CYBER SECURITY AND NUCLEAR POWER PLANTS: INTERNATIONAL FRAMEWORK

Assoc. Prof. Ahmet Han

Advisor to the Rector and Faculty Member - Kadir Has University

Board Member - EDAM

Prof. Mitat Çelikpala

Dean, Graduate School of Social Sciences - Kadir Has University

1. Introduction

Hoping to add nuclear energy to its energy mix, Turkey has planned to build three nuclear power plants (NPP) to generate 20% of its electricity production from nuclear power by 2023. The 20% target is almost equal in proportion to the electricity generated by NPPs in the United States.[1] As seen clearly, this marks an ambitious goal. For this reason, maintaining cyber security is a topic in need of diligent attention. This paper, which focuses upon the international aspect of nuclear power plant cyber security, will discuss particular international steps and developments, rendered crucial for the case of Turkey.

2. Cyber Space, Cyber Attack, Cyber Crime: A Conceptual Introduction

Cyber space is a borderless, timeless, and relatively unknowable platform. Although discrepancies in how cyber space is defined exist, it can be generally referred to as all forms of networked, digital activities conducted through digital networks that are used to store, modify, and communicate information, including the actions taken within the domain of such networks.[2] As such, cyber space "includes the internet, but also the information systems that support … businesses, infrastructure, and services."[3] Information travels in this space; who or what controls the network, what its underlying motive is, as well as its capabilities and aims are generally difficult to discern. Despite the recent developments in the efficiency and quality of the service provided to CI network systems, the cost that institutions using this system bear to sustain its security, has greatly increased.

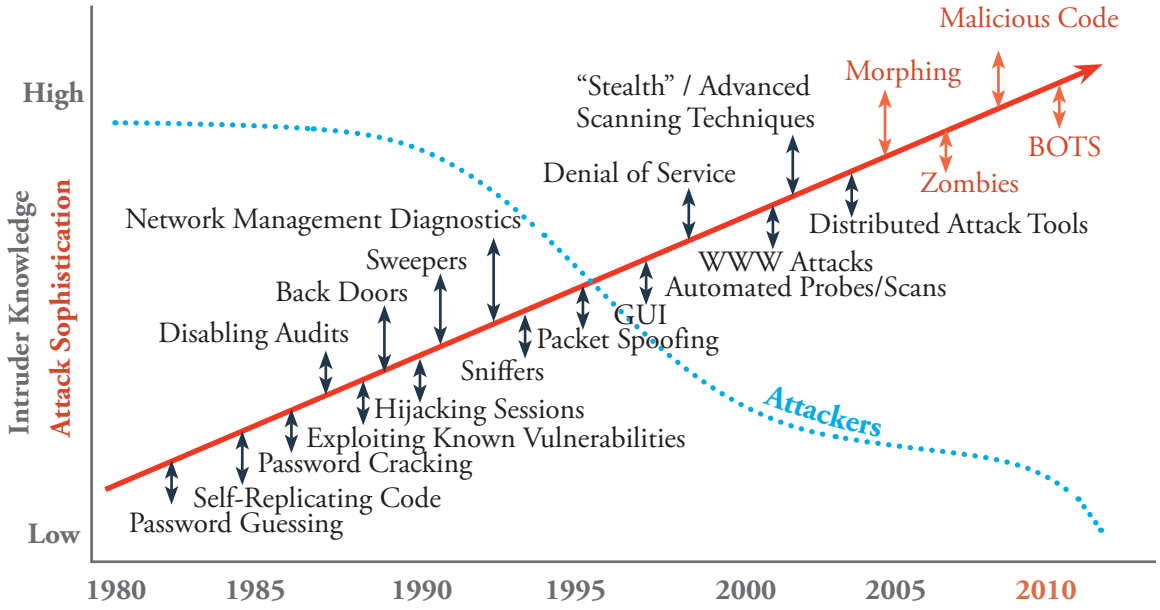
It can be seen that states and certain international organizations are attempting to generate a definition for cyber attack, which threatens the security of systems operating within cyber space. The U.S. Department of Defense (DoD) defines a cyber attack as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[4] This definition includes initiatives that aim to degrade or destroy infrastructure, thereby not limiting the intended consequences of such an attack to physical computer systems or data alone. Rule 30 of NATO's Tallinn Manual defines a cyber attack as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[5] These attacks aim at impairing the confidentiality, integrity and availability of information, which are considered the standard goals of security in an IT environment.[6] Confidentiality hereby refers to "keeping the data private". Integrity refers to making sure that the data is not "improperly altered or changed without authorization" so that it might be relied upon. Availability means "being able to use the system as anticipated."[7] Due to its definition, these attacks refer to almost all state activities and critical infrastructure. The mutual concern of the different definitions of cyber attack posits it as attempt that directly penetrates IT systems and/or elements of critical infrastructure, pursuing strategic aims. Whilst executing cyber attacks, attackers use complex methods and attempt at impairing the confidentiality, integrity and availability of information.

