FIRST NATIONAL EXERCISE IN COMPUTER SECURITY IN THE NUCLEAR SECTOR IN SLOVENIA

S. TOMAŽIČ
Slovenian Nuclear Safety Administration (SNSA)
Ljubljana, Slovenia
Email: samo.tomazic@gov.si

I. BERNIK
Faculty of Criminal Justice and Security
Ljubljana, Slovenia

M. TOMAŽIČ
Slovenian Nuclear Safety Administration (SNSA)
Ljubljana, Slovenia

Abstract

Whether we like it or not, acknowledge or not, the number of cyber-attacks is increasing. Malicious actors are becoming more and more sophisticated, they are highly motivated, some also well-funded, and focused on the nuclear sector. If cyber-attacks in the nuclear sector were to be successful, consequences of such an attack could potentially be catastrophic for people or the environment. Therefore, our efforts in computer security have to increase. One example are computer security exercises, which are an essential element in ensuring a high level of computer security in nuclear security. The main objectives of exercises are awareness, testing internal procedures, identifying gaps in computer security measures, testing the efficiency of the computer security plan, and training the Computer Security Incident Response Team, etc. All these objectives, and more, can be achieved by different types of exercises: table-top, drills, red vs. blue, and simulated and combined exercises, etc. To our knowledge, there were only a handful of computer security exercises conducted in the nuclear sector to date. In order to substantiate our beliefs, we conducted a research, comprised of a descriptive analysis of various publicly available sources, structured interviews with national and international experts in the nuclear sector, and verified our findings with emergency preparedness experts employed at the Slovenian Nuclear Safety Administration. The results of our research represented a structured and comprehensive approach in preparing, conducting and evaluating computer security exercises. Based on the results of the research, we started preparing the first national exercise in computer security in the nuclear sector in Slovenia, called KIVA^{2019}. It was a one-day table-top exercise with a short storyline and a cyber-attack scenario based on current incidents in critical infrastructure. The exercise was attended by participants from all key stakeholders in the nuclear sector: nuclear facility operators, competent authorities, technical support organizations, and suppliers of computer software and hardware equipment. Due to the importance of the topic on a national level, the exercise was attended by many other external observers: Ministry of Interior, Ministry of Public Administration and Faculty of Criminal Justice and Security. As we have predicted, the evaluation revealed several areas where there are possibilities for improvement. These areas are not new to nuclear security, and include an improvement of information sharing on the national and international level, and harmonization of internal procedures of all key stakeholders in the nuclear sector. Findings were then analyzed and a detailed action plan was developed. KIVA^{2019} represents a starting point for computer security exercises in Slovenia. Knowledge gained from this research and KIVA^{2019} will help prepare for future exercises, enhance cooperation with the emergency preparedness team, and improve computer security in the Slovenian nuclear sector in general.

1. INTRODUCTION

In the last decade, the expert, scientific and sector-specific literature focused primarily on raising awareness of computer security. It emphasised the basic of computer security, implementation of management system, risk analyses, etc. However, trends indicate that this is not enough. It is necessary to focus on narrower segments of computer security [1], such as legislation, process systems, supply chain, responding to cyber-attacks, education and exercises, etc. All this indicates that key personnel, both in leadership and technical positions, are aware of the issues and wish to raise the level of computer security. With such approaches, we move from the time where we only waited for a cyberattack and responded to an incident, to a time where we actively prepare for cyber-attacks.

Cyber-attacks can be defined in many ways. One of the key definitions is the division into un-targeted and targeted attacks. While un-targeted attacks do not select their target, targeted cyber-attacks are focused on specific, chosen target.

In the nuclear sector, there are many potential targets, with nuclear power plants, research reactors, and repositories being the largest and most interesting ones. Nuclear facility systems are based on security principle of graded access and defence in depth [2]. Successful cyber-attacks are therefore less likely; however, this does not mean that they will never occur. Quite the opposite – the nuclear sector has been the target of several publically known targeted cyber-attacks [3]. The first such attack, called Stuxnet [4], happened in 2010, and it disabled the uranium-enrichment centrifuges in a nuclear facility in Iran. In 2015, the largest Korean energy organisation and nuclear facility operator – Korean Hydro and Nuclear Power – was a target of a cyberattack. The purpose of this cyberattack was to steal sensitive information and spread fear in public [5]. There were also several un-targeted cyber-attacks in the nuclear sector. In 2014, the control room of the Monju Nuclear Power Plant in Japan was hit by an un-targeted cyberattack. The attack did not impact the operation of the nuclear facility; however, unauthorised access to certain control systems was detected. The last publically known un-targeted cyber-attack hit the Gundremmingen Nuclear Power Plant in Germany in 2016. The attack infected a large number of information systems in the business section of the nuclear facility, while the process side of the power plant remained unaffected.

To avoid such cyber-attacks, we have to conduct so-called assurance activities [6], which include preparation of appropriate guides, training, information exchange, participation in working groups, etc. Assurance activities also include preparing, conducting and evaluating the exercises [7] for checking awareness, testing internal procedures, identifying gaps in computer security measures, testing the efficiency of the computer security plan, and training the Computer Security Incident Response Team, etc. All these objectives, and more, can be achieved by different types of exercises: table-top, drills, red vs. blue, and simulated and combined exercises, etc. [8].

Such an exercise, KIVA^{2019}, was organised, conducted and evaluated by the Slovenian Nuclear Safety Administration (SNSA) in 2019, on the basis of a multi-year research and a cyber-attack response model in nuclear facilities. Key stakeholders in the Slovenian nuclear sector participated in the exercise: representatives of the operator at Krško Nuclear Power Plant operator, regulator Slovenian Nuclear Safety Administration (SNSA), technical support organisation (SI-CERT), and two suppliers of computer software and hardware. In addition to active participants, there were also external observers: representatives from the Faculty of Criminal Justice and Security, Ministry of the Interior (regulator for nuclear security), and the Ministry of Public Administration – IT Directorate. The main goal of the exercise was to check the adequacy of the prepared cyber-attack response model in nuclear facilities. Using the exercise, we checked existing internal procedures of stakeholders, communication channels, reporting and cooperation in the event of a cyber-attack targeting a nuclear facility. The exercise has shown that there are still many challenges that need to be addressed in this area. All participants welcomed the exercise KIVA^{2019}, were very positively and expressed their wish for such exercises in the future, which represents a good basis and encouragement for improving the response to cyber-attacks in nuclear facilities in Slovenia and indirectly elsewhere.

2. METHODS

When preparing the model used for KIVA^{2019}, we used descriptive methods and structured interviews with national and international experts in the nuclear sector, and verified our findings with emergency preparedness experts employed at the Slovenian Nuclear Safety Administration. At the end, we used the synthesis method to summarise the findings and to structure them in an innovative and comprehensive cyber-attack response model, intended for key stakeholders in the Slovenian nuclear sector. We used the model as a framework for preparing, conducting and evaluating the KIVA^{2019} exercise.

As part of the first, descriptive research method, we reviewed articles, dissertations, books and journals, and reviews publicly accessible physical and electronic sources, such as national legislation, national reports, regulation, guidelines, standards, best practices, recommendations, regulatory documents, and reports of international organisations, e.g. International Atomic Energy Agency – IAEA. The detailed review covered areas of computer security management, cyber-attack responses, and legislative framework of nuclear regulators. In the legislative framework review, we included countries with at least one operating nuclear power plant.

