RESULTS OF THE 2019 IAEA WORKSHOP "COMPUTER SECURITY APPROACHES AND APPLICATIONS IN NUCLEAR SECURITY" IN BERLIN

D. SOMMER
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
Cologne, Germany
Email: Dagmar.Sommer@grs.de

A. SCHUG
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
Cologne, Germany
Email: Alexander.Schug@grs.de

Abstract

Computer security within a nuclear security regime requires continuous improvement of computer security measures to face ever increasing adversary capabilities. For this, one key factor is exchange of information (e. g. application of effective methods, technologies and tools in new and innovative ways) and identification of good practices regionally, nationally and globally. With this knowledge not only the national but also the international security level of nuclear material, nuclear facilities, other radioactive material and associated activities can be enhanced. One way to achieve this is exchanging good practices and other interesting information in the field of nuclear security in meetings like the IAEA Technical Meeting on "Computer Security Approaches and Applications in Nuclear Security" held from 23rd to 27th September 2019 in Berlin, Germany. The objectives of this meeting were to discuss regional; national and international approaches to enhance computer security and to describe implementations of computer security measures by organizations having roles and responsibilities within the nuclear security regime. Over 140 participants from 68 IAEA member states with different roles such as executive management, regulatory bodies, computer security managers, administrators and technicians, physical protection system managers and administrators, sensitive information managers, and engineers from all domains of nuclear security took part in the meeting. The paper gives an overview of the challenges and solutions of national and organizational approaches to computer security specific to each domain of nuclear security (e. g. nuclear material and facilities, other radioactive material and associated activities, and material out of regulatory control) discussed at the 2019 IAEA workshop in Germany. Further, current developments in international regulations on computer security are outlined. The approaches are compared, and differences are pointed out. Special attention is paid to experiences and best practices identified in different countries bringing the regulatory approaches into practice.

1. INTRODUCTION

In recent years computer security within nuclear security regimes became an increasingly demanding topic for regulators, operators and governance. Spectacular state driven attacks like Stuxnet on nuclear facilities in September 2010 [1], BlackEnergy on critical infrastructures in December 2015 [2] or the global campaign of WannaCry in March 2017 [3] led to a massively growing interest in this topic. Together with a trend to implement digital Instrumentation and Control (I&C) systems [4] and commercial-off-the-shelf (COTS) components [5] [6] in nuclear facilities computer security became one of the leading topics in current actions of security regulation for these facilities. To support international regulators, the International Atomic Energy Organization (IAEA) and the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) organized the Technical Meeting "Computer Security Approaches and Applications in Nuclear Security" from 23rd to 27th September 2019 in Berlin, Germany. According to the IAEA this Technical Meeting (TM) was one of the largest and most visited TM of its kind to date, showing the large interest of the member states in this topic. With the participants representing executive management, regulatory bodies, computer security managers, administrators and technicians, physical protection system managers and administrators, sensitive information managers, and engineers from all domains, the TM covered the topic computer security from all perspectives of the nuclear security regime.

The IAEA is currently developing guidance material for computer security in the nuclear security regime. Both documents, NST 045 "Computer Security for Nuclear Security" [7] and NST 047 "Computer Security Techniques for Nuclear Facilities" [8] are available as drafts for the member states and shall be finalized with

input from the TM. 17 presentations and different open panel discussions concerning all domains of nuclear security (e. g. NSS 13 - nuclear material and facilities, NSS 14 - other radioactive material and associated activities, and NSS 15 - material out of regulatory control) were held, as well as a workshop on computer security in smaller working groups. The TM was able to give a detailed view of the current challenges and regulatory approaches on computer security in nuclear security to support the further development of the NST-drafts.

The main goals of the Technical Meeting were to support the development of NST 045 and NST 047 drafts, to provide an overview of ongoing activities in the member states concerning computer security, to enhance the knowledge and capabilities of participating member states in the field of computer security and to extend the international cooperation between member states.

2. STRUCTURE AND OVERVIEW OF THE TECHNICAL MEETING

The Technical Meeting was structured into five topics hosted and moderated by experts in these fields. In the following subsections an overview of the topics and their content is given.

2.1. Topic #1 - IAEA Computer Security, Terminology, Context

The first topic of the Technical Meeting consisted of three presentations to introduce the main topics of the TM to its participants. The IAEA Division of Nuclear Security and its Computer Security Program were introduced, the work of the division was summarized and the help and support programs as well as support options by the IAEA were presented. The current International Framework for Stability in Cyberspace was presented to the participants with a focus on current international handling of cyberattacks and the growing presence and risk of Advanced Persistent Threats (APTs) [9]. To counteract cyberattacks, response organizations like Computer Emergency Response Teams (CERT) [10] as well as international standards and good practices to prevent the success of these attacks were introduced to the audience. The last presentation of this topic covered expectations and reality of cyberattacks. APTs and counter measures were introduced to the audience as a critical discourse on effectiveness of unusual attacks. With a focus on new ways of attacks like supply-chain attacks, improbable attacks [11] and newly discussed hardware attacks [12] the presentation reflected new trends and developments in threats for computer security. Each lecture was followed up by a brief discussion between the presenting expert and the participants of the TM.

2.2. Topic #2 - Approaches to Computer Security Risk in Nuclear Security

In this topical session, the regulatory approaches of different IAEA member states were presented. Seven presentations from six different member states showed the approaches and cyber security activities of seven national authorities:

- United States of America: Nuclear Regulatory Commission (NRC)
- Germany: Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)
- South Korea: Korea Institute of Nuclear Nonproliferation and Control (KINAC)
- United Kingdom: Office of Nuclear Regulation (ONR)
- Switzerland: Swiss Federal Nuclear Safety Inspectorate (ENSI)
- United States of America: National Nuclear Security Administration – Office of Radiological Security (NNSA ORS)
- Georgia: State Security Service of Georgia (SSSG)

The lecturers showed their approaches to computer security in specific nuclear security domains. Due to their different backgrounds and focus areas on as regulatory competences, graded approaches, security measures and risk assessments, the lecturers offered an overview as well as examples of the national approaches to computer security in nuclear security domains covering NSS 13, 14 & 15. The topic was closed with a panel discussion of all speakers in which the challenges and chances of future regulatory actions were discussed.

2.3. Topic #3 – International Standards and Publications

International standards build an international framework for requirements on computer security in the nuclear domain. The topic consisted of three lectures reporting on current and future international standards developed for computer security in the nuclear security regime. With IEC 61513 (Nuclear power plants – Instrumentation and control important to safety – General Requirements for Systems) a basic standard for nuclear facilities is available which is expanded with the standards IEC 62645 (Nuclear power plants – Instrumentation and control systems – Requirements for security programs for computer-based systems) and IEC 62859 (Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity). Further the standard IEC 63096 (Nuclear power plants Instrumentation, control and electrical system – Security controls) is currently in development and will be launched in 2020 as a specific standard for computer security in nuclear facilities. The standard introduces requirements on measures and provisions to avoid, detect, counteract, or minimize cybersecurity risks based on a graded approach. The standard shall support national regulators with detailed requirements for computer safety in nuclear facilities. The topic was closed with a panel discussion of all speakers giving an outlook on future regulatory approaches, supporting international standardization and approaches to computer security within the framework of international standards.

2.4. Topic #4 – Functional and Organizational Computer Security Working Sessions

The biggest topic of the Technical Meeting consisted of a workshop split into five working group sessions. All participants of the Technical Meeting took part in the workshop and were divided into 12 groups with each one having a different expertise focus on one of the domains of nuclear security: nuclear material and facilities, other radioactive material and associated activities, and material out of regulatory control. In the working sessions all participants developed individual approaches to computer security in compliance with the IAEA drafts NST 045 and NST 047. The participants followed a functional or organizational approach, shown in table 1 to develop an individual computer security concept.

TABLE 1. WORKSHOP STRUCTURE

Workshop Session	Functional approach	Organizational approach
Session 1	Identifying functions in nuclear security	Identifying organizations in nuclear security
Session 2	Grading the nuclear security functions	Grading the nuclear security organizations
Session 3	Digital technology used for nuclear security functions	Digital technology used by nuclear security organizations
Session 4	Measures to ensure computer security	Measures to ensure computer security
Session 5	Preparation of results and presentation	

In each working session the participants were asked to apply a graded approach for functions or organizations in nuclear security: Therefore, as the first step the functions or organizations of the facility or country had to be identified, followed by assigning the appropriate security levels in a second step. In the third step the respective technologies were identified and finally in step four specific security measures for the identified technologies were defined. The final working session enabled the participants to refine their results to report back to the IAEA as well as to present the results to all participants of the TM followed by its discussion.

2.5. Topic #5 – Computer Security within the German Nuclear Security Regime

The final topic of the TM outlined the country specific realization of computer security in nuclear facilities in Germany. Four presentations dealt with German actions and measures to ensure computer security followed by a panel discussion with all participants.

As an introduction to the topic the German Guideline for the Protection of IT Systems in Nuclear Plants and Facilities of Protection Category I and II (Malicious Acts Guideline IT) enacted in 2013 was presented. A lecturer from the authority of the German state Schleswig-Holstein gave an outline of their experiences gained in the implementation of supervisory procedures. After presenting the implementation phases of the Malicious Acts Guideline IT for the facilities in Schleswig-Holstein, the lecturer concluded with lessons learned for the authority: The time requirements, personnel requirements and the complexity of verification and implementation of the guideline's requirements were severely underestimated. No deficits concerning the guideline's protection objectives were detected during the implementation of the guideline, while a significant increase of sensitization of personnel concerning computer security was recognized as well as a general improvement of the computer security level in the facilities.

Following up the operator perspective was presented with a focus on the operator association VGB on nuclear security and computer security. The VGB organizes Technical Committees (TC) with Technical Groups (TG) for engineering and security aspects of different industrial sectors in Germany. One of these Technical Groups is the Electrical and I&C Engineering TG within the Nuclear Power Plants Technical Committee. This TG offers support for facility operators in Germany by developing a compendium for all topics of the Malicious Acts Guideline IT, compatible rules for mobile IT devices, a concept for the IT-security in the transition to and during decommission as well as providing training courses for plant cyber security personnel.

To allow further insight into the implementation of the "Guideline for the Protection of IT Systems in Nuclear Plants and Facilities of Protection Category I and II" from the perspective of a technical support organization (TSO) the third lecturer presented examples from the implementation of a computer security concept according to the guideline, implementation of an IP-based leased line in an NPP and outsourcing of plant computer systems to an external data center considering the Malicious Acts Guideline IT.

The final presentation gave an overview of the basic German computer security approach, the IT-Grundschutz (IT basic protection). The IT-Grundschutz is a holistic standard for information security developed by the German Federal Office for Information Security (BSI) and shall provide companies and authorities with a basic approach on how to design and install basic information security concepts and measures. The IT-Grundschutz can be used to integrate a computer security regime licensed under the IEC 27001. The topic ended with an open panel discussion about details concerning experiences and challenges which came up since the release of the German Malicious Acts Guideline IT.

3. CHALLENGES OF COMPUTER SECURITY

During the Technical Meeting several challenges of computer security in nuclear security were introduced by the lectures and the participants. Most mentioned and discussed topics were the computer security for radioactive material and their associated facilities, nuclear and other radioactive material out of regulatory control, supply-chain security and ensuring availability of personnel with the necessary expertise in computer security.

3.1. Challenges of computer security concerning radioactive material and associated facilities

Radioactive material and their associated facilities are defined by the IAEA as radioactive material outside of nuclear power and weapon production, specifically all material apart from Uranium-233, Uranium-235, Plutonium-239 and irradiated nuclear fuel. These radioactive materials make up the bulk of all stored and used materials, for example in hospitals, research institutes or industry processes [13]. During the TM participants and lecturers alike concluded that these materials are often considered less than material in nuclear facilities while they are stored in facilities that are open to the public, like hospitals or factories, and thus are more susceptible to malicious acts. During the topics two and five of this meeting it became clear that most regulatory approaches focus on nuclear material and facilities while keeping radioactive material and associated facilities in mind for further regulation.

As such the German Guideline for the Protection of Computer Based Systems in Nuclear Facilities against Malicious Acts has been published in 2013 for nuclear facilities, while the first draft for other radioactive sources and associated facilities was drafted in 2017 and has yet to be finalized. Several member states of the IAEA do not own nuclear facilities, but most own facilities with other radioactive sources and thus have great interest in this topic. While not having developed full regulatory control mechanisms like states with nuclear facilities, they

lack the experience in regulating such facilities and material and thus need support in developing the regulation of radioactive material and associated facilities.

With the fact that facilities with radioactive sources are often open to the public (e.g. hospitals) and that security measures for the transportation of these materials are less stringent than for the transportation of nuclear materials [14], the challenges for computer security are different to those for nuclear facilities and materials. Likewise, the risks associated with these materials are different from nuclear material as they cannot be used for criticality incidents but can still pose a risk to the public as the Goiânia-Incident [15] has shown in 1987.

During the TM it was concluded that the challenges for radioactive material and their associated facilities need specific security approaches to ensure appropriate computer security during all lifetime stages of these materials. A recommendations level document for the security of radioactive material and their associated facilities has been developed by the IAEA (NSS 14) [16]. More detailed support should be provided with further documents which are currently under development such as NST 044 [17], NST 045 [7] and NST 048 [18]. A non-serial publication "Information and Computer Security for Activities Involving Radioactive Material" is currently being drafted by the IAEA for publication in 2020. The TM concluded that further development of regulations and support of regulators and operators is needed for radioactive material and their associated facilities with regards to computer security.

3.2. Challenges of computer security concerning nuclear and radioactive material out of regulatory control

Nuclear and radioactive material out of regulatory control are defined as material that due to a certain chain of events has left the regulatory control of a state and its location and usage are either unknown or under no regulatory influence [19]. The events leading to non-regulated nuclear and radioactive material can have different reasons such as theft, loss, uncontrolled import or forgotten materials. With thousands of facilities and transports of nuclear and radioactive materials, events leading to material out of regulatory control are not unlikely to occur on a regular basis [20]. While these materials are per definition out of regulatory control, regulators must take measures to prevent, detect and remove such materials before harmful acts can occur. With the ongoing digitalization these measures are based on/supported by digital systems which must be protected adequately.

With the presentation of the boarder monitoring and control system in Georgia by a representative of the Georgian SSSG and specialized working groups the materials out of regulatory control became an important topic of the Technical Meeting. As measures concerning unregulated material are to be taken by different authorities as the measures taken for nuclear or radioactive material, e. g. customs and boarder protection agencies or the national police, different measures for computer security have to be considered and specific regulatory approaches should be in place.

In this context the IAEA supports its member states with the document NSS 15 [19] in dealing with and prevention of unregulated material and currently prepares the document NST 045 for computer security measures in general nuclear security, but a specific support document for the computer security in this regard is not available.

3.3. Supply-Chain risks for computer security

Computer security in the supply-chain has become an emerging topic in industry [21] and nuclear industry [22]. Common analog I&C products are constantly being replaced by digital systems with reasoning regarding the costs, the capabilities or declining availability of analog systems. As digital systems for nuclear facilities are also purchased from vendors or developers not specially designing components for nuclear facilities, e. g. commercial off-the-shelf (COTS)-components, new risks for their computer security must be considered. So called supply-chain attacks [21] have become of public interest after famous attacks like the NotPetya attack [23] or Shadowhammer on certain ASUS computers who have used 3rd party suppliers to infect networks or specific computers.

During the TM several member states asked for support documents and assistance in dealing with supplied digital products and their respective computer security. Global supply-chains and to be replaced I&C equipment in older facilities require new answers from regulators and experts in the nuclear industry to ensure computer security in this field. International standards like the IEC 61508 and IEC 61513 were shown as base points to

enable national regulators to develop new frameworks for dealing with COTS components and supply-chain risks. Measures to monitor supply-chain incidents and rapid responses to ensure computer security in case of known weaknesses were discussed as regulatory tasks for this issue.

3.4. Professional staff and training

An ongoing topic during discussions, presentations and in breaks was the challenge to find adequately skilled staff to fill all necessary positions for the regulation and implementation of computer security in the nuclear domain. With computer security and information security becoming more deeming topics for every application and industry national regulators compete for the limited computer security experts and professionals. Several member states expressed their difficulties to find adequate personnel for open positions or to replace retired personnel. There was an exchange on strategies and solutions to overcome this shortcoming.

Representatives of several government bodies laid out their strategies to counteract a shortage of professional staff. These comprised of three core points:

- Training of current staff: The representatives of the agencies emphasized that each agency has a certain number of staff with a potential for training and retraining in computer security. Depending on the political developments, other national agencies who are reduced in size or tasks are also a potential source of competent staff for training or retraining.
- Cooperation with universities: By cooperating with universities high potential staff can be acquired directly from the national universities. Support programs, internships and other measures help bringing future graduates to the national agencies. Fostering the contacts with universities enables the agencies to get in touch with future talents and getting staff before competing with the industry.
- Scholarships: Scholarships enable getting professional computer security personnel while also being a socially responsible measure giving the state a social steering effect at hand. A minimum contractual company affiliation of sponsored students after their university degree enables long term personnel planning.

All strategies to overcome the shortcoming of professional staff are developed to either empower current personnel or foster new personnel in computer security. Several representatives from regulatory authorities pointed out that they could fill all needed positions by using existing staff in their or other state organizations. As an example for the increasing need for personnel in computer security, a representative from the German Federal Office of Information Security (BSI) laid out that the BSI grew from 600 employees in 2016 to over 940 in 2019 and plans to employ 350 more in the following years.

4. REGULATORY APPROACHES

The approaches on developing regulations and guidelines for computer security in nuclear security by the different nations and agencies can be subdivided in two different basic design approaches: Threat- or scenario-based approaches and prescriptive approaches.

Regulatory approaches using threat- and scenario-based approaches design their guidelines and regulations considering developed cyber threat scenarios, in which all kind of plausible and possible malicious scenarios are evaluated and listed. Using regular risk assessments, the scenarios are updated in a certain time frame. When implementing computer security measures, the operators must ensure that their computer systems are protected against the named scenarios and their possible outcomes. Combined with a graded approach a detailed framework for operators and regulators is designed, the implementation of which shall ensure a high level of protection against all assessed threats.

Prescriptive approaches develop requirements for computer security measures that must be fulfilled to ensure computer security. These requirements are based on consequences potentially entailed by cyber-attacks. When introducing and implementing computer security measures, the operators have to ensure that all requirements are met. Combined with a graded approach to computer security, a detailed framework for operators and regulators is designed to ensure a high protection level against known and unknown threats.

The so designed regulations and guidelines must be implemented in all facilities of the regulating nation. The control of the operators' actions and measures to ensure a full implementation of all regulations and guidelines is one of the core tasks of authorities. Three different approaches have been presented during the TM to ensure full compliance of the operators to the regulations:

— Regular detailed facility-checks: The operators are responsible for the compliant implementation of all regulations and technical guidelines. The operators must ensure that their facilities follow all regulations at a certain date. Facilities in operation are regularly inspected by the authorities in a set interval, while special inspections are done in case of license modifications. New facilities are reviewed and approved by the authorities before start of operation.
— General implementation and modification approval system: Facilities in operation and new facilities must develop concepts for the implementation of the computer security regulations and guidelines. These concepts are reviewed by the authorities which can enforce amendments if necessary. After approval the operators implement the computer security measures following the developed concepts. The implementation is reviewed by the authorities. Afterwards any modification to the facility must be reviewed and approved by the authorities.
— Independent technical expert licensing: Each operator has to prove that an independent technical expert has approved the computer security measures as sufficient to be compliant with the regulations. The approval by the independent technical expert has to be done on a regular basis and furthermore for each single modification or start of operation.

Each approach was presented with the respective advantages or disadvantages. It was pointed out that there is no international "one-fits-all" tailor-made solution but individual fitting approaches to implement computer security in the nuclear domain.

5. FUTURE DEVELOPMENTS

All authorities from countries operating nuclear power plants and presenting in the meeting have developed regulatory approaches to computer security in nuclear power plants. With the full implementation and review of these regulations by all national nuclear power plants either finished or under way, most authorities started to develop further regulations and guidance for small duty holders, radioactive material and their associated facilities or supply-chains. As the regulations for nuclear power plants cannot be transferred one-to-one to research reactors, industry, hospitals or other non-power generating facilities, new regulations for computer security regarding these facilities are in development. Supply-chain attacks have brought up the topic of supply-chain compliance and necessary regulation and as such several representatives of authorities expressed their concerns over possible insufficiencies in the regulation of supply-chains. Regarding international supply-chains an enhanced international cooperation can support increased computer security in this domain. The last core point of the ongoing and future developments are the regulatory reactions to new threats. With hardware attacks, more and more sophisticated attacks by APTs and unicorn attacks there is a constant number of new emerging threats for computer security in nuclear facilities. As such all the parties involved in computer security must stay up-to-date in this fast-developing field and adapt and expand regulations and measures continuously to counteract new threats, cover new developments and ensure secure operations. International conferences like the IAEA Technical Meeting on "Computer Security Approaches and Applications in Nuclear Security" support the international exchange of information on current and future threats, on developments and best practices of different nations. With presentations of national approaches to computer security in nuclear security all participating nations gain an overview over the different approaches, the experience of their implementation and their challenges. International workshops enhance the cooperation and the spread of knowledge between the participating states.

REFERENCES

[1] S. KARNKOUSKOS, “Stuxnet worm impact on industrial cyber-physical system security,” *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society,* pp. 4490-4494, 2011.

[2] R. KHAN, P. MAYNARD, K. MCLAUGHLIN, D. M. LAVERTY and S. SEZER, “Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid,” *ICS-CSR 16,* pp. 1-11, 2016.

[3] Q. CHEN and R. A. BRIDGES, “Automated behavioral analysis of malware: A case study of wannacry ransomware,” *16th IEEE International Conference on Machine Learning and Applications,* 2017.

[4] B. WAHLSTRÖM, “Differences between analog and digital I&C,” *Proceedings of the 9th International Conference on Nuclear Plant Instrumentation, Control & Human–Machine Interface Technologies,* 2015.

[5] S. JUNG, E. KIM, J. YOO, J. Y. KIM and J. G. CHOI, “An evaluation and acceptance of COTS software for FPGA-based controllers in NPPs,” *Annals of Nuclear Energy 94,* pp. 338-349, 2016.

[6] Q. HUANG and J. JIANG, “A Radiation-Tolerant Wireless Monitoring System Using a Redundant Architecture and Diversified Commercial Off-the-Shelf Components,” *IEEE Transactions on Nuclear Science 65.9,* pp. 2582-2592, 2018.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, “Computer Security for Nuclear Security,” *IAEA Nuclear Security Series DRAFT No. 45,* Vienna (2017).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, “Computer Security Techniques for Nuclear Facilities,” *IAEA Nuclear Security Series Draft No. 47,* Vienna (2017).

[9] P. CHEN, L. DESMET and C. HYUGENS, “A study on advanced persistent threats,” *IFIP International Conference on Communications and Multimedia Security,* pp. 63-72, 2014.

[10] E. HUBER, Sicherheit in Cyber-Netzwerken: Computer Emergency Response Teams und ihre Kommunikation, Springer-Verlag, 2015.

[11] C. TEZCAN, “Improbable differential attacks on Present using undisturbed bits,” *Journal of Computational and applied mathematics,* pp. 503-511, 2014.

[12] T. HOQUE, X. WANG, A. BASAK, R. KARAM and S. BHUNIA, “Hardware Trojan attacks in embedded memory.,” *IEEE 36th VLSI Test Symposium,* pp. 1-6, 2018.

[13] C. D. FERGUSON, T. KAZI and J. BIRIRA, Commercial radioactive sources: surveying the security risks, Monterey Institute of International Studies, Center for Nonproliferation Studies., 2003.

[14] R. GELDER, J. S. HIGHES, J. H. MAIRS and K. B. SHAW, “Radiation exposure resulting from the normal transport of radioactive materials within the United Kingdom,” *National Radiological Protection Board,* 1984.

[15] J. L. LIPSZTEIN, D. R. MEOL, C. A. N. OLIVEIRA, L. BERTELLI and A. T. RAMALHO, “The Goiânia 137Cs Accident-A Review of the Internal and Cytogenic Dosimetry.,” *Radiation protection dosimetry,* pp. 149-154, 1998.

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, “Nuclear Security Recommendations on Radioactive Material and Associated Facilities,” *IAEA Nuclear Security Series No. 14,* Vienna (2011).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, “Security of Radioactive Material in Transport,” *IAEA NUCLEAR SECURITY SERIES DRAFT NO. 44,* Vienna (2017).

[18] INTERNATIONAL ATOMIC ENERGY ORGANIZATION, “Security of Radioactive Material in Use and Storage and of Associated Facilities,” *IAEA NUCLEAR SECURITY SERIES DRAFT NO. 48,* Vienna (2016).

[19] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS A, *Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control,* IAEA Nuclear Security Series No. 15, Vienna (2011).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, *trafficking database (ITDB). Incidents of nuclear and other radioactive material out of regulatory control,* 2016 Fact Sheet.

[21] D. SHACKLEFORD, "Combatting cyber risks in the supply chain," *SANS.org,* 2015.

[22] Y. WU, K. CHEN, B. ZENG, H. XU and Y. YANG, "Supplier selection in nuclear power industry with extended VIKOR method under linguistic information," *Applied Soft Computing 48,* pp. 444-457, 2016.

[23] M. MCQUADE, "The untold story of NotPetya, the most devastating cyberattack in history," 2018.

[24] D. ALBRIGHT and K. KRAMER, "Neptunium 237 and Americium: World Inventories and Proliferation Concerns," *Institute for Science and International Security,* vol. 6060, pp. 1-24, 2005.