INTRODUCTION TO CYBER SECURITY FOR NUCLEAR FACILITIES

Assoc. Prof. Salih Bıçakcı

Faculty Member, International Relations - Kadir Has University

1. Introduction: Actors and Roles in Cyber Security

Cyber security is an indispensible part of the security regime of nuclear power plants. Since the rise of cyber security culture is a relatively new issue, several nuclear power plants were designed without concern for cyber attacks.

With the civilianization of the Advanced Research Projects Agency Network (ARPANET), the U.S. Defense Department's research brainchild, the Internet entered the mainstream. The limited Internet connectivity with the dial-up modem in the 1990's quickly reached the level of hyperconnectivity in the first decade of the 21st century. Personal computers, mobile phones, tablets, and digital sensors have expanded network coverage and transformed the way the world works. These new tools also increased the scale of data production and storage.

The digitalization of data and the extensive use of information management systems carried the world to a new era. On the practicality and feasible use of systems is getting an advantage to the governors to control the societies and have a better grasp on the indicators of management. This advantage comes with a cost. The digitalization of infrastructure makes these systems vulnerable to cyber threats and hybrid attacks.

This study aims to shed light on the cyber security of nuclear power plants and help decision-makers in this regard. In Turkey, the planned nuclear power plants will be included in the critical infrastructure list under the category of energy infrastructure; however, the various nuclear facilities present different risks and vulnerabilities and must follow unique methods of resilience. Not only do Turkey's prospective nuclear energy plants have the vulnerabilities of electricity grids but they also create risks for the other energy grids in the country.

The planned nuclear power plants would be the first examples of the build operate and own (BOO) classification. This solution also bring inter-operability problems among stakeholders and security culture integration issues to the energy sector of Turkey. Russia and Turkey signed an agreement for ROSATOM to build, own, and operate the Akkuyu Nuclear Power plant in Mersin, Turkey. The second plant will be built in Sinop by a Franco-Japanese consortium and China is in line for the third nuclear power plant in İğneada Kırklareli.

The first power plant will in effect become a testing ground for future integration problems at all levels and in all dimensions. The necessary legislation and regulatory preparation must sustain the compatibility of information systems and communication among stakeholders while also focusing on fostering an effective nuclear security culture. The protection of nuclear power plants really depends on the nuclear security culture, which encompasses nuclear safety, cyber security, physical security, transportation, and storage security.

To manage the nuclear security culture, actors have different responsibilities at various levels of organization:

International community:

- To coordinate states, prepare necessary regulations, and form an international warning system

State:

- To define general protection objectives to distribute responsibilities
- To protect information regarding nuclear safety and security
- To inspect the necessary institutions and audit their compliance to regulations

Organizations:

- To implement all relevant security policies for the protection of Nuclear Power Plant such as:
  - Specifying threat levels
  - Designing physical protection systems
  - Identifying the security significance of individual systems
  - Protection of sensitive information
  - Reporting
  - Record keeping and logging
  - Measures for the detection of, and response to, malicious acts
- To manage the structures in the facilities by defining roles, responsibilities and accountability for each level of the organization, including security and other interfaces
- To control and allocate sufficient financial, technical, educational and human resources to implement the assigned security responsibilities
- To review ongoing procedures and make necessary improvements

Managers in Nuclear Power Plant organizations:

- To define responsibilities
- To define and control best practices
- To vet and train personnel
- To motivate personnel for security applications and give incentives to report any abnormalities of operation
- To audit and review necessary procedures

Personnel:

- To cultivate strict and prudent approaches to information security
- To maintain vigilance
- To shorten response time to any unexpected activity or to any emergency cases

Even though, there is a distribution of roles, there are "true uncertainties, enforced by rapid technological innovations and accelerated societal responses, [which] are creating a fundamentally new global risk landscape. In all these new uncertain risk technologies, we are separated from the possible end results by an ocean of not knowing."[1] Stuxnet was a major development in attacks against computer sytems of critical infrastructure. It reversed the belief that SCADA systems were not vulnerable to attacks since they were protected with an air gap.[2] After the Stuxnet attack, the cyber security of nuclear power plants became crucial to sustaining nuclear safety. To separate information and communications technology (ICT) from the Internet was no longer a solution.[3] In addition to the technological modifications to the infrastructure of nuclear power plants, the human relationship with technology also changed. Now nuclear power plant staff was also hyperconnected with its smartphones and tablets.[4] The urge of being present in social media increases day by day. In its nature, these smart devices are a fundamental source of socialization for many individuals. People tries different techniques to connect the internet and to be online. However, these devices are also source of major threats for cyber security of the strictly controlled areas, especially in a critical infrastructure facility. For this reason, it is possible to foresee that it would be really hard for the nuclear power plant workforce to lock their electronic devices in their boxes.

The cyber and hybdrid risks are geometrically increasing due to the changing political and economical environment in the world. The primary cyber risk calculation formula rests on vulnerability, assets, and cyber threats.

2. Vulnerabilities

2.1. Design

The design of a nuclear facility has to be made along with its risk evaluation. In other words, threat perceptions closely effect the design features of facilities. The study of this relationship is named Design basis threat (DBT) is the fundamental principle for the protection of the facility.[5] DBT is based on a state's current evaluation of a threat. Recent discussions on the protection of nuclear power plants has shown that cyber DBT is a necessary component of securing a power plant. In addition to the cyber DBT, operators will also need to design the nuclear power plant in a way that secures it on a limited budget. Furthermore, operators must decide between the robustness and functionality of the nuclear power plant. Any mistakes during in the design of a nuclear power plant will trigger cyber and physical vulnerabilities.

2.2. Hardware

The choices made in the design of a nuclear power plant determine the hardware used in its facilities. Over time, additional needs and changing security contexts present new problems that are incompatible with the old ICT infrastructure, which could result in unanticipated vulnerabilities. Stuxnet (as well as dragonfly, HAVEX, and black energy) has proven that even small electronic hardware components and their codes and drivers in the background are important for securing nuclear facilities.[6]

Setting up a well-designed system is only the first step in ensuring nuclear safety and security. To keep the nuclear power plant working without major setbacks, hardware vendors also play a major role in maintaining the security and safety of a nuclear power plant. In 2013, a Russian news source claimed that a technician discovered a "spy chip" in a batch of an imported Chinese iron. These tiny electronic circuits added to the main electronic configuration, were mostly being used to spread viruses by connecting to any computer within a 200 meters radius which was using an unprotected wireless network[7]. This example demonstrates that nuclear safety and security is just as dependent on trustworthy vendors as it is on DBT. All operational nuclear power plants need to attain their spare parts from a trustworthy vendor. For each individual spare part, there would have to be a verification process that could test whether the hardware was fit to be used in its nuclear power plants.

Because nuclear power plants operate for many years, plant operators must create a life cycle management strategy to keep the systems up and running and prevent vulnerabilities resulting from the aging of the facility and its hardware.

Since many hackers and Advanced Persistent Threats (APT) attackers get their information from waste bins, in addition to nuclear waste management systems of power plants, appropriate security measures must be put in place for conventional wastes of nuclear facilities. There have been instances in which hackers obtained discarded hardware from recycling systems and auction sites in order to improve their hardware-specific know-how and plan their attack. To prevent this, each nuclear power plant should have a well-organized waste management system to dispose of non-radioactive material. Nuclear power plant operators have to establish life cycle management programs that help control spare hardware against malware and exploitation. The lack of such capabilities can cause the nuclear power plants to stop functioning.

2.3. Software

Nuclear facility computer security experts are responsible for checking the security of the software before installation. Zero-day exploits[8] and special communication protocols[9] top the vulnerabilities list. The sophisticated and experienced attackers prefer to use less known vulnerabilities when attacking a highly secured nuclear facility, with the pursuit that they will be confronted with less resistance. In addition to these threats, IT centers in nuclear facilities request new codes to integrate into their systems from time to time. Since these quickly written codes are designed for functionality without considering security and safety needs, they might expose the nuclear facility to risks. Therefore, they must be regularly tested by a group of experts before being implemented into the main system.

Another software security concern is the use of default security settings. The IT sector often relies on default settings for the software, but most of these settings are optimal for average systems, not facility-specific advanced nuclear systems. Because each nuclear facility is unique, engineers and IT staff need to set up all software (firewall, Intrusion Detection Systems (IDS), networking, and safety-related programs) according to the needs and special policies of the facility.

Outsourcing the cyber security of nuclear power plants to third-party companies carries potential risks. The first topic to raise concern is integration. Although IT companies promote their software as being compatible and robust, unexpected integration problems can arise during the installation of the software in the facility. The second problem stems from outsourced companies not sharing technical know-how with facility operators during the installation process. Most third-party companies do not share any information about their codes or programs during the testing period to protect their relatively competitive advantage in the market. Because there is no oversight mechanism in place during this process, these secret codes could produce unexpected vulnerabilities to the security of nuclear facilities. It is strongly advised that all regulators subject operators to a strictly controlled, rigorous testing process of cyber products to ensure that the facilities are not vulnerable to attack.

One other potential risk fact comes from giving third-party companies' staff, access to server rooms for maintenance purposes. Hence, both physical and cyber security departments should coordinate efforts to escort third-party personnel around the facility and throughout the installation process. This way, the integrity of the data and software in facilities can be protected more effectively. Regulators and IT management departments should also request that operators give regulators control of solid patch management systems for updating the systems.

Most of the nuclear power plants have antivirus programs that are programmed to catch the static coded malwares. Since these static codes form a pattern, the antivirus programs can easily recognize and identify these malwares. However, an increasing threat to the IT sector is; the ability of self-modifying malwares to alter their behavior or use code obfuscation techniques to beat dynamic analyzer antivirus programs. These malwares evolve and adapt to different layers of software while infecting the computers. Due to the sudden and continuous changes in their coding structure, antivirus programs have the difficulty to catch these polymorphic malwares. Today, the highest level of such malware coding is evolutionary programming[10]. Evolutionary programming is a method for simulating evolution to find out the most versatile and robust codes that serves the programmer's goal. Evolutionary programming refers to the evolutionary simulation method that targets finding the most appropriate variables and durable codes that serves the needs of the programmer[11].

2.4. Human Capital

Equipment, hardware, and software are only as smart as the human that operates them. In nuclear power plants, insider threat is listed as a critical vulnerability, especially for nuclear theft. Nevertheless, humans in the general security context are perceived as one of the most complex issues because the moral judgment of an otherwise reliable individual may be affected.[12] Similarly, insider threat is a major cyber security concern because insiders can be complicit in cyber attacks or outsiders can exploit insiders in order to breach the ICT systems.[13] Although only a few documents, like that compiled by the IAEA, address ICT system breaches,[14] there is a large body of cyber security literature on the role of insider threats in the system.

Unintentional misuse can also greatly impact the operations of a nuclear power plant. Although management of these plants mostly focus on the staff, contractors and other outside workers also pose a risk. Stuxnet provided "a useful blueprint for future attackers by highlighting the royal road to infiltration of hard targets"[15]. Rather than trying to directly infiltrate the system by crawling through fifteen firewalls, three data diodes, and an intrusion detection system, the attackers used less direct means by infecting soft targets with authorized access to the center of the nuclear power plant[16]. Therefore, regulators should systematically conduct background checks not only for operators and their staff but also for contractors.

The cyber security of power plants focus on the four following points:[17]

- Unauthorized access to information (loss of confidentiality):
  - Malicious or unaware employees;
  - Attackers who exploit the carelessness of employees into revealing information through phishing;
- Interception and change of information, software, hardware etc. (loss of integrity):
  - Viruses, worms, and Trojan horses, code that may damage, reveal, or capture information;
  - Attackers who steal remote systems which, in turn, provide access to information;
- Blockage of data transmission lines and/or shutdown of systems (loss of availability):
  - Fire, floods, and earthquakes resulting in electrical outages, equipment and hardware failures;
- Unauthorized intrusion into data communication systems or computers (loss of reliability):
  - Attackers who steal computers or enter server rooms, file cabinets, or offices;
  - Attackers who try to compromise systems exposed on a public network or try to spoof or imitate remote systems.

Currently, being on offense is more advantageous than being on defense, but the rules of the cyber arena have yet to be clearly defined. Defensive and offensive cyber capabilities are constantly developing. Regulators and operators should remember that cyber security begins even before the power button is turned on. Regulating nuclear safety and security on paper is the easy task. The difficult road ahead lies in the creation and interoperability of effective communication channels among actors on the ground.

3. Cyber Incidents

The use of SCADA and industrial control systems in nuclear power plants brings cyber security problems and computer incidents to the attention of researchers. Not only nuclear power plants but also all relavant information in this category are highly critical. Attacks against platforms that hold rich information on nuclear power plants can be witnessed.[18] The seven cyber incidents outlined below offer insight into the scale and severity of cyber malfunctions and attacks.

3.1. The Slammer Worm and David Besse Nuclear Power Plant (NPP)

The Slammer worm cannot be regarded as a typical malware in that it is not written with the explicit purpose of infecting end-user machines. Instead, the Slammer worm aimed to infect Microsoft SQL servers and computers running with the Microsoft Data Engine (MSDE) 2000. Since the worm was not infecting any file for it was not placed into the hard disk of computers, technical staff removed the worm by simply rebooting the system. The worm's main role was to increase the network load and make SQL servers invisible to users by exploiting a buffer overflow.[19] The number of infected machines reached its peak on January 24, 2003, in the United States, including those at the Davis-Besse NPP in Ohio.

After the disinfection process, researchers found out that the worm had reached the NPP from a contractor's network, called First Energy Nuclear. It was understood that the worm squirmed its way through the licensee's T1 line connected to David-Besse's corporate network. Although the firewall at David-Bessa NPP was programmed to block the port that the Slammer worm used, the presence of various bypasses from the David-Besse's business network created such a condition. Eventhough Microsoft Corporation had published information about the network patches approximately six months before the Slammer worm hit the NPP, the plant's computer engineers had not installed the network patches. SecurityFocus, a website that conducts security-oriented studies, revealed the minutes of the timeline of events as the following:

> "By 4:00 p.m., power plant workers noticed a slowdown on the plant network. At 4:50 p.m., the congestion created by the worm's scanning crashed the plant's computerized display panel, called the Safety Parameter Display System (SPDS).
>
> An SPDS monitors the most crucial safety indicators at a plant, like coolant systems, core temperature sensors, and external radiation sensors. Many of those continue to require careful monitoring even while a plant is offline, says one expert. An SPDS outage lasting eight hours or more requires that the NRC be notified.
>
> At 5:13 p.m., another, less critical, monitoring system called the Plant Process Computer (PPC) crashed. Both systems had redundant analog backups that were unaffected by the worm, but, "the unavailability of the SPDS and the PPC was burdensome on the operators" notes the March advisory.
>
> It took four hours and fifty minutes to restore the SPDS, six hours and nine minutes to get the PPC working again."[20]

The Davis-Besse incident clearly underlined the fact that nuclear power plants were vulnerable to malware attacks and that remote-monitoring connections to SCADA systems were eminently increasing the risk of cyber attacks.

3.2. Browns Ferry NPP

Built in 1974 near Athens, Alabama, the Browns Ferry NPP is one of the world's largest nuclear power plants. The incident in August 2006 proved that critical reactor components were also vulnerable to disruptions by cyber attacks.[21] After two water recirculation pumps failed, due to high traffic in the network, operators of the Tennessee Valley Authority (TVA) had to manually shut down one of the plant's two reactors. These recirculation pumps were critical to controlling the flow of water to the reactor, managing the power output of the boiling-water reactors. As a Nuclear Regulatory Commission (NRC) report elaborated, "The licensee determined that the root cause of the event was the malfunction of the [recirculation pump] VFD (variable frequency drive) controller because of excessive traffic on the plant ICS network."[22] Although the ramifications of shutting down recirculation pumps are known, there is no sound explanation for the excessive network traffic that contributed to the malfunction.

Eric Byres, CEO of Byres Security Inc., suspected that the problem was due to faulty networking code that the controllers used for the plant's recirculation pumps. He claimed, "it has a known bug that can cause a crash by generating too much networking traffic"[23]. However, a report by the NRC mentioned that: "unless and until the cause of the excessive network load can be explained, there is no way for either the licensee (power company) or the NRC to know that this was not an external distributed denial-of-service attack[24]". To justify these claims, an independent inspection of the logs and associated data is necessary.

3.3. Hatch NPP

The Hatch NPP incident highlighted the drawbacks of network connectivity in nuclear facilities. The Hatch NPP near Baxley, Georgia, witnessed a forced emergency shutdown for 48 hours due to a software update. Unit 2 of the NPP was functioning properly just before the computer engineer of the licensee firm's, Southern Company, updated the software on the plant's management network. When the engineer rebooted the computer after the software update, the computer started collecting diagnostic data from the process control network. As a result, the control system understood the reset of the synchronization program as a sudden drop in water reactor reservoirs, initiating an automatic shutdown.

Southern Company spokeswoman Carrie Phillips explained that the emergency systems that came into play were designed to protect the safety of the nuclear power plant. She added that the engineer, who installed the update, was not aware that the software was designed so that any reboot following a system reset would force all other networks to reset.[25] "The Hatch event illustrates the unintended consequences that could occur when business information technology systems interconnect with industrial control systems without adequate design considerations". The Hatch incident proved that the protection of SCADA systems requires a response strategy with detailed division of labor.