The second method used was structured interviews. We conducted 15 interviews, with each interview lasting one hour and a half on average. Interviews were conducted with experts employed at nuclear facilities, regulatory bodies, technical support organisations, computer hardware and software suppliers, and others responsible for computer security in the nuclear sector. We conducted the interviews in person. Before starting the interviews, we ensured the anonymity of interviewees and their country of origin or stakeholder that employs them. All interviewees had the opportunity to review the questions before the interviews, some even had several day or weeks, as they had to obtain permissions from their supervisors or other competent state bodies to participate in the interview. At the start of the interview, we provided a brief description of who we are, where we come from, what we are doing, and – most importantly – what is the purpose of our study. The purpose of the interviews was to check the findings of the literature review. The interviews provided an additional insight into the current cyber-attack response readiness situation in the nuclear sector. We obtained an additional insight into the current situation with additional interviews with emergency preparedness experts at the SNSA. Emergency preparedness experts have several decades of experience in organising exercises, use highly perfected, verified internal procedures, and have implemented appropriate communication channels, management systems during emergencies, and special-purpose premises and information and communication equipment. This made preparing, conducting and evaluating the KIVA^{2019} exercise easier.

3. PREPARING, CONDUCTING AND EVALUATING KIVA^{2019}

The organisation of the exercise consisted of several stages, as international standards and best practices specifically recommend three, four or even more stages [9]. Organisation of KIVA^{2019} consisted of three stages (Figure 1). The first stage represent preparation, and is the most important stage. It requires the most organisational resources from the organiser (time, employees, and money). If the first stage is not executed appropriately, it affects both later stages. The second stage represents execution. This is the shortest stage, but sums up everything set in the first stage of preparation. The purpose of the last stage, evaluation, is to conduct an in-depth evaluation of both previous stages, as part of the preparation of report, and to propose recommendations for further improvement as part of an action plan, which can be included in the exercise report or represent an independent document.

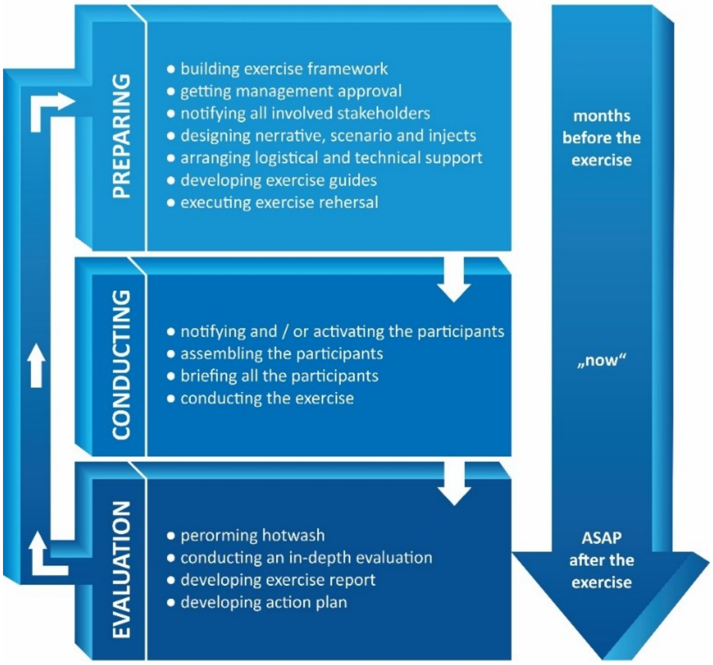
PREPARING
• building exercise framework
• getting management approval
• notifying all involved stakeholders
• designing nerrative, scenario and injects
• arranging logistical and technical support
• developing exercise guides
• executing exercise rehersal
CONDUCTING
• notifying and / or activating the participants
• assembling the participants
• briefing all the participants
• conducting the exercise
EVALUATION
• perorming hotwash
• conducting an in-depth evaluation
• developing exercise report
• developing action plan
months before the exercise
„now“
ASAP after the exercise

FIG. 1. Organization of KIVA^{2019} exercise.

A description of how SNSA prepared, conducted, and evaluated the KIVA^{2019} exercise is presented below.

3.1. Preparing the exercise

As before every project that requires an organisation to dedicate time, human and financial resources, we obtained the management's approval for the organisation of the KIVA^{2019} exercise during the preparing stage. To obtain the approval, we had to prepare a precise framework of the exercise, which included a detailed list of organisational resources, participating stakeholders, exercise goals and type, planned scenario, etc. The management agreed to the start of exercise preparation on the basis of this framework.

The next step was the presentation of the above exercise framework to key stakeholders in the Slovenian nuclear sector. With each individual stakeholder, the exercise framework was supplemented or modified, and ultimately unanimously approved. We continued with the preparation of the story, exercise scenario, and injects, while simultaneously developing the criteria for assessing the effectiveness of exercise. The criteria involved both expected measures and actually implemented measures, optimal time of execution and actual time of execution.

The exercise scenario was as follows: "An employee at a nuclear facility attended an international conference, bringing with him his personal smartphone, tablet, and company laptop. At the event, he had to transfer certain data to his laptop using an USB key, as he could not actively participate otherwise. As he did not have his own USB key, a foreign acquaintance lent him his. When he returned to work, he turned on his company laptop. The antivirus software immediately warned him of a potential malware infection. As he was in a hurry to get home, he decided to notify his supervisors the next day, and he left his laptop turned on and connected to the local network. During the night, the infection spread to several computers in the business network. The following morning computer infections began occurring on the business network, and the Security Information and Event Management system triggered an alarm due to a large quantity of transferred data from personnel records to the Internet, with security staff reporting on interruptions and malfunctions of security cameras."

Table 1 shows injects received by exercise participants at specific time intervals. The first column lists the inject time, followed by event, sender, and recipient.

TABLE 1. EXERCISE INJECTS

time	event	sender	recipient
09:00	START	exercise lead	all
09:10	Hackers attacking critical infrastructure!!!	media	all
09:15	Malware on desktop computer	facility	facility
09:25	Unknown flying object (drone)	police	facility
09:30	Problems of a citizen	citizen	technical support
09:30	Kovter malware	technical support	regulator
09:30	We would like to buy different Axis cameras	citizen	supplier
09:45	Cameras not working properly	facility	facility
10:15	OT-CERT advisory – Triton (Trojan.Trisis)	technical support	all
10:40	Cameras not working at all	facility	facility
11:00	SIEM report of unknown data transfer	facility	facility
11:00	Axis 2.x cameras critical vulnerability found	sub-supplier	supplier
12:00	END	exercise lead	all

Key stakeholders participated in the exercise, and each stakeholder had a different scenario. However, all the stakeholders had to cooperate in order to successfully resolve the incident.

In order to successfully conduct the exercise, we knew that we required appropriate premises, information and communication equipment, and technical support in the event of any problems. All logistical and technical support was provided by the Division of Emergency Preparedness with its staff and its emergency response centre – NUID centre.

Once all participants were known, the story, scenario and injects, and logistical and technical support prepared, we began preparing the instructions for participants. We prepared different instructions for the KIVA^{2019} exercise. Every stakeholder received instructions for its organisation. We also prepared additional instructions for evaluators and external, independent observers. At their exercise locations, all participants had access to basic instructions on the use of information and communication technology and a list of important contacts.

Several days before the exercise, associates of SNSA conducted a rehearsal as part of the preparation for the exercise, in order to review the comprehensibility of the story and scenario, timing for providing injects, usability of information and communication equipment, and effectiveness of the logistical and technical support. At the rehearsal, all four stakeholders were played by SNSA associates. Despite the careful preparation of the exercise, the rehearsal allowed us to identify a series of problems, which would otherwise hinder a successful execution of the actual exercise (e.g. problems in understanding the scenario, inoperable login accounts, inadequate initial presentation for participants, and use of too many abbreviations).

During exercise preparation, we conducted many other, less complex activities, which were just as time consuming, specifically: arranging physical and logical access, coordinating schedules for meetings and exercises, sending invitations, preparing graphic design, preparing training for participants, catering organisation, arrangement of a photographer, cooperation with the media, etc.