Despite these attacks, which generally harbor political goals, crime-oriented cyber attacks are also at stake. Posing serious hindrances for IT, "cybercrime is an extension of traditional crime but it takes place in cyberspace-the nonphysical environment created by computer systems."[8]

Cyber criminals using this environment effectively "are able to reach out from just about anywhere in the world to just about any computer system, as long as they have access to a communications link."[9] In this new borderless and relatively unknown environment, time, location and physical limitations are eventually rendered irrelevant. Where know-how and sophistication marks almost everything, cyber criminals take advantage of their know-how and the anonymity or the international aspect of the digital world to network with other cyber criminals and create criminal gangs. In this regard, it would not be wrong to suggest that the tools and means that are used by cyber criminals are also utilized by "cyber warfare agents".

Due to the nature of cyber environment, these attacks are difficult "to be contained, can spread uncontrollably and can potentially create many hazards for critical infrastructure," also "in the nuclear field".[10] As Figure 1 underlines below, whilst there is a steady increase in the number of sophisticated of cyber attacks , the level of knowledge required by the perpetrator to organize such an attack is decreasing. In this regard it can be deduced that as the depth of knowledge of cyber attacker's sophistication threshold shrinks, risk continuously evolves and escalates. This reality compels computer security programmes to reach an evaluation stage that encompasses an increased number and scope of potential attack scenarios.[11] An increase in the uncertainty of cyber attackers' motivation, interest and capabilities will result in rendering the vulnerability of IT systems more publicly visible.

Figure 1. Sophistication and Proliferation of Cyber Attacks*



*IAEA, Computer Security at Nuclear Facilities, p.38.

2.1. The Nature of the Beast: Cyber Attackers

It is possible to categorize cyber attackers based upon their stance against the agencies and institutions on target. In this context, we are faced with, at least on paper, two main groups: insider or outsider attack/attacker. Insider attacks refer to actions perpetrated by people who are 'on the inside', i.e. people that are formally employed and authorized by the organization to access the ICT systems, and external threats stem from the third-party outsiders. Whereas outsider attacks are conducted by individuals and institutions that fall outside of the institution at hand.

According to multiple surveys published by the Computer Emergency Readiness Team (CERT) of Carnegie Mellon University's Software Engineering Institute, since 2010, almost 30 percent of cyber attacks were committed by insiders.[12] Another important finding of the survey was that inside attacks have been 46 percent more costly than attacks executed by external perpetrators.[13] However, analyzing these results more carefully denotes that 43 percent of responding organizations were not able to distinguish whether internal or external attacks caused more harm and even whether the attackers were insiders' or outsiders'.[14]

Frankly, the involvement of insiders in any attack substantially increases the probability of success. The risk posed by internal factors remains an important heading for all agencies and institutions, including nuclear facilities. However, it is extremely difficult to detect the threat at the right time. Additionally, in case an appropriate security/safety culture is not in place, the possibility of insider factors unknowingly becoming tools that are exploitable by outsiders remains. For this reason, it is risky to heavily rely upon one-sided and one-layered security structures as well as a single aspect of the security/safety culture. Even more importantly, initially loyal facility personnel, construction workers and maintenance workers can willingly turn against or be coerced into opting for the 'other side' in the course of time. In this regard, notions such as institutional culture and employee satisfaction could serve as defining factors, amongst others. Indeed "threats come in diverse and complex forms" and it is important to constantly assess and test the risks and the system "as realistically as possible".[15]

The tables below[16] chart the main internal and external threats to nuclear power plant facilities, including the agents' resources, time needed, tools, and motivations for cyber attacks:

Table 1. Internal Threats

Attacker	Resources	Time	Tools	Motivation
Covert agent	Facilitated 'social engineering'. System access at some level. System documentation and expertise available.	Varied but generally cannot devote long hours.	Existing access, knowledge of programming and system architecture: - Possible knowledge of existing passwords; - Possibility to insert specifically crafted backdoors and/or Trojans; - Possible external expertise support.	Theft of business information, technology secrets, personal information. Economic gain (information selling to competitors). Blackmail.
Disgruntled employee/user	Medium/strong resources. System access at some level. System documentation and expertise available on specific business and operations systems.	Varied but generally cannot devote long hours.	Existing access, knowledge of programming and system architecture. Possible knowledge of existing passwords. Ability to insert 'kiddie' tools or scripts (potentially more elaborate if they have specific computer skills).	Revenge, havoc, chaos. Theft of business information. Embarrass employer/ other employee. Degrade public image or confidence.

Table 2. External Threats

Attacker	Resources	Time	Tools	Motivation
Recreational hacker	Varied skills, but generally limited. Little knowledge of the system outside of public information.	Lots of time, not very patient.	Generally available scripts and tools. Some tool development possible.	Fun, status. Target of opportunity. Exploitation of 'low hanging fruits'.
Militant opponent to nuclear power	Limited resources, but may be financially supported through secret channels. Access to tools of the cyber community. Little knowledge of the system outside of public information.	Attacks may be targeted at certain previously known events (e.g. Celebrations, elections). Lots of time, patient and motivated.	Computer skills are available. Possible support from the hacker community. 'Social engineering'.	Conviction of saving the world. Sway public opinion on specific issues. Impede business operations.
Disgruntled employee/ user (no longer employed)	Limited resources if not engaged in a larger group of people. May still possess system documentation. May use unmanaged former access. Possible ties to facility personnel.	Varied and depending on the associated group of people.	Possible knowledge of existing passwords. May use unmanaged former access. May have created system backdoors while still an employee. 'Social engineering'.	Revenge, havoc, chaos. Theft of business information. Embarrass employer/other employee. Degrade public image or confidence.
Organized crime	Strong resources. Employment of cyber expertise.	Varied, but mostly short term.	Scripts, home grown tools. May employ 'hacker for hire'. May employ former/ current employee. 'Social engineering'.	Blackmail. Theft of nuclear material. Extortion (financial gain). Play upon financial and perception fears of business. Information for sale (technical, business or personal).
Nation State	Strong resources and expertise. Intelligence gathering activities. Possible training/ operation experience on the system.	Varied.	Teams of trained cyber experts. Sophisticated tools. May employ former/ current employee. 'Social engineering'.	Intelligence collection. Building access points for later actions. Technology theft.
Terrorist	Varied skills. Possible training/ operating experience on the system.	Lots of time, very patient.	Scripts, home grown tools. May employ hacker for hire. May employ former/current employee. 'Social engineering'.	Intelligence collection. Building access points for later actions. Chaos. Revenge. Impact public opinion (fear).

Another approach to categorize cyber attackers involves looking into their motivation. A classification of this sort unwraps in a wide spectrum, ranging from hackers to criminals[17]. Another suggested distinction of cyber attackers that is based on their intent might categorize them under; hackers, those that are "motivated by achieving prohibited access, inspired by boredom and desire for intellectual challenge"; vandals, that are "motivated to cause damage and as much harm as possible… often disgruntled"; and criminals, that are "motivated by economic gain; use of espionage and fraud, among other tactics, to accomplish their goals."[18] Predicting the intentions behind possible attacks is crucial for identifying potential targets and taking precautions.

The internet use of social activists' and terrorists', whose main goal is to influence political decision-makers, is on the rise. It can be seen that these groups, in addition to the tools necessary to turn cyber space into a real battlefield, have gained technical and institutional methods, posing a serious threat to critical infrastructure. Although it is not very plausible for groups that gravitate towards similar activities to attain their political targets, accessing computers that belong to an administration is nonetheless empowering, and appealing to the media.

3. Nuclear Power Plants and Critical Energy Infrastructure

The term infrastructure refers to the fundamental physical and/or organizational system that maintains a bridge between various interdependent facilities and the sustainable functioning of a society via its operations. According to the US Department of Homeland Security, critical infrastructure (CI) consists of "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[19] Similarly, Turkish Prime Ministry Disaster and Emergency Management Authority (AFAD) defines critical infrastructure as: "the networks, assets, systems and structures that, the partial or complete loss of their functionality hampers the continuity of public services and public order and bears detrimental effects on the citizens' health, security and economic activity".[20]

There are three factors that determine how critical an infrastructure is: its symbolic importance, the dependence on it, and complex dependencies.[21] A nation's faith in its governments' control over CI holds not only symbolic but also vital importance. Damage to critical infrastructure would not just result in a loss of government's capacity to work regularly, but, more importantly shackle the citizen's confidence and trust in the government or the regime. These infrastructures are interrelated and interdependent; any disruption, damage or failure of one component could cause wide range of setbacks in another, otherwise called a cascade, or butterfly effect.

Via IT systems, components such as professional expertise, financial and technological information or scientific and intellectual property rights that are used in nuclear power plants (NPP), come together in the form of programs, databases, and programmed logic sequences. Thus, an NPP is more then just CI; its operation requires the existence and healthy functioning of IT systems. A single harm to the IT systems can potentially cause comprehensive damage, possibly even physical loss. For this reason, physical security and computer/cyber security plans should be designed in a complementary manner.

A comprehensive definition of cyber attacks that involves "nonmalicious" attacks and takes into consideration the strategic, political and criminal dimensions is provided by the U.S. Nuclear Regulatory Commission (US NRC) in its Regulatory Guide 5.71 titled "Cyber Security Programs for Nuclear Facilities." It reads:

> "The manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may (1) originate from either inside or outside the licensee's facility, (2) have internal and external components, (3) involve physical or logical threats, (4) be directed or non directed in nature, (5) be conducted by threat agents having either malicious or non malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to critical digital assets or critical systems. [T]he cyber attack may occur individually or in any combination."[22]

Despite the reality that nuclear facilities are currently the target of multiple cyber attacks, only a limited number of steps have been taken in favor of maintaining global coordination and cooperation on aspects including the sharing of information and best practices.[23] Majority of countries, as well as operators within the private sector, approach this subject as "sensitive information"[24], and are thereby reluctant to disclose public information regarding cyber

attacks. The international milieu is increasingly more sophisticated; numerous actors, ranging from hacktivists, insider threats, criminals, states, and terrorist organizations, such as ISIS, which is effective in a diverse territory spanning from Syria to Iraq, have increased their capabilities to carry out cyber attacks. Given that amongst the cyber attacks that were carried out in the U.S. in 2014, almost 35% were reported to target critical energy infrastructure and 2% were directed at nuclear facilities, the urgency of the situation manifests itself. It should be underlined that 55% of these attacks "involved advance persistent threats (APT) or sophisticated actors."[25]

The critical infrastructure of adversaries, particularly their critical energy infrastructure and related energy networks are defined as "natural targets".[26] Nuclear energy facilities, in this regard, could be perceived as "legitimate" goals. Compared to earlier times, there is a considerable increase in the number of actors that may be deemed as enemies. Particularly, the increasing state of dependency to networks that is caused by the digital world is allowing for the realization of malicious intentions.

It is generally emphasized that NPP operators, compared to other stakeholders in the energy sector, are less prepared against cyber-attacks. It should also be noted that cyber remains a novel field vis-à-vis security issues. This infers that, all evaluations and sanctions as well as guiding institutions are novel within this field. Hence, as the cyber industry is itself in the process of accumulating and processing knowledge, it is left to take care of itself in terms of security.

The generic assumption to the question of whether NPP's are well prepared against a cyber attack dictates that they are closed systems that operate as analog, which renders worrying unnecessary. Adopting a similar approach, the US NRC argued that:

> "Nuclear power facilities use digital and analog systems to monitor, operate, control, and protect their plants. 'Critical digital assets' that interconnect plant systems performing safety, security, and emergency preparedness functions are isolated from the Internet. This separation provides protection from any cyber threats. Even so, all power reactor licenses must implement a cyber-security plan under the NRC's cyber security regulations."[27]

In a similar train of thought, the US nuclear energy industry's policy organization, American Nuclear Energy Institute (NEI), posits that cyber security is an area strictly regulated by NRC, thus one in need of no additional regulation.[28]

Actually the nuclear industry was relatively quick to try to develop a response to the emerging cyber threats. In 2002, the industry implemented a cyber security program to protect critical digital assets and the information they contain from sabotage or malicious use. NRC claimed that nuclear energy facilities were safe because they are "isolated from the internet" and that "nuclear power plants are designed to shut down safely should their systems detect a disturbance on the electrical grid", and are protected by security measures "layer upon layer". Going even beyond that, the NRC declared itself as the coordinating body of all cyber security efforts within the industry. For this reason, in 2009, the NRC defined a set of compulsory rules to be implemented by commercial reactors. Despite the insecurity the 9/11 sent forth, the NRC maintained its confidence in the security of the nuclear sector, for which it believed the rules and requirements it codified in 2009, obliging operating companies to execute, helped provide.

In 2014, the NEI petitioned the NRC to revise its cyber security rule "with the intent to protect public health and safety by preventing radiological sabotage." This recommendation contained that the NPP's cyber security must be provided in a centralized manner and that the NRC should become its "single regulator".[29]

However, the fact that the security environment and its requirements are rapidly changing has made this impossible. Further to that, NPP operators have increasingly "been moving towards open protocols and off-the-shelf hardware to manage their process control systems, even connecting them to the Internet—sometimes inadvertently."[30]

There are two reasons for this development. Firstly, equipment manufacturers have quit producing analog systems. Secondly, business networks and process control systems have begun to communicate more via internet connections both between and within themselves. The latter was effected by process optimization, which emerged as a result of the use of technologies dependent upon new software.

Finally, as NPPs have modernized extensively, most of their operation and safety related components became computerized and digitalized, making them dependent on IT. The increased integration of technologies that increase the possibility and vulnerability for cyber attacks have jeopardized cyber security. This revealed the necessity to take measures that go beyond physical precautions when dealing with CI. Various software-based systems have been developed to respond to this need.[31] Amongst agencies that show particular sensitivity to this issue, the International Atomic Energy Agency (IAEA) is a leading name.

4. IAEA's Nuclear Energy Infrastructure Security Approach and Cyber Aspect

The IAEA is the most important international institution working on nuclear infrastructure security and its standardization on a global scale. In a well-directed manner, the IAEA defines the computer security environment as a rapidly changing and evolving scenario[32]. The Agency's GC(55)/RES/10 labeled rule, directed against nuclear security, marks a valid example to the growing concerns on the matter. In this rule, the IAEA places emphasis on awareness raising initiatives for increasing cyber attack threats and the effect these bear on nuclear security[33]. It underlines the provision of physical protection and computer security measures as essential for maintaining nuclear security.

In order to urge efforts in this regard, the IAEA published a guideline for nuclear facilities' cyber (computer) security, which comprises of the necessary rules to be considered in cyber security programmes and rests on the lessons learnt from applied programmes[34]. In this document the Agency defines the security of IT systems as increasingly becoming a matter of life and death, and stresses the importance of establishing and developing computer systems that hold a critical role for the provision of security of digital systems[35].

Examining this document evinces that the IAEA refers to its approach for maintaining the cyber security of NPPs as "defense-in-depth". This is implemented "primarily through the combination of a number of consecutive and independent levels of protection that would have to fail or be defeated before a computer system compromise could occur."[36] The understanding here accentuates that such safety measures, which are multiply layered, must work in tandem.

Nuclear security culture is another notion that the IAEA prioritizes, which refers to "the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security… The foundation of nuclear security culture is a recognition that a credible threat exists and that nuclear security is important."[37] The formation of such a culture "is ultimately dependent on individuals: policy makers, regulators, managers, individual employees and —to a certain extent — members of the public… The concept of a nuclear security culture — and its promotion and enhancement — is refined with a view to establishing international guidance and raising the level of awareness of all concerned, including the public and private sectors"[38]. In this regard, the IAEA has called for a comprehensive nuclear security regime, which rests on an understanding of nuclear safety and security alike, and has urged for the development of global standards for the establishment of such a regime. According to the Agency, a nuclear security regime includes a wide range of elements and activities, such as "legislation and regulation; intelligence gathering; assessment of the threat to radioactive material and associated locations and facilities; administrative systems; various technical hardware systems; response capabilities and mitigation activities."[39]

In the context where nuclear security and cyber security are intertwined, IAEA recommends that "the responsible State authority should periodically issue a threat evaluation including threats to the security of computer systems and information on current attack vectors related to the security of computer systems used at nuclear facilities. …It is vital that facilities maintain an active and ongoing threat assessment, which is regularly briefed to management and operations."[40] The realization of this recommendation necessitates a basic understanding of nuclear security/safety culture that works in tandem with a computer security culture.

Unfortunately, despite the seemingly obvious presence of threats and risks, the coalescence of different stakeholders to deliver a solution to this problem does not go far in the past. IAEA has convened its very first conference tackling the issue, the International Conference on Computer Security in a Nuclear World, only in June 2015.[41] The timing of the conference indicates that this topic has only recently been on the agenda. Further to that, international organizations, such as the IAEA, do not hold any enforcement power in this field.

The Regulatory Authority of the Conference as well as the Director of the IAEA Yukiya Amano has "called for an international response to tackle the global threat posed by criminals and terrorists bent on launching cyber attacks against nuclear facilities."[42] Conference attendants included representatives of nuclear regulators and plant operators, law enforcement agencies, system and security vendors, as well as "650 experts from 92 Member States and 17 regional and international organizations".[43] Indeed, the range of the organizers and attendees demonstrate the multi-dimensional and multi-national nature of global cyber security threats, directed at nuclear infrastructure's cyber security. In short, the increased usage of digital systems and information networks as well as the deepened dependency towards information technology, has enabled states and societies to consider cyber attacks as a crucial matter. Therefore, the concepts of risk and risk management must be prioritized and duly elaborated upon.

5. Risk Management

Claiming that cyber attacks that target NPPs are a globally widespread phenomenon is not reflective of truth. Having said that, given a threat of this sort against nuclear facilities, the risks that appear are noticeably serious, with a limited level of tolerance. The cyber setting constitutes an integrated area of risk. In this regard, differing between 'insider' and 'outsider' in the evaluation of network environments is bound to be unclear and insignificant to some extent. Additionally, due to the source, method and offender of a cyber attack risk against NPPs, it cannot be reduced to a particular and exclusive area of the cyber setting. Thus, the efforts to approach cyber risks as a whole and realize and coordinate international regulatory arrangements to tackle this issue are vital in this sense.

Accordingly, the foundation of an international agreement in the field of cyber security has regularly been brought to the agenda. To this day, the most successful step taken towards the realization of these efforts is the 2001-dated European Commission, Cyber Crime Convention[44]. This Convention, which constitutes the most extensively, approved text by the public, and which has been ratified even by non-member countries, is an international agreement aspiring to harmonize national laws grounded on cyber crimes[45]. As seen in the constitution, signature and execution stages of this document, the most pressing challenge international arrangements on cyber risks, be it of interest to nuclear facilities or not, face is the differing authorities and priorities of nations. However perhaps even more crucial is the lack of consensus on what defines a cyber crime and what does not in a cyber setting. All of these challenges heighten the obscurity, risks and threats embody as part of their nature, and uncloak a 'grey area' that renders international cooperation and arrangement efforts problematic. This situation has reflected onto the Convention, in the sense that even for a document that enabled broad participation, Russia, for example, refrained from signing and the U.S. signed, albeit with drawbacks, stemming from its internal laws.[46] The Convention, though not referring specifically to nuclear facilities, is important for, due to the integrated nature of the cyber environment, its potential contribution to the international and inclusive framework on compulsory measures to prevent NPPs from future risk.

Another initiative in the international arena has been the "Nuclear Security Summits" assembled following Barack Obama's 2009-dated speech in Prague[47]. The first of these summits, organized in Washington in 2010, was fundamentally interested in nuclear guns and their dissemination. The second, which was dramatically influenced by the Stuxnet attack, was held in Seoul in 2012 and referred to cyber security within the framework of nuclear facilities. In this regard, the Seoul declaration addressed the IAEA's documents and perspective in calling forth developing efforts towards international cooperation and developing and further strengthening measures at the national and facility level[48].

As it is understood, given that international efforts are only at the initial phase, the state's evaluation, management and prevention of cyber risks against NPPs, under the framework of their business administration, as well as the risk and threat analysis they will conduct, dependent upon the structure of the facility, are highly effective. Hence the IAEA recommends that "the responsible state authority should periodically issue a threat evaluation including threats to the security of computer systems and information on current attack vectors related to the security of computer systems used at nuclear facilities. …It is vital that facilities maintain an active and ongoing threat assessment, which is regularly briefed to management and operations."[49] Simultaneously, division of tasks and cooperation must be maintained between facility operators and legitimate institutions regarding their areas of responsibility. Further to that, all of these efforts must be constituted in such a way that prioritizes the

establishment of a comprehensive security culture.

In this regard, risk management involves all stages of the system's life cycle, including its design, development, operation and maintenance. "Risk in the computer security context is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."[50] Risk evaluation in this framework, contributes to the identification of activities and the effective dissemination of sources, necessary for the detection of vulnerabilities and their liabilities for exploitation. Assessing risk and vulnerabilities as a whole in the context of risk, paves the foundation for preventing against attacks against computer systems or taking necessary measures to relieve its results.[51]

In February 2013, the U.S. government began establishing a general framework for the maintenance of critical infrastructure cyber security and risk management.[52] In accordance with the Executive Order of the President of the United States, the document titled "Improving Critical Infrastructure Cybersecurity" was a first of its kind, calling for "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[53] Although this framework determines a series of standards and guidelines, it does not argue for a "one-size-fits-all" approach in managing risks. Instead recognizing that each organization bears unique risks, different threats, vulnerabilities, and risk tolerances. For this reason, all relevant parties are summoned to coordinate, integrate and share information[54].

Similar to the US, the IAEA also attaches importance to risk management and highlights:

> "After having established adequate support and resources, the initial steps in developing a computer security programme should focus on understanding potential threats based on credible attacker profiles and attack scenarios. A possible first step would be to create an attacker profile matrix listing credible attackers, motivations, and potential objectives. The attacker profile matrix could then be used to build plausible attack scenarios; the following subsections examine this process in greater detail….An important tool commonly used to determine threat levels and as a basis for developing a security posture is the design basis threat (DBT). The DBT is a statement about the attributes and characteristics of potential adversaries (internal and/or external). A DBT is derived from credible intelligence information, but is not intended to be a statement about actual prevailing threats."[55]

As the Stuxnet example clearly displayed, given the ambiguity of intents and possibility of easy access to most capabilities, overcoming cyber risks effectively is not an easy task. To do so, nuclear facility operators "would require the kind of funding and actionable intelligence that comes from state sponsorship".[56] Therefore the best approach for structuring cyber safety/security seems to be DBT, as advised by both IAEA and NRC. Originally structured to provide security to nuclear infrastructure against physical and kinetic attacks, the DBT also provides a suitable template for the effective protection of nuclear facilities against cyber risks, as it focuses on the characteristics, priorities, modus operandi and potentials of internal and/or external adversaries. In doing so, it provides the basis for the design of the security structure. By determining criteria and templates for measuring performance and system effectiveness, it establishes a connection between precautions and needs. It prevents excess spending and clarifies the delineation of responsibility amongst different agencies. Such an approach should be continuously updated, keeping in mind the transforming demands and structures of IT systems and the capabilities at hand. This is so even though; the "systems and network architectures supporting nuclear plant operations are not standard computer systems in terms of architecture, configuration, or performance requirements."[57]

6. Inferences for Turkey

The nuclear power plants Turkey is planning to build will be important both for the vital role they will play in the country's energy policy and meeting its electricity demand, and due to the risks and necessities associated with having nuclear technology. In this context, Turkey faces a set of specific threats associated with transitioning into nuclear energy. In order to transform its budding cyber and nuclear security understanding into a "culture", Turkey has to work in unison with its international partners Russia, France and Japan, all of which have different behavior patterns, understandings, priorities and approaches to nuclear and cyber security. It is clear that unless the existing differences are not ironed out, the sides will face many convoluted problems. Hence, Turkey has to play an active role in coordinating and harmonizing the approaches of the sides in line with a roadmap that it drafts in advance.

On the other hand, Turkey's case is further complicated by the model it has chosen to realize its nuclear goals. Two of the country's nuclear facilities will be constructed through the direct importation of nuclear technology (the details on the third facility have not been finalized yet). The first of these, Akkuyu Nuclear Power Plant, will be built according to the build – own – operate (BOO) financial model. This model has drawn criticism from the domestic audience, many of which has focused on the physical security and safety of the facility.[58] This is because the Russian operator which will build the facility, will also own it for the duration of its lifetime, which will considerably limit Turkey's say on how the facility is managed.

As Turkey is an IAEA member with the prospect of generating nuclear energy, it has to embrace and implement the agency's general approach. As its first nuclear facility will be constructed on the build-own-operate model, the country's compliance with IAEA arrangements should not be limited to facility operation manuals and legal regulations. Beyond that, Turkey should work to ensure that all of the country's nuclear stakeholders act in accordance with IAEA standards and regulations.

7. Conclusion

The 9/11 attacks on the World Trade Center have brought along concerns about the potential effects of attacks that target critical national infrastructure. The information that al-Qaeda members used cyber communication tools and digitally planned the attack, has exacerbated the worries that cyber space will be the new front of competition between states and asymmetric forces.

Time and space in cyber space are not symmetric concepts as in the physical world. This fact gives actors the ability to create strategic asymmetries beyond the physical world. In a conflict that plays out in a symmetric world, adversaries see each other and view each other's moves in a specific time and space. Yet in a cyber attack, the victim cannot easily know the attacker's identity, location and true purpose with certainty. Hackers may not works in shifts, and certainly do not care about that of their victims. In short, the asymmetric and flexible nature of cyber threats, turn the mostly symmetrically designed nature of governments, their agencies, relations, hierarchical structures and cultures, into disadvantages in the context of nuclear energy facilities and elements of critical infrastructure.

In our digital world, trying to control every connection and network seems like a futile undertaking. Even in countries that have the most advanced regulations on the field, nuclear power plant owners and operators operate in an environment characterized by limited legal regulations, especially on reporting and sharing information with the public. This fact complicates the development of industrial standards through the collection, sharing and analysis of data on incidents and developments, known as best practices.[59] The cyber-attack on Iran's facilities at Natanz, allegedly by Israel and the US,[60] presents a strong example of how states may use cyber-attacks against critical infrastructure to harm their adversaries. This reality has made the existing risks more visible and complicated the sector's protection of nuclear facilities.

Cyber security is a newfangled area of risks and threats for all involved, both in government and private industries. Tellingly, in the United States, the country which is arguably the most absorbed in cyber security efforts spending roughly 15 billion dollars only in 2012,[61] has only launched its Federal Risk and Authorization Management Program (FedRAMP), a certificate program to enable government contractors to be cleared for providing "services for the entire civilian US government", in 2013.[62] Clearly in such a field where the experience, knowledge, models and standards are globally limited, and questions still outnumber the viable answers, Turkey, that is rather a peripheral country in information technology and is on the way to improve and develop its CI and ICT security regulations, framework and institutions, will have considerable challenges. On the other hand, Turkey's nuclear infrastructure and respective approach to security are in the process of moving from the "sketch board" phase to the implementation phase. If Turkey manages to form its own model and regulations by closely following international best practices and expertise, it may turn the process of shaping its nuclear security culture into an advantage. In this context, it is vital for the Turkish bureaucracy to adopt a pro-information sharing, transparent and accountable approach and push nuclear facility operators in this direction.

1- Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Volume 10, Issue 1, Spring 2011, p. 18.

2- The definition is based on two documents by the government of the United Kingdom. UK Cabinet Office, Cyber Security Strategy of the United Kingdom, Safety, security and resilience in cyber space, Norwich, The Stationery Office, 2009, p. 7. and UK Cabinet Office The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, London, UK Cabinet Office, 2011, as referenced in Melissa E. Hathaway, Alexander Klimburg, "Preliminary Considerations: On National Cyber Security" in National Cybersecurity: Framework Manual, Alexander Klimburg (Ed.), Tallinn, NATO CCD COE Publications, 2012, fn. 35, p. 8.

3- Ibid

4- Joint Terminology for Cyberspace Operations, p.5.

5- Tallinn Manual on the International Law Applicable to Cyber Warfare, Michael N. Schmitt (Ed.), Cambrige University Press, Cambridge, 2013, p. 106.

6- P.W. Singer ve Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, p.36

7- Ibid. p. 34 - 35.

8- Ed Gabrys, "The International Dimensions of Cyber-Crime, Part 1", Information Systems Security, Vol. 11, No.4, p.23.

9- Ibid.

10- Thalif Deen, "World's Nuclear Facilities Vulnerable to Cyber-Attacks", August 17, 2015 (online) http://www.ipsnews.net/2015/08/worlds-nuclear-facilities-vulnerable-to-cyber-attacks/ (September 1, 2015)

11- IAEA, Computer Security at Nuclear Facilities, p.38.

12- 2014 US State of Cyber Security Watch Survey, Software Engineering Institute, CERT, Carnegie Mellon University, 2014, p. 8 online at resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf accessed (Nov. 19, 2015)

13- Ibid. p. 6

14- Ibid. pp. 5-6.

15- Matthew Bunn ve Scott D. Sagan, A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes, Cambridge, MA, American Academy of Arts and Sciences, 2014.

16- Ibid., pp. 40 – 42.

17- Ibid.

18- Christine Hess Orthmann ve Karem Matison Hess, Criminal Investigation, Clifton Park, Delmar, 2013, s.535.

19- http://www.dhs.gov/what-critical-infrastructure.

20- AFAD, 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi", September 2014, p.4.

21- Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", Military and Strategic Affairs, Vol. 3, No.2, November 2011, p.62-63.

22- Cyber Security Programs for Nuclear Facilities, RG 5.71, US Nuclear Regulatory Commission, Washington DC., January 2010, p. 35.

23- Ibid.

24- Martin Matishak, "Nation's Nuclear Power Plants Prepare for Cyber Attacks", August 27, 2010 (online) http://www.nti.org/gsn/article/nations-nuclear-power-plants-prepare-for-cyber-attacks/ (September 9, 2015).

25- ICS-CERT Monitor, September 2014 – February 2015, Department of Homeland Security, Washington DC., p. 1 An APT is defined as "A cyberattack campaign with specific, targeted objectives, conducted by a coordinated team of specialized experts, combaining organization, intelligence, complexity, and patience." See P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What

everyone needs to know, Oxford, OUP, 2014, p.294.

26- James Andrew Lewis, The Electrical Grid as a Target for Cyber Attack, Center for Strategic and International Studies, Washington DC., March 2010, p. 1.

27- Backgrounder on Cyber Security, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html and Telecommunications Board Division on Engineering and Physical Sciences Policy and Global Affairs Division Washington D.C., The National Academies Press, 2010, within s. 207

28- "Cyber security is strictly regulated by NRC and thus no additional regulation is needed," Policy Brief, March 2014, http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy-Briefs/Cyber-Security-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf

29- "Cyber Security for Nuclear Power Plants", Policy Brief, April 2015, http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit.

30- Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Volume 10, Issue 1, Spring 2011, p. 17.

31- André Lochthofen and Dagmar Sommer, "Implementation of Computer Security at Nuclear Facilities in Germany" Nuclear Energy, Vol.XXX, p.1-5.

32- IAEA, Computer Security at Nuclear Facilities, p.13.

33- IAEA, GC55/Res/10 Nuclear Security, Adopted by the General Conference on 23 September 2011, Paragraph 17, p. 3

34- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Vienna, 2011.

35- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Vienna, 2011, p. 1

36- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Vienna, 2011, p.13.

37- IAEA, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No.7, Vienna, 2008, p. 19.

38- Ibid., p.2

39- Ibid., p. 4.

40- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Vienna, 2011. p.13-14.

41- The IAEA has conducted this meeting in cooperation with various international organizations such as the International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), The United Nations Interregional Crime and Justice Research Institute (UNICRI) and International Electrotechnical Commission (IEC)

42- Jeffrey Donovan, "IAEA's Amano Calls for Strengthened Computer Security in a Nuclear World", June 1, 2015, (online) www.iaea.org/newscenter/news/iaea%E2%80%99s-amano-calls-strengthened-computer-security-nuclear-world, (September 10, 2015).

43- Ibid.

44- Also known as the Budapest Convention, entered into force in January 1st, 2004. The text of the Convention might be reached from www.europarl.europa.eu/meetdocs/2014_2019/documents /libe/dv/7_conv_budapest _/ 7_conv_budapest_en.pdf accessed (September 10, 2015) The Convention has been signed by Turkey and is in effect since January 1st 2015.

45- Michael A. Vatis, "The Council of Europe Convention on Cybercrime", Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy Computer Science

46- For the debate around the Convention see "Overall assessment: Nascent governance, growing gaps", e Monitor: The Internet, The Council on Foreign relations, Global Governance www.cfr.org/global- governance/global-governance-monitor/p18985? gclid=CjwKEAiApYGyBRCg_jIstuduV8SJABCEzhZYJFEw 3x1y11- p_nTMWeBQJJgrY5PSZXF6LTS0sxo5BoCRcTw_wcB#!/internet?cid=ppc-Google-grantGGM _Internet_Gen-102115 Accessed on: 23 October 2015

47- The last of these meetings will be held in Washington on March 2016 "Statement by the Press Secretary on the 2016 Nuclear Security Summit", 10 August 2015,www.whitehouse.gov/the-press-

office/2015/08/10/statement-press-secretary-2016-nuclear-security-summit, Access Date: 25 October 2015

48- "Seoul Communiqué", 2012 Seoul Nuclear Security Summit, 26 – 27 March 2012, Paragraph 12, p. 6. www.un.org/disarmament/content/spotlight/docs/Seoul_Communique.pdf, Accessed on 25 October, 2015.

49- IAEA, Computer Security at Nuclear Facilities, p.13-14.

50- Ibid, p.36.

51- Ibid., p.36.

52- Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 National Institute of Standards and Technology, February 12, 2014 online at www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf accessed (October 23, 2015)

53- "Executive Order of the President of the United States 13636 - Improving Critical Infrastructure Cybersecurity", Feb. 12, 2013, online at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity accessed (October 23, 2015)

54- Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 National Institute of Standards and Technology, February 12, 2014 online at www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf accessed (October 23, 2015) p.2

55- IAEA, Computer Security at Nuclear Facilities,p.38-9.

56- Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Volume 10, Issue 1, Spring 2011, p. 22-23

57- IAEA, "Design Basis Threat (DBT)", www-ns.iaea.org/security/dbt.asp?s=4 Accessed on: November 30, 2015.

58- Sinan Ülgen (ed.), Türkiye'de Nükleer Enerji ve Emniyeti, EDAM, Istanbul, 2015, http://edam.org.tr/document/NuclearBook3/edam_nukleeremniyet2015_tam.pdf.

59- For detailed information, please see Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Volume 10, Issue 1, Spring 2011

60- Ellen Nakashima ve Jaby Warrick, "Stuxnet was the work of Us and Israeli Experts, Officials Say", Washington Post, Haziran 2, 2012.

61- P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, p.200

62- P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, p.198