3.4. Malware Attacks to US Nuclear Power Plants

Since the vulnerability of nuclear power plants is listed as critical information, many incidents are not published in mass media. NRC reports cited various incidents regarding the functionality, storage, security and transportationof computers between 2008 and 2010.[26] The revelation of Stuxnet, changed the perception towards threats regarding SCADA/ICS systems

used in nuclear power plants. The use of infected Universal Serial Bus (USB) during the Stuxnet attack created sensitivity to these types of tools.

Similar experiences in the United States showed that USB drives could threaten critical infrastructure. In October 2012, when a technician inserted a compromised USB into a power plant's network during a scheduled outage for equipment upgrades, he inadvertently kept the plant offline for three weeks.[27] The third-party technician did not know that the USB was infected. The Department of Homeland Decurity did not mention the name or location of the power plant but identified the malware in the third-party contractor's USB as a variant of the Mariposa virus.[28] On cyber security lists, Mariposa is classified as a botnet, not a virus, which steals personal data, account information, usernames, passwords, and banking details from compromised computers. These infected computers can also be used for distributed denial of service (DDoS) attacks.

Another similar incident occurred when an employee had trouble with his USB drive and brought it to IT to have it checked. Once the IT staff inserted the USB into a computer with updated antivirus software, the program found that one malware, out of three, was a sophisticated virus.[29] Upon seeing the results, the IT staff checked several computers to find out that some were infected with the sophisticated malware.

All these examples have presented that the usage of USB drives are critical for cyber security of nuclear power plants. In a presentation at a BlackHat Conference, two researchers demonstrated that a USB drive attack that could threaten nuclear power plants could be executed not only by a specific malwared USB drive but also all other peripherals (including printers and scanners), which are communicating via USB ports.[30]

3.5. International Sabotage and Break-in Attempts at Nuclear Power Plants

Amongst the list of threats that target critical infrastructure, cyber reconnaissance activities' come first, as top-notch hackers try alternative ways to control the systems integral to everyday life. Two distinctive hacking examples in the United States demonstrate how national states are testing other states' critical infrastructure and key resources protection capacity.

A group of hackers attacked several North American natural gas producers, testing for possible ways to breach the system. In one attack, the hackers stole the subscriber contact list of a nuclear management newsletter and sent spyware-loaded e-mails to the e-mail addresses on the contact list before the newsletter was sent.[31] This attempt ended with the successful breaking into the computer network of Diablo Canyon nuclear plant at the north of Santa Barbara.

Another example to this types of attack took place in August 2012, when a Chinese hacking team attempted to infiltrate a U.S. nuclear facility. The Department of Homeland Security (DHS) did not disclose the name of the nuclear power plant or other plants that experienced similar attacks, to protect the facilities from potential future attacks. Meanwhile, Chinese military hackers took control of a senior plant manager's computer. The plant's incident team investigators concluded that Chinese hackers wanted to identify security and operational vulnerabilities of U.S. nuclear reactors.[32]

3.6. Monju Nuclear Power Plant

A computer, normally used to file company paperwork by on-duty facility employees in the Monju nuclear reactor facility in Tsuruga, Fukui Prefecture, began to suspiciously send and receive data from an unknown website at 3:00 PM on January 2, 2014. Upon closer inspection it was revealed that, the computer was infected during a regular update of a video playback program. Although the infected computer contained sensitive e-mails, employee data sheets, and training logs that could be used for another attack, the Japan Atomic Energy Agency claimed that no data that could compromise the safety of the plant was leaked. The incident at Monju NPP proved the importance of having an incident investigation team for the protection of facilities against cyber atacks.[33] Since having an incident investigation team was deemed not feasible and costly by NPP operates, such tasks are generally allocated to facility engineers. However, incident investigation requires unique techniques to detect, track and trace cyber attacks.

3.7. Stuxnet: A Milestone for ICS and SCADA Systems

At beginning of June 2010, a security engineer from Iran called the anti-virus software development company, VirusBlokAda, located in Belarus. The screens of computers running the Windows operating system kept freezing with blue screen and were automatically rebooting. Sergey Ulasen, responsible for system rescue techologies at VirusBlokAda, and his security engineer counterpart in Iran, recognized the problem after the initial inspection, however were unable to provide its diagnosis. Ulasen was granted remote access to conduct an in-depth inspection of the problem. After the initial analysis, Ulasen noticed that the malware was introducing itself as a driver to the operating system, which was signed with genuine digital certificates of Realtek Semiconductor, a trusted hardware maker in Taiwan, and was using zero-day vulnerabilities[34]. It then became clear that even well-patched Windows computers could be infected by Stuxnet and that digital certificates could be stolen. On June 12, VirusBlokAda contacted Microsoft to report this vulnerability and later shared its findings in a security forum. On July 15, well-known security bloggers disseminated this information, which received attention within the security sector. Recent research conducted by Symantec revealed that the first version of Stuxnet 0.5 have been in operation since November 2005.[35]

The malware “Rootkit Tmphider”, named by VirusBlokAda, was first called “W32 Temphid” by Symantec and was later changed to “W32 Stuxnet”. Stuxnet was not designed to spread through the Internet but by means of an infected USB for a targeted Programmable Logic Controller (PLC) within a local network. When the malware infiltrated the system via a USB drive, it was programmed to connect to the command-and-control servers. Thus, Stuxnet gave attackers more flexibility and allowed for more malicious codes, via the infected computer.

Stuxnet emerged by the way of a USB drive infecting a system. Stuxnet used four zero-day vulnerabilities and stolen digital certificates. One of these zero-day vulnerabilities was a print spooler error in Windows computers, which helped it spread across machines using a shared printer. Microsoft quit using this patch, after a Polish security magazine revealed this vulnerability in April 2009.[36] All these clues show that the attackers knew their target was not connected to the Internet. Symantec’s reverse engineering efforts disclosed, “Stuxnet had three main parts and 15 components, all wrapped together in layers of encryption like

Russian matryoshka. The malware targeted to hijack the Programmable Logic Controller in Siemens control systems by injecting malicious code."[37] The use of industrial control systems has spurred speculations that this was an attack targeting either the Bushehr or Natanz nuclear plants in Iran. Following investigations clarified that Stuxnet infact targeted the Natanz NPP.

Inspections also revealed insights on Stuxnet's operational code. The malware settled in the system for two weeks and reconnoitred, potentially to learn how the system functioned. The attack began quickly and quietly by increasing the frequency of the rotor engines of the centrifuges, with which Iran enriches its uranium levels, from a normal frequency of 1,064Hz to 1,410Hz for 15 minutes. The malware then stayed silent for 27 days before the next set of attacks, which lowered the frequency to 2Hz for 50 minutes.[38] The seemingly random pattern of attacks concealed the malware from antivirus programs. Since the control monitors were blocked, operators in the control room did not notice any abnormal activity caused by the malware.

Stuxnet did not only attack facilities in Iran. According to data from the Kaspersky Security Network, by the end of September 2010, more than 100,000 computer systems in approximately 30,000 organizations around the world were infected by Stuxnet.[39] Subsequent malwares, such as Flame, Duqu and Regin, have threatened numerous sectors from energy to banking. These malwares have shown remarkable similarities to the coding mentality of Stuxnet.

4. Supervisory Control and Data Acquisition (SCADA) and Human Interaction

There are no secrets better kept than the secrets that everybody guesses.
George Bernard Shaw

In the 21st century, national security is tied to the economy, which is highly dependent on energy and critical infrastructures. High electricity production as well as consumption forces states to focus on energy security. Most states use different sources of energy to fullfil their electric needs. The electric grid and its components are almost always controlled by information technology. National security in the modern age relies on hardware, software, and human-machine interaction more than ever before. For this reason, it is possible to paralyze a nation with sophisticated cyber attacks.

With the realization of what devastating cyber attacks can lead to, states have begun to develop national strategies defining their cyber positions and capabilities in the event of an attack. Through defining major threats, these national cyber strategies determine how agencies and institutions should prepare themselves. States must harmonize their efforts to address structural and technological challenges resulting from changes in mentality, data, and the Internet.

4.1. Human-Machine Interaction

Before 1957, computer technology had limited capabilities, executing tasks one at a time in a process known as batch processing. Researchers had no direct access to computers. In addition to insufficient processing capabilities, computers were physically big, requiring huge rooms equipped with coolers. Before the advent of more advanced, modern technology, using computers was a long and time-consuming process.

The direct connection to servers that researchers achieved in 1957 was seen as a major milestone in computing technology, even though remote connection to servers had its limitations. High demand led to the time-sharing concept, which permitted different researchers to directly connect to servers over a limited period of time. This concept first emerged so that multiple users could share the processing power of a single computer. This process also created user accounts and management strategy to access the server. Computer technology in the 1960's was far from user-friendly, usable, and accessible. The necessity to connect scholars pushed researchers to create a network that permitted users to share files.[40] The space race between the U.S. and U.S.S.R. facilitated the improvement of computing technology.

In the 1960's, universities were relucant in sharing their computer resources with other users on ARPANET, pushing them to use a small computer called the Interface Message Processor (IMP) before the mainframe to control the network processes. The mainframe was only responsible for the initialization of programs and data files. The interaction of networks thus led to the Network Control Protocol (NCP), in which the Transfer Control Protocol verified the various computers on the network.

The rising number of participants introduced new technological improvements to the net. The introduction of e-mail, inter relay chat (IRC) systems, and Bulletin Board System (BBS) boosted the number of network users.[41] These platforms also paved the way for computer-mediated communication and initiated the sharing of information among different groups. Hacker groups and technology fans mostly used these earliest forms of computer-mediated communication platforms. After the 1990's, the growing number of Internet users drastically changed human-machine interaction. This development quickly evolved into intensive computer-mediated communication. Hackers and cracker groups[42] in different parts of the world shared their technological expertise. These groups also played an important role in cultivating hacker culture and capabilities. Unauthorized access to computers increased swiftly in places where the network was available. For example, Group 414, formed by a group of teenagers from Milwaukee, launched attacks against Los Alamos National Laboratory, Sloan-Kettering Cancer Center, and Security Pacific Bank. Attacks instigated by the hacker group Legion of Doom forced the government to take steps toward the computer security act.

As computer technology continued to develop, automation became more common, requiring less human intervention in its routine processes. The major process control computing technology is the supervisory control and data acquisition (SCADA) system. In the early years of computing technology, SCADA systems were monolithic structures, which generally held all operations on a mainframe but limited the capabilities of monitoring systems. After the improvement of time management capabilities of central processing unit (CPU) in mainframe, industry started using distributed SCADA systems.

Distributed SCADA systems often share control functions and real-time information with other computers in the local area network. These types of SCADA systems also perform limited control tasks better than monolithic SCADA systems. In most nuclear power plants, the following three components comprise SCADA systems:

- Sensors that measure the condition in specific locations;
- Operation equipment such as pumps and valves;
- Local processors which communicate between sensors and operation equipment[43].

There are four different types of local processors, including Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Unit (IED), and Process Automation Controller (PAC). The following are the main goals of processors: to collect sensor data; turning on and off operating equipment based on internal programmed logic or based on remote commands; translating protocols for the communication of sensors and operation equipment; identifying alarm conditions; and short-range communication between local processors, operation equipment, and sensors. This type of communication mostly flows through short cables or wireless connections.

Host computers act as the central point of monitoring and control. The human operators monitor activity from host computers and take supervisory action when necessary. It is possible to change the rights and privileges of host computers by accessing the Master Terminal Unit (MTU). Long-range communication travels between the local and host computers, using different methods like leased lines, satellite, microwave, cellular packet data, and frame delay. These types of SCADA systems can communicate through Wide Area Networks using ethernet or fiber optic connections.

SCADA systems use several programmable logic controllers (PLC) to monitor the different processes and to make necessary adjustments for the regular flow of operation. These PLCs also alert the operator when human intervention is required. The rising connectivity of SCADA systems permits including human operators to monitor the process with real-time data through a monitor. Yet connectivity makes the system more vulnerable to network

attacks. In these networked SCADA systems, carry the human machine interaction into another level. The networked SCADA systems underlined the importance of human operators and their role to monitor the alarms for the survival of the critical infrastructure.

Human operators form the vital nodes for the function of critical facilities like nuclear power plants. In nuclear power plants, human operators are the first level of protection in preventing an accident or noticing a problem. In the control room, the operator has to check designated indicators of its station and make the necessary adjustments to sustain the continuity of the process. The process of human-machine interaction faces two major problems: human centered and hosting computer interface-centered.

The software that controls and communicates with SCADA systems is designed to provide required information and initiate alarms to alert human operators when a problem arises. Early designs of SCADA systems showed interface designs that were primitive and not focused on the cognitive and psychological awareness of the operators. The biggest problem with interfaces comes from static design which is characterized by a lack of movement and animation. Poor graphics accompanied the interface and only change when triggered by alarms. The alarms themselves had no varying alarm types according to the threat level. In some cases, the size of the alarm messages prevents the operator from seeing other information on the screen. Peripheral equipment, such as monitors and keyboards, were also not designed to permit the operator to easily comprehend the information and respond quickly with as little effort as possible.

In the old interface designs, information was dispersed across three to four monitors. Insufficient screen space was one of the problems reported by the operators. In a modern nuclear power plant, the interface has to be designed with a higher resolution, permitting operators to follow the entire process on one large monitor no smaller than 40 inches. During the acquisition process, hardware experts specializing in screens must determine the monitor.[44] The large screen promotes teamwork in noticing errors and increases the situational awareness of the operators. The host computer's interface is critical to catching anomalies that might be the result of a cyber attack.[45]

4.2. Problems Induced by the Human Factor

Following such a static monitoring process requires a high level of alertness and attentiveness and is not easy for an operator to sustain this mode throughout his or her shift. This is not a personal problem but an issue of human cognitive and physical capabilities. As different SCADA systems use different interfaces, human operators need time to adapt to the new interfaces. In the early months of training, the interfaces confuse operators with the multitude of alarms, messages, and information. After the adaptation period ends, the development of tunnel vision appears as a risk as human operators acclimate to static interface designs and tedious repetitions.[46] In the beginning, being a human operator seems like a dynamic post, but as time goes by, the alarms become routine and daily tasks extend response time. According to one report on this topic, "the maximum manageable alarms per hour per operator are around 12, and around 300 alarms per day and most of the required operator actions during an upset (unstable plant and required intervention of the human) are time critical. Information overflow and alarm flooding often confuse the operator, and important alarms may be missed because they are obscured by hundreds of other alarms."[47]

Operators complain of many distractions in the control room, including human interruption

and phone calls. Peace and quiet in the control room is critical to allowing operators give their full attention to the screens they are monitoring. Consequently, unauthorized personnel in the control rooms would further jeopardize the security of facility.

Since the human machine interface is the only window to monitoring nuclear energy plants, the human operator and his or her host computer are critical in preventing an accident or security breach. However, most human machine interfaces bring their own set of security concerns due to problems in design. Most of the Human Machine Interfaces (HMI) is designed to provide relevant information to human operators in 2D graphic design. The main focus of HMI designs are functionality, usability and visibility. The neatly and interactive desings are crucial to support the attention of the operator. Thus, the human - machine interface is transforming into a front for cyber defence. The HMI also functions as the defender of a system against abnormal activities.

The basic principle of a sustainable security system is to implement a precise and clear security policy, of which major points have to be defined by state regulations and institutional details must be written by organizations. Formulating a security policy would help managers to build measurable and self-perpetuating systems where the division of labor is clear-cut. Computers and electronic devices connected to local networks maintain the physical security of power plants. Their network connectivity, however, makes them especially prone to cyber attacks. Therefore, strong communication and cooperation among the managers of physical and cyber security fields is a must. Both managers have to know the others' field to grasp the details and prepare for possible threats.

Security has to be understood as a continuously evolving cycle that must be assessed regularly according to the changing nature of threats. In nuclear power plants, the conventional security approach draws fixed limits for physical and cyber security sectors. In the age of hybrid entities, the international community must implement smart security policies that provide flexibility, adaptability, and cooperation. For the new facility in Turkey, the physical and cyber security managers of the nuclear power plant (or critical infrastructures) have to follow these major points:

- Understand legal and regulatory requirements in Turkey and internationally;
- Integrate security into the organizational culture and insist on the perception by all stakeholders;
- Develop effective risk assessment programs;
- Develop holistic governance programs for managing information risk;
- Assess the impact of human factors and security strategies and potential breaches of security;
- Develop emergency management policies;
- Develop and ensure quality control in information assurance and security management;
- Improve alternative communication technologies for emergency cases;
- Follow new technologies to upgrade the security level of the facility.

On the first day of operation, the nuclear facility is equipped with the latest technology to work smoothly and securely. However, the emergence of new technology presents the question of how frequently a power plant should update its technology. There are various academic assumptions that focus on the market competition of a facility. Facility managers and government officials must periodically discuss emerging technology and assess the current condition of plants from a security perspective. The maintenance and update of the security system is as critical as writing the security policy of the plant.[48]

The technological protections tailored to specific nuclear power plants create over-reliance on

these tools at the expense of human capacity. However, the capabilities of a plant's personnel are critical to the planning, update, and maintenance of the facility. Safe security systems could be breached due to poor training, inattentiveness, and lack of necessary maintenance of staff. Continuous training and coordination of the disparate security systems in the nuclear power plant are vital to sustaining nuclear safety. Attacks on nuclear facilities can require the coordination of perimeter security officials, cyber security managers, and SCADA engineers. In such an environment, division of labor must be clearly defined and implemented by managers to prevent a chaotic environment in the case of an emergency.

Another critical security aspect is dissemination. It is a known truth that facility employees rarely read security policies and amendments to security regulations. Motivating employees to follow these technical information and policy documents, and to take necessary caution when disseminating information presents a challenge. An administrator has to find ways to motivate the employees to abide by the security culture once it is established.

In the Turkish case, the language barrier presents another issue. Operator companies (Russians in Akkuyu and the French and Japanese in Sinop) have to ensure that technical and policy documents are available in Turkish in order to overcome any misunderstandings and prepare for contingencies.

4.3. Security Levels and Security Clearance

Cyber protection of nuclear power plants requires commensurate attention to perimeter security. Physical security comprises an indispensable part of cyber security since nuclear power plants run its firewalls and intrusion detectors on physical servers. Accessing them would be the first step in an attack. Fiber optic cables and other exposed connections must be protected from malicious attack. In some cases, scissors would be more harmful than Trojan viruses. Therefore, the protection of computer systems, cables, and connections to the electrical grid should be categorized as high-risk assets. Inside the power plant, computers should be categorized according to their security clearance level. Lower-level computers' access to high-security computers should be banned. These security protocols should be checked periodically with the assumption that security rules are not being followed.

All these security measure are tied to the control of any equipments which has electromagnetic capacity used in the screening process at the entrance of a protected area. Since the coverage of electromagnetic devices are so large, the site management will decide how to limit these types of devices. Stuxnet showed that mobile devices, cellular phones, USB devices, NFC devices, RF devices, external hard disks, laptops, CPU-operated devices, and any device with bluetooth and wireless connectivity could be used to transfer malware. Admitting entry to these devices into facility grounds must be limited and under strict control. There are examples of facility employees that to use their relationship with screening officers to bring their magnetic devices into protected or vital areas. All visitiors have to follow screening process of the facility and drop (and lock) their electromagnetic devices to the reserved boxes for their usage. To prevent tailgating, the use of mobile phones in the entrance of checkpoint has to be restricted.[49] The electromagnetic devices have to be collected from visitors and must be kept in a Faraday cage in the protected area of a nuclear power plant to prevent possible intrusion to the network's system. The screening process should be repeated upon exiting the facility to ensure no magnetic devices are taken out of the site.

The computer and network systems of a nuclear facility are another major security concern.

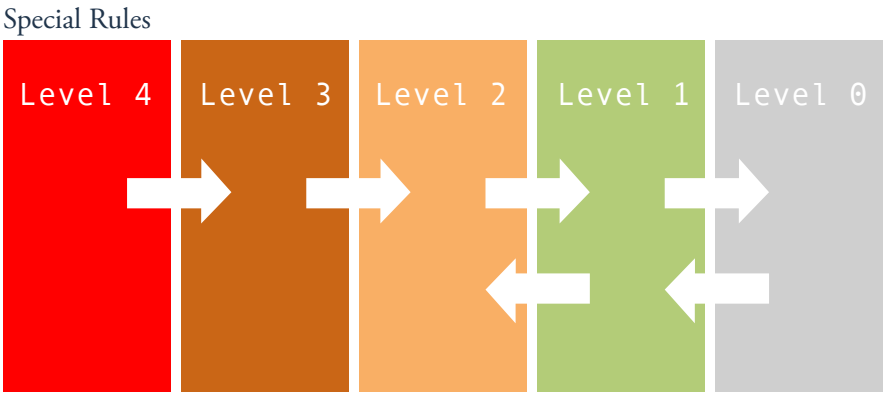
Nuclear power plant systems require hardware replacements and maintenance from time to time. The regulator has to organize how the operator will design the hardware support system. All new hardware should be tested and observed by national authority of test bed. Since the processes take time, the regulator has to encourage the operator to create a hardware management system before the operation of the facility to stock the spare parts. By this way, in any breakdown the facility management quickly replaces the required parts without any delay.

Also, third-party contractors should go through background checks. Since Heating, Ventilation, Air Conditioning (HVAC) management systems are designed for functionality and robustness but not security, these are considered less secure components of nuclear power plants. However, today's HVAC systems are IP-taking appliances which are connected to local networks. To upgrade and patch the systems, the contractors access the HVAC servers from outside the facility. The vulnerabilities of these servers are quickly turning into systemic risks. Any intrusion to these HVAC systems could easily be used for a hybrid attack. The regulators and operators of nuclear power plants must be sensitive to the HVAC systems at all levels of security.[50]

4.4. Security Zones

Cyber and physical security staff should jointly divide nuclear power plants into security zones before construction of the facility begins. The most widely applied technique is implementation of the graded approach from Level 4 (high security) to Level 1 (low security).

In nuclear power plants, every operator has different security level models.[51] There are different approaches to the cyber security defensive architecture, with some starting with Level 1 and counting up. In some cases, the cyber security defensive architecture is designed from Level 4 down to Level 0.



4.4.1. Level 4 (Vital Area – Control and Safety System):

Digital assets at Level 4 have to be under total security in terms of their communication features. Any breach in this level will jeopardize the nuclear safety of the power plant. There is no networked data traffic allowed in this level. Depending on the design of the system, the operator can only permit one-way outward communication. However, the one-way communication could also have some reliability and integrity issues.[52] The operators have tendency to create exceptions for reasons such as economic feasibility, practicality and to start the production quickly. The IAEA strongly encourages operators to choose security oriented solutions and is considering exceptions on a strict case-by-case basis. All unnecessary

applications, services, and protocols have to be blocked. The IAEA also advises the following points:

- No remote maintenance access is allowed.
- Physical access to systems is strictly controlled.
- The number of staff given access to the systems is limited to an absolute minimum.
- The two-person rule is applied to any approved modifications made within the computer systems.
- All activities should be logged and monitored.
- Every data entry to the systems is approved and verified on a case by case basis.
- Strict organizational and administrative procedures apply to any modifications, including hardware maintenance, updates and software modifications.[53]

4.4.2. Level 3 (Protected Area – Data Acquisition Network):

- Only an outward, one-way networked flow of data is allowed from level 3 to level 2 systems.
- Only necessary acknowledgment messages or controlled signal messages can be accepted in the opposite (inward) direction (e.g. for TCP/IP).
- Remote maintenance access may be allowed on a case-by-case basis and for a defined working period. When used, it must be protected with strong measures, and users must respect a defined security policy (contractual).
- The number of staff given access to the systems is kept to a minimum, with a precise distinction between users and administrative staff.
- Physical connections to the systems should be strictly controlled.
- All reasonable measures to ensure the integrity and availability of the systems have been taken.
- Vulnerability assessment involving actions on the systems may lead to plant or process instability, and should therefore only be considered using test beds, spare systems, during factory acceptance tests or during long planned outages.

4.4.3. Level 2 (Owner-Controlled Area – Site Local Area Network):

In addition to general security measures, level 2 protective measures should be used for supervising real-time systems not required for operation in a control room for medium-level cyber threats. A firewall with access control and communication filtering rules can help segregate communication among the various security levels to prevent unnecessary redundancies. These protective measures may include the following:

- Access to the Internet from level 2 systems should not be allowed.
- Logging and audit trails for key resources should be monitored. The IT staff has to check these logs and audits regularly against any alterations.
- Security gateways should be implemented to protect this level from uncontrolled traffic from level 3 systems, and allow only specific and limited activity.
- Physical connections to systems should be strictly controlled.
- Remote maintenance access should be allowed on a case by case basis after the confirmation of the cyber security officers. All these exceptions have to be controlled periodically and unused access must be terminated. In the case of access, the remote computer and user must

respect a defined cyber security policy.

- System functions available to users should be strictly controlled by mandatory access control mechanisms and be based on the 'need to know' principle. Any exception to this principle has to be carefully discussed with the managers and cyber security officers. The computers and network access pathways should be protected against unauthorized usage.[54]

4.4.4. Level 1 (Corporate Accessible Area – Wide Area Network):

At this level, business systems, such as technical data maintenance systems and operation activity management (e.g. work permit, work order, tag out, and documentation management) are typically connected to a plant intranet. In addition to general security measures, the connection between the process control networks and the business system networks require special attention and segregation. The IAEA defined the limitations for Level 1 in the following[55]:

- Only approved and qualified users shoud be allowed to make modifications to the systems. These users and their positions have to be screened periodically by human resources and the cyber security office. Inactive user accounts have to be terminated as soon as possible.
- Access to the Internet from level 1 systems may be given to users after adequate protective measures are applied. These systems have to be inspected regularly and the users of the systems have to be warned against the phishing attacks.
- Security gateways should be implemented to protect this level from uncontrolled traffic from external company or site networks and to allow specific activities which are controlled such as downloading executable files, blocking to access the black listed web pages, etc.
- The physical connections and access to these systems should be controlled. All access to these systems have to be logged. The cyber security officers have to inspect the logs periodically for unexpected activity.
- Remote maintenance access may be allowed in a controlled fashion. The remote computer and user must respect a defined security policy, which should be specified in the contract and controlled.
- System functions available to users should be controlled by access control mechanisms. Any exception to this principle has to be carefully studied and protection should be ensured by all means. The cyber security officers must check these exceptions regularly and inactive ones should be terminated.

4.4.5. Level 0 (Public Accessible Area):

Level 0 is for systems not directly related to technical control or operations, e.g. office automation systems, system management servers, and patch management and anti-virus servers. These systems are lower level cyber threats. In addition to facility specific measures, Level 0 measures include the following:

- Only approved and qualified users should be allowed to make modifications to the systems. The list of these users has to be checked periodically. The inactive accounts have to be terminated by cyber security officers.
- Access to the Internet from level 0 systems may be allowed if adequate protective measures are applied. Access has to be controlled by a firewall system to stop unnecessary communication. The users in this level have to be warned against phishing attacks.

- Remote external access may be allowed in order to make necessary controls. The cyber security officers should inspect controls and block access in the case of alteration.

In a nuclear power plant site, cyber security zones are linked to physical security. If possible, the head of the cyber and physical security departments should create new security plans which would secure the facility against hybrid threats.

In order to design a robust cyber security policy, the operator has to set facility specific rules, enforce these rules, and warn the necessary departments if they suspect any violations. The IAEA gave examples of these rules in its Computer Emergency manual[56]:

- All users have to understand and obey the cyber security operating procedure.
- Staff permitted access to the system must be suitably qualified and experienced and security cleared where necessary.
- Users are given access only to those functions on those systems that they require for carrying out their jobs.
- The ICT appliances have appropriate access controls and user authentications.
- Application and system vulnerabilities are monitored, and appropriate measures are taken.
- The system vulnerability assessments are undertaken periodically.
- Computer and network security components should be strictly maintained intrusion detection systems, intrusion prevention systems, virtual private network servers are strictly logged and monitored.
- Appropriate backup/recovery procedures have to be checked periodically.

Physical access to components and systems is restricted according to their functions.

5. Cyber Security and Nuclear Power: The Turkish Context

5.1. Organization

From a cyber security perspective, Turkey has limited experience as a regulator for nuclear power plants. Stuxnet attacks directed against Iran's nuclear power plants, along with similar threats and attacks have increased Ankara's concerns. According to the Critical Infrastructure Protection Report of Disaster and Emergency Management Authority (AFAD) the energy sector has several regulatory agencies, such as the Ministry of Energy and Natural Resources, Turkish Atomic Energy Authority (TAEK), AFAD, and the Energy Market Regulatory Authority (EPDK). During the NPP licensing process, all of these agencies and ministries have different jurisdictions. The Ministry of Energy is responsible for the organization, planning, and execution of the NPP project. EPDK manages the legislative and regulatory processes of electricity production and sales. TAEK is the licensing authority of Turkey for nuclear safety and security of the facilities. AFAD is in control of NPP emergency preparedness. Moreover, the Ministry of Interior controls the physical security of the facility and coordinates the private security of the NPP in case of any emergency. The Ministry of Interior should also prepare the legislative background for private security, which would be tasked with protecting these sensitive facilities, and should be well-trained, vigilant and have a comprehensive security understanding.

The main problem that may concern the cyber security of Turkish nuclear power plants, is the lack of necessary and adequate laws and regulations in this field. Current legislation on the protection of critical infrastructure does not provide measures specific to nuclear power plants. At the moment, Turkey has a general-purpose Cyber Emergency Response Team (CERT) under the Presidency of Telecommunication; however, the cyber security of industrial control systems demands more sophisticated, specialized know-how.

As the NPP licensing authority, the Energy Market Regulatory Authority (EPDK) completed the pre-licensing process of Akkuyu NPP on June 25, 2015. Pre-licensing process is a milestone for reducing the risk of licensing and making the outcome of a licensing process more predictable. However there is limited open-source information on the Akkuyu plant on the licencing process, and especially on security. The main question is whether or not cyber security-related plans were factored into the pre-licensing process. The EPDK or TAEK has to inspect and analyze the cyber security plans of ROSATOM for both high security and low security areas. The NPP design plans also have to include the implementation of HVAC services as well as third-party actors' cyber security approaches. How do Akkuyu and ROSATOM plan to organize the protective maintenance of HVAC infrastructure? Who will be responsible for the cyber security of HVAC servers? Will third-party contractors have remote access to infrastructure protective maintenance? How do third-party contractors update their servers and infrastructure? A number of questions such as these are awaiting answers prior to the licencing process.

The counterpart for the NRC in Turkey is considered to be TAEK. The Turkish administration has the same approach, which is evidenced by the fact that TAEK was given the authority to supervise the security of the nuclear power plant. Yet, it is not clear how TAEK views the issue of cyber security for the facilities or how it will check cyber security plans. Similar questions

concerning HVAC and third-party contractors are also current with regards to TAEK and the Akkuyu plant.

The fact that Akkuyu nuclear energy plant operation center will have at least three connections makes the issue more complicated on a higher level: first with Akkuyu Project Company, second with ROSATOM, and third with the power grid. These connections have the potential/threat of creating a complex cascade effect. For companies, controlling local area networks (LAN) will be much easier. Yet "who will be in charge of managing security issues that would arise from national electricity grid network and how?" remains a question that needs to be answered.

5.2. Sharing Information, Monitoring Security, and Managing Incidents

The EU and the US have created systems for the timely sharing of information regarding nuclear facilities without constituting a security vulnerability. NPPs have to report any cyber or physical incidents or intrusion attempt to available authorities. In turn, this authority is tasked with informing all related units and warning all facilities against similar threats and emergencies.

The lack of such a vital system puts all operations at risk. Nevertheless, the sparsity of cyber attacks against nuclear power plants and the secretive nature of the issue, has created a false perception of confidence on nuclear facility security amongst both operators and regulators. In general, it is seen that especially as a result of this perception, nuclear facility operators cooperate less with other sectors on issues pertaining to cyber security. Yet, through the use of common hardware, it is possible to create the space for more efficient cooperation that would cover all industrial control systems against potential threats.

The main priority of nuclear cyber security is to monitor security and potential threats regularly. This task requires to go beyond simply focusing on nuclear power plants, and involves gathering intelligence and having the capability to mine data through the depths of cyber space. In terms of creating fake identities and contacting international hacker groups and other organized criminal networks, it is seen that Turkey's cyber intelligence capabilities remain limited. The National Intelligence Agency (MIT) and the Intelligence Department of the Turkish Police collect data from cyber space for cyber intelligence purposes. Even if the quality of this intelligence is high, the answers to how much and how fast this information would be shared with the units in charge of the security of Akkuyu NPP remains unknown. Therefore, there may be the need for a private cyber intelligence company that informs the NPP operators on a regular basis.

In this perspective the cyber security of a nuclear facility consists of two main stages; the digital protection of all software, communications and critical digital assets, and the protection of all infrastructure, necessary communications hardware or other tools that affect the functionality of the facility, by a physical security team. The second stage, i.e. the physical protection of a NPP, will be managed by private security under the coordination of the Ministry of Interior. All these parties must also remain in contact with fiber optic cable providers and other infrastructure-related bodies to best protect NPPs. The physical protection unit should prepare a cooperation and communication plan, which foresees and provides the details of a collaboration with law enforcement forces. In addition, law enforcement forces should design the critical and strategic communications regarding the facility's physical protection. The specific legal arrangements concerning the authority to use lethal force by private

security companies and their employees in the face of attacks, as well as their extent, should be prepared at once. It should be kept in mind that when the security of nuclear facilities is concerned, reaction times are vital in preventing tragedies that result from attacks.

As the number of hybrid threats that include both cyber and physical threats are increasing, the physical security team has to work closely with the cyber security team. The physical and cyber security teams must cooperate on at least two main points. First, the CCTV systems that all servers use have to be protected against any hostile attack. Second, all cyber security infrastructures are also vulnerable to physical attacks and breaches. The physical security team must have a basic understanding of cyber security and IT infrastructure to protect devices against cyber attacks.

As examples of successful cases show, most NPPs have an elaborate incident response plan that designates the roles of each employee for several emergency scenarios. Employees learn their roles based on different exercise scenarios. These exercises carry importance for they enable employees to repeatedly put in practice all the necessary preparations and actions that surge in the face of an attack. However, in actual scenarios pressures such as fear, time and risk highly affect human judgment and the decision-making process.[57] It is possible for even the most experienced employees to freeze and underperform during a real emergency. To prevent such situations, the cyber security team has to develop contingency plans that teach them how to behave under various conditions.

It should not be forgotten that reacting to the incident in the NPP is not a standalone activity. The facility management should inform the necessary bodies to activate the facility, corporate and national-level plans. As the facility remains a smaller unit compared to the national level, it should develop more comprehensive action plans for larger scale and convoluted incidents. These plans should be shared with all related stakeholders and should be updated. In this context, in Turkey's case, AFAD has to prepare a master emergency preparedness plan in coordination with TAEK, the Ministry of Energy, the Ministry of Interior, the Presidency of Telecommunication, ICS-CERT (if available), and Prime Minister's Office. A crisis management center that should be formed according to this plan and the relevant regulations, should be established to respond to the crises in the right place and at the right time. While preparing this plan, the details should be shared with stakeholders such as ROSATOM and AREVA. Direct lines of communication should be established among the sides. The emergency preparedness plan should prioritize targets that are easier to establish prior to the moment of emergency. The management should decide what to do to protect the facility in cyber emergencies. For cases where national teams remain inadequate in delivering solutions and need outside help, this master plan should include the option of an international high-level ICS-CERT. AFAD should test this emergency response plan at least once a month and encourage new employees to abide by the necessary codes. To ensure its preparedness, AFAD has to utilize a third-party penetration tester regarding a cyber attack to the NPP and the crisis management authority.

The management team must also consider the potential communication friction between technology engineers, responsible for operational tasks, and cyber security staff. In many cases the problem is exacerbated by the fact that cyber security personnel is located off-site. Management must ensure the harmony and integrity of both parties involved as well as express that all employees are vital for the well-being of the facility.

For many private sector enterprises, including nuclear facilities, the level of investment in security reflects tradeoffs between risk and outcomes that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or within resource constraints. The regulator in Turkey has to

consider this balance. To minimize risk, before licensing a NPP, the regulator has to check the NPP for design problems. From the cyber security perspective, the inspection of necessary software is critical to sustaining security and preventing possible vulnerabilities. During operation, NPP hardware needs patches and updates in the long run. Yet false software updates are one of the most frequently used exploits by malicious cyber intruders. The IT team should regulate the patching process and conduct detailed tests before implementing to a NPP cyber system. The NPP operator must also create a renewal management plan to prevent the aging of hardware. From time to time, the regulator has to push the operator company to update existing hardware and software to ensure the security. It can be difficult and expensive for the operator to keep up with technological developments. Design features of the facility or financial reasons may act as obstacles against refurbishments. However, an outdated system jeopardizes the nuclear safety and security of NPPs.

In Turkey, including at Akkuyu, all NPPs have to connect to the electric grid to transfer the electricity produced. This means that all vulnerabilities of the electric grid are transferred to the NPP. The recent electricity blackout in Turkey, gave rise to arguments that cyber attacks originating from Iran were at its source, while others attributed it to a malfunction of a few power plants affecting the whole electric grid. Whatever the reason for the blackout, the incident demonstrated the possibility of cascade effect that could occur due to the interdependency of the electric grid[58]. Even if NPPs like Akkuyu are assumed to be durable against attacks, they would still be affected by cyber attacks targeting the electric grid. Therefore, NPPs have to be fortified against not only physical attacks but also unintended digital ones.

Last but not least, high-altitude electromagnetic pulse attacks are one of the most effective assaults against critical infrastructure, including the NPPs. An electromagnetic pulse (EMP) is a high-intensity burst of electromagnetic energy caused by the rapid acceleration of charged particles. This lightning-like pulse flows through electric transmission lines, overloading and damaging power lines, fuses, and transmission distribution centers. This broad band, high-amplitude EMP, when coupled with sensitive electronics, has the capability to produce widespread and long-lasting disruption and damage to critical infrastructure.

SCADA systems of NPPs are also vulnerable to EMP attacks. The American commission has conducted tests in several different settings to evaluate the magnitude of the EMP threat. The results show that all tested systems were knocked out when subject to EMP.[59] It is actually relatively easy to obtain or construct an EMP device. The large number of and widespread reliance on SCADA systems represent a systemic threat to their continued operation following an EMP event. Additionally, the necessity to reboot, repair, or replace large numbers of systems will considerably impede the nation's recovery from such an assault. Therefore, Ankara has to force the operators to take necessary precautions to protect themselves from such attacks and to add EMP assaults to their possible attack scenarios.

6. Conclusion

After the Stuxnet attack, the protection of critical infrastructures and key resources became more evident in the international arena. International organizations underlined the importance of cyber security in this sector and focused on raising situational awareness. The cyber security of nuclear power plants has a particular place among all critical infrastructures. Since industrial control systems are not designed with a security perspective, the regulatory bodies and organizers of the facilities have to show utmost attention to the cyber security ofnuclear power plants by implementing policies and forming an effective cyber security culture. The cyber security incidents listed above, showed that no state is completely immune to any cyber attack targeted at nuclear facilities. The states' nuclear regulatory bodies have to implement necessary legislations and policies to control the practice of the nuclear power plants, with an emphasis on risk management, highly organized coordination and strategic communication.

In spite of all these precautions, we are witnessing new types of attacks, which exploit new vulnerabilities every day. IAEA is also trying to establish a detailed computer security roadmap, which would guide its members. Nation states are key actors to follow these steps to secure their critical infrastructures and key resources. In Turkey, the nuclear power plant case is more peculiar than other applications, with its build-own-operate model. The contractors of the project Russian ROSATOM and Turkish Akkuyu Nuclear Corporation, are trying to meet the requirements and expectations of the Turkish legislation on nuclear plants via training technical experts, planning and preparing reports. The first major problem that both companies have to face is human capital. In such a facility, the cyber security staff has to be bilingual as well as having adequate information on the security cultures of both societies. The cyber security in a nuclear power plant requires specific expertise on the ICS as well as other required knowledge on IT infrastructures. At the moment, there is remarkable effort to train nuclear engineers but there is no recorded information on cyber security experts for Turkish nuclear power plants.

The second part of the problem has two dimensions. Firstly, Ankara is still trying to prepare necessary regulations and legislations to be ready for a proper establishment of the facility's infrastructure. All ministries and public offices are approaching the problem from a micro perspective and are regulating their areas of interests. However, there is no coordinating authority to concentrate these micro perspectives into a macro one. Secondly, Turkey has no ICS specific cyber security organization, which could coordinate the private and state stakeholders in the sector. By considering the recent political developments in Turkey and the ambiguity of international law on cyber attacks, Turkey has to develop its own defensive and offensive cyber security capacity. Ankara has to persistently focus on coordination and strategic communication among necessary parties.

1- Joshua Yates, "Interview with Ulrich Beck",The Hedgehoc Review, 5:3, Fall 2003, p. 97.

2- Mordechai Guri, Matan Monitz, Yisroel Mirski, Yuval Yelovici. "Bitwhisper: Covert Signalling Channel Between air-gapped computers using Thermal manipulations". http://arxiv.org/pdf/1503.07919v1.pdf;

3- Kim Zetter, "Researchers hack air gapped computer with simple cell phone". Wired, 27 June 2015, http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/ (Accessed on 29 June 2015)

4- Kim Zetter, "How attackers can use radio signals and mobile phones to steal the protected data". Wired, 03 November 2014, http://www.wired.com/2014/11/airhopper-hack/ (Accessed on 01.07.2015)

5- DBT is a description of the attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system is designed and evaluated. For further details, see; "Development, use and maintenance of the design basis threat: implementing guide". Vienna: International Atomic Energy Agency, 2009.

6- We have seen similar tendencies in Havex, Dragonfly, and Blackenergy malware.

7- Russia: Hidden chips 'launch spam attacks from irons, BBC News, 28 October 2013, http://www.bbc.com/news/blogs-news-from-elsewhere-24707337

8- Zero-day exploit: "Abbreviated as 0-day exploit, it capitalizes on vulnerabilities right after their discovery. Thus, zero-day attacks occur before the security community or the vendor of the software knows about the vulnerability or has been able to distribute patches to repair it. For this reason, these exploits allow crackers to wreak maximum havoc on systems." Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, p. 371.

9- Special Communication Protocols: are to be developed to control communication. A tailored set of formal rules describing how to exchange data on embedded systems.

10- David B. Fogel, "What is evolutionary computing?" Spectrum IEEE, 37(2), 2000, pp. 26-32.

11- David B. Fogel – Lawrence J. Fogel, "An Introduction to Evolutionary Programming", Artificial Evolution, Springer: Volume 1063 of the series Lecture Notes in Computer Science, 2005, p. 21.

12- WINS, Human Reliability as factor in nuclear security, World Institute for Nuclear Security, 2012, p. 3.

13- "The term internal threat is used to describe individuals (employees or contractors) with authorised access to a facility, transport operations, or sensitive computer and communications systems who use their trusted position for unauthorised purposes." Wins, "Managing Internal Threats (Rev. 1.0)", World Institute of Nuclear Security, 2010, p.3.

14- IAEA, Preventive and Protective Measures against Insider Threats, Vienna, 2008.

15- Ralph Langner, "To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve", November 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (Accessed on 19 October 2015)

16- Ralph Langer, "Stuxnet's Secret Twin". Foreign Policy, 19 November 2013, http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack (Accessed on 26 August 2014)

17- IAEA, Computer security at nuclear facilities : reference manual ,Vienna, 2011, pp. 39-40.

18- Matt Paulson, "Cyber-Terrorism Struck the Nuclear Regulation Commission Three Times in Three Years", 19 August 2014, http://it.tmcnet.com/topics/it/articles/2014/08/19/386959-cyber-terrorism-struck-nuclear-regulation- commission-three-times.htm

19- W32/Slammer, http://www.f-secure.com/v-descs/mssqlm.shtml

20- Kevin Poulsen, "Slammer worm crashed Ohio nuke plant network", SecurityFocus, 2003, http://www.securityfocus.com/news/6767

21- United States Nuclear Regulatory Commission, "Effects of Ethernet-Based, non-safety related controls on the safe and continued operation of nuclear power stations", http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info- notices/2007/in200715.pdf

22- United States Nuclear Regulatory Commission, "Effects of Ethernet-Based, non-safety related controls on the safe and continued operation of nuclear power stations", http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info- notices/2007/in200715.pdf

23- Robert McMillan, “Nuclear Plant Shutdown by Network Trouble”, PCWorld, 2007, http://www.pcworld.com/article/132118/article.html

24- Robert Lemos, “Data Storm blamed or nuclear - plant shutdown”, Security Focus , 2007, http://www.securityfocus.com/news/11465

25- Brian Krebs, “Cyber Incident Blamed for Nuclear Power Plant Shutdown”, Washington Post, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html

26- For further details on these reports, see; http://www.nrc.gov/reading-rm/doc-collections/event-status/event/

27- Reuters, “Malicious Virus Shuttered US Power Plant”, January 2013, http://www.voanews.com/content/us-power- plant-computer-virus/1585452.html

28- Industrial Control Systems Cyber Emergency Response Team, “ICS-CERT Monitor”, October/November/December 2012, http://ics-cert.us-cert.gov/monitors/ICS-MM201212

29- Industrial Control Systems Cyber Emergency Response Team, “ICS-CERT Monitor”, October/November/December 2012, http://ics-cert.us-cert.gov/monitors/ICS-MM201212

30- Karsten Nohl, Sascha Krissler, Jakob Lell, “Bad USB. On accessories that turn evil”. https://srlabs.de/blog/wp- content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf

31- Michael Riley - Dune Lawrence, “Hackers linked to China’s Army seen from EU to D.C.”, Bloomberg, June 2012, http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html

32- Michael Riley - Eric Englaman, “Why congress hacked up a bill to stop hackers”, Bloomberg, November 2012, http://www.businessweek.com/articles/2012-11-15/why-congress-hacked-up-a-bill-to-stop-hackers

33- “Monju power plant facility PC infected with virus”, Japan Today, 7 January 2014, http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus

34- Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon. Crown Publishers: New York, 2014, p. 21.

35- Geoff McDonald, Liam Murchu, Stephen Dolerty, Eric Chien, “Stuxnet 0,5 The missing link”, 6 February 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_lin k.pdf

36- Kim Zetter, “How digital detectives deciphered Stuxnet, the most menacing malware in history.” Arstechnica, 11 June 2011, http://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing- malware-in-history/3/

37- Ralph Langner, “To kill a centrifuge A technical Analysis of what Stuxnet’s Cretors tried to achieve”, November 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

38- Nicolas Falliere, “Exploring Stuxnet’s PLC Infection Process” Symantec, 22 September 2010, http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

39- “US - Israeli computer super-worm hit Russian nuclear plant Kaspersky” Reuter, 12 November 2013, http://rt.com/usa/kaspersky-russia-nuclear-plants-612/

40- Salih Bıçakcı, 21yy Siber Güvenlik (21st century Cyber Security), İstanbul: İstanbul Bilgi Üniversitesi Publication, 2013.

41- A Bulletin Board System is a computer system running software that allows users to connect and log into the system using a terminal program.

42- Crackers (general term): Black Hats who break into others’ computer systems without authorization, dig into code to break a software’s copy-protection provisions, flood Internet sites, deliberately deface Websites, and steal money or identities. Sometimes the terms “network hackers” or “net-runners” are used to describe them. Often the media incorrectly substitute the word hacker for cracker—a behavior that irritates many in the Computer Underground. Webster’s New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, p. 73.

43- Mini S. Thomas – John D. McDonald, Power System SCADA and Smart Grids, Boca Raton: CRC Press, 2015.

44- Erica Harefors, "Use of large screen displays in nuclear control room" Unpublished graduation thesis, Institute Energiteknikk, Uppsala Universitet, 2008. http://www.utn.uu.se/sts/cms/filarea/0804_härefors.pdf

45- One category of cyber attacks is semantic attacks. These attacks aim to destroy trust in the system and information by manipulation, change of information, and deception, which can be harmful to the decision-making process.

46- Tunnel vision: A tendency to think only about one thing and to ignore everything else. http://www.merriam- webster.com/dictionary/tunnel%20vision (accessed on 27 August 2014)

47- Dileep Buddaraju, "Performance of control room operators in alarm management", Unpublished Master thesis, Lousiana State University, 2008, p. 2.

48- During security planning, the computer systems should be designed to meet multi-level security strategies, thus strengthening information integrity.

49- Tailgating: "Tailgating is an attack that you can use in any environment that makes use of proximity door controls. In principle, the concept is simple enough but in practice, it requires a little forethought for successful execution. You (or an intruder) are unable to open proximity door locks without an activated token. A classic approach is to 'talking' on mobile phone near the door and conclude the call just as someone passes you in the hallway and opens it. Then you follow them. Give the impression that you've just gone out to take or receive a phone call, which you've now concluded and are returning inside." Will Allsopp, Unauthorised Access: Physical Penetration Testing for IT Security Teams, Wiley: Sussex, 2009, p. 34.

50- Steve Huff, "Access HVAC Systems via Big Security Holes". Observer, http://observer.com/2012/12/hackers-in- the-vents-cyber-intruders-could-access-hvac-systems-via-big-security-holes/ (Accessed on 11 March 2015)

51- Security level model is a way of applying elevating security measures at different levels in a critical infrastructure. For further information see; IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, pp. 29 – 35.

52- George Kamis, "Resolving the Critical Infrastructure Cybersecurity Puzzle", Signal AFCEA, March 2014, http://www.afcea.org/content/?q=resolving-critical-infrastructure-cybersecurity-puzzle (Accessed on 29 December 2015)

53- IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, p. 32.

54- Majed Al Breiki, "Cyber Security Design Methodology for Nuclear Power Control and Protection Systems", http://www.automation.com/pdf_articles/Cyber_Security_Design_Methodology.pdf (Accessed on 5 October 2015)

55- IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, p. 30.

56- IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, pp. 29 - 35.

57- Kenneth R. Hammond, Judgments under Stress, Oxford University Press: New York, 2000; Judgment and Decision making at work, S. Highhouse, Reeshad S. Dalal, E. Salas (eds.), Routledge: New York, 2014.

58- TEİAŞ – ENTSOE, "Report on Blackout in Turkey on 31st March 2015", 21 September 2015, https://www.entsoe.eu/Documents/SOC %20documents/Regional_Groups_Continental_Europe/20150921_Black_Out_Report_v10_w.pdf (Accessed on 21 October 2015)

59- "Report to the Commission to Assess the threat to the United States from Electromagnetic Pulse Attack, Critical National Infrastructures", April 2008, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf (Accessed on 15 September 2015)