The interplay between cyber and nuclear security in Republic of Moldova

Aurelian BUZDUGAN[1], Artur BUZDUGAN[1,2]
[1]*National Nuclear Security Support Center, Technical University from Moldova,*
[2]*Department of Microelectronics and Biomedical Engineering, Technical University from Moldova*
aurelian.buzdugan@yahoo.com, artur_buzdugan@yahoo.com

***Abstract* — In this paper we will reflect upon the necessity to follow the national cyber security requirements, which are also addressed to operators of nuclear and highly radioactive materials (NR). We will begin with an overview of the current state of cyber security in the NR domain from the legislative and technical perspective and we will present for consideration an overview on the recently approved Minimum Cyber Security Requirements for state entities [1], which includes the regulatory authorities (RA) and NR operators of category I and II. The implementation of these requirements will lead to an increased level of cyber security and will upgrade the regulatory processes. These requirements will also provide clear technical guidance for the all entities, including the ones from the NR domain in order to apply these controls within their infrastructure. The document on Minimal Security Requirements describes cyber security and some physical security controls, as well as contains requirements for security testing, design basis threat (DBT) and inclusion of cyber security requirements in all processes in the organization.**

***Index Terms* — cyber security, nuclear security, regulatory framework, Republic of Moldova.**

I. INTRODUCTION

In the NR objectives the operators should take the first prevention, detection and response measures to the unauthorized actions in NR domain. The tasks of operators are to assure the control of NR material and to prevent any unauthorized acts and an operator can achieve this by implementing specific security policy or controls measures within the organization [3]. This is valid not only for combating illicit traffic, but also for the safe and secure use of NR activities. Therefore, the operators have to be guided by the national strategy, policy, legislation and regulation for their domain of activity and to follow these requirements in order to assure the safety and security of the systems. Generally, the regulations at the national level set the minimum requirements to be implemented, which as a good practice are developed based on the DBT [4]. According to the DBT, the RA and other organizations with responsibilities in the field need to assess the current threats in order to develop effective countermeasures, however the current national legislation and other aspects such as costs can also be taken into account when defining the security requirements.

On the other hand, computer technologies are being used by most of the operators, for example in physical security systems, or by the NR material accountancy systems [5]. By defining requirements for security of computer systems, which are also used in such environments, would simplify the operator’s or RA’s tasks in understanding and choosing the correct controls to implement and would complement the Regulation on Physical Security on Nuclear and Radiological Activity [2]. This could facilitate the authorization or evaluation processes. In addition, this would add extra burden on the organization that maintains such requirements to adjust them periodically in line with the threat assessments or DBT. Overall, the acknowledgement of cyber security as a part of the nuclear security has motivated member states to adjust their legal frameworks and include cyber security as part of regulations or recommendations, Republic of Moldova not being an exception to this.

In para II we will briefly describe the current cyber security state. We will make an overview of NR domain by stating the progresses in the legislation update, and present the relevant components of the approved Regulation on Physical Security on Nuclear and Radiological Activity [2], which acknowledges and mentions cyber security as intrinsic party of the physical security systems. In para III we will pay attention to the recent cyber security development to establish minimum computer security requirements for all public authorities, RA, including and NR operators too. We will conclude with a general assessment of the current legal frameworks and we will suggest recommendations for future developments.

II. CURRENT STATE AND PERSPECTIVE OF DOMESTIC CYBER SECURITY

The cyber security topic is widely discussed on the international level by national authorities, organizations or research entities. Republic of Moldova is at the development phase on establishing a national cyber security framework and defining the responsibilities and roles within the country. This paper is a continuation of the analysis presented at the 2015 IAEA Computer Security Conference and the 3rd International Conference of Health Technology Management [6], where we also mentioned about the benefits of having a National Cyber Security Program for 2016-2020 years and the positive effects of such a high-level policy [7]. Approved by the Government in October 2015 the Program describes among the objectives - capacity building for cyber defense and the education, lifelong learning and training in cyber security. We would like to mention that these objectives also refer to critical infrastructures from NR domain, and will be supported by the following actions listed in the program:

- defining the responsible authorities and developing defense capacity,
- establishing a cyber security research and training center,
- updating the cyber security curriculum,
- raising awareness in terms of cyber security risks,
- defining requirements for professional competencies for computer security practitioners from public and private sector and
- conducting workshops and training sessions for critical infrastructures staff.

These actions will guide the authorities in focusing their efforts and resources in strengthening cyber security at a national level as well to create a baseline that would introduce the cyber security in all public and private institutions. Without regards to this, the effects will not be instant as the security culture, both in cyber and nuclear domain is overall low in the country. Besides, by focusing on the user awareness, research and education in this area the actions will have equally a short and long-term effect. Due to the importance of this subject there is already a visible result worth mentioning - the opening in October 2016 of the Cyber Security Laboratory within the Faculty of Computers, Informatics and Microelectronics of the Technical University of Moldova [8]. That was done in close in cooperation with the S.E. Center of Special Telecommunications, which is the governmental technical operator and Computer Emergency Response Team provider for public authorities. This success was not possible without external assistance such as NATO “Science for Peace and Security” Program and with support of the US Embassy in Moldova and Estonian Embassy in Moldova. We would also like to mention that in October 2016 the Government approved the draft of the Law on Informational Security Concept, and has awarded it to the Parliament for approval [9]. Taking into account that it is being discussed by the Parliament Commissions, this draft document is too earlier to be analyzed in this paper.

The nuclear security and non-proliferation domains are in a continuous improvement process. In February 2013, the National Nuclear Security Support Center (NNSSC) was established within the Technical University and IAEA Office of Nuclear Security and Swedish Radiation Safety Authority support its working program. NNSSC has the objectives to update the curricula in nuclear safety, security and non-proliferation, teach young specialists and train other staff from relevant organizations, provide technical support as well as conduct research in this field. On the other hand, Moldovan Government introduced the cyber security component as intrinsic part of the physical security systems in the requirements for the authorization process of NR operators [2,10]. This aspect of the definition of sectorial, responsibilities is important in the context of cyber security, where the knowledge is very specific and insights from the system have to be known when describing such requirements. In our opinion, without an updated Contravention Code and legislation in NR domain, there is a low probability that the operators will implement sufficient security controls to deter the current threats.

As was mentioned above, among the achievements in the legal framework for NR domain, which includes cyber security aspects, is the approval by the Government of the Regulation on Physical Security on Nuclear and Radiological Activity [2]. The major provisions of the draft of this regulation was presented and discussed in the presentation of the 2015 IAEA Computer Security Conference, and we will list here only the most important aspects that refer to both NR and cyber security in the context of physical security systems. The regulation stipulates that upon the establishment of a physical security system it will also be taken into account the cyber security role, information security as well as the technical requirements for software and hardware used in these physical security systems. The development of operator’s cyber security plans can be done individually or as part of the physical or nuclear security of the operator’s assets. The operator is also responsible for defining the defense in depth security controls and levels of cyber security, based on a risk assessment in order to assure a high level of physical and nuclear security. Beside this, the regulation stipulates the requirement for reporting to the Ministry of Interior, Information and Intelligence Service and RA upon:

- any attempt to extract information related to the physical security;
- cyber or physical attacks that could lead to shutting down or altering the functioning of one or more computers in charge of physical and nuclear security of the objective or NR materials;
- hybrid attacks (cyber and physical) on the core computers;
- NR material theft or any other violation of the physical security system.

When it comes to information management, it is required to secure in relation to the category of the objective the information regarding the physical security of the nuclear and/or radiological objective as well as nuclear material classified as “restricted” or higher. The regulation also sets the operator responsible for assuring the confidentiality of data regarding the physical security systems, NR installations and materials, and has to establish adequate security controls to assure the confidentiality of data regarding the physical security during the use, transportation or storing of NR materials in dependence of its category. Furthermore, the access to data that might compromise the physical security systems of the objective, NR installations or materials has to be restricted whereas potential vulnerability information of the physical security systems, in dependence of domestic legislation, must be treated as secret or confidential. The physical security system should include cyber security procedures, as well as protect the characteristics of confidentiality, integrity and availability of electronic databases or cyber systems and processes that might negatively influence upon the physical security system of the objective or protected materials.

