantee the continuous availability of business and personal systems' connectivity. Connectivity is also an essential precondition for the functioning of critical infrastructure [see Purpura 2013] in a variety of sectors. Therefore, both national security and our everyday lives depend on connectivity.

Research shows that the number of cyberattacks has increased substantially in the past decade [see Onyeji et al. 2014]. Attackers are increasingly resourceful and apply new techniques in carrying out their cyberattacks [see Baylon et al. 2015]. However, these are not only targeting the business sector, but are also directed against critical infrastructure, which is an essential functional element of every society. There have been many successful cyberattacks directed to areas like; transport, energy, and health. Today's public and private transport is totally dependent on digital technologies (on-board computers, GPS, assistance systems, etc.), which were targets of many cyberattacks [see Loukas 2015]. One of the most well-known cyberattacks on energy sector was cyberattack on Ukraine energy grid [see Lee et al. 2016]. It compromised the information systems of three energy distribution companies in Ukraine and temporarily suspended electricity supply to approximately 230,000 households. In the past few years, ransomware is on a rise [see SI-CERT 2018] and health sector is not an exception [see ZDNet 2019]. In 2018 a hospital in US had to pay a large amount, in order to get their sensitive information decrypted. Cyberattack on German Still Facility in 2014 has been considered as critical, because it caused multiple operational technology components to fail [see SANS 2014]. It was one of a few known cyberattacks that resulted in physical damage.

Nuclear sector, as many others, is also not immune to cyberattacks. Thus far, there were two widely reported and notorious cyberattacks against the nuclear sector. The first cyberattack [see Falliere et al. 2011] was conducted by using the Stuxnet malicious software to target uranium enrichment infrastructure at a nuclear facility in Iran, while the second cyberattack [see Lee and Lim 2016] targeted the largest Korean energy producer and nuclear facility operator, i.e. the Korean Hydro and Nuclear Power (KHNP). The aim of the latter was to steal sensitive information and spread fear in the general public, which could also be considered as an act of cyberterrorism [see Bernik 2014] targeting a key stakeholder in the nuclear sector [see ENISA 2017, OSCE 2013].

Therefore, an interesting situation arises: on one hand, electricity has become indispensable, thus raising the importance of the corresponding critical infrastructure facilities and powerplants, which generate electricity. On the other hand, information and communication technologies are interconnecting all of these facilities into a single cyberspace. If a cyberattack were successful, powerplants would cease to generate electricity and the cyberspace would fully or partly switch off. At the same time, this would probably also affect other services, which depend on electricity, such as water supply, sewage systems, passenger and freight transport, financial transactions, food supply and storage, the functioning of national security systems, etc. Therefore civilization legitimacy and social damage are affected [see Bučar-Ručman 2019]. Humankind would thus be pushed back into the Middle Ages.

Responses to cyberattacks have not been harmonised and coordinated at the international level. Therefore, each country is attempting to resolve the issue individually and partially or not at all.

Descriptive analysis during our research study showed, many nuclear regulators have developed legislation and regulations which operators should follow. However, only a few have developed guides on how to implement the provisions, stated in the legislation and regulations [see Tomažič 2019]. Therefore, operators are left to themselves to implement the appropriate computer security measures. International standards or guides from organizations like; IAEA [see IAEA 2016], NIST [see NIST 2012], SANS [see SANS 2011], ENISA [see ENISA 2010], CREST [see CREST 2013], and ISO [see ISO/IEC 2016] do offer partial solutions, but are not totally applicable to relevant stakeholders in nuclear sector. Table 1 lists above mentioned standards and guides on the left, and key areas of incident response planning to be covered in nuclear sector on the top.

	Focus on Critical Infrastructure / Nuclear Sector	Development of Response Plans and Procedures	Cooperation of Key Stakeholders in Nuclear Sector	Escalation Levels	Information Exchange / Reporting / Notifying	Connection to Emergency Preparedness
IAEA	+	+	o	+	o	o
NIST	–	+	o	–	+	–
SANS	–	+	–	–	–	–
ENISA	–	+	o	–	+	–
CREST	–	+	o	–	+	–
ISO	–	+	–	–	o	–
OUR MODEL	+	+	+	+	+	+

+ Very useful information for Nuclear Sector
o Parts can be used in Nuclear Sector
– Almost no useful information for Nuclear Sector

Table 1: Comparison of international standards and guides with our model

This paper thus presents an innovative approach, previously unfamiliar to the international nuclear community, since the proposed Cyberattack Response Model represents an innovative and comprehensive view of coordinated and consistent responses in the event of a cyberattack.

Section 1 covers the need for electricity, connectivity, vital role of critical infrastructure sectors, and recent and most widely reported cyberattacks to date. It also explains the need for legislation, regulation, and standards or guides, which would help nuclear sector in order to better prepare, detect, and respond to a cyberattack. Key stakeholders in nuclear sector in Slovenia are listed, including nuclear facility operators, regulators, technical support organizations, and computer equipment suppliers. Difference between nuclear safety and nuclear security is explained. Descriptive analysis and structured interviews are presented in Section 2. Cyberattack Response Model, which represents our final result, is presented in Section 3. In Section 4 we discuss about the findings, theoretical and practical implications, limitation, and future work.

1.1 Key Stakeholders in the Nuclear Sector in Slovenia

The nuclear sector is composed of numerous stakeholders involved in the provision of cybersecurity at nuclear facilities.

A nuclear facility operator is a stakeholder managing and operating a nuclear facility on the basis of an operating licence. In Slovenia, there are three nuclear facilities (the Krško Nuclear Power Plant (Nuklearna elektrarna Krško (NEK)), the research reactor with a hot cell in Podgorica and the central interim storage for radioactive waste in Brinje) and three nuclear facility operators (NEK, the "Jožef Stefan" Institute and the Radioactive Waste Management Agency).

The Slovenian Nuclear Safety Administration (SNSA), a body affiliated to the Ministry of the Environment and Spatial Planning, is the national nuclear safety regulator in Slovenia, responsible for oversight of the areas of radiation and nuclear safety, activities involving ionising radiation and use of radiation sources. The Ministry of the Interior (MoI) is the nuclear regulator responsible for providing the physical security of nuclear facilities and nuclear and radioactive materials (the term "nuclear regulator" used henceforth therefore refers to both bodies). Both, the SNSA and MoI are therefore responsible for oversight of nuclear facilities in Slovenia.

