Journal of Learning and Teaching in Digital Age, 2023, **8**(2), 237-244
https://dergipark.org.tr/en/pub/joltida
ISSN: 2458-8350 (online)

Review Paper

Cyber Terror Threats Against Nuclear Power Plants

Hüseyin Kuru*[a]

[a](ORCID ID: 0000-0002-7464-9860), Gazi University, Turkey, husseyinkuru@gmail.com

*Corresponding author

ARTICLE INFO

Received: 3 November 2022
Revised: 3 February 2023
Accepted: 3 February 2023

Keywords:
Terrorism
Cyber Terror
Nuclear Power Plants
SCADA systems
Cyber Security

doi: 10.53850/joltida.1198872

ABSTRACT

After the Cold War period, with the restructuring of the world, globalization, the revolution in information technology and the reconstruction of capitalism have created a new type of society, the "network society". The dependence of countries on information technologies, especially the internet, has increased day by day, and it has become almost impossible for individuals, state institutions and private companies to continue their activities independently of cyberspace, which is described as the fifth operational area. This situation has made it a critical priority to ensure the physical and cyber security of nuclear power plants, which carry the energy burden of the societies and at the same time pose great security risks. In this period, states, state-sponsored and radical terrorist groups that wanted to close the power deficit against military and economically strong states, started to develop asymmetric methods of struggle. In the end new threat vectors such as cyber terrorism have emerged and states that have moved many institutions and services to cyberspace have become more vulnerable to malicious attacks and terrorist activities. In this study, the concept of terrorism and cyber terrorism have been examined and focused on the SCADA systems of nuclear power plants and in the last section cyber security of these systems have been evaluated. This Implementation of this model aims to simplify the process for all organizations in the Nuclear Sector—regardless of their size, cybersecurity risk, or current level of cybersecurity sophistication—to apply the principles and best practices of risk management. Ultimately, the framework and this implementation model are focused on helping individual organizations reduce and better manage their cybersecurity risks, contributing to a more secure and resilient sector overall. The main goal in this work is to improve SCADA system vulnarabilities, show terror groups abilities and present suggestions to safeguard nuclear plants.

INTRODUCTION

Human beings use the technological competence devised by the developing knowledge to reach higher quality benchmarks in every facet of their life. This distribution and widespread use of technology are generally built on the foundation provided by energy. In other words, every technological innovation increases the need for energy in the background. As a natural consequence of this situation, sustainable energy sources are needed to maintain and further develop the existing order.

Energy exists in nature in two different formats, renewable and non-renewable. Most of the non-renewable energy sources are still obtained from fossil fuels in nature (Hubbert, 1956). Non-renewable energy sources are not found in infinite quantities in nature and will one day be depleted. In addition, the widespread and intensive use of fossil fuels damages the ozone layer surrounding our world and causes global warming and climate changes that affect human life. This situation, which was also brought to the agenda in the Kyoto protocol signed in 2014, has caused human beings to turn to cheap, clean and sustainable energy sources that will not harm environment (UN Climate Summit, 2014). Recently, increasing environmental awareness all over the world and efforts to combat climate change have made nuclear energy a necessity rather than a choice as an environmentally friendly energy acquisition method when used cleanly and safely. Although nuclear energy showed itself as a powerful force multiplier on the battle ground in the first period of its discovery, with the understanding that it could be used for peaceful purposes, it was transformed into a budget and nature-friendly energy acquisition solution.

With the integration of modern technologies, critical infrastructures have become more integrated with information systems and the protection of these systems, which are vital for social order and health, has become a critical issue for the survival of countries. Critical infrastructures are vital for the country's defense, social order and welfare. Critical infrastructures, operating in all areas of social life, from electricity infrastructure to rail systems used every day, from natural gas pipelines to stadiums, from nuclear power plants to banking applications, have become the primary targets of cyberattacks. The vulnerabilities of these systems, which are called SCADA systems, have the potential to produce devastating results when blended with potential terrorist attacks, imprudence, misapplications.

Cyber security is an indispensable security component for nuclear power plants. Nevertheless, cyber security is a concept that has come to the fore more frequently and given importance recently, many nuclear power plants constructed in the first period were designed with a view away from the concern of cyberattacks (Bıçakcı, Ergun, & Çelikpala, 2015). In addition to this fact, Cyber-

attacks continue to increase and become more specific with each passing day and terrorist organizations tend to use the cyber environment for their purposes. Today, cyber terrorist attacks have become a real threat.

Countries have to protect their critical infrastructure. Threats to critical infrastructures appear in every source and form. Today, traditional wars have been replaced by structures called hybrid wars. In this concept, there are different attack vectors, including the cyber environment, as well as traditional techniques (Ng Eng, 2016). Figure 1 shows the Hybrid Warfare Components

Figure 1. Hybrid Warfare Components, adapted form (Ng Eng, 2016)

Before 9/11, cyberspace risks and security issues were only discussed within small groups of technical experts. However, since those days, it has become clear that the cyber world creates serious defense vulnerabilities for societies that are increasingly interdependent (NATO Review Magazine, 2011).

There have been many examples of cyber-attacks targeting states' critical infrastructure. Many of these occurred in the 2000s, before awareness had developed as to the nature of this kind of threats. One of the most prominent cyber-attacks or let's say warfare example at the end of the Cold War was occurred in Estonia. Tension between Russia and Estonia that had begun in response to Estonia's rapprochement with the North Atlantic Treaty Organization (NATO) alliance became heightened due to Estonia's decision to remove a Soviet-era statue from Tallinn Square. Immediately after this decision, a large-scale Distributed Denial of Service (DDoS) attack was launched against Estonia's critical infrastructure. The cyber-attacks aimed to collapse the country's internet infrastructure by targeting the websites of Estonia's political parties, its state institutions, parliament, media organizations, banking and financial systems. The internet sector of Estonia's critical infrastructure became unaccessable for a week as a result of the attacks. Estonia recovered with the help of NATO, and the decision to close access to Estonia's national web from abroad (Daricili, 2014).

In another instance, a cyber-attack involving the Stuxnet Virus was launched against Iran's nuclear installation in Natanz in June 2010; the installation was physically damaged and the development of its nuclear energy capacity was delayed as a result. Although Iran blamed the U.S. and Israel as the backers of the attack, no one has claimed responsibility to date (Boothby, 2015).

Other examples of cyber-attacks targeting critical infrastructure were observed during Russia's intervention in Ukraine, which began in 2014. The use of mobile phones in Crimea in the first days of close combat in March 2014 was prevented by destroying the infrastructure of Ukrtelecom, Ukraine's official mobile phone company. Another cyber-attack was carried out against a power plant in the Prykarpattyaoblenergo Region of Ukraine on December 23, 2015, causing a power outage there. According to Ukraine's allegations, these cyber-attacks were conducted by Russian intelligence services and affiliated hacker groups (Case, 2016).

Another example of cyber-attacks targeting a state took place in Turkey. On November 24, 2015, Turkish F-16s shot down a Russian Su-24 fighter jet for violating Turkish airspace—an incident that created significant political tension between Turkey and Russia. The tension increased in December 2015 when "DDoS" cyber-attacks aimed to erode Turkey's critical infrastructure, including its banking and finance systems, public institutions and e-state, by targeting the bandwidth used by the system where ".tr" extension names are kept. The attacks had the potential to affect 400,000 websites in Turkey. Russia is alleged to have been behind those attacks, but has not recognized such claims (Daricili, & Özdal, 2017).

Nuclear power plants are also at risk of being affected by attacks by terrorists from the cyber environment. Particularly, a part of the critical infrastructure belonging to nuclear power plants can be cut from the internet or any network as a part of security measures and these systems can be destroyed with a very sophisticated cyberattack as a result of which nuclear explosion can occur (Valo, 2014).
Nuclear security can also be compromised by other means such as cyberattacks, including sabotage at nuclear facilities. In addition, threats related to nuclear terrorism also come from many sources, such as sophisticated and well-organized terrorist organizations, nuclear smugglers or hackers who can launch devastating cyberattacks against information and computer systems in nuclear

facilities. All of these challenges affect how these threats are managed by facility operators, nuclear regulatory agencies and organizations responsible for emergency planning and response.