Upon the implementation of the physical nuclear security it is required that the holder of the radiological authorization together with experts from physical and nuclear security will identify the assets and systems, including cyber ones, that are vital for the installation and objective.

The regulation is in line with IAEA recommendations and good practices and mentions the cyber security requirements towards the physical security systems or data that relates to it. We believe this effort is a novelty in the Moldovan NR legislation, and it is necessary to continue the inter-domain cooperation between cyber and nuclear, in order to develop policies and update requirements that are actual to the current threat landscape.

III. MINIMUM CYBERSECURITY REQUIREMENTS FOR PUBLIC AUTHORITIES

In May 2016, the Moldovan Ministry of Information Technologies and Communication has published for discussion the draft on proposal on minimum security requirements to ensure cyber security of IT systems, which was approved by the Government later in 2017 [1]. The document refers to a list of computer security topics and sets requirements for development and usage of IT systems. By definition, requirements or regulations can be performance based, when these are described at a high level, or prescriptive, when more technical details are listed. These rules are also used in NR regulations, however are applicable for other complementary domains such as cyber security [10, 11]. This document was developed by combining both the prescriptive and performance based approaches and contains a list of security controls at the administrative and technical level that have to be implemented by all state authorities, which include the NR operators of category I and II as well as the RA. It also defines the systems that should meet these requirements and introduces an obligatory information security management system for the constituency, as well as separates between base security controls and advanced security controls based on a risk assessment. The security categorization process is described in the annex of the document, and contains factors such as availability of the system, type of information processed as well as importance of these systems within the organization. The proposal describes also security requirements for usage of information systems, such as password complexity, connection to the Internet or email use policy, requirement to create backups or conditions for outsourcing the management of these systems. We can also make a parallel to the IAEA NSS-17, since similar recommendations can be found in this document proposal, such as creating of a security policy enforced by the management or having a responsible officer for cyber security [11].

By implementing these requirements, the overall level of cyber security for public authorities will increase, including for the operators of category I and II. This could also serve as guidance for implementers and evaluators, however some of the prescriptive requirements could create issues in understanding and implement them, as well as these requirements could become outdated in a short period due to the rapidly changing threat landscape and security solutions. This debate is common in states with a low level of security culture, as each new requirement is perceived as a necessity of more resources and knowledge on the implementer side. In addition, the prescriptive requirements from the document would be easy to audit upon, however could reduce the audit process to a compliance check rather than raising security awareness and culture. Nonetheless, the proposal itself could help the IT system administrators in creating a checklist against their environment to evaluate the existing controls or those that need to be implemented. In the long-term process, it is necessary to invest effort and resources to keep such documents updated, as well as maintain a certain level of flexibility from the auditors. It is also welcoming the fact that these security requirements could be enforced on a high level, and therefore it will guide the public authorities, including the NR operators of level I and II. This document will generally help towards creating a baseline for computer security requirements within the public authorities, which would considerably improve the overall defense and resilience against cyber incidents.

IV. CONCLUSION

The Moldovan cyber and nuclear security legislations are updated continuously in the last years, due to the importance of the security subject and potential threats to the states. The approval of the Regulation on Physical Security on Nuclear and Radiological Activity concept, , preceded by approximately 2.5 years of discussions and survey, was presented as a report at the last IAEA Computer Security Conference and we consider it is an important step forward in creating the necessary legislative background. However, the lack of IT qualified human resource in NR domain could unfortunately lead to the low implementation of the requirements from this regulation. In this respect, we consider important the role of Technical Support Organizations (Universities, NGOs) in covering the knowledge and experience gaps and provide specialized support such as contracting experts or organizations that have the required skill in applied cyber security in strategic niche fields as the NR one.

On the other hand, the National Cyber Security Program could support the training and development of human resources in cyber security for public authorities, which would have a positive effect on the high-risk domains as well such as the NR domain. This would be a long-term action after entering into force as the operators and the RA would need to take concrete actions to align with the requirements set in this Regulation.