A technical support organisation (TSO) is any organisation employing adequately qualified personnel and using suitable technical equipment for responding to cyberattacks. In Slovenia, such organisations currently include the Slovenian Computer Emergency Response Team (SI-CERT), the Ministry of Defence and the Ministry of the Interior. However, a Security Operation Centre (SOC), which could also act as a technical support organisation in the future, is currently being set up at the Ministry of Public Administration. TSOs in Slovenia do work together with critical infrastructure facilities, as well as nuclear facilities in various areas of information security (awareness, security culture, incident response planning, etc.).

A computer equipment supplier is any organisation or company supplying, maintaining, upgrading or updating computer equipment in the nuclear sector.

All of the above stakeholders have a common goal: they wish to duly prepare for and respond to potential cyberattacks. Failure to achieve this goal could be catastrophic. It is true that financial ramifications are normally considered as the most significant consequences of a cyberattack in a business environment [see Bernik 2014]. However, a cyberattack in the nuclear sector could produce unacceptable radiological consequences for people and the environment. The prevention of such consequences lies primarily in the hands of nuclear facility operators and only then in the hands of a nuclear regulator, whereas both ought to be supported by other stakeholders.

In 2015, SNSA established a national working group on cyber security at nuclear facilities (NWG), where all key stakeholders in nuclear sector in Slovenia share information, knowledge, and experience [see Tomažič 2015]. NWG is also a contact point with international environment (IAEA, other member states, WINS, etc.).

1.2 Nuclear Safety and Nuclear Security

The concept of nuclear safety refers to the achievement of adequate conditions for nuclear facilities' operation, which are crucial for preventing or mitigating the effects of nuclear accidents [see IAEA 2019]. Nuclear safety also provides for the protection

of workers, the general public and the environment against the threats of ionising radiation.

In contrast, nuclear security [see IAEA 2011] is defined as the prevention, detection and response to malicious acts (theft, sabotage, unauthorised access, unauthorised information transfer, etc.), involving nuclear material, other radioactive substances or related facilities.

According to the IAEA Nuclear Security Series documents, states should define nuclear security requirements for nuclear or other radioactive material and associated facilities based on a threat assessment or a Design Basis Threat (DBT). A DBT describes the capabilities of potential insider and external adversaries who might attempt unauthorized removal of nuclear and other radioactive material or sabotage [see IAEA 2009].

Nuclear safety and nuclear security are not completely isolated from one another and there is no clear distinction between these two concepts. In principle, nuclear safety deals with the prevention of harm caused to people and the environment due to ionising radiation, while nuclear security focuses on malicious acts performed by external actors [see IAEA 2013].

Emergency preparedness is also an essential part of providing nuclear safety. Thus, all competent organisations are required to put in place emergency preparedness plans enabling their personnel to quickly identify, evaluate and respond to a broad range of emergencies [see URSZR 2010]. In turn, cyberattacks may also cause situations which can put nuclear safety at great risk. In order to avoid cyberattacks, stakeholders are conducting activities aimed at guaranteeing a high preventive level of cybersecurity, thus also ensuring an appropriate level of nuclear security and nuclear safety. Such activities include:

- setting up a legal framework (acts, regulations, guides and other implementing rules),
- drafting plans, security policies, internal procedures and technical guidance notes,
- conducting regular education and training courses,
- organising and implementing exercises based on realistic scenarios,
- establishing a security culture, and
- evaluating the cybersecurity management system.

A systematic approach is required for achieving the highest level of cybersecurity, which can be attained by applying an innovative and comprehensive Cyberattack Response Model aimed at assisting the nuclear regulator in organising various activities for responding to cyberattacks, which can have serious consequences for the provision of nuclear safety. In order to guarantee comprehensive nuclear safety by protecting nuclear facilities and responding to cyberattacks, this innovative Cyberattack Response Model consists of four stages and an escalation system. The model is intended for the nuclear regulator, which is responsible for providing comprehensive nuclear safety. It also introduces a basic approach to providing the highest level of response to cyberattacks targeting all critical infrastructure sectors, since they are all facing similar or comparable issues.

2 Methods

The research study, the aim of which was to complete the development of the Cyberattack Response Model presented herein, was conducted by applying the descriptive research and structured interview methods. Findings were then synthesised and structured systematically into an innovative and comprehensive Cyberattack Response Model intended for the nuclear regulator.

The aim of descriptive research was to review scientific articles, doctoral dissertations, books and journals, as well as publicly available sources and electronic sources, such as national legislation repositories, national reports, regulations, guides, standards, best practices, recommendations, documents issued by competent authorities and reports of international organisations, such as the International Atomic Energy Agency (IAEA). The review encompassed the fields of cybersecurity management, cyberattack response and legal frameworks of different nuclear regulators. The review of such frameworks focused on countries having at least one operating nuclear power plant.

Structured interviews represented the second research method. A total of fifteen interviews, each with an average duration of ninety minutes, were conducted with international experts working at nuclear facilities, nuclear regulators, organisations providing technical support, computer equipment suppliers and other organisations responsible for providing cybersecurity in the nuclear sector. Interviews were conducted either in person during various events (conferences, meetings, training courses) or via the video-conference system. Prior to their interview, respondents had the opportunity to review the questions, some even several days or weeks in advance, since they had to acquire authorisation from their superiors or other competent national authorities. Respondents also received information about researchers' background and, most importantly, the aims and objectives of the research study. The anonymity of respondents and their respective countries was guaranteed prior to their interviews. The aim of the interviews was to validate and upgrade the findings of the underlying literature review. The interviews therefore provided an additional insight into the current level of preparedness for responding to potential cyberattacks in the nuclear sector. Apart from an extremely high level of cybersecurity, the interviews also revealed certain shortcomings, which were subsequently analysed in greater detail and eliminated from the final version of the Cyberattack Response Model (henceforth: "the Model").

The Model was developed on the basis of the research study and a detailed analysis of sources. The Model's structure and content are thus drawing from findings obtained in scientific literature, an in-depth review of existing cyberattack response models and the analysis of interviews conducted with international experts in the nuclear sector.

Apart from an extensive literature review, the two existing and crucial cyberattack response models developed by the IAEA and the National Institute of Standards and Technology (NIST) were also studied in great detail. The IAEA model was selected because its guidelines are the only directly applicable guidelines in the nuclear sector, while the NIST model was examined because it deals most closely with both the information and the operational side of IT systems. Apart from the

IAEA and NIST guidelines, the guides published by organisations, such as SANS, ENISA, CREST and ISO, were also reviewed.

All existing models include a uniform set of basic activities to be conducted by stakeholders, such as, for instance, drafting a response plan, distributing tasks and responsibilities, using adequate technical equipment, drafting analyses, etc. However, they lack additional content related to the provision of cybersecurity in the critical infrastructure sector, information exchange, cooperation between key stakeholders, provision of assistance, as well as incident notification and reporting. The Model was finalised on the basis of answers obtained through interviews with international experts in the nuclear sector. The respondents were presented with the following eleven main questions, which were fleshed out with a set of five to seven additional questions:

- Could you please introduce yourself?
- Do you have regulations and guides related to cybersecurity?
- Do you have a cyber-Design Basis Threat (DBT)?
- Do you have regulatory inspections regarding cybersecurity?
- What kind of a systematic approach to cybersecurity do you practice in your organisation?
- How is your organisation prepared for cyberattacks?
- How are cyberattacks handled at your nuclear facilities?
- What kind of information sharing is established among stakeholders in the nuclear sector in your country?
- How is reporting of cyber incidents or events organised at the NFs level?
- Do you perform exercises involving cyberattacks?
- Are there any best practices you would like to highlight regarding incident response in your country?

The answers obtained through the aforementioned interviews were used to improve the Model. Interview with international experts helped us to obtain additional information or clarification, and identify issues they have while preparing, detecting, and responding to a cyberattack. It turned out that the majority of shortcomings were observed in those areas that were not touched upon in the most frequently used guides, which included:

- drafting appropriate regulatory guides,
- devising cyber design basis threat,
- qualifications and skills of key personnel,
- carrying out exercises based on realistic scenarios,
- exchanging information, knowledge and experience, and
- cybersecurity management at the state level (working groups).

The synthesis of findings obtained through literature review and structured interviews thus served as the basis for producing the final result of this research study, which is an innovative and comprehensive Cyberattack Response Model.

3 Results

The Model, presented in Figure 1, represents a final result. It is aimed at assisting the nuclear regulator in organising its activities for responding to cyberattacks, which may gravely affect the provision of not only nuclear security, but also nuclear safety, and emergency preparedness. At the same time, the Model is also intended for other stakeholders implementing the escalation system and various activities pertaining to the four stages described below. All four stages are the same for all stakeholders, while some individual activities may differ. Therefore, stakeholders are able to organise a coordinated response to cyberattacks and remedy the situation in order to resume normal operations.

3.1 Cyberattack Response Model as a Tool

The Model is based on the escalation of a cyberattack and contains four stages of response. It also includes suggestions for fostering cooperation between nuclear regulators and other key stakeholders in the nuclear sector. Furthermore, it advocates the exchange of information and a common approach to problem-solving.

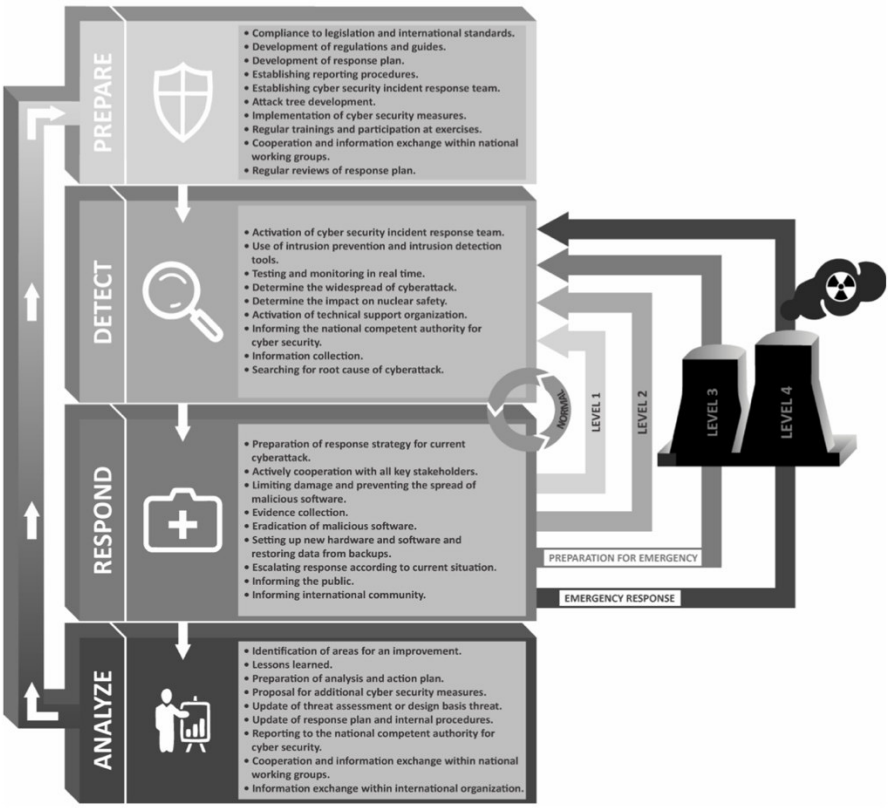

Figure 1: Innovative and Comprehensive Cyberattack Response Model

In the event of an actual cyberattack, the Model proposes an escalation system, which depends on the consequences that such an incident may entail. In the nuclear sector, the most severe consequences include the unacceptable radiological consequences for people and the environment. Therefore, all stakeholders strive to maintain a situation, in which operations run smoothly, in order to avoid such consequences. Such a situation means there are no deviations from normal operation. If the situation changes, the cyberattack escalates from level one to level four. The Model is thus composed of four stages and the escalation system.

The four stages of response include preparation, detection, response and analysis. The circular process enables the return from the last stage of analysis to the first stage of preparation and corresponds to the escalation of a cyberattack from the response to the detection stage. The Model thus enables continuous improvement and adaptation to the situation at hand. The following sections describe the escalation system and activities proposed in individual stages.

The Model may be slightly adapted in order to be implemented in other sectors of critical infrastructure, such as energy, transport, food and water supply, healthcare, finance, environmental protection, ICT networks and systems. The model itself is really, and in deeply, focused on nuclear sector, but general enough, so it can be used, with some modifications, in other sectors of critical infrastructure, as well as in other business environments. The main focus of one applying it, should be tailoring the model to their own needs, capabilities, and resources.

3.2 Escalation

In the nuclear sector, the escalation of a cyberattack is directly related to the consequences that an incident of this type may generate. Such consequences range from the temporary loss of control over individual processes to unacceptable radiological consequences for people and the environment. The impact of a cyberattack on nuclear safety must be established regardless of whether a cyberattack targets information technology (in the business premises of nuclear facility operators, in the premises of nuclear regulators or computer equipment suppliers) or operational technology (analogue and digital systems for monitoring, managing, controlling and conducting physical processes at a nuclear facility).

In the proposed Model, escalation takes place between the stages of cyberattack detection and response. It begins with level one and ends with level four. It is also possible to deescalate from higher to lover levels, depending on the circumstances. At level four, an emergency preparedness and response (henceforth: “EPR”) plan is activated, and the EPR team takes over all emergency management activities. The aim of everyone involved in such activities is to lower the level and resume normal operation.

Normal operation refers to a situation, in which everything runs smoothly and within the limits prescribed for regular operations, while monitoring activities are conducted in real time and systems are checked for potential warnings. A great deal of effort and financial means is required to achieve and maintain such a situation, which must not be taken for granted. The main objective is to provide a high level of confidentiality, integrity and availability.

The Emergency Preparedness and Response Division [see URSJV 2019] makes sure that the Slovenian Nuclear Safety Administration (SNSA) is fully prepared for

taking every measure in the event of an emergency (nuclear or radiological accident) and participates in drafting the EPR plan at national and international levels. The EPR plan and the EPR team are activated in the event of an emergency. The team's main objectives are to establish the origin of the emergency, assess the operational situation, analyse radiological conditions in facilities and their surroundings, propose different protective actions and inform the public and international community.

An emergency is a much broader concept than a cyberattack. If a cyberattack escalates and reaches level four, it may cause an emergency. As defined by the Ionising Radiation Protection and Nuclear Safety Act [see *Zakon o varstvu pred ionizirajočimi sevanji in jedrski varnosti (ZVISJV-1)* 2017], an emergency is a situation or an event, which is unusual and during which the radiation or nuclear safety or the level of protection against radiation are reduced. In such a situation or event, which is caused by an emergency, it is essential to immediately start the necessary preparations and implement all measures for preventing or eliminating the potentially harmful consequences for the health and safety of people and the quality of their lives, preventing the consequences for property and the environment or eliminating risks leading to such serious consequences.

3.2.1 Level One

Level one refers to untargeted cyberattacks, such as cases of social engineering, SPAM attacks, computer infections caused by inappropriate use, random port scanning and access attempts, etc. Level one also entails cyberattacks at other locations using the same or similar technologies. In most cases, level one cyberattacks do not produce direct effects and consequences, and are thus very similar to the normal operation situation. Nevertheless, a cyberattack response team is activated in order to analyse the current state-of-play and either raise the level of threat or lower it back to normal operation. Level one incidents do not need to be reported.

3.2.2 Level Two

Level two refers to targeted cyberattacks, which include attempts of targeted social engineering aimed at gaining specific access, detected system vulnerabilities, detected malicious software, misappropriation of non-sensitive information or data, scanning specific ports and attempts aimed at obtaining remote access to systems, etc. Level two cyberattacks also do not have any direct impacts or consequences, provided they are detected in a timely fashion. If, however, they are not discovered in time or if the response is inappropriate, level two can easily be raised to level three. The cyberattack response team has already been activated following a level one incident. If the incident began unfolding directly at level two, the team must be activated immediately. The nuclear regulator is required to report level two incidents to the cybersecurity regulator. At the same time, it receives information from facility operators, if the cyberattack takes place at a nuclear facility.

3.2.3 Level Three

Level three entails a cyberattack, which is ongoing or has already been carried out. The monitoring activities revealed anomalies, while detection systems discovered that unauthorised activities had been taking place in certain systems. Level three thus

refers to malicious software detected on different systems, service denial, abnormal activities, cases of unauthorised access to or the use of systems and the misappropriation of sensitive information or data. If level three cyberattacks are not detected on time and if an appropriate response had not been implemented, such cyberattacks may have serious consequences for nuclear security or even safety. The cyberattack response team has already been activated at levels one or two. If the cyberattack began unfolding as a direct level three incident, the team must be activated immediately. Preparations for the activation of the full or partial EPR team must also begin. The nuclear regulator is required to report level three incidents to the cybersecurity regulator. At the same time, it receives reports from facility operators, if the cyberattack takes place at a nuclear facility.

3.2.4 Level Four

Level four represents the highest and most significant cyberattack level. Level four cyberattacks put nuclear security and safety at severe risk. The consequences of such a cyberattack may include the temporary loss of control over processes or unacceptable radiological consequences for people and the environment. The cyberattack response team has already been activated at levels one, two or three. If the cyberattack began unfolding as a direct level four incident, the team must be activated immediately. This also requires a full or partial activation of the EPR team, which takes over emergency management activities. The cyberattack response team actively cooperates with the EPR team. The nuclear regulator is required to report level four incidents to the cybersecurity regulator. At the same time, it receives reports from facility operators, if the cyberattack takes place at a nuclear facility. When the EPR team is activated, reporting takes place in line with the EPR procedures and on the basis of predetermined time intervals.

3.3 Response Stages

The response stages presented below entail a range of activities implemented by the nuclear regulator in order to achieve the highest level of response to cyberattacks, thus guaranteeing the highest level of cybersecurity in general. These stages, as well as individual activities, guide the nuclear regulator towards continuous improvements, since individual stages are process-based, which enables regulators to detect vulnerabilities rather quickly and implement the necessary cybersecurity measures. The Model is composed of the following four stages:

- preparation,
- detection,
- response, and
- analysis.

These form two sets of cyclic processes. The first cycle corresponds to the transition from level four to level one, while the second cycle corresponds to the escalation system or, in other words, the transition from the response stage to the detection stage and all the way to resuming normal operation.

3.3.1 Preparation

During the preparation stage, nuclear regulators must analyse the applicable national legislation and international standards. Compliance with national legislation is imperative, while compliance with international standards is a reflection of their responsibility and an expression of their awareness of current cybersecurity-related issues.

Nuclear regulators are also required to draft regulations imposing obligations on nuclear facility operators in terms of providing cybersecurity. These regulations are of general nature, which is why nuclear regulators also draft guides in order to help the nuclear facility operators in meeting the requirements defined in regulations. Such regulations, which are drafted by nuclear regulators, also define information and reporting procedures to be applied in the event of a cyberattack. In fact, adequate communication between all stakeholders in the nuclear sector is crucial at all stages of cyberattack response.

The review of national legislation is followed by the setting up of a cyberattack response plan (in line with the legislation), an information security policy, as well as internal procedures and technical guides. Individuals' roles and responsibilities must also be defined during this stage and a cyberattack response team must be established. In order to provide a broader overview of individual processes, the aforementioned team must have a multidisciplinary composition and a clear hierarchical structure. The tasks of the team and its individual members are defined in the response plan.

Developing attack tress is important activity which feed information into the next step of implementation of cybersecurity measures. Cyberattack response team has to work together and think like a perpetrator in order to find all the possible vulnerabilities of the systems. The attack tree is composed of perpetrators' goal at the top and activities he has to reach in order to achieve the main goal.

The implementation of cybersecurity measures begins in cooperation with information system operators, technical support organisations and computer equipment suppliers. These are closely linked to the previously drafted risk and vulnerability analyses. Cybersecurity measures may include administrative, technical and physical cybersecurity measures, the aim of which is to reduce risks and vulnerabilities. A proposal for implementing or upgrading such cybersecurity measures may also originate from attack trees or the fourth stage, i.e. the analysis stage.

Education and training programmes are planned on the basis of tasks and competences of individual members of staff. It is important for the nuclear regulator to set up an education and training programme, and keep a record of competences possessed by all employees, particularly those who are in any way involved in providing cybersecurity and cyberattack response. This allows the regulator to quickly identify the needs for additional training and take the necessary steps.

The organisation and execution of joint exercises is crucial for testing the cyberattack response team's reactions, validating internal procedures and technical guides, evaluating the adequacy of coordination and communication activities, checking the use of technical and ICT equipment, and identifying potential vulnerabilities. Such exercises are divided into table-top and field exercises [see IAEA 2018a].

The establishment of a national cybersecurity working group, which includes representatives of all key stakeholders in the nuclear sector, is an example of best practice in numerous countries with an operating nuclear power plant. The goals of such groups benefit all participating stakeholders and include:

- exchange of information, knowledge, experience and contacts,
- coordination regarding their participation in meetings, courses, conferences, etc.,
- cooperation and assistance in responding to cyberattacks,
- assistance in drafting internal procedures and guides, and
- creating a circle of mutual trust among stakeholders.

The existing cyberattack response plan is reviewed and evaluated at least once a year. The plan should also be reviewed and revised, if necessary, after each exercise or following an actual cyberattack. Such reviews are aimed at ensuring that data and information contained in the plan are up to date. In the preparation stage, nuclear regulators also define the roles and responsibilities of individuals involved in cyberattack response activities. The creation of a cyberattack response team, which is activated at this stage and must provide an appropriate response, is one of such responsibilities.

3.3.2 Detection

A cyberattack may take many different shapes and forms, which are almost impossible to predict. It is, however, possible to come up with different scenarios in order to prepare for a potential cyberattack during exercises. Nevertheless, the detection stage may occur at any time during the normal operation of a nuclear facility. Therefore, intrusion prevention systems (IPS) are deployed to prevent cyberattacks. These are used together with intrusion detection systems (IDS). In addition, network-based intrusion detection systems (NIDS) are also used in order to monitor the traffic between hosts and host-level IDS or host-based intrusion detection system (HIDS). HIDS are used to monitor the traffic directly at the host level. Such a complementary use of systems aimed at preventing and detecting cyberattacks is able to drastically increase the level of cybersecurity.

Real-time testing and monitoring activities aimed at detecting potential cyberattacks are carried out in order to accurately diagnose and determine the extent and the cause of a cyberattack. Such an activity may be performed by the computer equipment owner. However, if it concluded the necessary contractual relationship with a technical support organisation or a computer equipment supplier, they could perform these activities on its behalf. All administrators must participate in regular education and training programmes, and be able to demonstrate the required level of competence.

Once the cyberattack response teams are activated, they start determining the extent of the cyberattack. They cooperate with one another and exchange information. If necessary, they may also help each other on the spot, however, this must be clearly agreed in the form of a contract or defined in a cyberattack response plan. This helps the teams to determin the extent of a cyberattack and enables the system to resume normal operation much faster.

Nuclear regulators employ experts who are able to determine the impact of a cyberattack on nuclear safety. If the provision of nuclear safety had been reduced, jeopardised or disabled due to a cyberattack, the cyberattack response must be escalated accordingly. When necessary, or if the cyberattack reaches level four, the EPR team is activated. As soon as a cyberattack is detected or as soon as information about a cyberattack against a nuclear facility operator is received, a technical support organisation is also activated.

The nuclear regulator is a member of the State administration and of the extended public administration, which has its own cybersecurity regulator and its own Governmental Computer Emergency Response Team (GOV-CERT). The nuclear regulator is obliged to report to the GOV-CERT on the basis of the Act on Information Security [see *Zakon o informacijski varnosti (ZInfV)* 2018].

Information collection is essential for a faster and more efficient solution in the event of a cyberattack. Information may be collected from publicly available sources or from sources, which are only available to authorised persons and may contain sensitive data. This is why the collection of information is entrusted to nuclear regulators, who have access to certain sensitive information. The transfer of such information between stakeholders must take place via predetermined and preestablished secure connections.

While responding to a cyberattack, its root causes must also be looked for. It is important to find the cause of a cyberattack in order to prevent the repetition or reoccurrence of the same cyberattack after the restoration of data from backups. The detection of the cyberattack and the identification of its cause trigger the implementation of the next stage, i.e. response.

3.3.3 Response

During an actual cyberattack, it is necessary to respond rapidly and to prepare a response strategy tailored to the current cyberattack. It is also necessary to understand the vectors and types of cyberattacks, since a response strategy will require completely different response in the event of an IT system infection in comparison with an operational technology system infection. In any case, response must be fast, efficient and transparent. During the response stage, nuclear regulators cooperate actively with all other stakeholders. In doing so, they make sure that information required for an easier and faster response to the ongoing cyberattack is available to everyone. Nevertheless, the primary responsibility for responding to the cyberattack successfully lies in the hands of the stakeholder – usually the nuclear facility – who has actually been targeted by the cyberattack. Nuclear regulators may, in order to facilitate cooperation, provide all stakeholders with a secure communication tool, which is also a single-stop-shop for the collection of all crucial information. It is important to establish such communication channels before an actual cyberattack, so that they may be used efficiently during an actual cyberattack. In this context, communication refers to conventional communication, i.e. a conversation, cooperation at the technical level, timely reporting and assistance provided by staff present at the location of the unfolding cyberattack.

The first step aimed at preventing the escalation of the situation is to limit the damage and prevent the spread of malicious software. The stakeholder under cyberattack holds the primary responsibility for implementing this activity, but it may

also request the assistance of other stakeholders, if necessary. The technical support organisation plays a crucial role, since it has the greatest deal of experience with damage limitation and preventing the spread of malicious software in other sectors, particularly in other segments of the critical infrastructure sector.

The purpose of evidence collection [see NIST 2012] is not only to rectify the ongoing situation. It may also be aimed at, for instance, instituting future legal proceedings against perpetrators and organising their prosecution. The nuclear regulator must adopt appropriate internal procedures and technical guides related to the collection of evidence. At the same time, these documents must comply with the applicable national legislation. In collecting evidence, it is recommended to copy the entire disk or make the co-called image clone and not merely copy individual files or folders. If possible, it is also advisable to take photographs of screens and equipment or physical activities caused by the cyberattack.

Once the damage has been limited, the spread prevented and the evidence collected, the malicious software needs to be removed from hardware and/or software. It is important not to remove the still functioning hardware and/or software inconsiderately, since it may continue to perform a vital function. When malicious software has been removed, it is necessary to take further steps in order to resume normal operation. At this stage, the task of the cyberattack response team is also to prepare and verify replacement hardware and/or software. Such verification is the ultimate step before restoring data from backups and running the new equipment.

If the implementation of new hardware and/or software has not been successful or if a new dimension of the cyberattack has been detected, the response must be escalated accordingly. As described in the section dedicated to escalation, an incident may escalate towards the positive or negative side of the cycle between levels one and four. Escalation is triggered by the nuclear regulator, however, if the cyberattack takes place at a nuclear facility, the nuclear facility operator is responsible for triggering the escalation process, while the regulator participates in the response.

The nuclear regulator acts in public interest. It must conduct its tasks transparently and inform the public of risks that may affect people's quality and way of life. In the event of a cyberattack qualified as level one or higher, the nuclear regulator provides verified general information about the cyberattack. The press release must be transparent, clear and easy to understand, and not contain any abbreviations or scientific terms.

The nuclear regulator concludes agreements concerning the exchange of information with other countries (particularly bilateral agreements with neighbouring countries) and international organisations. Apart from informing the public, it thus also informs the international community via preestablished communication protocols and ICT equipment.

3.3.4 Analysis

The analysis is aimed at identifying potential vulnerabilities and drafting proposals for improving the existing state-of-play. At this stage, it is crucial to guarantee the active participation of all stakeholders, particularly those who had been involved in the response stage. The identification of areas requiring improvements should be conducted soon after the incident, since individuals' memories tend to become distorted over time [see Areh 2016]. However, it should not take place too quickly

after the incident [see ENISA 2010], as participants tend to believe they had already done enough during the response stage itself.

One of the key advantages of lessons learned also stems from the fact that everyone may learn from an incident that happened to someone else, thus improving their own timely response. Once the answers had been obtained and lessons learned duly considered, the drafting of a detailed analysis and the final analysis document, i.e. the action plan, may begin. The responsibility for devising the action plan lies with the stakeholder which was targeted by a cyberattack. If the implementation of an additional cybersecurity measure at the nuclear facility operator's site affects the provision of nuclear safety, such a modification must be approved by the nuclear safety regulator. The implementation of the action plan must be supervised, while all undertaken activities must be reported to the competent persons. When the nuclear regulator proposes cybersecurity measures regarding its own systems, it discusses their adequacy with the technical support organisation and the computer equipment supplier. The implementation is carried out by the regulator itself or by its subcontractors.

A design basis threat [see IAEA 2018b] is a description of characteristics of potential internal and external adversaries, who could attempt to perform unauthorised acts to remove nuclear material or seek to commit sabotage, which represent the basis for devising and evaluating the physical protection system. The threat assessment must be updated following each individual cyberattack that may have jeopardised nuclear safety. Threat assessments are usually drafted by authorities responsible for the physical protection of nuclear facilities, as well as nuclear and radioactive substances, in cooperation with other state bodies. In Slovenia, this procedure is governed by the Rules on the Physical Protection of Nuclear Facilities, Nuclear and Radioactive Materials and the Transport of Nuclear Materials [see *Pravilnik o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi* 2013]. If the cyberattack response plan, corresponding internal procedures, technical guides, implemented cybersecurity measures and the qualification of personnel involved in such response activities were perfect, the cyberattack would fail. Therefore, after the identification of vulnerabilities following each exercise or an actual cyberattack, the response plan, internal procedures and technical guides must be updated and responsible personnel must undergo further training, if necessary. The updating of documentation and additional training represent an administrative protection measure, which must also be included in the action plan.

The nuclear regulator is part of the State administration and is thus obliged to appoint responsible persons [see *Uredba o informacijski varnosti v državni upravi (Decree on Information Security in State Administration)* 2018] and report any cyberattack to the GOV-CERT. When determining the significance of an incident and its impact [see *Zakon o informacijski varnosti (ZInfV) (Act on Information Security)* 2018], the regulator must consider the number of affected users, the duration of the cyberattack and its geographical scope. Nuclear regulators are cooperating closely within the international community. They are members of international organisations, such as the IAEA, the European Nuclear Security Regulators Association (ENSRA) and the Western European Nuclear Regulators Association (WENRA). Apart from

information exchange, the aim of their cooperation is also to harmonise approaches to the provision of nuclear safety and nuclear security.

The principal aim of national working groups is to strengthen their cooperation and exchange information. A timely notification of all key stakeholders in a specific country about potential threats allows a more efficient preparation for response, as well as a faster and better implementation of cybersecurity measures.

The presented Cyberattack Response Model is essentially fit to be implemented in the nuclear sector. With slight adaptations, it may also be implemented rather quickly and efficiently in other critical infrastructure sectors, such as energy, transport, food and water supply, healthcare, finance, environmental protection, as well as information and communication networks and systems.

4 Discussion and Conclusions

Cyberattacks are becoming ever more frequent and sophisticated, while their perpetrators are increasingly motivated. They are constantly training and practicing, researching, cooperating with one another and looking for vulnerabilities in order to carry out successful cyberattacks.

The main objective of information systems' administrators is to ensure normal operation and provide an adequate level of preparedness to cyberattacks. In order to achieve this objective, it is imperative to conduct activities, such as planning, training, education and, in particular, carrying out exercises, so as to ensure a timely and adequate response, thus preventing the most severe risks and consequences arising from the nuclear sector, which also encompass the extremely harmful effects of ionising radiation on people and the environment.

However, the model itself it is not applicable only to nuclear sector, but can be used also in other sectors of critical infrastructure.

4.1 Theoretical Implications

The main theoretical contribution of this paper stems from a comprehensive review of scientific articles, doctoral dissertations, books and journals, as well as publicly available sources and electronic sources, such as national legal frameworks, national reports, regulations, guides, standards, best practices, documents issued by nuclear regulators and reports of international organisations, such as the International Atomic Energy Agency (IAEA). The aforementioned review covers the areas of cybersecurity management, cyberattack response and nuclear regulators' legal frameworks. The review of legal frameworks focuses on countries with at least one operating nuclear facility. This comprehensive theoretical review thus serves as the basis for developing an innovative and comprehensive Cyberattack Response Model. In turn, the Model represents a practical contribution towards providing a higher level of cybersecurity and, consequently, a higher level of nuclear safety in the nuclear sector and a higher level of national security in other critical infrastructure sectors.

4.2 Practical Implications

The aforementioned research activities gave rise to an innovative and comprehensive Cyberattack Response Model. In Slovenia, the significance of the Model has already been recognised by the nuclear safety regulator, which has, by now, implemented a major part of the Model in its business and quality assurance processes. Most importantly, it dedicated a great deal of attention to strengthening the cooperation between all key stakeholders in the nuclear sector, which resulted in:

- the establishment and management of the national working group bringing together representatives of key stakeholders in the nuclear sector,
- the exchange of information, knowledge and experience, and
- the organisation and implementation of joint exercises.

So far (beginning of 2019), the Model has been mostly, but not fully implemented. The reasons lie in the legal framework, which has not been adapted yet, the lack of clearly agreed division of competences in the field of cybersecurity at the State level and the rather complex and expensive implementation of technical cybersecurity measures.

The full implementation of the proposed Cyberattack Response Model is expected to improve the response to cyberattacks both in the nuclear sector, as well as in other critical infrastructure sectors, thus setting the foundations for further development of expertise in this field and eliminating minor shortcomings.

The findings of the research study, which served as the basis for the proposed Model, will help experts in Slovenia and abroad in providing nuclear safety and nuclear security. The Model is useful both at the decision-making level, as well as on the technical level. It is particularly useful to all those, who are involved in amending legislation, adopting internal procedures and technical guides, and implementing cybersecurity measures.

4.3 Limitations and Future Work

Since the field of providing cybersecurity in the nuclear sector remains rather under-researched, it is expected that additional research activities will take place in the following areas:

- blended physical and cyberattacks,
- connections between business and process networks,
- relations between nuclear safety, nuclear security and emergency preparedness,
- understanding the risks, threats and vulnerabilities,
- preparation of legal acts, regulations and guides,
- managing the supply chain,
- implementing IoT (Internet of Things) at nuclear facilities,
- using wireless technology at nuclear facilities, and
- exchange of information, knowledge and operational experience on the national level and also in the international environment.

Such research studies will further improve cybersecurity at nuclear facilities and other critical infrastructure sectors.

The main limitation of the present paper stems from the fact that the Model is currently adapted to the legislation applicable in Slovenia, which is, nevertheless, mostly harmonised with international requirements. However, the Model may be simply transferred and adapted to fit other countries' legal restrictions.

The research study presented herein is a sound starting point for further research. As the same time, it proposes some new ideas about the currently under-researched or pertinent issues arising from the daily provision of cybersecurity in the nuclear sector.

Acknowledgements

This paper is partially based on a research project entitled Safety and security of cyberspace users – Criminological, victimological and preventative aspects (J5-9345, 2018-2020), financed by the Slovenian Research Agency. The project is carried out by the Faculty of Criminal Justice and Security, University of Maribor, Slovenia.

References

[Areh 2016] Areh, I.: "Forenzična psihologija, predstavitev, pričanje in ugotavljanje laži"; Fakulteta za varnostne vede / Ljubljana (2016).

[Baylon et al. 2015] Baylon, C., Brunt, R., Livingstone, D.: "Cyber Security at Civil Nuclear Facilities Understanding the Risks"; Chatham House Report / London (2015).

[Bernik 2014] Bernik, I.: "Cybercrime and cyberwarfare"; Wiley / London (2014).

[Brezavšček 2015] Brezavšček, A.: "Stochastic approach to planning of spares for complex deteriorating industrial system"; Quality technology & quantitative management, 12, 4 (2015), 465-480.

[Bučar-Ručman 2019] Bučar-Ručman, A.: "What is crime? A search for an answer encompassing civilisational legitimacy and social harm : overview and preventive measures." Crime, law and social change, (2019) [Online], Available from: https://doi.org/10.1007/s10611-019-09812-1

[CREST 2013] Cyber security incident response guide, (2013) [Online], Available from: https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

[ENISA 2010] European Union Agency for Network and Information Security: Good Practice Guide for Incident Management, (2010) [Online], Available from: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport

[ENISA 2017] European Union Agency for Network and Information Security: Communication network dependencies for ICS/SCADA Systems, (2017) [Online], Available from: https://www.enisa.europa.eu/publications/ics-scada-dependencies

[Falliere et al. 2011] Falliere, N., O Murchu, L., Chien, E.: "W32.Stuxnet.Dossier, Version 1.4"; Symantec / Cupertino (2011).

[IAEA 2009] International Atomic Energy Agency: Nuclear Security Series No. 10 - Development, Use and Maintenance of the Design Basis Threat: Implementing Guide, (2009) [Online], Available from: https://www-pub.iaea.org/mtcd/publications/pdf/pub1386_web.pdf

[IAEA 2011] International Atomic Energy Agency: Nuclear Security Series No. 13 - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities

(INFCIRC/225/Revision 5): Recommendations, (2011) [Online], Available from: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf

[IAEA 2011] International Atomic Energy Agency: Nuclear Security Series No. 13 - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5): Recommendations, (2011) [Online], Available from: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf

[IAEA 2013] International Atomic Energy Agency: Nuclear Security Series No. 20 - Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals, (2013) [Online], Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

[IAEA 2016] International Atomic Energy Agency: Computer security incident response planning at nuclear facilities, (2016) [Online], Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL005web.pdf

[IAEA 2018a] International Atomic Energy Agency: Preparation, Conduct and Evaluation of Exercises to Test Security Contingency Plans at Nuclear Facilities, (2018) [Online], Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL-008web.pdf

[IAEA 2018b] International Atomic Energy Agency: Nuclear Security Temporary 058 - Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements: Draft Implementing guide, (2018) [Online], Available from: https://www.iaea.org/sites/default/files/18/08/nst058.pdf

[IAEA 2019] International Atomic Energy Agency: The IAEA Mission Statement, (2019) https://www.iaea.org/about/mission, last accessed 2019/01/20.

[ISO/IEC 2016] International Organization for Standardization: ISO/IEC 27035:2016. Information technology — Security techniques — Information security incident management (2016).

[Mihelič and Vrhovec 2018] Mihelič, A., Vrhovec, S.: "Obligation to Defend the Critical Infrastructure? : Offensive Cybersecurity Measures"; J.USC (Journal of Universal Computer Science), 24, 5 (2018), 646-661.

[Lee and Lim 2016] Lee, K.-B., Lim, J.-I. (2016) The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd., In KSII Transactions on Internet and Information Systems, vol. 10 (2016), pp. 857-880.

[Lee et al. 2016]. Lee, M. R., Assante J. M., Conway, T.: "SANS Industrial Control Systems: Analysis of the cyber attack on the Ukrainian power grid."; SANS / Washington, (2016) [Online], Available from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[Loukas 2015] Loukas, G.: "Cyber-physical attacks how they work and how to protect against them"; Kidlington, Butterworth-Heinemann / London (2015).

[Markelj and Markelj 2016] Markelj, B., Markelj, Z. S.: "Comprehension of cyber threats and their consequences in Slovenia"; CLSR (Computer law & security review), 32, 3 (2016), 513-525.

[NIST 2012] Computer security incident handling guide: Recommendations of the National institute of standards and technology, (2012) [Online], Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[Onyeji et al. 2014] Onyeji, I., Bazilian, M., Bronk, C.: Cyber Security and Critical Energy Infrastructure, in The Electricity Journal, vol. 27 (2014), pp. 52-60.

[OSCE 2013] Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, (2013) [Online], Available from: https://www.osce.org/secretariat/103500?download=true

[*Pravilnik o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi* 2013] (2013).

[Purpura 2013] Purpura, P.: "Security and Loss Prevention (Sixth Edition)"; Kidlington, Butterworth-Heinemann / London (2013).

[SANS 2011] System Administration, Networking, and Security Institute: The incident handler's handbook, (2011) [Online], Available from: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

[SANS 2014] SANS ICS: ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack, (2014) [Online], Available from: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[SI-CERT 2018] Slovenski odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij: Poročilo o omrežni varnosti za leti 2016 in 2017, (2018) [Online] Available from:

https://www.cert.si/wp-content/uploads/2018/04/SI-CERT_LP_2016_2017.pdf

[Tomažič 2015] Tomažič, S. (2015, 1-5 June). *Slovenian case study on building and sustaining computer security culture*. Presented at the International Conference on Computer Security in a Nuclear World, Vienna, Austria.

[Tomažič 2019] Tomažič, S. (2019). *Model odziva na kibernetske napade v jedrskih objektih* (Unpublished doctoral dissertation), University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia.

[*Uredba o informacijski varnosti v državni upravi* 2018] (2018).

[URSJV 2019] Uprava RS za jedrsko varnost: Področje dela in organizacijska struktura, (2019) http://www.ursjv.gov.si/si/ursjv/podrocje_dela_in_organizacijska_struktura/, last accessed 2019/01/20.

[URSZR 2010] Uprava Republike Slovenije za zaščito in reševanje: Državni načrt zaščite in reševanja ob jedrski ali radiološki nesreči, Verzija 3.0, (2010) [Online] Available from: http://www.sos112.si/slo/tdocs/jedrska.pdf

[US NRC 2010] United States National Regulatory Commission: Regulatory Guide 5.71: Cyber security programs for nuclear facilities, (2010) [Online], Available from: https://www.nrc.gov/docs/ML0903/ML090340159.pdf

[Vrhovec et al. 2015] Vrhovec, S., Trkman, M., Kumer, A., Krisper, M., Vavpotič, D.: "Outsourcing as an economic development tool in transition economies: scattered global software development"; Information technology for development, 21, 3 (2015), 445-459.

[*Zakon o informacijski varnosti (ZInfV)* 2018] (2018).

[*Zakon o varstvu pred ionizirajočimi sevanji in jedrski varnosti (ZVISJV-1)* 2017] (2017).

[ZDNet 2019] ZDNet: US hospital pays $55,000 to hackers after ransomware attack, (2019) https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/, last accessed 2019/05/28.