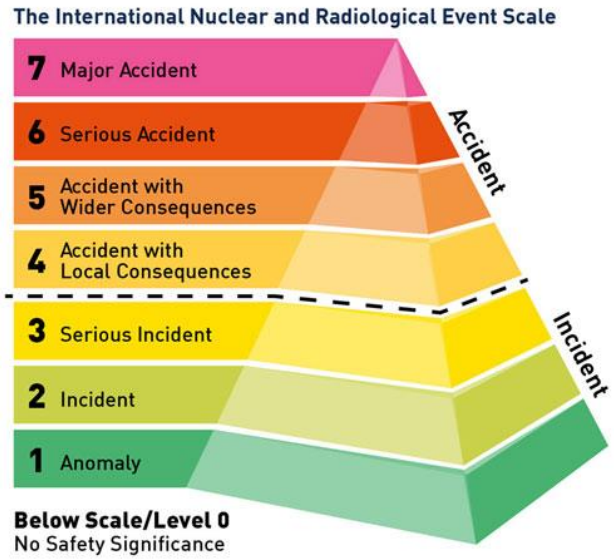

Figure 2. International Nuclear and Radiological Event Scale (INES), Adapted from NRC (2023)

As a result of any attack on nuclear facilities there may be serious consequences starting from "No safety significance" to "major accident". The International Atomic Energy Agency (IAEA) has an International Nuclear and Radiological Event Scale (INES), shown in Figure 2. The accidents at the Chernobyl and Fukushima nuclear power facilities were a 7 on this scale, whereas the event in Goiânia, Brazil was a 5 (IAEA, 2021).

The aim of this research is to prepare a content that will raise awareness about the cyber terrorist threats against nuclear power plants, which will become an alternative energy source for Turkey in the near future and present it to the personnel working in the relevant units to enhance personel awareness.

Terror and Terrorism

Before explaining the concept of cyber terrorism, it is necessary to define terror and terrorism. The term Terror, which takes its root from the Latin word 'terrere', means "to be shaken by fear" or "to cause terror with fear", and it is first encountered in the supplement of the Dictionnarire de l'Academie Française published in 1789 (Güzel, 2002).

In the 1st article of the Anti-Terror Law No. 3713, which is still in force in the Republic of Turkey (Amended - 19.07.2003/25173) (Şimşek, 2016); "*Terror; all kinds of criminal actions to be taken by a person or persons belonging to an organization with the aim by using force and violence to change the characteristics of the Republic, political, legal, social, secular and economic order specified in the Constitution, to disrupt the indivisible integrity of the State with its territory and nation, to endanger the existence of the Turkish state and the Republic, to weaken the state authority, or destroying fundamental rights and freedoms, disrupting the internal and external security of the State, public order or general health.*"

When we look the definition of Grant Wardlaw, he claims (Wardlaw, 1989), "*(Political) terrorism is the use, or threat of use, of violence by an individual or a group, whether acting for or in opposition to established authority, when such action is designed to create extreme anxiety and/or fear-inducing effects in a target group larger than the immediate victims with the purpose of coercing that group into acceding to the political demands of the perpetrators".* We can realize some covering features in these definitions.

Declaring oneself and one's motivation through terrorism, in short, through armed actions; Terrorism, on the other hand, can be said to be a discipline and movement of thought that upholds these actions, explains, transfers and develops their strategies. Terrorists go underground, work in secrecy, carry out their actions and ultimately turn to propaganda for the purposes of their actions. Terrorism comes into play after this stage. In other words, terrorism is strategic action, terrorism is strategic discourse (Bal, 2006).

Terrorism And Cyber Terrorism Capabilities

Along with the developing technology, terrorist methods also change their shell in parallel with these developing technologies and threaten all countries in the world with a new type of terrorism, cyber-terrorism attacks. Recently, the cyber space has become an area heavily used by state-supported hacker groups as well as independent aggressive groups. The evolution of cyber threats is seen in Figure 3 (Anand, Krishnan, & Devendra, 2014).