The new Cyber Security Program and Proposal on Minimum Cyber Security Requirements is an advance in the process of securing critical systems and information in terms of computer and information security. The actions are expected to have a general security improvement for public authorities and operators that use NR data or materials. The development on a risk based approach of the regulation on physical security of NR activities and its approving at the Government level is appreciated by us as a good practice in establishing security regimes. However, it is not always easy to find the balance between too technical and general regulations. The specified requirements in the documents have to be clearly defined by additional norms and be realistic to implement by the operators and derive from the objectives of the security strategies or programs. The requirement definition process is tedious since it requires a deep knowledge and experience in IT security - too detailed requirements could be hard to implement and could become outdated in a short period, where general ones could leave space for interpretation. Therefore, good practices in developing requirements should be taken into account as well as possible past experiences from other states. In addition, it is also advisable a close cooperation between regulatory authorities in NR and bodies responsible for cyber and information security. It is difficult to underestimate also role of Universities, specialized research Centers and NGO.

The progress in legislatives field in NR domain in Republic of Moldova during 2007-2016 years is a relevant example where cooperation between different specialized organizations on a national level led to fruitful and measurable results. In order to raise security awareness and level of the nuclear security culture, it is necessary for a continuous cooperation framework, which would include consulting experts from other areas including cyber. Another reason to promote this cooperation is limited number of national experts in related fields. Also, the implementation of the cyber security requirements will require the cross-participation of such experts in order to ensure correct understanding of requirements for specific strategic field as NR. As a recommendation, the IAEA NSS-17 [11] helps the operators in implementing these controls, as it offers guidance on defining security tiers as well as technical and administrative controls. It also helps in understanding the role of computer security for industrial control systems or physical security and safety, as well as offers a good starting point to develop security policies within the organization. Future development in cyber and nuclear security should be based also on the cooperation on the national and international level, as nowadays the threats shape the policies and requirements that states develop and enforce in their security strategies and regulations.

REFERENCES

[1] Minimum security requirements for ensuring cyber security. Government Decision no. 201 from 28.03.207. Monitorul Oficial al Republicii Moldova no. 109-118 from 07.04.2017.

[2] Regulation on physical security on nuclear and radiological activity. Government Decision no. 1268 from 23.11.2016. Monitorul Oficial of the Republic of Moldova, no. 415 from 29.11.2016.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series No. 6: Combating Illicit Trafficking in Nuclear and other Radioactive Material, Vienna (2007) http://www-pub.iaea.org/MTCD/publications/PDF/pub1309_web.pdf.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series No. 10: Development, Use and Maintenance of the Design Basis Threat, Vienna (2009) http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf.

[5] 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), Vienna (2011) http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

[6] Aurelian Buzdugan. Role of Cyber Security along with Nuclear and Radiological Safety in Medicine. Book of Abstracts. 3rd International Conference of Health Technology Management. Ed. in Chief Victor Sontea, Chisinau, Pontos (Europress), p. 102, (2016). ISBN 978-9975-51-774-4.

[7] On National Cyber Security Program of Republic of Moldova for 2016-2020 years, Government Decision no. 811 from 29.10.2015, Monitorul Oficial of the Republic of Moldova, no. 306-310 from 13.11.2015.

[8] Establishment of the cyber security laboratory, at Technical University from Moldova (06 October 2016), http://www.moldova.md/ro/content/premiera-pentru-republica-moldova-fost-lansat-un-laborator-de-securitate-cibernetica.

[9] The Law on information security concept (Draft), no 396 from 10 October 2016, Approved on 23 June 2017 in the first reading by the Parliament of the Republic of Moldova. http://parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/language/en-US/Default.aspx

[10] Law no. 132 from 08 June 2012 - On safe deployment of nuclear and radiological activity. Nuclear Law Bulletin no.91, p.p. 161-188, OECD (2013), NEA no. 7152.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series No. 17: Computer Security at Nuclear Facilities, Vienna (2011), http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.