Exercise preparations were the most time consuming and complex part of the exercise. Deficiencies during preparation most often became apparent in the execution and evaluation, which we partially managed to alleviate with the rehearsal. The time for exercise preparation always depends on the type of exercise, goals pursued, and the number of participants. To prepare exercise KIVA^{2019}, we needed approximately one year.

3.2. Conducting the exercise

The execution is the second stage of the exercise and includes several steps. First, it is necessary to notify the participants, have them gather at the planned location, provide them with all necessary security and safety instructions and instructions for participating in the exercise, and finally execute the exercise. As for the start of preparations, the start of the exercise required the management's approval. It is recommended that the management attends and starts the event with an introduction.

Exercise KIVA^{2019} was started by the director of SNSA, Dr Andrej Sitar, who highlighted the importance of nuclear and computer security, conducting such exercises, and the participation of all key stakeholders.

3.2.1. Notifying and activating participants

The procedure for notifying participants depends on how the exercise is conducted. If the exercise is unannounced, the participants are notified via communication channels established beforehand. These can be mobile or stationary phones or pager. Who to notify, and which system to use must be clearly defined in internal procedures. Contact information of participants must be regularly updated. In our case, the activation procedure for exercise KIVA^{2019} was simple, as the exercise was announced in advance, meaning that participants were informed of where and when they have to arrive at the defined location, and what role they will play.

3.2.2. Assembly

Premises where the exercise is conducted are often the same premises used for responding to actual incidents. Security system, procedures for accessing these areas and using the information and communication equipment are designed accordingly. Consequently, we had to provide suitable access to these areas and accompaniment for all participants for the entire duration of the exercise. Upon arrival, every participant received a tag showing their name and surname, as well as the organisation or role at the exercise. This ensured that all participants, who were generally not acquainted, were able to easily identify each other. The assembly is complete once all participants are gathered on location, and the exercise can begin. Assembly for exercise KIVA^{2019} required approximately 20 minutes.

3.2.3. Instructions

Instructions include not only basic information on the exercises, but also directions on following security and safety instructions, use of ICT equipment, communication channels and procedures in the event of a real emergency incident (nuclear or radiological incident, fire or building evacuation, etc.). As we used real-world systems, which the participants were generally not familiar with, it was necessary to pay special attention to correct use of ICT equipment and areas of the NUID centre.

Basic instructions for the exercise were divided into several parts. The first part was intended to familiarise the participants with the exercise, i.e. the course of the exercise, the use of the cyber-attack response model in nuclear facilities, organisers' contact information, basic incident information, planned breaks and the location of each function. The second part was intended and adapted to specific roles of individual participants. We prepared and handed out manuals for: (1) nuclear facility operator, (2) nuclear regulator, (3) technical support organisation, (4) computer equipment supplier, and (5) independent observers.

3.2.4. Exercise execution

In the execution of the exercise, it was necessary to consistently follow the scenario and the story. Injects used to follow the scenario must be delivered to participants promptly and at the time logged on the injects. It is important that different participants receive different, realistically plausible injects, adapted to their role.

An important role in the execution of the exercise is the exercise lead. They must appropriately follow the scenario, adapting the scenario based on the situation, either accelerating or slowing the scenario, or even stopping the exercise. During exercise KIVA^{2019}, the exercise lead accelerated the scenario because participants carried out individual tasks faster than expected.

For the purpose of the evaluation, important and relevant observations should be written down promptly during the exercise. All participants can manage such notes for themselves, while the exercise lead and observers should pay them special attention. For this purpose, the version of the instructions for observers at the KIVA^{2019} exercise included pre-defined, expected measures of participants, in addition to the overview of the entire scenario, model and all injects.

In addition to their own notes, exercise KIVA^{2019} was conducted using the online inter-ministerial emergency communication system (hereinafter: KID), which has been in use in Slovenia during nuclear or radiological accidents since 2008, to ensure a better evaluation and archive of the exercise. Using KID, the participants received injects via a simulant (on paper, in addition to via KID), logged their activities, and communicated with each other. Simulant represents a person, who doesn't actually play in the exercise, but would be involved in an actual event. Due to the type of exercise (security exercise and work with sensitive data), KID used private communication exclusively.

All participants at the exercise also used the information and communication equipment in the NUID centre: telephones, computer, multi-purpose devices (printers and optical scanners), KID, projectors, interactive multimedia board, and LED displays. During the exercise, we had to ensure the general well-being of the participants (food, drink, ventilation, appropriate breaks).

The exercise scenario, i.e. the practical part of exercise KIVA^{2019}, was completed in three hours, between 9:00 and 12:00. After 12:00, the exercise was evaluated, which lasted one hour.

3.3. Exercise evaluation

The evaluation of exercise KIVA^{2019} was conducted immediately after the completion of the exercise. The immediate analysis – so-called hotwash – was conducted in order to analyse all activities as soon as possible, while memory was still fresh and undistorted. During the hotwash, all participants presented their opinions and comments on the exercise organisation, course of the exercise, scenario, injects, used ICT equipment, technical and logistical execution, positive aspects, and observed options for improvement. Notes by independent observers were very valuable for a comprehensive analysis.

Based on the exercise lead's observations, proposals made by active participants, independent observer and external observers, we prepared a comprehensive analysis of the exercise one month after its completion. The analysis includes an evaluation of the course of the exercise, performance criteria (differences between expected and implemented measures), SWOT analysis (Strengths, Weaknesses, Opportunities, Threats), used to identify areas that are currently not yet appropriately covered or addressed, and a validation and verification of cyber-attack response model in nuclear facilities.

The key part of the analysis, in addition to the validation and verification of the cyber-attack response model in nuclear facilities, is the action plan, in which we listed the identified deficiencies of response capabilities to cyber-attacks and proposed possible improvements of the current situation.
The execution

4. DISCUSSION

Exercises such as KIVA^{2019} are necessary to ensure a high level of computer security. With the implemented system for ensuring computer security, which includes exercises, we continually identify deficiencies and on this basis propose action plans. On their basis, we attempt to quickly resolve such deficiencies.

4.1. Findings

Exercise KIVA^{2019} was the first such exercise in the nuclear sector (and in the area of the entire critical infrastructure) in Slovenia, and one of the very few in the world. During the exercise, the participants followed the prepared comprehensive cyber-attack response model in nuclear facilities. The participants agreed that the model is useful, intuitive and understandably guides stakeholders through all cyber-attack response steps. As the most important observation in this model, they highlighted the integration of key stakeholders in national working groups and exercises, such as KIVA^{2019}. It prepares stakeholders for mutual cooperation and, above all, trains them for responding to a real-world situation, such as a cyber-attack on the nuclear sector.

The participants pointed out that the model could be used in other parts of critical infrastructure, both domestically and abroad. The validation of the cyber-attack response model in nuclear facilities, which was the central part of the exercise analysis, has shown that the model provides additional instructions for areas not yet completely covered:

- legislation and stakeholders' internal procedures;
- communication, including reporting and notification of stakeholders and regulatory bodies;
- notifying domestic and foreign public;
- cooperation in working groups;
- professional education and training of participants;
- determining responsibilities of individuals and organisations;
- establishing Computer Security Incident Response Teams;
- establishing suitable and secure information and communication tools;
- ensuring a secure supply chain;
- harmonisation of response by all stakeholders.

The analysis has shown that communication, notification and exchange of information were mostly deficient among the stakeholders during the exercise. Due to these deficiencies, the stakeholders lacked an overview of the entire situation, had more issues connecting the circumstances of the incident, and more problems identifying the cyber-attack. In terms of notifications, there were questions on who to share information with, when to share the information, at what level, what are the criteria for sharing information, etc.

It was also pointed out that there are already working groups on the level of the state, where specific information on threats is already shared. This knowledge needs to be systematically shared with stakeholders who require such information. It is also necessary to improve coordination and integration of key stakeholders, particularly state bodies, and determine appropriate notification protocols, as joint responses to cyber-attacks is the most effective.

During the exercise, the participants used the KID system and telephone lines for communication. As neither the KID system nor traditional telephone lines are secure communication lines, it was proposed that a unified secure platform is established for exchange of sensitive information on the national level. Due to the nature of its work, the nuclear sector is very sceptical about sharing information with the public, particularly information related to nuclear security. The primary reason is, of course, the potential for theft, modification or inaccessibility of sensitive information, while the second reasons is to maintain reputation in the eyes of the profession and the public.

As it became evident during the exercise, blind following of internal procedures, without using common sense, negatively impacted certain decisions. Because cyber-attacks can be very diverse and because it is impossible to foresee all combination of diverse attack types and vectors, the use of common sense and experience in responses and adaptable procedures is essential during such incidents.

4.2. Action plan

The action plan is essential to improve the system checked at any exercise. The action plan transposes all findings, primarily weaknesses, opportunities and threats, into activities necessary to eliminate all identified weaknesses and threats, or to take advantage of identified opportunities. At the KIVA^{2019} exercise, we recorded eight findings in the action plan, which require eight measures by different stakeholders with competences and responsibilities for responding to cyber-attack on a nuclear facility in Slovenia, including specifically for responding to a cyber-attack on the Krško Nuclear Power Plant. SNSA has undertaken supervision of the implementation of measures, and most measures are planned to be completed in 2020.

4.3. Future exercises

As KIVA^{2019} was the first cyber-attack response exercise in nuclear facilities in Slovenia, the participants at the exercise emphasised several times that future exercises in this field are necessary and highly desirable. Accordingly, the action plan includes a measure for SNSA to draw up a technical document together with IAEA, which will present a programme for such exercises (organisation, execution and evaluation), and then to implement this programme in SNSA procedures. Considering the resources required to conduct such exercises, it is necessary to carefully plan appropriate schedules, scope, and the type of exercise, in terms of execution. Of course, it is good if the exercise includes as many stakeholders possible, but it is also very beneficial if such exercises are conducted in a smaller scope. Small scope exercises, which include only several stakeholders, allow participants to separately or partially test their systems and tasks in responding to cyber-attacks in a shorter time.

This year, SNSA has already started preparation for KIVA^{2020}, which will be organised in cooperation with the IAEA and the Austrian Institute of Technology (AIT). It is expected to be carried out in the second half of 2020, and its purpose is to test internal procedures of participants that ensure security of critical infrastructure and cyber-attack response readiness in nuclear facilities. One of the goals of KIVA^{2020} is to invite as many relevant international organisation, which are involved in cyber-attack responses in nuclear facilities, such as ENISA, EUROPOL, and INTERPOL.

REFERENCES

[1] TOMAŽIČ, S., BERNIK, I., "Cyberattack Response Model for the Nuclear Regulator in Slovenia", Journal of Universal Computer Science, (2019).

[2] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5), Nuclear Security Series nº 13 (2011).

[3] BAYLON, C., BRUNT, R., LIVINGSTONE, D., "Cyber Security at Civil Nuclear Facilities Understanding the Risks", Chatham House Report, London (2015).

[4] FALLIERE, N., O MURCHU, L., CHIEN, E., "W32 Stuxnet Dossier, Version 1.4", Symantec, Cupertino (2011).

[5] LEE, K.-B., LIM, J.-I., "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) 857-880.

[6] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Fundamentals - Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Series nº 20 (2013).

[7] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct and Evaluation of Exercises for Security of Nuclear and Other Radioactive Material in Transport, Non-serial Publication nº TDL007 (2018).

[8] SIRC, I., TOMAŽIČ, M., "Conducting Trainings of SNSA Emergency Response Team", The 28th International Conference Nuclear Energy for New Europe - NENE2019, DJS, Ljubljana (2019).

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