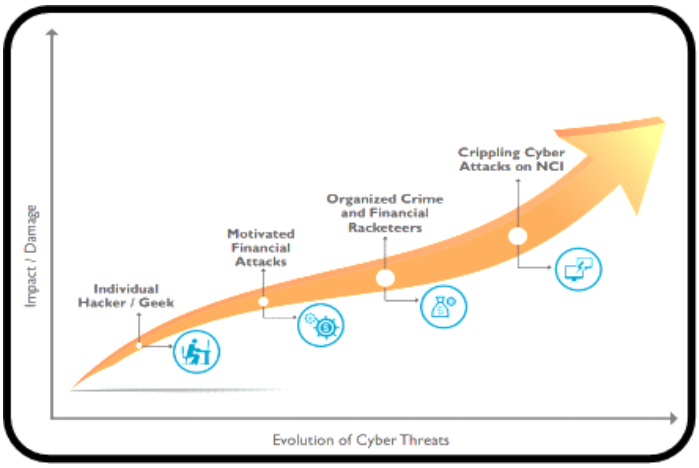

Figure 3. Evolution of cyber threads, Adapted from Anand, Krishnan, & Devendra (2014)

The terrorist incident that took place in the USA on September 11/9 affected the world and showed that terrorists and terrorist groups could act without borders using the internet and technology and obliged all the countries to learn from this event on their own and take necessary precautions. The September 11 attacks, which targeted highly strategic centers in the USA and cost the lives of thousands of people, revealed the extent of this danger in the clearest way and became a clear proof of how effectively terrorist organizations use computer systems.

Aside from the conspiracy theories about these attacks, when the elements such as breaking the Pentagon's so-called unbreakable security codes, deactivating the air radar systems, not receiving abduction signals from the pilots of the crashed planes, there is a common agreement that these are at least technology-intensive attacks. This shows that such risks are increasing for societies that are increasingly dependent on the blessings of technology.

From the perspective of terrorist organizations, it is seen that using the internet serves two different purposes. First, the internet can be used as a forum environment for the members of the organization to communicate with each other and to convey the messages they want in line with their ideologies to the masses and their sympathizers. Secondly, members of terrorist organizations can attack computer networks individually or in groups and carry out actions that are described as cyber terrorism or cyber warfare. In both forms of use, users take almost no risk, and "maximum impact with minimum risk" provides great advantages for these terrorist organizations to make their voices heard (Weimann, 2006).

By its very nature, the Internet is an ideal arena for the actions of terrorist organizations. Because it contains many opportunities and conveniences for terrorists. For example, Weimann (2006) indicates the following risks:

- Easy Access,
- Little or no regulation, censorship or other government controls,
- A huge potential user base around the World,
- High speed data transfer,
- Interactivity,
- Cheap cost,
- A multimedia environment (where video, graphics, audio and text can be combined and users can download movies, songs, books, posters, etc.),
- The ability to scope traditional mass media.

Desouza and Hensgen (2003) propose the following as a definition of cyber terrorism; "*Personally and politically motivated purposeful actions and activities aimed at the destruction of national balance and interests through the use of electronic means, computer programs or other forms of electronic communication in line with information systems*" (Desouza & Hensgen, 2003).

Cyber terrorism will be reflected as the new face of terrorism in the new century, where terrorists can open the gates of a dam with an electronic attack, enter the army's communications and leave misleading information, stop all the traffic lights of the city, paralyze the phones, turn off electricity and natural gas, complicate the computer systems, and water systems, collapse the banking and financial sector, disrupt the operation of emergency aid, police, hospitals and fire departments, upset government institutions, cause the system to come to a sudden halt (Özkışlalı, 2008).

Critical Infrastructures and Nuclear Power Plants

The concept of "Critical Infrastructure", which is defined as the physical and digital systems that are of serious importance for the smooth functioning of the economic and social life in a country, had been appeared as "infrastructure" in academic research and official studies before it was became an area of interest for national security and terrorism (Kara & Çelikkol, 2011). In this period, they are defined as facilities that host critical activities for the country's economy and need high-cost public investments at all levels

(Bennett, 2007). Protection activities and ensuring the reliability of these infrastructures, which constitute the lifeblood of modern society life, are indispensable elements for national security and economic sustainability.

According to the National Cyber Security Strategy and 2013-2014 Action Plan published by the Law No. 2013/4890 of the Council of Ministers in Turkey on 20 June 2013, critical infrastructures; They are defined as infrastructures containing information systems, when the confidentiality, integrity or accessibility of the information it processes is compromised, that can cause loss of life, large-scale economic damage, national security deficits or disruption of public order (Council of Ministers, 2013).

The features of the infrastructures that can be considered as the reasons for being critical are also the features needed to ensure the continuity of the services. Some of them can be listed as follows (Gelbstein, 2013):

- They work 24 hours a day and 7 days a week,
- They perform their operations through information technologies and networks, sensors and other devices for data collection,
- They manage physical devices such as pipeline systems, automation and signaling-based systems and robotic systems.
- They are part of service and supply chains. In case of disruption, they may be deeply affected in the end.

It is considered that the following substances can be added in addition to the features stated in Gelbstein's study;

- They assume indispensable roles in daily life,
- It has interconnections and dependencies with other infrastructures. (For example, in case of disruption in the electricity infrastructure may affect many other infrastructures.)
- They are almost impossible to replace in case of loss.

The word nuclear is of English origin, the adjective form of the noun "nucleus"[24]. TDK's Nuclear Energy Glossary defines nuclear energy as "the total energy released per unit mass of a nuclear fuel" (Boyla, M., & Canküyer, 1995). The American Energy Information Administration (EIA) refers to Nuclear Energy as small particles in molecules that make up solids, liquids and gases (EIA, 2021).

The theoretical explanation of the concept of Nuclear Energy is on the Turkish Atomic Energy Agency website, “What is Nuclear Energy?” explained in detail under the heading. Uranium, the basic component of nuclear energy; It is a heavy, slightly radioactive and metallic element used in many civil and military fields such as reactor fuel, nuclear weapons, stabilizers for aircraft tails, and armor-piercing munitions (Ferguson, 2015).

Nuclear power plants, which are the facilities where nuclear energy is converted into electrical energy, have also evolved with the developing technological infrastructures. This development extended to the fifth-generation nuclear power plants. In this context, the features of the fifth-generation power plants can be listed that they are highly economical, enriched with enhanced safety, they minimized wastes and got the capability of nuclear weapons resistance (Mariotte, 2016).

Supervisory Control and Data Acquisition

Industrial Control Systems is a concept that covers control systems that support industrial production processes, mostly used in common with SCADA (Supervisory Control and Data Acquisition) systems (Shawn, 2013).

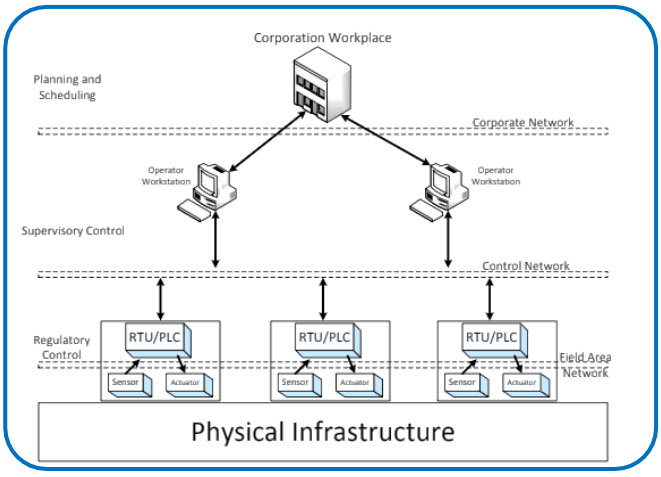

Figure 4. Architecture of an industrial control system

Figure 4 shows a common architecture of an ordinary industrial control system; at the first level the physical infrastructure is instrumented with sensors and actuators. These field devices are connected via a field area network to programmable logic controllers (PLCs) or remote terminal units (RTUs), which in the end turn implement local control actions (regulatory control). A control network carries real-time data between process controllers and operator workstations. The workstations are used in area

supervisory control, planning the physical infrastructure set points. The higher level is the site manufacturing operations, which is in charge of production control, optimizing the process, and keeping a process history (Cárdenas, Amin, & Sastry, 2008).
SCADA systems that have been in use for more than 50 years; they are not designed to meet today's security concerns. The networks used in SCADA operation are simple in structure, without encryption and at low speed. This makes it a reasonable target for cyberattacks (Eduardo, 2013). With the rapid change in technology in recent years, control systems; especially systems with open architecture with high communication capability have become more flexible/variable in terms of their interoperability and sustainability. This progress in SCADA and similar systems has also caused cyber security weakness es. The interaction between computers, communication systems and infrastructures has led to increased risks to critical infrastructures. Complex infrastructure systems; In addition to providing unique capabilities in operation, control and analysis processes, it causes vulnerabilities within the scope of cyber security (Chee-Wooi, 2010).

The Concept and Types of Nuclear Terrorism

The concept of nuclear terrorism is defined by the International Atomic Energy Agency as "'theft, sabotage, unauthorized access, illegal transfer or other malicious act involving nuclear material, other radioactive materials or their associated facilities (IAEA, 2007). With the 21st century, the world has entered a new nuclear era. While the risk of major nuclear war seems to be decreasing around the world, regional instability and the risk of the explosion of a single nuclear weapon, facility or device raise the international concerns (NTI, 2021).

The debate over the prospects of nuclear-armed terrorists dates back to the 1970s and has continued in the same vein ever since [35]. Reviving the debate has occurred since the mid-1990s, following the terrorist bombings of the World Trade Center in 1993, the Oklahoma City federal building in 1995, and the sarin gas attack in Tokyo that same year (Allison, 2018).

The 44th President of the United States, Barack Obama, also explained the threat of nuclear terrorism as follows: "The greatest threat to the security of the United States may be the possibility of a terrorist organization acquiring nuclear weapons in the near, medium and long term..."(BBC, 2010).

The types of nuclear terrorism can vary according to the way they occur. As stated in the preamble to the International Convention for the Suppression of Acts of Terrorism (ICSANT), 2005, "acts of nuclear terrorism can have serious consequences and pose a threat to international peace and security" (Allison, 2018). Nuclear terrorism can manifest itself in various ways, nuclear explosion, emission of radioactive radiation and spread of radioactive materials (UN, 2005).

Nuclear Explosion

This form of nuclear terrorism is the largest in terms of casualties, colossal destruction, human health impacts and deadly long-term effects on the environment. Identified terrorist groups can acquire and detonate any nuclear bomb in probable ways as follows [38];

- Seizing a bomb in politically unstable states/cities by stealing, deception, or by stealth entering nuclear facilities and capturing the facility,
- Receiving a bomb from a state that supports their actions,
- Purchase bombs from a supporting state or individuals with access to a nuclear device,

Radioactive Radiation Emission

This can be accomplished significantly by damaging nuclear power plants, thereby providing a wide release of radioactive material with effects similar to those experienced in the Chernobyl and Fukushima accidents. The deliberate release of radiation can occur in several ways (Dickstein, & Vanunu, 2016):

- Attacking the nuclear core of the power station by plane,
- Stand-Off missile attacks,
- With a commando type infiltration, terrorists penetrate the power station and destroy the nuclear core,
- Sabotage of persons assigned by the terrorist organization,
- Leveraging cyberterrorism remotely by taking over control systems and creating the conditions for nuclear fuel to melt down.

Spread of radioactive materials

These nuclear terrorism instruments can be carried out in a variety of ways:

- Dirty-Bomb; It is a conventional TNT bomb that activates radioactive materials. As the bomb is detonated, it has the traditional explosive effect with the spread of radioactive particles and aerosols. Dubbed a "dirty bomb," this device is viewed not as a weapon of mass destruction, but rather as a "weapon of mass disintegration" because of the fear inflicted on humans from non-susceptible radiation (Richelson, 2012).

- The spread of radioactive materials such as medical diagnosis, medical treatments and industrial radiography will expose people to radiation and cause radiation sickness. A relatively large area that may be contaminated should be evacuated and subjected to cleaning procedures. The closure of the region for a significant period of time brings with it economic, ecological and complex socio-psychological effects.
- It can also be in the form of local radioactive poisoning, by introducing radioactive sources into food and water supplies, or by concealing the source of nuclear radiation in an area where people are exposed to radiation. At this level, the foundations of nuclear terrorism also vary. In the table below, the types and causes are given together.

PRECAUTIONS AND CONCLUSION

Cyber security risks have increased in recent years and this has brought the safety of nuclear power plants back to the agenda. Turkey is struggling with many terrorist organizations in its geography. most of these organizations have the capacity to attack nuclear power plants. Necessary security measures should be taken against such attacks, both in the cyber environment and physically. Cyber terrorism is an act of hacking, blocking and computer contaminating in order to restrict legally authorized persons to access computer resources in general and to gain or obtain unauthorized access to any information which is a restricted information for the purpose of security of the state, or foreign relation (Raj & Yadav, 2022).

In cyberspace, attack always dominates defense. Therefore, the security measures taken cannot prevent threats whose existence is not yet known. The studies of domestic and foreign independent organizations operating in the field of cyber security should be supported and the reports they publish should be given due importance. Since it is not possible to talk about a national cyberspace, all efforts must be met on an international basis.

Cyber security policies should be constantly updated with an innovative approach. Changes and developments in cyberspace occur so rapidly that; this is a must situation that we keep in touch with cutting edge technology. While developing all these measures, a good balance should be established between all the areas like national security, personal rights and freedoms, democracy, investment costs and benefits. Precautions to be taken to protect critical infrastructures are vitally important. It should not be forgotten that security can be ensured when all elements in the systems fully perform their duties. However, despite all the precautions, in the event of a large-scale attack, the emergency response systems and teams will play a critical role overcoming the negative effects efficiently.

In addition to the studies still being carried out in our country, there is a need to establish an independent and central authority, whose main task is to coordinate the efforts for the protection of critical infrastructures, equipped with powers over the private sector and public institutions. In order to increase the level of cyber deterrence, necessary legal arrangements should be completed and efforts for effective international cooperation should be accelerated.

In addition, cyber security training and practices at all stages and at all levels that will increase awareness should be supported. Considering that individual studies will be insufficient in protecting critical infrastructures, it is necessary to adopt an information sharing and cooperation approach between sectors and institutions in order to create unity.

Ethics and Consent: Ethical approval was not sought for the present study because data set has not been used. Ethics committee permission is not applicable because this article does not contain any studies with human or animal subjects.

REFERENCES

Allison, G. (2018). *Nuclear terrorism: Did we beat the odds or change them*. Harvard Kennedy School Cambridge United States.

Anand, K., Krishnan, P., & Devendra, K. P. (2014). Facing the reality of cyber threats in the power sector. *Energy Policy, 65*, 126-133.

Bal, İ. (2006). *Terrorism – National and Regional Experiences in Combating Terrorism, Terrorism and Global Terrorism*, USAK Publications, Ankara.

BBC (2010). *US President Barack Obama Warns of Nuclear Terrorism*, URL: https://www.bbc.com/news/av/world-us-canada-35948480

Bennett B.T., (2007). *Understanding, Assessing and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, John Wiley & Sons, Inc., Hoboken, New Jersey, 51

Bıçakcı, S., Ergun, F. D., & Çelikpala, M. (2015). Cyber security in Turkey. *Economics and Foreign Policy Research Center (EDAM) Cyber Policy Papers Series 1*, 1-35.

Boothby, W. H. (2015). Deception in the modern, cyber battlespace. In J. D. Ohlin, K. Govern and C. Finkelstein (Eds.), *Cyberwar: Law and ethics for virtual conflicts*. New York: Oxford University Press, 195-214.

Boyla, M., & Canküyer Y. (1995). *Glossary of Nuclear Energy Terms*, Ankara: Turkish Language Association Publications.

Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. *HotSec*, *5*, 15.

Case, D. U. (2016). Analysis of the cyber-attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, *388*, 1-29.

Chee-Wooi T. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modelling, *IEEE*, 40(4), 853-865.

Council of Ministers (2013). Decision No. 2013/4890, *National Cyber Security Strategy and 2013-2014 Action Plan*, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm

Daricili, A. B. (2014). Analysis of Cyber Attacks Alleged to Originate from the Russian Federation. *Uludag University Journal of Social Sciences Institute, 7*(2), 5–7.

Daricili, A. B., & Özdal, B. (2017). Analysis of Russian Federation-Turkey Relations in the Context of the Information Warfare. *Istanbul Gelisim University Journal of Social Sciences 4*(1), 19-40.

Denk, E. (2011). Efforts to Ban nuclear weapons as a Weapon of Mass Destruction, *Ankara University Journal of Social Studies Faculty, 66*(03), 28,93-95.

Desouza, K. C., & Hensgen, T. (2003). Semiotic emergent framework to address the reality of cyberterrorism. *Technological forecasting and social change, 70*(4), 385-396.

Dickstein, P., & Vanunu, S. (2016). *Nuclear Terror: The Essentials, Threats, Effects and Resilience*.

Eduardo E. G. (2013). Designing a Security Audit Plan for a Critical Information Infrastructure, Christopher Laing et al. (Ed.), *Securing Critical Infrastructures and Critical Control Systems*, IGI Global, 262-285.

EIA (2021). Nuclear energy is energy in the core of an atom https://www.eia.gov/energyexplained/index.cfm?page=nuclear_home#tab1

Falkenrath, N., and Thayer, A. A. H. (1998). Nuclear, Biological and Chemical Terrorism and Covert Attack., Cambridge Mass., MIT Press.

Ferguson, C. D. (2015), *Nuclear Energy: What Everyone Should Know, Ankara, Buzdagi Publishing House, First Edition*.

Gelbstein, E. E. (2013). Designing a Security Audit Plan for a Critical Information Infrastructure, Christopher Laing et al. (Ed.), *Securing Critical Infrastructures and Critical Control Systems*, IGI Global, 263.

Güzel, C. (2002). Fear of Fear: Terrorism. *Terror in the Face of Erased Faces*, 7-19.

Hubbert, M. K. (1956). *Nuclear Energy and Fossil Fuels*, Houston, Texas: Shell Development Company Exploration and Production Research Division, No. 95, p.23.

IAEA (2007). *Concept and Terms: IAEA Safety Standards*, URL: http://www-ns.iaea.org/standards/concepts-terms.asp

IAEA (2021). https://www.iaea.org/resources/databases/international-nuclear-and-radiological-event-scale.

Kara, M., & Çelikkol, S. (2011). Critical Infrastructures: Electricity Generation and Distribution Systems SCADA Security, 25-26., *IV. Network and Information Security Symposium Proceedings*, TMMOB Chamber of Electrical Engineers, Ankara.

Mariotte, M. (2016). *Wishful Thinking: the Basis of New Nuclear Economics*, https://safeenergy.org/2016/03/28/wishful-thinking-the-basis-of-new-nuclear/#more-13790

NATO Review Magazine (2011). New Threats: The Cyber-Dimension: URL: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm

Ng Eng H. (2016). Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply Debate 2016, posted 8 Apr 2016, http://www.mindef.gov.sg/content/imindef/ press_room/official_releases.sp.html.

NRC (2023). International Nuclear and Radiological Event Scale https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/emerg-classification/event-scale.html

NTI (2021). Global Nuclear Policy: reducing reliance on nuclear weapons, preventing their use and their spread, and ultimately ending them as a threat to the World, URL: http://www.nti.org/ about/global-nuclear -policy, Last Accessed: 21.09.2021

Özkışlalı, G. (2008). Globalization, the Internet and the Changing Face of Terrorism; Cyber Terrorism. *Published Master's Thesis*. Hacettepe SBE, Ankara, 71.

Raj, P., & Yadav S. (2022). Cyber Terrorism: A Threat to Cyber World. *Emerging Trends in Technology & its Impact on Law*, 1.

Richelson, J. T. (2012). Nuclear Terrorism: How Big a Threat?. *National Security Archive Electronic Briefing Book*, 388.

Shawn C. (2013). *Industrial Control Systems Cyber Security Presentation*, ASIS: 4th Middle East Security Conference, Dubai.

Şimşek, M. (2016). Terrorism: A Conceptual Study. Academic Perspective. *International Refereed Journal of Social Sciences, 54*, 319-335.

UN (2005). *International Convention on Suppression of Acts of Nuclear Terrorism*, URL: http://www.un-documents.net/icsant.htm, Last Accessed: 21.05.2021

UN Climate Summit (2014). https://www.un.org/climatechange/summit

Valo, J. (2014). Cyber Attacks and the Use of Force in International Law, University of Helsinki, *Unpublished Master's thesis*. https://www.iaea.org/resources/databases/international-nuclear-and-radiological-event-scale.

Wardlaw, G. (1989). *Political terrorism: Theory, tactics and counter-measures*. Cambridge University Press.

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. US Institute of Peace Press.