Contribution ID: **344** Type: **Paper**

INTEGRATING CYBER AND PHYSICAL SECURITY: ENHANCING SECURITY CULTURE FOR NUCLEAR POWER PLANTS (NPP) –A PROSPECTIVE METHODOLOGY FOR TURKEY

Nuclear Power Plants (NPP) are globally most protected critical infrastructure in the sector. The Fukushima accident was a wake-up call for reminding the international community about the possible outcomes. Today, methods to protect critical infrastructures in the security sector are rapidly transforming due to the rapid changes in cyber, physical and hybrid threats which are exponentially increasing because of the global political and economic shifts. In addition to the physical security threats, cyberspace is becoming a major concern for the NPP operators and governments. The continuous integration of the cyber and physical domains in NPPs is not only representing risks, but it also presents various opportunities such as the reduced costs and higher efficiency. However, the rapidly growing digitization and over reliance on the computer-based systems in the operation returned nuclear material accountancy and the perimeter security systems of the NPPs into targets for cyber/physical attacks.

On the other hand, physical and cyber security were largely seen as two distinct domains and cultures in the past, today, in contrast, the equipment also used in the physical protection in critical infrastructures (CI) such as CCTV cameras, sensors, any physical access regulating systems also rely on the computing systems which are mostly not segmented and connected to a network. This functional integration also makes them vulnerable to cyber attacks particularly those which could create a devastating impact in the physical and kinetic world. Even though the problems and threats identical, the staff in the cyber and physical security disciples are generally approaching same problems from different perspectives and they have limited communication among themselves.

Both parties have their own security cultures due to their backgrounds and approaches. When the recent threat range and implementation of the hybridity is considered, to build an integrated security culture is a necessity. In that respect, the integration of cyber-physical security cultures seems as a must in order to timely detect the security incidents as well as to respond them in real time in order to enhance resiliency. At that point, it should be underlined that simplistic security management merging cannot help to solve the problems. Integrated security culture requires an effective cooperation which also should include a proper information sharing practice, collaborative planning methods, strategic communication, launching new training platforms, implementing shared risk management practices and much more where the different security experts of the both disciplines could combine resources to achieve to protection goals.

From the Turkish perspective, Turkey is a relatively newcomer to NPP environment with respect to diversifying its energy supply sources to meet its constantly increasing energy demand. In that respect, even though currently there is no NPP in operation in Turkey, it is planned that Turkey will install the first nuclear power plant that started to be constructed and will be operated in Akkuyu -Mersin Province with the ROSATOM. However, particularly from a cyber security perspective, it could be said that currently Turkey has limited experience as a regulator for NPPs. Even though, Turkey has intention to implement crucial and effective policies in the cyber security field like launching a national cyber security strategy as well as the creation of Cyber Emergency Response Team (CERT), it is possible to claim that the increasing cyber-physical security challenges, as well at rapidly transforming threat landscape requires a more sophisticated knowledge and specialized know-how particularly for securing NPPs including an integrated cyber-physical security approach. More importantly, this approach and integration must be embedded in an effective security culture.

In that respect, this research paper merely aims to focus on the following research questions: How the cyber-physical security integration could be performed for an integrated security culture for Turkish nuclear energy agenda? Since human factor is vital for an effective nuclear security, how the skilled human capital could be trained to achieve this goal? What should be the role of national regulator agency and the operator in this respect?

Gender

State

Turkey

Authors: Prof. BIÇAKÇI, Ahmet Salih (Associate Professor, Kadir Has University, International Relations Department; Center for Cybersecurity & Critical Infrastructure Protection); Mrs GÜCÜYENER EVREN, Ayhan (PhD Student/Project Specialist, Kadir Has University, Center for Cybersecurity & Critical Infrastructure Protection)

Presenter: Prof. BIÇAKÇI, Ahmet Salih (Associate Professor, Kadir Has University, International Relations Department; Center for Cybersecurity & Critical Infrastructure Protection)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability