Nuclear Engineering and Technology 54 (2022) 2467–2474

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Thinking multiculturality in the age of hybrid threats: Converging cyber and physical security in Akkuyu nuclear power plant

A. Salih Bıçakcı*, Ayhan Gücüyener Evren

Kadir Has University, International Relations Department, Turkey

ARTICLE INFO

Article history:
Received 6 April 2021
Received in revised form
27 January 2022
Accepted 27 January 2022
Available online 1 February 2022

Keywords:
Nuclear power plants
Nuclear security
Security culture
Nuclear security culture
National culture
Cyber-physical security

ABSTRACT

Nuclear Power Plants (NPPs) are the most protected facilities among all critical infrastructures (CIs). In addition to physical security, cyber security becomes a significant concern for NPPs since swift digitalization and overreliance on computer-based systems in the facility operations transformed NPPs into targets for cyber/physical attacks. Despite technical competencies, humans are still the central component of a resilient NPP to develop an effective nuclear security culture.

Turkey is one of the newcomers in the nuclear energy industry, and Turkish Akkuyu NPP has a unique model owned by an international consortium. Since Turkey has limited experience in nuclear energy industry, specific multinational and multicultural characteristics of Turkish Akkuyu NPP also requires further research in terms of the Facility's prospective nuclear security. Yet, the link between “national cultures” and “nuclear security” is underestimated in nuclear security studies. By relying on Hofstede's national culture framework, our research aims to address this gap and explore possible implications of cross-national cultural differences on nuclear security. To cope with security challenges in the age of hybrid threats, we propose a security management model which addresses the need for cyber-physical security integration to cultivate a robust nuclear security culture in a multicultural working environment.

1. Introduction

Threat landscape for Nuclear Power Plants (NPP) is changing in the age of hybrid threats. Stuxnet which targeted a NPP and BlackEnergy which damaged a Power Plant demonstrated emerging vulnerabilities in critical facilities. Even though NPPs are one of the most protected Critical Infrastructures (CIs), hybrid threats are on rise with extensive usage of digital components [1]. According to World Institute for Nuclear Security (WINS) *The State of Security in 2020* report, “a cyber attack on a nuclear facility” is reported as the most likely security incident for a NPP [2].

The most critical element of cyber security in NPPs is human-computer interaction. Even the most sophisticated cyber security tools should be operated by human. Meanwhile age of hybridity brings up new forms of threats with smart combination of cyber and physical components. Most of the perimeter security systems are digitalized and its hardware/software security are consigned to third parties. This creates a situation in which physical security department uses digitized devices to protect facility and cyber security department has to protect its network with limited cooperation with physical security department.

Turkey aims to reduce its dependence on fossil fuels and diversify energy resources. In this respect, Turkey and Russian Federation signed an agreement to build a NPP in Turkey's Akkuyu province in 2010. Turkish NPP model differs from the world-wide NPPs since its contract is the first example for participation of foreign capital in a NPP to be built under the Build-Own-Operate (BOO) model. Such model might be beneficial for newcomers by solving nuclear waste disposal challenge [3]. Nevertheless, safety and security culture should be re-considered as this model can undermine a host country's practices unless local partners are well trained [4]. In the Akkuyu NPP's financial structure, Rosatom, Russian Federation State company, is in a consortium with Turkish companies: Cengiz Holding, Kalyon Construction and Kolin Construction. According to the agreement while at least 51% of the shares of all investment should belong to Rosatom, Turkish companies has 49% of the shares.

Since hybrid threats are focusing on gaps and minor cracks within a structure, any negligence in communication and

* Corresponding author. Kadir Has University, International Relations Department, Kadir Has Cad, Fatih, 34081, Istanbul, Turkey.
E-mail addresses: asbicakci@khas.edu.tr, ayhangucuyener@hotmail.com (A.S. Bıçakcı).

https://doi.org/10.1016/j.net.2022.01.033
1738-5733/

cooperation among different departments could return back as a devastating attack. Newly established NPPs have an opportunity to redesign their systems to respond hybrid threats. One of the rising solutions for Akkuyu NPP is blending cyber and physical security systems to reinforce nuclear security. Turkey could easily implement such strategy to build up a robust facility. However, the human capital presents a problematic. Multicultural and multinational working environment in Akkuyu NPP would require a diligent planning.

Dealing with Turkey's first nuclear energy experience, this research aims to address following questions: What are the major working characteristics of Russian and Turkish cultures? What are the weaknesses and advantages in a BOO model in terms of nuclear security? Since it is one of the earliest BOO models implemented in a NPP, what would be most convenient cooperative model for blending cyber and physical security units? The significance of this research and its contribution to the literature can be found in two streams: First, we aim to construct a framework to explore the link between characteristics of national cultures and expectations of the nuclear security. Second, since Akkuyu is the first NPP of Turkey, this experience would be an organizational model that would inspire future NPP projects[1]. To sum up, this study aims to start a discussion on blending in cyber and physical security in a multinational BOO model and to encourage further research in this field.

2. Related works, research design and methodology

IAEA defines nuclear security as “prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities” [5, p. 18]. While appropriate equipment and workforce are the vital pieces of nuclear security, none of these variables function well without a culture of security.

Increasing interest on nuclear security and nuclear security culture encourage cultivation of specific literature [6–11], best practices [12,13], as well as implementation guidelines [14–17]. Despite the substantial interest on culture, research field related to “influence of national cultures on nuclear security” remains less researched and underestimated in nuclear security studies.

Few studies concentrate upon link between characteristics of national cultures and organizations' security culture. A research which compares two countries' security awareness confirms that individuals in different cultures might address risks in dissimilar way and “people in different cultures have different levels of security sensitivity depending upon their social and technical environment” [18, p. 365]. Other research proposes that “process-oriented cultures which are characterizes as ‘more conservative toward innovation and risks’ is believed to lead increased compliance with information security policies” [19, pp. 184–185].

A NPP is a cultural organization. However, during literature review, only one research is found which explicitly recognizes that “national cultures strongly influence the development of nuclear safety/security cultures” [20]. Different from our research motivation, this research focuses on individual societies' and nations' attitudes in developing nuclear safety/security culture. Our research article is one response to this need and aims to assess how nuclear security can be elaborated in multinational working environments such as Akkuyu NPP. At that point, we decided to apply Geert Hofstede's model of national cultures which is the first to quantify cultural orientations in more than 60 countries. There are several in-depth methods in literature aimed to measure the cultural differences in particular groups. However, these methods require detailed interviews which are hard to implement in NPPs because of security concerns. In addition to Hofstede's method, there are other methodologies such as Schwartz's cultural value orientations. While Schwartz relies on universal human value types[2] to compare national cultures, we argue that Hofstede's six pillars is more applicable to assess business management environments. As a result, we argue that Hofstede's metrics are helpful for exploring how multiculturality might influence a NPP's nuclear security and employees' attitudes towards security. Yet, it should be noted Hofstede's approach is designed to measure the cultural settings for a specific age range at a certain time period. Therefore, there might be slight changes in it.

In addition to the analysis which sets forth the influence of cross-national cultural differences on nuclear security, we also try to construct a model for blending cyber and physical security units to overcome challenges resulted from hybrid threats. For building this model, we follow a cyber resilience design process which has underlying principles including *abstraction, cohesion, coupling, decomposition,* and *encapsulation* [*21, p. 167*]. While we propose this model, we acknowledge that there is limited information available regarding Akkuyu's prospective organizational structure. Therefore, we build the model at the most fundamental level to make it eligible for further modifications (*abstraction*). In design process, we tried to protect the consistent relationship among the units to create a traceable outcome (*cohesion*). In the real design, there might be slight changes up to the structure of the managerial system. In the human level, to sustain multiple control advantages, we also prefer to build up teams (i.e., buddy system in the scuba diving) from different mindsets and perspectives to minimize the risks (*coupling*). In our model, a platform is created to discuss and decompose the problems in the NPP from the perspectives of the cyber and physical security units (*decomposition*). Regular meeting of this platform enhance communication with public authorities and also increase managerial level's awareness on actual threats. This awareness would be preemptive to protect the facility and reinforce nuclear security (*encapsulation*).

3. Nuclear security in the age of converged threats: case for Akkuyu and current regulations

Contemporary security environment is dynamic which reduces the minimum level of knowledge to make an attack while increasing the sophistication of the attack levels [22]. In addition, there is a remarkable change in threat landscape. For instance, malicious use of Unmanned Aerial Vehicles (UAV) is a growing threat for NPPs. However, physical protection systems were designed before emergence of UAV technologies [23]. Nuclear supply chain emerges as another source of vulnerability which has long been overlooked in NPP security studies [24].

Cyber-physical attacks are also new threats which are regarded as “particular category of cyberattacks that, whether intentionally or not, adversely affect physical space by targeting computational and communication infrastructure that allows people and systems to monitor and control sensors and actuators” [25]. With respect to these threats, security problem of NPPs is no longer the protection of different types of assets (cyber/physical) by two different

[1] Turkey has been planning to build and operate NPPs for more than 50 years. Since Akkuyu NPP is the only confirmed project so far, it is announced that the second NPP might be constructed in Sinop, İnceburun and the third project might be built in İğneada, Kırklareli. Yet for second and third projects construction and operation dates and stakeholders are not determined yet.

[2] Schwartz proposes six individual values which he labelled as “conservatism vs autonomy”, “hierarchy vs egalitarianism”, “mastery vs harmony”.

departments. Threats converge in various stages of the attack process, but the organizations built for "stove piped security functions" are inadequate to respond these new challenges. The silo mentality "leaves too many gaps and provides no reliable way to evaluate an enterprise's risk position" [26, p. 64]. In classical outlook, physical threats are responded by physical security whereas cyber threats are handled by cyber security units. Yet, these approaches fail to respond requirements of multilayered interactions among connected components, shifting networks of relationship, and cyber connections [12, p. 14].

Cherkashyn states that before 2005, physical protection was considered to be self-sufficient in terms of security of NPPs as IT security was dealing with administrative and operational networks [27]. However, as cyber-physical threats continue to converge, a new approach is required. For instance, an information security breach may derive from a physical security incident since an intruder may install devices on computers that enables stealing of login information [28]. Also, physical protection systems' itself now includes digitalized CCTVs, back-up systems, emergency alarm stations, etc. Vulnerability of digital control systems in NPPs was already underlined with Stuxnet attack in 2011 [29,30]. Thus, the mentality regarding nuclear security has changed as Stuxnet taught a great lesson about the security risks of digitalized control systems. Even the ultimate target was not a NPP, cyber-attack to Ukrainian Power Plant and recent Triton attack targeted a petrochemical complex demonstrated the rise of hybrid attacks.

Each state has to build up its nuclear security regime based on its own dynamics. Regulations have vital roles in this process as IAEA asserts "a legislative and regulatory framework is an essential element of a State's nuclear security regime" [31, p. 1]. In Turkish case, from the perspective of nuclear security, there are currently two major regulations which Akkuyu NPP has to follow: *Regulation on Management System in Nuclear Facilities* [32] and *Regulation for Physical Protection of Nuclear Facilities and Nuclear Substances* [33]. Both regulations are drawing broad guiding lines for the operator without presenting any insight how to solve the recent security management problems.

Regulation on the Management System in Nuclear Facilities defines the role of Regulation as "to establish and maintain a management system within the organization that establishes, operates, discharges or shuts down a nuclear facility, prioritizing security, developing leadership capabilities at all levels of management and supporting a strong security culture to regulate the basic requirements to ensure the improvement" [32]. In this regulation nuclear security is defined as "to take necessary physical protection measures to prevent, detect and respond to theft, sabotage, unauthorized access and other malicious attempts targeting nuclear materials and facilities and to maintain their effectiveness". Yet, the regulation on management systems is not openly addressing converged threats or emphasizing the question how to manage and protect the digital systems in the NPP.

The Regulation for Physical Protection of Nuclear Facilities and Nuclear Substances focuses on physical protection. Purpose of the regulation is defined as "to protect nuclear material and facilities throughout peaceful nuclear activities within the borders of Turkey against theft and sabotage and to regulate the principles relating to physical protection measures" [33]. Cyber security has downsized to information security and explained as "protection of information against acts such as unauthorized access, use, disclosure, tampering, modification, inspection, copying, recording or destroying, in order to maintain confidentiality, integrity and validity" in Article 4. Overall, in the current Turkish regulations, there is an ambiguity about how state and operator should handle the converged threats against the NPPs. There is also possibility that the state would publish follow-up regulations to deal with this problem. At the moment, regulations are inadequate to respond the needs of converged threats. In addition to the regulations, there is also unclarity about how the operator should cooperate with whom in case of a crisis. Some of the crises in nuclear security are time sensitive but the tempo of bureaucracy might not be compatible to handle such cases.

Nuclear security is not a basic design or elaborated regulation but a consensus or a habitus that is build throughout time to respond threat scene and form a culture. While creating a nuclear security regime, discussions on "human nature" is vital especially on the issue of integrating separate security compartments of cyber and physical under one blended approach. However, the nature of threats in these two domains are different from each other in terms of deterrence and protection. In the physical protection field, threats are apparent and visible to the protection teams. Thus, security staff's visual capabilities are mostly enough for them to prevent a possible incident. However, threats on the cyber domain is not easily noticeable.

There is almost no certain information about how Akkuyu NPP's security system will be structured. To understand possible administrative structure, it would be better to focus on nuclear security structures in other states. For instance, in the structure of Ukrainian NPP, the role of cybersecurity and physical security is remarkably different than its counterparts [34]. Information and technical department positioned under financial director and physical protection are allocated under first deputy director. In Russian example, facility directors are personally liable for nuclear security breaches and they are required to establish an adequate physical protection system [12].

Even though complex security environment presents apparent risk for nuclear security, Akkuyu NPP has advantages to design an integrated management system for controlling physical and cyber security. Thus, throughout the design process, Ankara should build a sophisticated nuclear security which includes a smart management for blending cyber and physical security systems based on good supervision, open communication, and continuous improvement of the performance.

4. Addressing cultural differences: A blurred line for nuclear security?

While it is difficult to measure them, cultural differences create a blurred line, and the impact of a national culture can even persist in life-and-death situations like in case of a nuclear security incident [35]. Culture is constructed via inter-subject interaction and based on shared assumptions or beliefs about reality. Even though there are universally agreed standards on security, how these standards going to be practiced changes from culture to culture. Khripunov mentions that "nuclear security is first rooted in a country's security culture" [7, p. 14]. From this aspect, it is possible to claim that each country's approach to achieve nuclear security culture depends on its overall culture including its history, traditions, and working culture.

As mentioned in the Methodology section, Hofstede model presents a useful outlook to assess Akkuyu NPP's future nuclear security environment. Hofstede's framework was firstly developed to measure job attitudes of international employees of IBM from 1967 to 1973 through a large survey and extensive data via in-depth interviews. Hofstede updated his methodology and added social

Table 1
Scores of Turkey and Russian Federation in Hofstede model.

Categories	Turkey	Russia
Power Distance Index (PDI) [Small PDI vs. Big PDI]	66	93
Individualism (IDV) [Individualism vs. Collectivism]	37	39
Uncertainty Avoidance Index (UAI) [High UAI vs Low UAI]	85	95
Masculinity [Masculinity vs. Femininity]	45	36
Long Term/Short Term Orientation [Long vs. Short Term Orientation]	46	85
Indulgence/Restraint (IVR) [Indulgence vs. Restraint]	49	20

restraint category to his survey in 2010. Following, framework's validity was tested by subsequent studies. In that sense, his methodology was broadly accepted as a reliable and institutionalized tool to measure various cross-cultural phenomena such as international management or communication. Since Akkuyu NPP is a joint project between Russian Federation and Turkey, both two countries' national culture parameters should be taken into consideration. To this end, Turkey's and Russian Federation's scores related national cultural differences were demonstrated by relying on Hofstede's original framework [36,37] (Table 1).

4.1. Power Distance Index (PDI)

PDI is defined as “the extent to which the less powerful members of organizations and institutions accept and expect that power is distributed unequally” [38]. In high PDI scores, the boss is the principal source of authority and the subordinates avoid debating and criticizing them [39]. Subordinates are not encouraged in enhancing their authorities and they are unlikely to work well in team exercises. In high PDI scored cultures, feedback from employees is not considered as a necessity. From these aspects, PDI scores could provide useful inputs in ameliorating an NPP's nuclear security setting.

A recent study which uses Hofstede's framework assessing nuclear safety and security in East Asia countries confirms that among all six dimensions of Hofstede, PDI may have direct implications on NPP's safety/security cultures. It is noted that “in societies where power hierarchy is so entrenched” questioning and feedback mechanisms might not be properly encouraged [20, p. 1700]. In addition to this, while a leader coming from a high PDI culture, h/she expects the orders to be acted upon without question. In such environment, the employees from a low PDI's attitudes might be critical.

As outlined in Table 1, the gap between PDI scores of Turkey (66) and Russian Federation (93) requires particular attention for Akkuyu NPP. Russian Federation, scoring 93, shows a high PDI culture where role of leader is vital and leader is expected to provide detailed instructions [40, p. 18]. High PDI culture might also negatively affect flexibility of organizations in crisis times. Nuclear security in NPPs is a dynamic process, thus supporting proactive attitude to solve security problems is critical. Developing a solid nuclear culture necessitates to find a balance between flexibility, crisis management and leadership.

It is noted that “in countries and regions with a higher PDI, senior management must optimize its involvement to become role models in organizations to boost nuclear security culture, through their visible support and personal behavior” [6, p. 17]. Employee feedbacks and effective communication are other vital pieces of nuclear security culture. In that sense, in a high PDI culture, organizations should pay attention to keep two-way-communication effective and address any potential communication blockages [17].

4.2. Individualism versus Collectivism (IDV) Index

IDV explores the “degree to which people in a society are integrated into group” [38, p. 11]. Scores close to 0 stand for the most collectivist whereas scores close to 100 demonstrates for the most individualist society. In cultures having low values, communication is generally indirect, harmony of the group has to be maintained, and open conflicts are avoided. Saying “no” is seldomly used in collectivist societies which is associated with confrontation.

Turkish and Russian cultures have close values which indicate their collectivist nature. This might have consequences for leadership. Studies which examine leadership features with Hofstede's index claim that “dyadic relationship between a supervisor and subordinate may reflect influence of collectivism” and “collectivists may have greater tolerance and may feel more compelled to maintain a high-quality of exchange despite minor violations of trust by leader” [41, p. 266].

IDV index could provide foresights for employee's behaviors on information security. “Stronger loyalty in collectivistic individuals could cause them to strongly adhere to IT security policies as long as this adherence is seen as loyalty” [42, p. 94]. To assess the security culture of a NPP, this metric could be helpful. For instance, “in societies with a predominantly collectivist mentality, there is much better chance of success for nuclear security efforts if the initiative is spearheaded by a group of like-minded people committed to shared goals rather than by lone individuals” [6, p. 17]. In addition, faults of the managers can be quickly repeated by the staff without questioning or opposition. Employees might be reluctant to report security violations due to strong loyalty in collectivist societies. In these cases, nuclear security management has to establish a system which replaces disadvantages of collectivism with checks and balances to get prepared for uncertainty and unexpected events.

4.3. Uncertainty Avoidance Index (UAI)

UAI illustrates “the degree to which the members of a society feel uncomfortable with uncertainty and ambiguity” [43]. A lower UAI value indicates that a country is less concerned about ambiguity and uncertainty. Lower UAI is also characterized by a greater willingness to take risks [44] and being less resistant to change.

Researches illustrate correlations between UAI and security compliance levels. In particular, while low UAI countries are considered to be “less rule dependent and more trusting”, employees in such cultural context might challenge the strong rules for pragmatic reasons [40, p. 19]. These arguments would have clear implications on nuclear security culture as Turkey and Russian Federation have both high scores indicating a high UAI. In cultures with high UAI where the leader or manager is expected to issue clear instructions, a stronger need for rules and regulations might be more visible.

UAI metric also gives valuable clues on the prospects in welcoming innovations which are crucial to develop a vibrant nuclear security. The high values show employees' preferences with less risk-taking attitude as well as less individual responsibility. In other terms, high UAI culture emerges with little tolerance to risks [45, p. 313]. In such context, the NPP operator must implement a proper nuclear security agenda to mitigate disadvantages related to high UAIs since "preparing for uncertain and unexpected events is an important trait of safety-security cultures" [20, p. 1700].

4.4. Masculinity and femininity

While masculinity is defined as "a preference in society for achievement, heroism, assertiveness and material rewards for success", femininity represents "a preference for cooperation, modesty, caring for the weak and quality of life" [43]. While Turkish and Russian working culture both fall into the masculinity part of the index, Russian value is closer to masculinity. Masculinity is expected to be assertive with a concentration on material achievements which requires a fair management and open communication to prevent possible misunderstandings. Since Turkish and Russian cultures are both close to masculinity, some fields of security such as inspecting logs would not be seen as a field of achievement.

In addition to masculinity and femininity orientation in national cultures, the gender composition within organizations might have different implications on security environment. Researches find significant gender-wide differences regarding computer skills, security self-efficacy and self-reporting behaviors [46]. Therefore, to construct a mitigative nuclear security culture, NPP management should consider appointing female experts to these missions which necessitate better recognition and object location memory performance [47].

4.5. Long Term/Short Term Orientation (LSTO)

LSTO describes balance between long-term opportunity and short-term satisfaction [43]. A lower degree of this index (short-term) indicates that traditions, norms and history are valued whereas societal change is viewed with suspicion [43]. In contrast, societies with a high degree in the index reflect a more pragmatic character and see problem-solving as a necessity by emphasizing the future.

Differences in LSTO index could create impact on information security behavior. For instance, while IT leaders coming from long term-oriented culture would engage in long term planning in security architecture, short term view would focus on short term and hasty solutions [42]. This index demonstrates sizeable variance between Turkish and Russian culture. Turkish culture is represented with short-term orientation which might result with tendency to behave without thinking long-term consequences and expectations of immediate gratification. In contrast, long-term orientation culture would prefer delayed gratification and focus on holistic thinking. Long-term orientation group also has strong frugality tendencies which might affect the nuclear security culture on some occasions such as change management. In that respect, the rift between these two cultural orientations requires special attention in building a vibrant nuclear security culture which has to underline compromise and teamwork mentality.

4.6. Indulgence/Restraint (IVR)

IVR index refers to the "degree of freedom that societal norms give to citizens in fulfilling their human desires" [48, p. 519]. Relatively weak control is called as indulgence which is defined as "a society that allows relatively free gratification of basic and natural human desires" whereas "restraint" is associated with "a society that controls gratification of needs and regulates it by means of strict social norms" [43]. Scores close to 0 stand for a more restrained society whereas scores close to 100 stands for a more indulgent one. Restrained societies are more pessimistic and have a stricter work ethic. Indulgent societies are presented with their optimism and less moral discipline. In this dimension, Turkish culture (with score 49) differs from the Russian (with score 20) one. Thus, Akkuyu NPP's management layer has to show effort to open communication between groups and break the ice to cultivate a cooperative environment.

The Akkuyu NPP is a new model not only because of its business model but also its multinational staff. Building up of a functional organization is not easy because it requires converging differences and culture settings on security. Whatever technology is implemented, in the end, there is also a human component that interacts or uses these devices or machinery. Strategic communication, information flow, crisis management and open communication cannot not be sustained without focusing on the culture.

Hofstede Index presents commonalities and differences of both cultures which might guide the NPP operator to cultivate a working model that would help build up a robust nuclear security. To conclude, it is also critical to mention that the NPP operators are also prone to the problems of generational gaps among its staff. Since experience is highly appreciated in the sector, the baby boomers would work with millennials which would bring unexpected problems that jeopardize the nuclear security culture.

5. Developing A model for Turkish nuclear security culture

Akkuyu NPP is the first example with its business model. But the other problem is rise of converged threats for nuclear industry. Solution of combining physical and cyber security departments is on the table in the age of hybridity. To mitigate cyber-physical threats, three models are presented [49]. ***The first method*** combines physical and security departments under Chief Security Officer (CSO) or Chief Risk Officer (CRO). This model gives an exceptional responsibility to administration to secure both physical and cyber domains from border of the facility to byte of data produced. In such model, CSO or CRO has to show a remarkable effort to integrate business models of both departments to cooperate on the similar threat perception.

The second method is to keep both departments separate and ask them to report a CSO or CRO. S/He will make decisions upon the information compiled from these departments which will create some lag in the decision-making process. This type of model minimizes costs and reduce the redundancy. Yet, since both departments are not connected, it is quite difficult to build a unified nuclear security culture. ***The third method*** is to build a bridge and form human level communication channels among the departments. This can be done with forming a risk committee that combines both departments' functionality into a middle level decision making component. For Akkuyu NPP, by considering Hofstede's points, we propose to build up such an eclectic model. For Turkish NPP, we prefer a model (Annex 1) which forms a hub between the departments that shorten the decision-making process and improve the efficiency in the crisis management. Our model for the Akkuyu NPP also tries to overcome the generational gap problem through establishing vibrant communication channels among the departments.

Our model suggests that the operator keeps both departments under CSO or CRO and forms a risk committee between them with the participation of deputy of the physical security department and deputy of the cyber security department and deputy of CSO or CRO. The CSO or CRO also creates a liaison system for both departments. The liaison team is formed by a senior and a junior from each department to overcome the generational gap and transfer tacit knowledge regarding to security. The staff in the liaison system could make shifts and periodically new staff will take role in the system. With this way, different personnel in both departments would learn the functionality of their security. Cooperation and communication among the parties is also sustained continuously. Regular meeting with the liaison team and CSO/CRO hub would preemptively prevent possible threats. In addition, the risk committee under CSO/CRO directly communicate with State level cyber and physical security. Although our model encourages risk committee formation, the necessity of future researches on the committee in different settings is evident to test its viability and functionality.

Implementation of this model could be effective if the government agrees to design high-risk council which might bring all parties in a room to find efficient solutions to the possible threats. The high-risks council should regularly meet and have to be supported by all relevant public bodies and law enforcement agencies. This council could also have rights to organize hand-on, force-on-force, and table-top exercise to polish the skills of the NPP.

6. Conclusion

Increased use of digital systems in NPPs creates new security concerns such as emergence of hybrid threats which are seeking to exploit vulnerabilities arising from the convergence of cyber and physical realms. Rise of these hybrid threats affects all CIs. However, NPPs are the most critical facilities which require maximum attention with respect to consequences of a possible security breach. Traditional IT security approaches are not sufficient to address the NPP's new security requirements. This necessitates to implement a security system which blends cyber and physical security supervision and ensures smart communication between these two departments. It is quite crucial that these security concerns should be addressed at the very early stages of the design process. Turkey might use this opportunity for Akkuyu NPP Project as the facility is expected be operational by 2023. In order to build a strong nuclear security, Turkey is eager to take first steps such as forming regulations and cultivating the necessary human capital.

Akkuyu experience is unique as the NPP is owned by a multinational consortium. Thus, presence of multinational working cultures might create new problems in building a robust nuclear security culture. Nuclear security culture is strongly associated with a Country's security culture. However, literature on nuclear security pioneered frequently underestimates impact of different national cultures on formation of a NPP's security culture or on the security related behaviors of its employees. Our work primarily aims to address this gap and contributes the nuclear security literature by underlining the importance of paying regard to implications of multiculturality on nuclear security by focusing on Akkuyu NPP example.

To identify the possible impacts of cultural differences on nuclear security, Hofstede's national cultures' metric is useful since we identify different characteristics between Turkish and Russian working cultures which might create implications on nuclear security. For instance, there is a significant difference related to PDI records of Turkey (66) and Russia (93). In that respect, while Russian working culture might not encourage feedbacks coming from employees, Turkish working culture is more open to questioning.

For a vivid NPP security these differences should be taken into consideration with a smart management, open communication and culturally sensitive trainings. Our proposed model presented in Section 5 addresses not only risks arising from hybrid threats but also considering different working cultures by accelerating the communication between different departments. This model facilitates conversation between operator and State since State has to shape the nuclear security environment and to define expectations of the operator at the macro level. Additionally, Turkey's regulatory environment on nuclear security should support responding the risks arising from hybrid and dynamic threat environment.

Increasing risks in digitalized systems of the NPPs underline the need to focus on human-machine interaction and develop a human centric nuclear security regime. The “to-do list” that we have is to raise awareness, keep vigilance level high and establish a vivid nuclear security culture. Otherwise, despite the deployment of all technological solutions, it is not easy to fill the gaps that originated from human vulnerabilities. Therefore, we must understand cultural weaknesses of Turkish NPP setting and then create a model of cooperation to combine the cyber and physical security departments. Human does not learn rules, regulations and practices only by reading. Even if the staff understand all setting, second failure comes with quick adaptation (habituation) to environment which vanishes vigilance and reduces risk sensitivity. Therefore, future researches on nuclear security should focus on overcoming problems related to vulnerabilities in risk adaptation and strengthening cognitive capabilities. This is particularly important while future generation's workforce to be employed in NPPs and their differentiated working cultures are considered.

In this research, we discuss only operator's role in building a functional nuclear security culture. Yet, State's structure should be also compatible with the NPP's security needs. Building vigorous communication channels and supporting the operator's endeavors to construct a nuclear security culture are other major steps of a cycle which has to be enhanced with continuous trainings. When Ankara has this rhythm on nuclear security culture, the need for change in the regulations would be apparent.

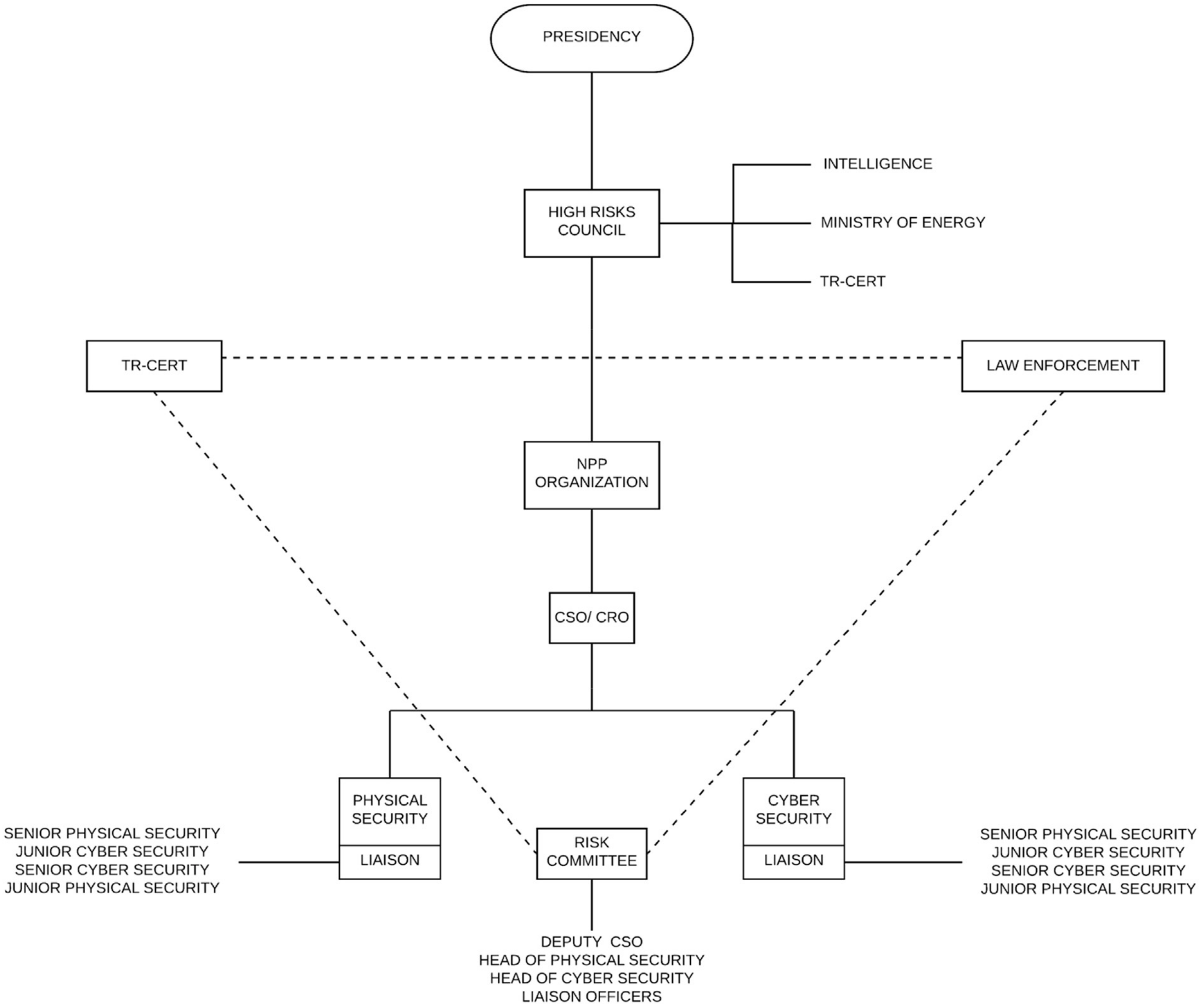
Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Annex 1. Proposed Turkish model for integrating physical and cyber security in the Akkuyu NPP



References

[1] The European Centre of Excellence for Countering Hybrid Threats, Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats, October 2019. Helsinki, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Nuclear-Research-Report-2019_web.pdf.

[2] World Institute for Nuclear Security, The State of Nuclear Security in 2020, 06 June 2020. Vienna, https://www.wins.org/document/the-state-of-nuclear-security-2020/.

[3] B. Taebi, M. Mayer, The Russian Nuclear Energy Proposal: an Offer You Can't Refuse, Belfer Center for Science and International Affairs, 5 June 2015. https://www.belfercenter.org/publication/russian-nuclear-energy-proposal-offer-you-cant-refuse.

[4] E. Lecavalier, Russian nuclear power: convenience at what cost? Bull. At. Sci. (16 October 2015). https://thebulletin.org/2015/10/russian-nuclear-power-convenience-at-what-cost/.

[5] IAEA Division of Nuclear Security, Nuclear Security Series Glossary Version 1.3, November 2015. Vienna, https://www-ns.iaea.org/downloads/security/nuclear-security-series-glossary-v1-3.pdf.

[6] I. Khripunov, Nuclear Security Culture: the State of Play, International Atomic Energy Agency, Vienna, May 2018. http://spia.uga.edu/wp-content/uploads/2018/05/INSEN-TEXTBOOK-Pages-1-8-NS24-Nuclear-Security-Culture-Textbook.pdf.

[7] I. Khripunov, A Roadmap for Nuclear Security Culture, The 1540 Compass, Winter, 2016, pp. 31–35. No: 11, http://spia.uga.edu/wp-content/uploads/2016/12/Compass_11-Winter2016.pdf.

[8] I. Khripunov, Nuclear safety vs security: can the two cultures be harmonized? Bull. At. Sci. (6 July 2018). https://thebulletin.org/2018/07/nuclear-safety-vs-security-can-the-two-cultures-be-harmonized/.

[9] D. Gupta, E. Bajramovic, Security culture for nuclear facilities, in: Proceedings of the International Nuclear Science, Technology and Engineering Conference Proceedings, vol. 1799, American Institutes of Physics, 2017, 050014, https://doi.org/10.1063/1.4972948.

[10] P. Carroll, Security culture: a personal perspective from the United Kingdom, in: N. Ischenko, J. Holmes (Eds.), Nuclear Security Culture: from National Best Practices to International Standards, I. Khripunov, IOS Press, Amsterdam, September 2007, pp. 23–30.

[11] C. Packer, Relationship of management systems, human performance, and security culture, in: N. Ischenko, J. Holmes (Eds.), Nuclear Security Culture: from National Best Practices to International Standards, I. Khripunov, IOS Press, Amsterdam, September 2007, pp. 43–53.

[12] I. Khripunov, J. Holmes, D. Nikonov, M. Katsva, Nuclear Security Culture: the Case of Russia, Center for International Trade and Security The University of Georgia, December, 2004. https://www.nti.org/wp-content/uploads/2021/09/analysis_cits_111804.pdf.

[13] UK Office of Nuclear Regulation, Maintance of a Robust Security Culture, UK Office of Nuclear Regulation, March 2020. https://www.onr.org.uk/

operational/tech_asst_guides/cns-tast-gd-2.1.pdf.

[14] IAEA, Safety and Security Culture, Vienna, https://www.iaea.org/topics/safety-and-security-culture, 2019.

[15] IAEA, Nuclear Security Culture: Implementing Guide, September 2008. Vienna, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf.

[16] IAEA, Self-assessment of Nuclear Security Culture in Facilities and Activities-Technical Guidance, November 2017. Vienna, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf.

[17] World Institute for Nuclear Security, Nuclear Security Culture Version 3.1, January 2019. Vienna, https://www.wins.org/document/1-4-nuclear-security-culture/.

[18] C.C. Chen, B.D. Medlin, R. Shaw, A cross-cultural investigation of situational information security awareness programs, Inf. Manag. Comput. Secur. 16 (4) (2008) 360–376, https://doi.org/10.1108/09685220810908787.

[19] M. Tang, M. Li, T. Zhang, The impacts of organizational culture on information security: a case study, Inf. Technol. Manag. 17 (2) (2016) 179–186, https://doi.org/10.1007/s10799-015-0252-2.

[20] J.C.I. Trajano, A policy analysis of nuclear safety culture and security culture in East Asia: examining best practices and challenges, Nucl. Eng. Technol. 51 (6) (2019) 1696–1707, https://doi.org/10.1016/j.net.2019.04.014.

[21] D. Shoemaker, A. Kohnke, K. Sigler, How to Build a Cyber-Resilient Organization, CRC Press Taylor & Francis Group, Boca Raton, 2019.

[22] G. Anthes, Digital Defense, Computer World, 22 December 2003, https://www.computerworld.com/article/2573633/digital-defense.html.

[23] S. Islam, M. Ahmed, S. Islam, A conceptual system architecture for countering the civilian unmanned aerial vehicles threat to nuclear facilities, Inter. J. Critic. Infrastruct. Protect. 23 (C) (2018) 139–149, https://doi.org/10.1016/j.ijcip.2018.10.003.

[24] S. Eggers, A novel approach for analyzing the nuclear supply chain cyber-attack surface, Nucl. Eng. Technol. 53 (3) (2020) 879–887, https://doi.org/10.1016/j.net.2020.08.021.

[25] G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat, Elsevier Inc, Waltham MA, 2015.

[26] S.M. Rahman, S.E. Donahue, Convergence of corporate and information security, Int. J. Comput. Sci. Inf. Secur. 7 (1) (2010) 63–68. https://arxiv.org/pdf/1002.1950v1.pdf.

[27] D. Cherkashyn, Balancing cyber-physical defense in the energy sector: nuclear energy lessons learned, in: G. Gluschke, M. Macori, M.H. Caşın (Eds.), Cybersecurity Policies and Critical Infrastructure Protection, Institute for Security and Safety, Institute for Security and Safety) Press, Potsdam, 2018, pp. 331–341.

[28] A. Aleem, A. Wakefield, M. Button, Addressing the weakest link: implementing converged security, Secur. J. 26 (3) (2013) 236–248, https://doi.org/10.1057/sj.2013.14.

[29] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown Publishers, New York, 2014.

[30] M. Molnár, V. Istvan, The Cyber-Physical Security Power Grid, IEEE Smart Grid November 2019 ENewsletter, 2019. https://smartgrid.ieee.org/newsletters/november-2019/the-cyber-physical-security-of-the-power-grid.

[31] IAEA, Developing Regulations and Associated Administrative Measures for Nuclear Security: Implementing Guide, 2018. Vienna, https://www-pub.iaea.org/MTCD/Publications/PDF/P1762_web.pdf.

[32] Turkish Official Gazette, Regulation on Management System in Nuclear Facilities, 8 April 2017. No. 30032, https://www.resmigazete.gov.tr/eskiler/2017/04/20170408-5.htm.

[33] Turkish Official Gazette, Regulation for Physical Protection of Nuclear Facilities and Nuclear Substances, 22 May 2012. No. 28300, https://www.resmigazete.gov.tr/eskiler/2012/05/20120522-7.htm.

[34] N.P.P. Zaporizhzhia, Organizational Structure, 2022. https://www.npp.zp.ua/en/about-us/structure.

[35] P. Ghemawat, S. Reiche, National cultural differences and multinational business, in: P. Ghemawat (Ed.), The Laws of Globalization and Business Applications, Uk, Cambridge University Press, 2017, pp. 239–279.

[36] Hofstede Insights, Compare Countries, 2022. https://www.hofstede-insights.com/country-comparison/russia,turkey/.

[37] G. Hofstede, Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations, second ed., Sage Publications, California, 2001.

[38] G. Hofstede, Dimensionalizing cultures: the Hofstede model, Online Read. Psychol. Culture 2 (1) (2011) 3–26, https://doi.org/10.9707/2307-0919.1014.

[39] Galina Balykina, Cultural Dimensions and Modern Russian Business (October 21, 2013). Növekedés És Egyensúly. A 2013. Június 11-i Kautz Gyula Emlékkonferencia Válogatott Tanulmányai, Győr: Universitas Győr Kht., 2014, pp. 87–95, https://doi.org/10.2139/ssrn.2342954.

[40] T. Dols, S.A.J. Gilbert, Exploring the influence of national cultures on non-compliance behavior, Commun. IIMA 10 (3) (2010) 11–31. https://scholarworks.lib.csusb.edu/ciima/vol10/iss3/2.

[41] E.K. Pellegrini, T.A. Scandura, Leader–member exchange (LMX), paternalism, and delegation in the Turkish business culture:An empirical investigation, J. Int. Bus. Stud. 37 (2006) 264–279, https://doi.org/10.1057/palgrave.jibs.8400185.

[42] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hud, M. Warkentin, R. Baskerville, Future directions for behavioral information security research, Comput. Secur. 32 (2013) 90–101, https://doi.org/10.1016/j.cose.2012.09.010.

[43] Hofstede Insights, National Culture, 2022. https://hi.hofstede-insights.com/national-culture.

[44] I. Akiner, W. Tijhuis, Cultural variables and the link between managerial characteristics in construction industry: reflections from Turkish and Dutch examples, in: International Conference on Multinational Construction Projects: Securing High Performance through Cultural Awareness and Dispute Avoidance, November 21-23, Shangai, 2008. An Also See; I. Akiner, Critical Viewpoints on the Management of Conflict in Multi-National Construction Projects, Organization, Technology and Management in Construction vol. 6, 2014, pp. 1038–1046, https://doi.org/10.5592/otmcj.2014.2.6, 2.

[45] K. Yıldırım, Negotiating with managers from Turkey, in: M.A. Khan, N. Ebner (Eds.), The Palgrave Handbook of Cross-Cultural Business Negotiation, Palgrave Macmillan, Cham, 2019, pp. 309–328.

[46] A. Mohd, H. Wu, A. Ivan, Y. Xiaohong, L. Ling, L. Xu, Gender difference and employees' cybersecurity behaviors, Comput. Hum. Behav. 69 (2017) 437–443, https://doi.org/10.1016/j.chb.2016.12.040.

[47] M. Coleman, K. Offen, J. Markant, Exercise similarly facilitates men and women's selective attention task response times but differentially affects memory task performance, Front. Psychol. 9 (2018) 1–19, https://doi.org/10.3389/fpsyg.2018.01405.

[48] G. Hofstede, G.J. Hofstede, M. Minkov, Cultures and Organization: Software of the Mind, McGraw-Hill, New York, 2010.

[49] J. Carney, Why Integrate Physical and Logical Security? " CISCO, 2011. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf.