A PRIMER ON CYBER SECURITY IN TURKEY AND THE CASE OF NUCLEAR POWER

Centre for Economics and Foreign Policy Studies
edam
The Centre for Economics and Foreign Policy Studies

The Centre for Economics and Foreign Policy Studies

A PRIMER ON CYBER SECURITY IN TURKEY AND THE CASE OF NUCLEAR POWER

Editor: Sinan Ülgen, EDAM

Associate Editor : Grace Kim, EDAM

Researchers:

Assoc. Prof. Salih Bıçakcı, Kadir Has University

Prof. Mitat Çelikpala, Kadir Has University

Assoc. Prof. Ahmet Kasım Han, Kadir Has University, EDAM

Asst. Prof. Can Kasapoğlu, EDAM

F. Doruk Ergun, EDAM

This research has been funded with support from the "The William and Flora Hewlett Foundation".

The views expressed in this report are entirely the authors' own and not those of the The William and Flora Hewlett Foundation.

Hare Sokak No: 16,

Akatlar 34335 Istanbul

Tel: +90 212 352 18 54

Email: info@edam.org.tr

www.edam.org.tr

First Publication, Istanbul, December 2015

ISBN: 978-9944-0133-7-6

Cover Design: Güngör Genç

A PRIMER ON CYBER SECURITY IN TURKEY

AND THE CASE OF NUCLEAR POWER

Centre for Economics and Foreign Policy Studies
edam
The Centre for Economics and Foreign Policy Studies

About EDAM

The Centre for Economics and Foreign Policy Studies (EDAM) is an Istanbul based independent think-tank. EDAM's main areas of research are:

- Foreign policy and security,
- Turkey-EU relations,
- Energy and climate change policies,
- Economics and globalization,
- Arms control & non-proliferation,
- Cyber policy.

EDAM aims to contribute to the policy making process within and outside Turkey by producing and disseminating research on the policy areas that are shaping Turkey's position within the emerging global order. In addition to conducting research in these fields, EDAM organizes conferences and roundtable meetings. Additionally, EDAM cooperates with numerous domestic and international to conduct joint-research and publications.

Organizational Structure

EDAM brings together a network of members from multiple sectors of Turkish society including academia, civil society, media and business. This diversified representation enables EDAM to create a productive and effective platform through which different visions and perspectives can interact.

EDAM's Executive and Supervisory Board consists of members from the academia, business community, civil society and media. Board members are assigned to supervise research projects in order to ensure their academic and editorial quality. While EDAM staffs a small number of permanent researchers, it also reaches out to select Turkish and international researchers to form ad hoc research teams based on the projects that it undertakes.

EDAM relies on project-based funding, matching grants and institutional donations in order to carry out its projects, and hence maintains its editorial independence. Additionally, EDAM undertakes joint projects and research with various civil society and international organizations on the basis of the principle of shared funding.

About the Authors

Assoc. Prof. Ahmet K. Han is with the faculty of International Relations at Kadir Has University in Istanbul. His research interests are strategic thinking, negotiations and foreign policy analysis. Dr. Han holds a B.A. in economics and international relations, an MA on political history and a Ph. D. on international relations from the Istanbul University and has studied negotiations in Harvard. He has been awarded a "Young Leaders of Europe" grant on U.S. Foreign policy by the Department of State of the U.S.A. and has been an observer for NATO on the state of the NATO/ ISAF Operation in Afghanistan twice, in 2005 and 2011. He has published extensively on Afghanistan, geo-strategy of energy politics, US Foreign Policy and Turkish foreign policy. Dr. Han has worked as a columnist in Turkish dailies Radikal and Referans. He is also the chief editorial advisor of the Turkish edition of the New Perspectives Quarterly. Dr. Han has extensive experience as an adviser and consultant to private sector in the field of strategic business development and negotiations. He has also served as the International Relations Advisor for Turkish Exporters Assembly, the umbrella organization of Turkey's exporting industries between 2003 - 2006. He has lectured for and held academic posts in Istanbul University, Bilgi University, İstanbul Commerce University, Turkish Armed Forces (TAF) War Academy (Staff College) and Air Force War College. From 2005 to 2008 Dr. Han was responsible for structuring and teaching of the "International Negotiation Strategies" course module for TAF, a must course for all senior officers assigned to international military postings including NATO. He has also served as a visiting scholar in University of St. Andrews's Center for Syrian Studies in Scotland in 2011.

Assoc. Prof. Salih Bıçakcı is Associate Professor of International Relations at Kadir Has University, Istanbul. He completed his B.A. on History at Marmara University Education Faculty in 1994, and his M.A. at Marmara University Turcology Research Institute on "Uzbek Migrants to Turkey" in 1996. Bıçakcı completed the Humanities Computing program at Bergen University in Norway in 1999 and received his PhD from Tel Aviv University in Israel in 2004. Dr. Bıçakcı began his academic career at Işık University and took part in numerous academic projects on identity, security and terrorism. He has thought classes in several national and international universities on the Middle East in International Politics, International Security, International Relations Theory and Turkish Foreign Policy. He has made evaluations and presentations on cyber security at the NATO Defence Against Terrorism Centre of Excellence (COEDAT), NATO Command and Control Centre of Excellence (C2COE) and NATO Maritime Security Centre of Excellence. He has though Cyber Security and Middle Eastern Security courses at the Armed Forces Academy of the Turkish War College. He has presented on international security and cyber security in several international academic conferences. He has also published articles on these issues in various academic journals.

Prof. Mitat Çelikpala is Professor of International Relations at Kadir Has University, Istanbul where he teaches graduate and undergraduate courses on Eurasian Security, energy and critical infrastructure security, Turkish Foreign Policy and the Caucasus politics, security and history, and supervises doctoral dissertations in these areas. His areas of expertise are the Caucasus, North Caucasian Diaspora, people and security in the Caucasus and Black Sea regions, Turkish-Russian relations, energy security and critical infrastructure protection. In addition to Kadir Has University, he lectured in Bilgi University, Turkish War College and Turkish National Security and Military academies on Turkish foreign policy, politics, history and security in the Caucasus and Central Asia and Turkish political structure and life. He served as an academic advisor to NATO's Center of Excellence Defense against Terrorism in Ankara, especially on the critical infrastructure protection. He has several numbers of published academic articles and media coverage and analyses on above-mentioned areas.

Asst. Prof. Dr. Can Kasapoğlu is a Research Fellow at EDAM. He is a War Studies and Security Studies academician and military analyst. Dr. Kasapoglu gained his Ph.D. degree from the Turkish War College-Strategic Researches Institute in 2011 by successfully defending his dissertation on Assessing Conventional Forces in Low Intensity Conflicts, and his M.Sc. degree from the Turkish Military Academy-Defense Sciences Institute in 2008 with his thesis on Turkish armed resistance and irregular warfare activities in Cyprus before 1974. Asst. Prof .Dr. Can Kasapoglu served at several reputable think-tanks as visiting researcher, including the BESA Center in Israel where he worked on Turkish - Israeli relations and strategic affairs in the Middle East, and the FRS in France where he worked on strategic weapons proliferation in the Middle East and Turkey's missile defense project, the T-Loramids. Assistant Prof. Dr. Can Kasapoglu specializes in strategic weapon systems with a special focus on chemical & biological warfare, missile proliferation and missile defense, hybrid warfare, NATO's collective defense and cooperative security issues, Turkish - Israeli relations, global and regional military modernization trends, geopolitics, and open-source strategic intelligence. Dr. Kasapoglu has spoken at the NATO Defense College, Baltic Defense College, annual conference of International Society of Military Sciences and other reputable military sciences platforms. He taught courses of War and Strategy Theory, Global Peace and Security, Civil-Military Relations, Contemporary Terrorism Studies, and Geopolitics at Girne American University. Dr. Kasapoglu is a frequent contributor to the reputable Israeli daily, the Jerusalem Post. He is currently serving as a visiting scholar at NATO Defense College in Rome.

F. Doruk Ergun is a Research Fellow at the Centre for Economics and Foreign Policy Studies (EDAM), where he works on Turkish foreign policy and security issues. He was previously a research assistant at the NATO Parliamentary Assembly. Ergun received his MA in international affairs with a focus on international security studies from the George Washington University in 2011 and his BA in social and political sciences from Sabancı University in 2009.

Index

INTRODUCTION

Rising threats in cyber security motivated EDAM to prepare this report that covers the basics of cyber security with a focus on critical infrastructure and especially nuclear power plants. This collection includes four complementary chapters to help the reader understand Turkey's cyber security challenges with a focus on nuclear power plants as components of the country's critical infrastructure.

The first chapter by Can Kasapoğlu introduces the concept of cyberwarfare as the next Revolution in Military Affairs (RMA). The chapter sets out current and potential hostile cyber trends and emerging state capabilities. It analyzes cyberspace as the fifth domain of fighting wars with a special focus on network-centric warfare. It also identifies non-state threats from Turkey's perspective.

The second chapter by Salih Bıçakcı, Doruk Ergun and Mitat Çelikpala examines the cyber security scene in Turkey. It investigates local actors that are currently "active" in the cyber space. Some of these actors include political hacker organizations, such as Redhack and Ayyıldız Team, and the organizations that the Turkish state has put in charge of cyber defense, such as the cyber divisions under the Turkish National Intelligence Organization (MIT) and the Turkish Armed Forces.

The third chapter by Ahmet Han and Mitat Çelikpala provides a conceptual introduction to cyber space, cyber attackers and cyber security, and their place in the context of critical infrastructure and nuclear power plants. It then focuses on the international aspect of nuclear power plant cyber security by exploring the cases of the United States, as one of the countries with the most matured organizational and regulatory structure on the field, and the International Atomic Energy Agency, as the key international organization on nuclear safety and security. The chapter concludes by drawing lessons and suggestions for Turkey.

The fourth chapter and final chapter by Salih Bıçakçı clarifies the concept of cyber-security and its relevance to nuclear power plants and facilities. It examines cyber incidents that have affected nuclear power plants and efforts on the international level to protect these critical infrastructures. Since most of the nuclear power plants are functioning over the industrial control and supervisory control and data acquisition (SCADA) systems, the interaction of the workforce with SCADAs and computers are critical for the safety and security of nuclear power plants. After covering the challenges of managing a nuclear power plant's security, the chapter evaluates Turkey's cyber defense capabilities from this perspective. It analyzes the country's current capabilities in terms of ensuring cyber security resilience. It summarizes Ankara's current cyber policies by assessing the organizations responsible for dealing with cyber security and cyber defense.

We hope that this compilation of original research will provide a useful and much needed background to the emerging discussion on cyber security, critical infrastructure and nuclear power in the Turkish context.

TURKEY'S FUTURE CYBER DEFENSE LANDSCAPE

Asst. Prof. Can Kasapoğlu

Research Fellow – EDAM

1. Introduction

Turkey's internet usage is rapidly growing through social media enhancements, private sectors utilization, and state-owned enterprise networks. Growing interconnectedness, Turkish critical national infrastructure's dependence on networks, and cyber attacks have introduced the complex realities of cyber security to the Turkish national security agenda. In this context, Ankara initiated the first legal framework for national cyber security coordination, The Decree on Execution and Coordination of National Cyber Security Affairs (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar), on October 20, 2012.[1] Furthermore, the "National Action Plan for Cyber Security" was adopted in 2013. The Action Plan underlined the hardships of detecting cyber attacks and placed special emphasis on the protection of critical national infrastructure and sensitive information.[2] In tandem, the Turkish administration launched the first inter-agency-level cyber drills in 2011, and a cyber command was established within the Turkish Armed Forces.[3]

Despite these efforts, cyber threats have been growing more swiftly than Turkish countermeasures. As a NATO member state, Ankara has to both ensure its own cyber security and contribute to the alliance's cyber defense. In doing so, both Turkey and NATO allies will need to develop a crystal clear understanding of cyber warfare, both in offensive and defensive terms.

It should be mentioned that even a purely policy-oriented study on cyber warfare requires vigorous theoretical conceptualization across military and security domains. For a comprehensive analysis of Western cyber security doctrines and concepts suggests that Turkey has a long way to go in perfecting the standardization of its threat calculus emanating from hostile cyber activity. Second, cyber warfare resembles air power discussions debating whether or not practice was derived from theory through creative conceptualization. In this regard, a 2002 study from the Center for Strategic and International Studies (CSIS) draws attention to a comparative assessment between cyber terrorism and the World War II air power theory and application:

> "Cyber-terrorism is not the first time a new technology has been seized upon as creating a strategic vulnerability. While the match between theories of cyber-warfare and air power is not precise, a comparison of the two is useful. In reaction to the First World War, European strategists like Douhet and Trenchard argued that aerial bombing attacks against critical infrastructure well behind the front lines would disrupt and cripple an enemies' capacity to wage war. Their theories were put to the test by the U.S. Army and Royal Air Forces during World War II in strategic bombing campaigns aimed at destroying electrical power, transportation and manufacturing facilities. Much of the first tranche of literature on cyber attacks resembles in many ways (and owes an unspoken debt to) the early literature on strategic bombing."[4]

In order to develop a good understanding of Turkey's vulnerabilities in confronting possible cyber attacks, one should first contextually explain the correlation between emerging technological trends and threat perceptions and how they shape future warfare. The following section will first shed light on the effect of cyber capabilities on warfare as the next Revolution in Military Affairs (RMA). It will then lay out current and potential hostile cyber trends and the state capabilities that Turkey and NATO should consider. The third section will explain cyber space as the fifth domain of fighting wars with a special focus on network-centric warfare. The fourth section will focus on non-state threats and provide a net assessment for Turkey. Finally, the study will present its conclusions and policy recommendations.

2. Conceptualizing the "Cyber-Blitz": Cyber Warfare as the Next RMA

Built on Soviet Military Chief Nikolai Ogarkov's concept of "military technological revolution," Revolution in Military Affairs (RMA) connotes more than mere technological shifts. RMA can be described as a decisive breakthrough in combat-effectiveness due to drastic changes in technology, strategic culture, organization, doctrine, training, strategy, and tactics. It is the application of technology into military systems combined with innovative concepts and organizational adaptation.[5] In Andrew Krepinevich's famous work on RMA titled "From Cavalry to Computer," he draws attention to computer-assisted design and manufacturing effects in advanced simulations, thereby, enhancing military organizations' abilities.[6]

Within this framework, it could be argued that cyber warfare should be considered as the next – or the current – Revolution in Military Affairs. In this regard, operating advanced battle networks to detect, identify, and track targets and managing intelligence-surveillance-reconnaissance (ISR) systems necessitate access to orbital and cyber dimensions of the global commons. As a result, the cyber arms race has already brought these dimensions to the forefront through counter-network attacks, anti-satellite systems, and directed-energy weapons systems. In fact, competition in space and cyber space domains, which advanced arms such as smart munitions depend on, would have direct and significant consequences on battlespace management, command & control (C2), and target acquisition with regard to information flow about real time and space[7].

Related but not limited to cyber warfare, cyber espionage is also an emerging field in which cyber-technological developments are translated into security tools. Cyber-technological breakthroughs made spying possible without leaving one's home country, and in return forced nations to run counter-espionage activities in the cyber domain. Furthermore, a new "non-profit" cyber espionage sector has already become efficient through public release of sensitive information[8].

One should avoid rigid distinctions between cyber functions when considering future warfare scenarios and strategic forecasting. In fact, cyber warfare blurs the "civilian-military divide." The product of decades of innovation and experimentation, cyber weapons and robotics will constitute the main pillars of the next RMA. These are all technology-intensive assets that are products of decades-long innovation and experimentation[9].

In order to develop an historical and policy-oriented context on cyber warfare, continuing to use military history to explain the effects of information superiority on the battlefield is key.

Without a doubt, new war-fighting capabilities have always brought critical superiorities as well as critical vulnerabilities. For example, Hannibal's war elephants were the heaviest and most formidable asset on the battlefield. However, at the Battle of Zama, Scipio Africanus's javelin units, the velites, blinded the elephants from close range, turning the war elephants into a threat to following friendly units rather than a reliable heavy vanguard.[10] The same could be said for the information and computer networks of modern armies. As modern armies enjoy better advantages in information superiority thanks to computer networks and advanced network infrastructures, these advantages also create opportunities for opponents to exploit "new attack surfaces."[11] Neither the Turkish Armed Forces nor NATO are exceptions.

From a military standpoint, it would be fair to argue that cyber warfare depends on information superiority and control over the battlespace. John Arquilla and David Ronfeldt analyzed the Mongolian hordes of the 13th century to conceptualize cyber warfare. According to the authors, although the Mongolians were frequently outnumbered, Mongolians' light and swift cavalry enabled the generals of the steppes to utilize information superiority through systematic command & communications.[12] Resembling the Mongolians' success in translating information superiority into combat capabilities, cyber war, as described by Arquilla and Ronfeldt, is "…conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first."[13]

Although much has been built on Arquilla and Ronfeldt's work their quote from Carl von Clausewitz at the beginning of the study depicts cyber warfare's transformational effects on war: "…knowledge must become capability."[14] They underline that having the best information about the battlefield is as crucial as putting more labor, technology, and capital in the battlefield.[15]

2.1. Tangibility and Visibility in the Next RMA

Cyber warfare entails not only a technological breakthrough but also a set of drastic improvements in organization, doctrine, concept, and military thought. American cyber defense spending hit a historic peak of $4.7 billion USD in President Obama's 2014 budget with an increase of some $800 million.[16] Comparatively, Washington's 2014 cyber defense budget was larger than what Denmark, Finland, or Jordan spent on overall defense in 2013.[17]

Re-organization within the U.S. Army accompanied the budgetary shift. In 2009, then U.S. Secretary of Defense Robert Gates directed the U.S. Strategic Command to establish Cyber Command (USCYBERCOM), which achieved initial operational capability on May 21, 2010.[18] The new command's mission statement indicates that USCYBERCOM "plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyber space operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyber space and deny the same to our adversaries."[19]

Similarly, the Israeli Chief of Staff Gadi Eizenkot decided to establish a branch within the Israeli Defense Forces (IDF) that would consolidate all the nation's cyber capabilities.[20] The news of the creation of Israeli Cyber Command surfaced around the same time as Defense Minister Moshe Ya'alon's public confirmation that Israel had been targeted by Iranian cyber attacks during the 2014 Gaza War, albeit with no significant damage.[21]

Russia, the usual suspect behind cyber operations against Estonia, Georgia, and Ukraine, is another country expanding its cyber capabilities. Moscow approaches cyber operations as part of its foreign policy and hybrid warfare strategies.[22] Seeing as how cyber offense played a battering ram role in the Russian aggression in Ukraine, it seems that offensive cyber operations have already been integrated into Moscow's military thought and even doctrine. In order to counter the cyber threat posed by Russia, NATO established the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, in 2008. The Center's mission is to "enhance

the capability, cooperation, and information sharing among NATO, its member nations, and partners in cyber defense…"[23] Furthermore, following the 2014 Wales Summit, NATO put more emphasis on cyber defense and security by endorsing a policy that confirmed cyber defense as a core task of collective defense.[24]

China can also be regarded as a rising power in cyber space. Chinese cyber warfare programs are more centered on fostering offensive capabilities compared to other players in the cyber domain. There are even analyses stating that modern Chinese cyber capabilities improved upon the KGB's industrial espionage methods and pose the gravest threat to U.S. technological superiority.[25] In terms of China's cyber doctrinal order of battle, it is believed that Unit 61398, a special cyber team under the Chinese General Staff's 3rd Department, is responsible for overseeing "computer network operations." China Telecom is reported to have provided special fiber optic communications for the unit, and the unit's personnel size is estimated to be between hundreds to thousands of soldiers.[26] The Chinese General Staff directly answers to the Communist Party's Central Military Commission. Thus, Unit 61398's cyber activities are subject to the highest level of political oversight and the highly centralized decision-making system under communist China.

Unit 61398's cyber activities can arguably be classified as an Advanced Persistent Threat (APT). APT "represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms."[27] APT's are one of the most important emerging threats as potential adversaries seek to harvest sensitive information using this method, targeting both industry and government.[28]

From a broader perspective, it would be fair to say that the People's Liberation Army's (PLA) warfighting concepts are evolving into the systematic incorporation of cyber warfare, signal intelligence, anti-satellite capabilities, psychological warfare, and information operations. The PLA's military geopolitical reading extends to battlespaces that are created by the electromagnetic spectrum, cyber space, and space, all of which culminates in a final "virtual battlespace."[29] In practice, such an approach would introduce a Chinese version of joint warfare and combined arms operations that includes electronic warfare, precision strike, and cyber warfare. Building on the Soviet concept of radio electronic combat (REC) during the Cold War, Chinese military strategists assess that by expanding the limited Soviet REC approach, which was only applied to limited battlespace or limited tactical situations, the PLA could elevate the REC approach to the strategic level. The key element of this approach is the integration of space and cyber space.[30]

Last but not least, the Iranians enter the picture as an emerging actor with high ambitions in cyber space. Like many other authoritarian regimes, Iranian cyber efforts initially focused on internal security. Following the 2009 protests, Tehran installed a sophisticated, Chinese-built surveillance system to monitor all communication within the country.[31] After experiencing the disruptive effects of cyber technology following Stuxnet, Supreme Leader Ayatollah Ali Khamenei authorized the establishment of a new Supreme Council of Cyber space in 2011 with a focus on both defensive and offensive duties. The Council consists of several intelligence and security branches as well as the ministries of culture and communications. The Islamic Revolutionary Guards Corps (IRGC) plays an important role in the Iranian cyber security apparatus. Moreover, Iran held its first cyber drill in 2012 and increased its cyber operations budget by $20 million since President Rouhani assumed office.[32]

Following Stuxnet's relative success in ruining about 20% of the nation's nuclear capabilities, Tehran began to more heavily invest in an assertive program to train "cyber warriors."[33] Within

this program and among these cyber warriors, "there is quite a substantial hacking community within Iran. The skills of these hackers range from unskilled amateurs that can use software tools that are developed to exploit already known vulnerabilities to skilled hackers that find new vulnerabilities and exploitations."[34] The featured members of the Iranian hacking community are Iran Babol Hackers Security Team, Ashiyane Digital Security Team, and Iran Hackers Sabotage Team.[35] Reported Iranian cyber attacks on Saudi Aramco and the Qatari RasGas showed the magnitude of Iranian cyber offensive capabilities in regards to sensitive energy assets in the Gulf region. Similarly, during the cyber attacks on the two key Gulf Arab energy firms, some American banks were also targeted by denial of service attacks.[36]

In light of this overview, it could be argued that Turkey and NATO will face more menacing cyber challenges in the 21st century. Apart from a state actor's cyber warfare capabilities, all the aforementioned capabilities could be translated into cyber proxy war threats within emerging security challenges. State actors could opt for launching false flag operations, use hackers, as well as third state parties. Such a complex threat landscape poses threats to Turkish national security as well as NATO cooperative security and collective defense. Along with actor-based assessments, cyber efforts should focus on cyber warfare as the fifth domain of war and how its effects are translated into a network-centric warfare environment, enabling Turkish and NATO allies to better understand the cyber threat calculus.

3. Conceptualizing the Fifth Domain of War: Cyber space and Network-Centric Warfare

The information systems environment that will form the cyber battlespace consists of three layers: physical, synaptic, and semantic. Cyber offensive capabilities and support operations for network-centric operations will operate in this three-layered landscape. The physical layer refers to hardware, computers, cables, and routers with circulation varying from radio frequency to energy to electrical signals and photons.[37]

This layer is vulnerable to kinetic military actions, especially given the current trends in precision-guided munitions (PGM), deep strike options, Special Forces operations, and stealth capabilities. The syntactic layer refers to the orders that instruct information systems with tasks that circulate through the physical system.[38] This layer is and will remain vulnerable to hostile hacker activity, and defensive cyber capabilities will be needed to protect information systems. Finally, "the semantic layer provides meaning to the information content," thus making it vulnerable to deceptive activities.[39] In this respect, it should be underlined that contemporary military parameters are harbingers of "non-obvious wars" in which "identity of the warring side and even the very fact of warfare are completely ambiguous" due to technological and organizational shifts.[40] Thus, this paper utilizes such a paradigm to categorize cyber warfare's role in future network-centric operations.

Cyber warfare's battlespace categorization aids decision makers in formulating future cyber warfare operations and topography. Although cyber space is perceived as a new domain of war, the physical layer of the information systems environment still necessitate the involvement of traditional land, naval, air, and space assets.. Furthermore, cyber operations in synaptic and semantic layers are tightly connected as hostile hacker activity might couple with non-kinetic and deceptive psychological operations. Hence a new form of "combined operations" in cyber space, which would simultaneously take place in the physical, syntactic, and semantic layers, could drastically alter the scope of offensive and defensive cyber operations.

Apart from its multi-layered landscape and topography given hitherto, perceiving cyber space as the fifth and new domain of war does not necessarily mean that such a categorization will isolate cyber space from other domains of war. On the contrary, this study anticipates that cyber space and cyber warfare will most probably play essential roles in future network-centric operations. As indicated in a 2012 study by Liles et al., applying military principles to cyber warfare means the

> "…layering of the digital information technology environment upon the weapons platforms of the Army. This gives the nation-state a significant information edge over the adversary. Layering cyber space capabilities onto terrestrial weapons platforms is not functionally different from using naval forces to support land forces. Another example might be space assets, such as reconnaissance satellites, that support all natural domains (air, land, sea) similar to how cyber supports command and control."[41]

The rise of network-centric warfare will give cyber assets a great advantage in terms of operational and tactical capabilities. The successful outcome of network-centric operations and warfare depends on information superiority over the adversary through generating combat power by effectively linking actors, sensors, and decision-makers.[42] From a military standpoint, such an approach drastically alters the correlation between time, battlespace, and deployed

forces. In other words, thanks to network-centric operations, widely dispersed forces can now be used in expanded battlespaces and enjoy improved communications and synchronization.[43]

Finally, it should be underlined that the antithesis of network-centric warfare, not only in terms of military technology but also military thought, is a platform-centric approach. Colonel Alvin Bailey from the U.S. Army formulates key limitations of platform centric warfare as follows:

> "The US Army has the most feared, sophisticated, and lethal armored vehicles in the world. The Abrams Tank and Bradley Fighting Vehicle moving at high rates of speed across the desert, brings fear to the US adversaries. The implementation of these platforms have been so successful, the enemies do not get themselves into a position where they are forced to engage US armored vehicles in the open desert. Although the Army has successfully used Platform Centric Warfare for many years, there are several problems with relying on them in future military operations. It is difficult to rapidly deploy these traditionally large platforms. The US Army has not successfully automated the platform utilizing modern technology across the entire force. Stovepiping of information presents information sharing between systems. Finally, bandwidth constraints have limited information sharing using existing technologies. The aforementioned key issues will be examined as they reveal limitations in the current Platform Centric Warfare approach and the need to pursue an alternative conceptual framework."[44]

Therefore, unless Turkey and its allies develop adequate offensive and defensive cyber capabilities, Turkey's network-centric concepts can be inevitably rendered abortive in future battlegrounds and reduced to "accidental platform-centric" concepts.

4. Cyber Weapons as Strategic Weapons: Rethinking a Capabilities-Based Model for Turkish and NATO Cyber Security

Another debate on cyber weapons is centered on whether or not they can be categorized as strategic weapons. It is vital to understand the nature and characteristics of the weapons systems to assess the threat perceptions for Turkey and its allies. The complex characteristics of strategic weapons include catastrophic destructive capabilities, psychological terror-weapon effects, and assured destruction.

According to Tabansky, the right way to conceptualize cyber warfare should be akin to the approach to any new weapon system. Analysts should work with familiar variables such as range, extent of destruction, and cost and political limitations of use.[45] Additionally, the first-strike advantage is fairly clear in cyber warfare. In this regard, the benefits of cyber technology in targeting command & control structures make attack more appealing than defense, thereby, curbing the adversary's retaliation capacity.[46] The availability of a broad target set, such as critical national infrastructure, the banking and finance system, sensitive communications, and Internet use, also makes cyber weapons even more menacing than conventional arms.

In tandem with the proposed methodology above, a Center for Strategic and Budgetary Assessments (CSBA) report considers a similar way to judge cyber weapons and cyber warfare:

> "One important quality that both nuclear and cyber weapons share is that the competition favors the offense. Put another way, given equal resources, the side that invests in offense has the advantage. With respect to the nuclear competition, the U.S. military, generally acknowledged to be the world's most technically sophisticated, has yet to develop an effective defense against nuclear ballistic missile attack despite over a half century of effort and hundreds of billions of dollars. Similarly, it appears that it is far less taxing to develop an offensive cyber capability than it is to defend against the various forms of cyber intrusion and attack. Were the case otherwise, cyber economic warfare, cyber crime, and cyber espionage would not be the problems they are."[47]

However, one cannot yet categorize cyber weapons as "perfect strategic weapon systems." If so, how can we categorize these emerging military and weaponized assets? A 2012 Royal United Services Institute (RUSI) study argues that high-potential cyber weapons can be compared to "anti-radiation missiles" that are "fire-and-forget" weapon systems, which require specific target intelligence to be programmed into the asset.[48] From a technical perspective, advanced anti-radiation missiles are designed to destroy integrated enemy air defense by employing emitter geo-location, active terminal guidance, and network integrated communications.[49] In military planning, anti-radiation missiles are mostly used in SEAD (suppression of enemy air defenses) missions to pave the ground for larger follow-up air strikes.

On the one end of the spectrum, cyber weapons are mostly malicious software, known as malware, that are able to influence systems but incapable of efficiently penetrating them for inflicting serious harm. The "high-potential end" of the spectrum refers to the malware that are capable of penetrating protected systems to inflict serious damage through autonomous hostile conduct.[50] Thus, as the potential for cyber weapons' ability to paralyze an adversary,

right before an engagement, rises, the anti-radiation missile analogy becomes more appropriate.

Without a doubt, cyber warfare enables belligerents to strike strategic and tactical targets remotely, while minimizing operational risks during a campaign. This advantage depends on the ambiguity of a cyber attack, which forces the victim to distinguish between an attack and a technical glitch, whilst rendering it difficult to connect an event with a result.[51]

From a military intelligence perspective, cyber's detection and identification of strikes shows similarities to those of biological warfare. At the outset of a cyber attack, the utmost priority is given to efficiently detecting and identifying the hostile activity and to take the necessary countermeasures.[52] Like biological weapons programs, cyber weapons programs are easy to hide and offensive capabilities can be fostered through dual-use technological improvements. As initial detectability varies by bio-agent, the same principle can be used to judge cyber-agents. Due to the involvement of private sector and individual contractors, identifying belligerents is highly demanding in the cyber warfare battleground.

As a result, like biological weapons nonproliferation measures, cyber weapons and cyber warfare necessitates advanced military intelligence capabilities to monitor state and non-state actors at the same time. The intelligence requirements in both biological warfare and cyber warfare should deal with a broad spectrum of capabilities and intentions, which have to cover commercially available tools for individuals, small extremist groups, and even lone-wolf aggressors.

5. Non-State Threat Assessment for Turkey: A Volatile Cyber Security Environment

As states in the Middle East are in decline in a Weberian sense, non-state violent groups show significant interest in cyber operations, leading to the spillover of conflict into cyber space. In this regard, the Syrian Electronic Army (SEA) deserves attention. The cyber operations group's main core is located in Dubai with other members in Syria. Funded by Bashar Assad's cousin Rami Makhlouf, The SEA is called "a real army in virtual reality" by the Syrian dictator Bashar al-Assad.[53] IHS Jane's intelligence briefing suggests that the modus operandi of the SEA is mainly carried out via "phishing emails, luring recipients into clicking links or entering login details for sites the SEA is trying to vandalize, which it captures."[54] Its cyber operations record has a sensational target set that includes The Washington Post, UNICEF, the U.S. Army website, Le Monde, International Business Times, and Reuters.[55] The group even has a volunteering section on its homepage along with a link for leaks.[56]

Open source intelligence suggests that the SEA is a cyber proxy war campaign by the Baathist Regime. According to The New York Times, "If researchers prove the Assad regime is closely tied to the group, foreign governments may choose to respond because the attacks have real-world consequences. The S.E.A. nearly crashed the stock market, for example, by planting false tales of White House explosions in a recent hijacking of The A.P.'s Twitter feed."[57]

It is known that the Syrian Computer Society (SCS), a tech group that was established by the late Bassel al-Assad and previously headed by Bashar al-Assad, provided the basis for SEA.[58] Furthermore, the Rami Makhlouf's connection warrants attention. The Makhlouf family, to which Bashar al-Assad's mother Anisah belongs, has always been a key player in the regime's inner circle. For example, Rami Makhlouf's brother, Hafez Makhlouf, was head of the internal branch of Syria's notorious General Security Directorate. Moreover, generals from the Makhlouf line, such as the former commander of the elite 105th Brigade of the Presidential Guard Brigadier General Talal Makhlouf hold an important position within the regime's military structure and are also accused of systematic crimes against humanity during the course of the civil war.[59] Coming from such a dark family legacy, Rami Makhlouf was seen as the key financial powerhouse of the Baathist regime and served as "an interlocutor between foreign investors and Syrian companies."[60]

At this point, the role and evolution of the SCS becomes crucial. Bashar al-Assad assumed the presidency of the Syrian Computer Society in the 1990s. The project was designed to serve two purposes, by Bashar's late brother Basel in 1989, who died in a car accident in 1994. On the one hand, it was a controlled and gradual charm offensive and social development program that aimed to introduce computers and internet into daily Syrian life, albeit in a manner that a Baathist dictatorship could manage.[61] On the other hand, in a non-kinetic fashion, it was intended to be an information warfare and psychological operations base to counter anti-Baathist propaganda in the internet.[62]

The SCS link to the Syrian Electronic Army shows that society adopted a cyber warfare mission under civil war conditions and began to run Baathist military campaigns in the fifth domain of fighting wars: cyber space. This study will argue that the Baathist Regime of Syria has developed a high level expertise in cyber operations during war-time situations and that

their current cyber capabilities can be improved upon to a menacing extent if the regime remains intact. Furthermore, allies of the regime, especially China and Iran, enjoy formidable cyber warfare capabilities, which could translate into foreign assistance in the regime's hostile cyber activities.

Apart from the SEA and SCS, the ISIS-affiliated Cybercaliphate is another important actor to which Turkey must pay attention. The most sensational cyber operation of the group was the hacking of French television network TV5 Monde on April 8, 2015, with the hijacked message of "Je suis IS."[63] More threateningly, the Cybercaliphate uploaded the reported personal IDs and resumes of French soldiers who fought in anti-ISIS operations.[64] Even more concerning, the radical extremist hacker group hacked the official Twitter account of the U.S. Central Command in early 2015.[65]

Indeed, ISIS has proven a much higher and more threatening presence in cyber space that should be taken seriously. As underlined by Hoffman and Schweitzer in April 2015:

> "Although the use of cyber space by jihad organizations is not new, ISIS uses the internet, and primarily social media, more than any other terrorist organization before it. In addition to the organization's technological capabilities, it appears that its primary innovation in its use of cyber jihad is its role in transforming ISIS from yet another Islamic fundamentalist terrorist organization into a global brand name that features prominently in the public discourse in the West, as well as in the Muslim world. As part of its efforts to influence Middle East and global public opinion and brand itself, ISIS disseminates propaganda materials using a well-designed online magazine in English called Dabiq and produces high quality movies that are disseminated on YouTube, Twitter, and various websites affiliated with the organization. Furthermore, the organization targets and exploits online social networks for its own needs on an unprecedented scale. ISIS makes extensive use of Twitter, Facebook, Tumblr, and Instagram, and according to senior American officials, operatives and supporters of the organization produce up to 90,000 tweets every day. A recent extensive study found that ISIS supporters operate at least 46,000 independent Twitter accounts, with 200-500 of these accounts active all day, thereby helping to disseminate the organization's propaganda. …In addition to the extensive use of social media by the organization's operatives and supporters, ISIS' cyber jihad includes offensive use of online space for attacks on websites."[66]

The Cybercaliphate's activities could pose a great threat to Turkey by igniting more extremism among religious youth, especially because Internet use in Turkey is higher than its Middle Eastern neighbors. Turkey could also face cyber attacks, which may target official websites and mainstream media networks.

5.1. The 2008 Pipeline Attack and the 2015 Blackout: A Cyber Wake-up Call for Turkey?

In regards to direct cyber attacks and hostile activities targeting Turkey, this study will shed light on two incidents: the 2008 explosion at the Baku-Tblisi-Ceyhan oil pipeline and the 2015 blackouts through Turkey. The first incident is the 2008 explosions at the Baku-Tbilisi-Ceyhan (BTC) pipeline near the eastern Turkish city of Erzincan. Pipelines have always been vulnerable to terrorist attacks in Turkey. A security survey suggests that between the years 1987 and 2010, 59 sabotage plots were perpetrated on targeting the Turkish pipelines, and 19 of the total 59 sabotages took place between 2007 and 2010.[67]

The 2008 attack, however, was not business as usual. According to some news sources, "Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line, according to four people familiar with the incident who asked not to be identified because details of the investigation are confidential. The main weapon at valve station 30 on Aug. 5, 2008, was a keyboard that shifted the internal pressure of the pipeline systems, which led to the massive blast."[68] The attack on the oil pipeline coincided with Russia's Georgia campaign in 2008, drawing suspicion since the BTC pipeline was running counter to Moscow's energy geostrategic interests in Eurasia.[69] It was revealed that there was indeed intense efforts to jam the pipeline facility, cutting off alarm systems and all communications, including those linking data to the satellite systems.[70]

The hackers deleted all security camera records, except one recorded by an infrared camera that clearly shows two people with laptops walking near the facility.[71] Prior to the Russo-Georgian War in 2008, Ankara's ties with Tbilisi were fairly warm, and the Turkish administration was in support of Georgia's accession to NATO. In this respect, it is equally important that during the course of the war, some Russian sources openly accused Turkey, claiming that Ankara played an important role in improving and encouraging Georgia's military capabilities.[72]

The second sensational cyber attack claims surfaced following the recent blackouts that affected 44 of the 81 provinces in Turkey on March 31, 2015. This time, the suspicion of a cyber attack was openly voiced by Prime Minister Ahmet Davutoğlu, and some press sources claimed that Iran was behind the attacks as a response to President Erdogan's accusation of Tehran for its regional dominance assertions along with his remarks in support of the ongoing operations in Yemen.[73] The day-long blackout halted production in 298 organized industrial zones and cost some $700 million.[74] Some experts presented an even more pessimistic damage assessment, estimating around $1 billion in losses emanating from the blackout.[75] Moreover, the fact that the eastern city of Van, which directly receives electricity from the Iranian electricity grid, was not affected by the blackout causes even more suspicion.[76] Yet, there is no adequate evidence to openly accuse Tehran.

In a 2010 study, James Andrew Lewis, a cyber expert at the Center for Strategic and International Studies (CSIS), underlined why electrical grids can become targets for cyber attacks:

> "The electrical power system has always been a high priority target for military and insurgents. It is cheap and easy for insurgents to blow up or simply pull down pylons and transmission lines or to attack power plants and substations. This is a normal part of guerrilla warfare. Militaries also normally plan to attack power plants, substations or hydroelectric facilities as part of a bombing campaign. … The Aurora tests conducted at Idaho National Labs a few years ago showed it is possible to exploit remote access to send commands to large generators that cause them to damage or destroy themselves. Researchers were able to remotely change the operating cycle of the generator, sending it out of control. A video of the incident shows that the target generator shakes, emits smokes, and then stops. … There is evidence that unknown foreign entities have probed the computer networks of the power grid. Some electrical companies report thousands of probes every month, although we do not know whether these were cyber crime or part of a military reconnaissance effort. There is also anecdotal reporting that potential military opponents have done the reconnaissance necessary for a cyber attack on the power grid, mapping the underlying network infrastructure and locating potential vulnerabilities."[77]

Strategically, electricity grids are high-value targets that can trigger a series of direct and indirect damage to the adversary. From a military perspective, the two optimal options to inflict the most damage to the grid is either high-altitude nuclear detonation or cyber warfare. States like Russia, China, Iran, and North Korea have hinted at their intentions to attack grids within the critical national infrastructure target set.[78]

5.2. Turkey's Quest to Boost its Cyber Capabilities

The possibility that the March 2015 blackout was a cyber attack was not taken as seriously as the 2008 pipeline explosion. Even if the blackout did not result from a cyber attack, it should be recognized as a wake-up call and prove the feasibility of a cyber attack that could cost around $1 billion a day, paralyze life in Turkey's urban centers and inflict damage. Since then, a wave of cyber attacks targeting Turkey's official Internet networks and websites have been detected since May 2015. The hostile activity was orchestrated by twelve "cyber warfare jump-off points" simultaneously.

The reported Baku-Tblisi-Ceyhan oil pipeline cyber attack in 2008 offered invaluable lessons for Turkish decision-makers. First, it was important for showing the kinetic effects of hostile cyber activity. Second, the attack pointed out the link between regional security issues, energy geopolitics, and political/military competition. Third, the cyber attack exposed the vulnerability of critical national infrastructure to the emerging threats of the fifth domain of war.

In response to the BTC attack, Ankara decided to boost its cyber defense capabilities. In 2010, Turkey's National Security Council (MGK-Milli Güvenlik Kurulu) took its first steps towards building cyber capabilities, leading to the establishment of the Cyber Command of the Turkish Armed Forces in 2012.[79] In 2011, Turkey conducted its first National Cyber Security Drill that included both hypothetical scenarios and actual red-team hostile activities.[80] Four years later, cyber security was supposedly incorporated into Turkey's famous "Red Book," the classified National Security Policy Document (Milli Güvenlik Siyaset Belgesi) that provides doctrinal principles and strategic guidance to the Turkish state's agencies and institutions.[81]

6. Conclusion and Policy Recommendations

From a military standpoint, it would be fair to say that a high-profile cyber weapon is the combination of a nuclear weapon, a biological weapon, a time bomb, an anti-radiation missile, Special Forces, and a medieval sword. A high-profile cyber weapon resembles a nuclear weapon in its ability to devastate critical national infrastructure and is similar to a biological weapon in its intelligence requirements for detection of a strike and the identification of a perpetrator. Cyber weapons might be put in the same basket as anti-radiation missiles because of its ability to track signals and pave the ground for follow-up strikes. To a certain extent, they are reminiscent of time bombs for the gap between the time of attack and the moment of impact can be designed by the attacker. Because cyber weapons are clandestine operation assets, they are comparable to modern Special Forces. Finally, in terms of deterrence and the defense versus offense calculus, cyber weapons can be likened to a medieval knight's sword in that they cannot be deterred solely by handling a shield.

In light of these military evaluations, this paper concludes that cyber warfare is a complex phenomenon that transforms war beyond a mere technological shift. Cyber warfare does consist of a technological breakthrough in terms of kinetic and non-kinetic military capabilities that have brought about new doctrines, organizations, concepts, strategies and tactics, offensive and defensive approaches, and more importantly a new warrior-class; however, cyber warfare refers to a new domain for fighting wars. As noted earlier, domains of war are interrelated, and the trajectory of engagements is leaning towards joint warfare and combined operations concepts. In other words, concepts like Air-Land Battle, Air-Sea Battle, compel air, land, and naval units' operations to increasingly adopt a more joint character and further promote network-based operations. In the last century, space has been integrated into this complex picture and has become an invaluable part of operations in other domains.

As of today, advanced missions, such as missile defense or intercontinental ballistic missile (ICBM) launches, cannot be considered without employing space-based assets. Artillery systems, main battle tanks, and even modern infantry benefit from GPS-based systems, guidance, and tactical intelligence networks at theater level.

Due to drastic shifts in cyber interconnectedness and electronic high-tech infrastructure, cyber space is now following suit and being closely integrated into the other domains of war. In this regard, network-centric engagements are becoming more and more computerized in terms of Command-Control-Communications-Computers-Intelligence-Surveillance-Reconnaisance (C4ISR) infrastructure and precision-guidance munitions. Under these circumstances, cyber weapons are entering the picture with their ability to paralyze and blind enemy command and control nodes. Furthermore, electronic warfare (EW), an integral element of all military branches but especially for modern air forces, is building a closer relationship with cyber warfare. The same could be said for information operations and psychological warfare.

As a result, cyber warfare looms large both as a new domain and military technological breakthrough. Therefore, as the Revolution in Military Affairs theory necessitates, adaptation capacity is becoming not only a defensive must but also a way to gain significant and offensive upper hand for state and non-state actors. Turkey is no exception as it has begun to face complex cyber warfare threats in the 21st century. Turkish economic growth is highly dependent on energy infrastructure, electricity generation, and dams with high hydro-strategic value. Turkey continues to pursue strategic objectives, such as becoming an energy hub and commercial aviation hub for the country's powerhouse, Istanbul. Most of Turkey's state

and private databases, banking and financial transactions, and information flow have been digitalized. Therefore, cyber security has become one of the main pillars of Turkey's security environment.

Accordingly, this paper suggests the following policy recommendations for Turkish decision-makers:

- This paper strongly endorses the establishment of a Cyber Command under the Turkish Armed Forces doctrinal order of battle. Deepened cooperation between Turkish Cyber Command, NATO's Cooperative Cyber Defense Center of Excellence, USCYBERCOM, and other allied cyber security organizations is encouraged.
- We appreciatively endorse the 2011 inter-agency cyber drill in Turkey. Unified efforts and cooperation in countering cyber threats are of critical importance. Unclassified information about Turkey's Cyber Command shows that there is no continuous and systematic red teaming and penetration testing. Thus, we suggest regular cyber drills with an effective red teaming activity.
- In light of emerging cyber security challenges, Ankara should renew its strategic calculus with regard to kinetic and non-kinetic threats to critical national infrastructure, sensitive information security, espionage and counterespionage activities, network-centric warfare, psychological warfare, information warfare, electronic warfare, and signal intelligence. For such a comprehensive transformation, we suggest establishing a multidisciplinary commission. The commission could answer to the Secretariat-General of the National Security Council (MGK) and be officially appointed to debate cyber issues at the highest level. Given that the MGK constitutionally assembles once every two months, the transformation agenda would allow a regular discussion and continuity on the subject.
- From a military theoretical and doctrinal perspective, this paper concludes that solely investing in cyber defense would be more or less trying to fly with one wing. Thus, this paper recommends finding a proper and legitimate legal framework for cyber offensive capabilities that would be in harmony with NATO capabilities.
- This paper strongly suggests establishing an inter-agency team comprised of military, law enforcement, internal security intelligence, foreign affairs, and legal bodies. Furthermore, the command level of Turkish Cyber Command could be graduated to higher levels in forthcoming years.
- Cyber security is an emerging area of expertise that is based on a multidisciplinary approach. Thus, we suggest setting new training programs for the Turkish security apparatus augmented by effective cooperation among academia, think tanks, and the private sector.
- The private sector and the state security apparatus are indispensable components of a holistic cyber defense and cyber security approach. Private organizations' cyber vulnerabilities can be exploited as cyber jump-off points by future adversaries. Additionally, security breaches can also serve subversive cyber espionage activities due to the interconnectedness of digital systems and rapid flow of information. Furthermore, Turkey does not have a clear organizational model or doctrinal approach for systematic cooperation between the private sector and state apparatus in terms of cyber security. Thus, this study strongly suggests the development of a comprehensive and holistic approach to handle cyber security and cyber defense issues both organizationally and culturally.
- Turkey's efforts for improving its cyber-defensive and cyber-offensive capabilities will be affected by NATO's perspective. NATO leaders are on the eve of making significant decisions on cyber issues in advance of the forthcoming 2016 Warsaw Summit. The said Summit can become a turning point for the development of NATO's cyber capabilities. The ongoing debate among NATO circles on this very issue has been centered on categorizing the cyber space as an equally recognized and operational field in addition to air, land,

and sea. Should cyber space become an equally recognized operational field for NATO operations, then the sharing of the Allies' cyber defensive and offensive capabilities can be undertaken akin to the current nuclear capabilities of the Alliance. Furthermore, NATO would be responsible with assisting Allied nations in terms of their cyber defense but also for setting out a roadmap, for the allied nations to improve their cyber capabilities.

- Turkey remains among the members of the alliance that champion a more assertive cyber doctrine for NATO. On the other hand, there are some NATO members, first and foremost the US that has opted for a more cautious approach, one that is undoubtedly based on a lack of enthusiasm for disclosing its own cyber capabilities and then being compelled to leverage them to help other NATO Allies. Other nations, such as France, have also resisted these attempts on different grounds that have more to do with favoring the European Union to lead cyber security efforts over NATO. However, prospects of an uptrend in cyber attacks remain highly likely in the foreseeable future, just like the recent incidents in Turkey in December 2015 Turkey. Thus, NATO leaders are expected to take firm decisions towards consolidating the Alliance's cyber doctrine, mission and capabilities at the 2016 Warsaw Summit. Such a decision would encourage Turkey to take further steps in the cyber field and to adopt a more consistent stance with regards to improving its cyber capabilities.

1- T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (Republic of Turkey Ministry of Transport, Maritime Affairs and Communication) "SOME-Sektörel Kurulum ve Yönetim Rehberi" (CERT-Sectoral Setup and Management Guide) 2014.

2- Turkey's National Action Plan on Cyber Security, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf, Accessed on: July 7, 2015.

3- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Accessed on: June 29, 2015.

4- James A, Lewis., Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats, CSIS, 2002. p.2.

5- Steven Metz and James Kievit., Strategy and Revolution in Military Affairs: From Theory to Policy, US Army SSI, 1995, pp. 2-3.

6- Andrew Krepinevich., "Cavalry to computer; the pattern of military revolutions." The National Interest n37 (Fall 1994 n37): 30(13). General Reference Center Gold. Thomson Gale. University of Florida. 19 Nov. 2006.

7- Barry D. Watts.,The Maturing Revolution in Military Affairs, CSBA, 2011, pp.15-20.

8- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, pp.28-29.

9- Paul J Springer., Thinking about Military History in an Age of Drones, Hackers, and IEDs, Air Command and Staff College, http://www.fpri.org/docs/springer1.pdf, Accessed on: July 7, 2015.

10- For a comprehensive assessment on the Roman light infantry, see: Adam, O. Anders., Roman Light Infantry and the Art of Combat, Cardiff University, 2011.

11- James A. Lewis., The Role of Offensive Cyber Operations in NATO's Collective Defense, The Tallinn Papers, CCDCOE, 2015, p.3.

12- John Arquilla and David Ronfeldt. "Cyber War is Coming" in In Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC 1997, p.24

13-Ibid. p.30.

14- Ibid.

15- Ibid. p.23.

16- Jennifer, J. Li and Lindsay Daugherty, Training Cyber Warriors, RAND, 2015, p.xi.

17- For detailed defense spendings see: IISS, Military Balance 2014.

18- US Cyber Command Fact Sheet, May 25 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces %20May%2021%20Fact%20Sheet.pdf, Accessed on: June 29, 2015.

19- Ibid.

20- http://www.al-monitor.com/pulse/originals/2015/06/israel-idf-cyber-intelligence-new-unit-eisenkot-war-future.html, Accessed on: June 29, 2015.

21- http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/24/israel-target-for-iranian-hezbollah- cyber-attacks/29210755/, Accessed on: June 29, 2015.

22- Joel Mullish. "Russia's Growing Reliance on Cyber Warfare Setting Dangerous Precedent for Future Foreign Policy", INSS, http://www.inss.org.il/uploadImages/systemFiles/Russia's%20growing%20reliance%20on%20cyber %20warfare%20setting%20dangerous%20precedent%20for%20future%20foreign%20policy.pdf, Accessed on: June 29, 2015.

23- NATO CCDCOE, https://ccdcoe.org/, Accessed on: June 29, 2015.

24- NATO, Cyber Security, http://www.nato.int/cps/en/natohq/topics_78170.htm, Accessed on: June 29, 2015.

25- Magnus Hjortdal., "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", Journal of Strategic Studies, Vol: 4 No: 2, Summer 2011.

26- For detailed information see: Mandiant, APT1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, Accessed on: July 28, 2015.

27- Eric, M. Hutchins et.al. Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven- Defense.pdf, Accessed on: July 29, 2015.

28- Ibid.

29- Larry M. Wortzel., The Chinese People's Liberation Army and Information Warfare, US Army SSI, 2014, pp.1-8.

30- Ibid. pp.12-13.

31- Ilan Berman., The Iranian Cyber Threat Revisited, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cyber security, Infrastructure Protection, and Security Technologies, 2013, p.2.

32- James Andrew Lewis., Cyber security and Stability in the Gulf, CSIS, January 2014.

33- Executive Cyber Intelligence, INSS-CSFI, April 1st, 2015.

34- Jason, P. Patterson and Matthew, N. Smith., Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran, Naval Postgraduate School, 2005, p.44.

35- Ibid, pp.44-50.

36- James Andrew Lewis., Cyber security and Stability in the Gulf, CSIS, January 2014.

37- Craig Stallard., At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force, School of Advanced Air and Space Studies, Maxwell Air Force Base, 2011, pp.35-36.

38- Ibid.

39- Ibid.

40- Martin, C. Libicki., "The Specter of Non-Obvious Warfare", Strategic Studies Quarterly, Fall 2012.

41- Samuel Liles. et.al. "Applying Traditional Military Principles to Cyber Warfare", 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012, p.171.

42- Jeffrey R. Witsken., Network-Centric Warfare: Implications for Operational Design, School of Advanced Military Studies-US Army Command and General Staff College, 2002, p.3.

43- Ibid. pp.17-18.

44-Alvin L. Bailey., The Implications of Network Centric Warfare, US Army War College, 2004, pp.2-3.

45- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Vol: 3 No: 1, May 2011.

46- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, p.25.

47- Andrew F. Krepinevich., Cyber Warfare: A Nuclear Option, CSBA, 2012, p.66.

48- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, February/March 2012, Vol: 157 No: 1, p.6.

49- Austin Miller. Advanced Anti-Radiation Guided Missile: Strengthening DEAD Capability in the Fleet, 43rd Annual Systems: Gun and Missile Systems Conference and Exhibition, April 21-24 2008 Brief.

50- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, February/March 2012, Vol: 157 No: 1, p.8.

51- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Vol: 3 No: 1, May 2011.

52- "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler" (The Importance of Cyber Security for National Security and Preventative Measures) Güvenlik Stratejileri (Security Strategies).

53- Jane's Intelligence Review, Middle East Conflict Spills into Cyber space, 2015, pp.3-4.

54- Ibid.

55- http://sea.sy/index/en, Accessed on: June 28, 2015.

56- Ibid.

57- http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=1, Accessed on: June 28, 2015.

58- Ibid.

59- Human Rights Watch, By All Means Necessary: Individual and Command Responsibility for Crimes Against Humanity in Syria, 2011, p.87.

60- Jeremy M Sharp., Unrest in Syria and U.S. Sanctions Against the Assad Regime, Congressional Research Service, 2011, p.4.

61- It should be noted that by the mid 1990s, there was only two computers for 1,000 in Syria, and it was in 1997 that a pilot group of 400 Syrians were allowed to access internet.

62- John B Alterman., New Media New Politics: From Satellite Television to the Internet in the Arab World, Washington Institute for Near East Policy, 1998, pp.40-41.

63- http://rt.com/news/248073-islamic-state-hackers-french-tv/, Accessed on: June 28, 2015.

64- Ibid.

65- http://rt.com/usa/221927-central-command-hackedcybercaliphate/, Accessed on: June 28, 2015.

66- Adam Hoffman and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)", Strategic Assessment, Vol: 18 No: 1, April 2015, p.73.

67- USAK, "Kritik Enerji Altyapı Güvenliği Sonuç Raporu" (Critical Energy Infrastructure Security Final Report).

68- http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar, Accessed on: June 29, 2015.

69- Ibid.

70- http://www.milliyet.com.tr/siber-savasin-miladi/dunya/detay/1982549/default.htm, Accessed on: June 29, 2015.

71- Ibid.

72- http://www.hurriyet.com.tr/dunya/9623756.asp, Accessed on: June 29, 2015.

73- http://www.dailysabah.com/diplomacy/2015/04/28/iran-allegedly-behind-nationwide-power-outage, Accessed on: June 29, 2015.

74- http://www.hurriyet.com.tr/ekonomi/28611619.asp, Accessed on: June 29, 2015.

75- "Elektrik Altyapısı ve Siber Güvenlik" (Electric Infrastructure and Cyber Security). http://www.edam.org.tr/tr/IcerikFiles?id=1028, Accessed on: August 3, 2015.

76- http://www.hurriyet.com.tr/gundem/28604226.asp, Accessed on: June 29, 2015.

77- James A. Lewis., The Electrical Grid as a Target for Cyber Attack, CSIS, 2010.

78- Cynthia E. Ayers and Kenneth D. Chrosniak., Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency, US Army War College Center for Strategic Leadership and Development, Issue Paper, Volume 1-13, 2013.

79- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Accessed on: June 29, 2015.

80- Information Technology and Communication Agency (Bilgi Teknolojileri ve İletişim Kurumu), http://www.tk.gov.tr/sayfa.php?ID=28, Accessed on: June 29, 2015.

81- http://www.haberler.com/tsk-siber-savunma-komutanligi-ndan-hacker-atagi-7035427-haberi/, Accessed on: June 29, 2015.

THE CYBER SECURITY SCENE IN TURKEY

Assoc. Prof. Salih Bıçakcı

Faculty Member, International Relations - Kadir Has University

F.Doruk Ergun

Research Fellow – EDAM

Prof. Mitat Çelikpala

Dean, Graduate School of Social Sciences - Kadir Has University

1. Introduction

The advent of the cyber realm brought along multiple security challenges to both users and security agencies of nation states. Cyber attackers have the potential to wreak havoc by targeting financial institutions, accessing and leaking national secrets, and as multiple examples, including the Stuxnet worm against Iranian nuclear facilities have shown, by causing actual physical damage akin to a kinetic attack to national infrastructure. Cyber-attacks are harder to attribute, as attackers rarely leave any traces and in fact work to obscure their origin. In most cases, cyber attackers do not need expensive and rare equipment; this is bolstered by the fact that accessibility to information technologies (IT) to the general public continues to increases and so does the role of IT in running both public and private sectors, thus creating more vulnerabilities. Except for a few exceptions such as distributed denial of service (DDoS) attacks, cyber-attacks take place by exploiting vulnerabilities of the target system and its cyber defense measures, [1] which makes them harder to defend against as the defender is not aware of where the attack could originate from. Furthermore, cyber attackers are harder to predict, disarm and deter, all of which give considerable advantages to offence over defense in the cyber realm.

Against these issues, nation states are left with their domestic capabilities to deal with cyber threats. Therefore the first marker of how susceptible nations are to cyber threats is their respective capabilities and the cyber security understanding in the country. Hence, this section begins with providing a timeline of developments in the cyber security policies, legislations and cyber defense capabilities of Turkey.

Cyber-attacks directed against a country's assets do not have to originate from within its borders. Yet Turkey has proven to be an interesting case, as by 2013 only 46 percent of its citizens had access to the internet, making it the 97th in the world, [2] while at the same time, Turkey was in the past ranked as the third biggest origin of cyber-attacks in the world.[3] Therefore, the paper will then examine the groups of Turkey based cyber attackers by providing accounts of their past attacks, motives and where possible, capabilities.

2. Capabilities and Tools of the Turkish Government

2.1. Legislation on Computer Crimes

Before moving on to become major national security concerns, cyber-attacks were more relevant to public order and law enforcement. Therefore before militaries began to pay more attention to cyber as a new domain of war in addition to land, sea, air, and space, the response of nation states initially focused on illegal uses of cyber space for criminal purposes. This trend has been visible in Turkey as well. Cyber-crimes were first introduced to the Turkish penal system on 6 June 1991 with Law No. 3756 targeting several amendments to the Turkish Penal Code. Article 20 of the amendment introduced a clause titled "Informatics Crimes" which penalized the unlawful seizure of programs, data, and other elements from a computer system along with their use, transfer, or copy with the aim of harming an individual.[4]

Subsequently, Turkish Penal Code no. 5237, implemented in September 2004, acknowledged the notion of cyber-crime within the framework of the Penal Code through extending its definition. Under Section 10 of the Turkish Penal Code, titled "Information Technology (IT) Crimes" three groups of activities were declared as criminal; item 243 on access to an IT system, item 244 on the denial of system as well as its disruption, data destruction or data modification, and item 245 on the misuse of debit and credit cards.[5]

Other relevant items that refer to crimes that can be executed through – but not exclusively by – utilizing IT systems like computers and telecommunication equipment include the following: crimes against personal life; illegal obstruction of communication; theft, fraud, and gambling; forgery and counterfeiting among others.[6] Consequently, cyber-crimes were recognized in the context of terrorism upon the amendment made in 2006 in Law No 3731, the Anti-Terror Law. The amendment states, "The crimes listed below are considered terror crimes if they are conducted as part of the activities of a terror organization established to carry out criminal actions with the aims listed in Article 1"[7] and with that cites multiple articles in the Turkish Penal Code. These include the list of crimes that may arise as a result of utilizing computer systems along with items 243 and 244 that refer to the access, denial and disruption of system, data destruction and data modification.[8] According to the second article of the Anti-Terror Law, even if people are not members of a terror organization, they are considered and penalized as terrorists if they conduct crimes in the name of a terror organization.

In the meantime, government agencies began proactively formulating policies on Ankara's presence in the cyber realm not just from a national defense perspective, but also from the standpoint of providing public services and regulating the use of the internet. Before being replaced by the Ministry of Development in 2011, the State Planning Organization released several documents on the matter, including "e-Turkey Initiative Action Plan-2002," "e-Transformation Turkey Project Short-Term Action Plan (2003-2004)," and "e-Transformation Turkey Project 2005 Action Plan."[9] In 2005, the State Planning Organization initiated a study titled "Information Society Strategy" and released both a strategy document covering the 2006-2010 period and an action plan, which listed security and confidentiality of personal information as one of its main themes.[10] The action plan stated that a Computer Emergency Response Team (CERT) would be established in order to monitor cyber security threats, post warnings, inform defensive measures, and coordinate responses. It also placed the National Research Institute of Electronics and Cryptology

(UEKEA) under the patronage of the Scientific and Technological Research Council of Turkey (TÜBİTAK) in charge of this operation.[11] Additionally, the 2006-2010 documents indicated that the Draft Law on the Protection of Personal Data would be codified until the end of 2006 and that additional regulations would be put in place to protect data related to national security and to improve the state's data security systems.

Despite these efforts, the Draft Law on the Data Protection and Privacy, originally submitted to Parliament in 2008, is still pending ratification.[12] The Draft Law on e-State and Information Society, which would govern state services provided online through the e-State portal and the planned Information Society Agency, is also pending approval by the Parliament since August 2009.[13]

Moreover, another law was drafted through the late 1990s and the first half of 2000s under the coordination of the Ministry of National Defense, namely the Draft Law on National Information Security Organization and Its Tasks. This law was originally planned to be finalized and ratified by mid-2003 according to the e-Turkey Initiative Action Plan laid out by the office of the Prime Ministry.[14] The draft law envisioned the foundation of a National Information Security Supreme Board under the auspices of the Prime Ministry, which would be tasked with directing the country's information security policies and consist of the Prime Minister, Ministers of Justice, National Defense, Interior, Foreign Affairs, Transport, Industry and Commerce, as well as the General Secretary of the National Security Council, the Undersecretary for the National Intelligence Agency (MIT), the Commander of General Staff Communications, Electronic and Information Systems, and the directorate of TÜBİTAK.[15] The Supreme Board would also be tasked with assessing threats, determining and guiding the country's information security policies and their implementation, and evaluating the proposed changes to information security legislation.

The law also envisioned the foundation of National Information Security Institution, which would be divided into five bodies; Planning and Coordination Department, Information Security Department, Cryptology Department, Information Support Department, Supervision and Education Department, each tasked with a variety of functions, ranging from determining threats, founding the country's information security architecture, and authenticating software and hardware to be used in crypto systems to licensing imports and exports on information security tools. The Institution was to be assisted by the Consultancy for International Affairs and Law and the Directorate of National Computer Security Center. In the end, however, the law was scrapped due to a lack of consensus on the final draft.[16]

2.2. Institutionalization of Turkey's Cyber Security Architecture

In parallel to these developments, Turkey has begun taking steps towards establishing agencies dedicated to running its policies in the cyber realm. As expected, the creation of dedicated agencies has served to hasten the country's policymaking efforts, multiply its regulations over the internet, and expand its capabilities. For the most part, these agencies have focused on the public order and law enforcement domain of cyber security, leaving the cyberwar aspect to the Turkish military. The primary exception to this has been research institutes, which continue to work in all aspects of the Turkish cyber security architecture with the aim of creating reliable national software and hardware, and therefore have continued to have a close relationship with the military.

2.2.1. Information and Communications Technologies Authority (BTK) and Presidency of Telecommunication (TİB)

The Telecommunications Authority that was founded in January 2000 was transformed into the Information and Communications Technologies Authority (BTK) on November 2008. BTK serves as the regulator of the telecommunications sector and is tasked with authorization, inspection, dispute resolution, protection of consumer rights, regulation of sectoral competition, issuing of technical regulations, and spectrum management and inspection. Additionally the organization is the responsible authority for information technology, which is relegated to the Presidency of Telecommunication and Communication (TİB). Established in 2005, the TİB reports directly to the Chairman of BTK and hosts, in addition to its personnel, one representative from the related departments of the National Intelligence Agency, Turkish National Police, and Gendarmerie General Command.

For the most part, TİB is tasked with surveilling, tracking, evaluating, and recording signal information and communications made through telecommunications tools, including the Internet. TİB also deals with the "safety" of the Internet service – regulating content, service providers, access providers, and public Internet access providers. Hence, the TİB has been a controversial institution as it lies at the center of the freedom of access versus Internet censorship and privacy versus network surveillance debates. Moreover, TİB is tasked with setting the acceptability criteria for the production of hardware and software for filtering, masking, and surveilling online services. As part of the national cyber security architecture, TİB also coordinates content, access and area providers and other institutions to detect and prevent cyber-attacks.[17]

2.2.2. The Scientific and Technological Research Council of Turkey (TÜBİTAK)

The roots of Turkey's civilian research institutions in electronics and cryptology can be traced back to 1968 when an Electronic Research Unit was established at Middle Eastern Technical University. Originally a five-person unit, the Electronic Research Unit was moved to Marmara Scientific and Industrial Research Institute – later renamed the Marmara Research Institute – and produced the country's first national encryption equipment, MİLON-1[18], in 1978 in a project awarded by the Turkish Armed Forces (TSK).

The unit was named the Electronic and Semi-Conductor Technology Department in 1991, only to be renamed National Research Institute of Electronics and Cryptology (UEKAE) in 1995. The Department signed a contract with the Ministry of National Security for the establishment of a Cryptographic Test and Design Center in 1994 and set up the facility in 1997. [19]

In the same year, the Network Security Group was established under the auspices of the Scientific and Technological Research Council of Turkey (TÜBİTAK). The Group worked on Microsoft and open source operating systems (OS), e-mail servers, databases and their vulnerabilities, and intrusion detection systems. A year later, UEKAE was also directly affiliated with TÜBİTAK. In 2000, TÜBİTAK signed a contract with the Ministry of National Defense to establish a Common Criteria Test Center, which was completed in 2001. The Center later adopted the capabilities of conducting Common Criteria assessments, communication security (COMSEC) tests, Side Channel Analysis, and Reverse Engineering.[20] In 2006, UEKAE was tasked with the responsibility for maintaining the security of the GÖKTÜRK satellite project. [21]

As a result of the 2006-2010 action plan, TÜBİTAK set up the Information Security Management System to four public organizations and began conducting information

technology security days for private and public organizations in separate events in 2007. In the same year, TÜBİTAK UEKAE began participating in NATO exercises with its products and began coordinating joint Cyber Emergency Response Team (CERT) exercises among institutional CERTs around this period. TÜBİTAK hosts one of the two accredited CERTs in Turkey, the ULAK-CSIRT, which is in operation for the purpose of research and education.[22] The other accredited CERT, the TR-BOME, is government-run. ULAK-CSIRT signed a memorandum of agreement in 2007 with NATO Computer Incident Response Capability (NCIRC) on issues including access to the NCIRC network, support on malicious code analysis, vulnerability database, alarm, warnings, and staff exchange. [23]

In 2010, TÜBİTAK UEKAE and the Information Technologies Institute (BTE) (which was originally under Marmara Research Center) were merged to become the Informatics and Information Security Research Center (BİLGEM). The same year, Turkey officially became a Certificate Generator country in the field of Common Criteria (ISO 15408) and hence Common Criteria certificates provided to IT products by TÜBİTAK BİLGEM OKTEM (Common Criteria test center) gained international validity. [24] Three more institutes were established under TÜBİTAK BİLGEM in 2012: the Software Technologies Research Institute (YTE), Cyber Security Institute (SGE), and Advanced Technologies Research Institute (İLTAREN). The following year, TÜBİTAK BİLGEM signed an R&D (research and development) agreement with NATO and a Memorandum of Cooperation with HAVELSAN[25] (Hava Elektronik Sanayi) – a government owned company focusing on aeronautics and electronics). Additionally in 2013, BTE designed and produced Turkey's first Real-Time Operating System (GIS).

TÜBİTAK was the responsible authority for cyber security until October 2012 when it relegated this role to The Ministry of Transport, Maritime Affairs and Communications with Cabinet Decision No. 2012/3842.[26] TÜBİTAK currently represents around 70 percent of all national crypto solutions. [27] Together with the Ministry of Transport, Maritime Affairs and Communications (UDH) and National Cyber Incidents Response Center (USOM), TÜBİTAK runs the country's honeypot cyber threat detection system, which gathers traffic from all 81 cities in Turkey in 164 separate locations.[28] The honeypot system, which consists of seemingly integral but essentially isolated and monitored data to bait attackers with the aim of uncovering and blocking them, was founded under the auspices of TİB.

So far there have been three national cyber security exercises in Turkey, one in 2008 by TR-BOME and two others led by TÜBİTAK and BTK in 2011 and 2013. The 2011 national exercise involved the participation of 41 public, private, and non-governmental entities with close to 200 personnel. In addition to IT professionals, the participants included those from the finance, education, health, law, and defense sectors. The exercise in 2013 included 61 organizations, 20 of which were observers. The scenarios played out in this exercise included log analysis, port scanning, distributed denial of service (DDoS), WEB security scan, WEB application scan, social engineering, and a capture the flag contest.[29]

2.2.3. Establishing a Response Capability

A report released by the staff of the Information and Communications Technologies Authority (BTK) in May 2009 suggested that in addition to the aforementioned draft laws, the country needed to enact several measures to reinforce its national cyber defense legislation.[30] These included the need for regulations on how cyber-attacks would be inspected, how evidence would be gathered, how states would proceed on the matter, and how to clarify the authority of security forces and the judiciary on the topic of cyber space. The report also pointed to the lack of technical experts among both the security forces and the judiciary and highlighted the need for realistic and applicable contingency plans for emergencies in the cyber space.

While most of these gaps still persist, there has been growing momentum in Ankara's efforts to increase its cyber defense capabilities in the last few years. For one, cyber security was introduced to the National Security Policy Document (i.e. the Red Book) in October 2010.[31] The following July, the Turkish National Police established the Combating IT Crimes Department (renamed Combating Cyber Crimes Department in February 2013).

Following the Cyber Security Strategy Workshop conducted in June 2012, a recommendation document penned by members of the Turkish Information Security Association (Bilgi Güvenliği Derneği in Turkish) was drafted. The document called for the following measures to be implemented:[32]

- The release of the National Cyber Security Strategy Document
- The foundation of National Cyber Security Council
- Increasing awareness on cyber security and disseminating cyber security culture
- Taking stronger measures on protecting personal and institutional data
- Strengthening international cooperation (the document lists EU, ENISA, Council of Europe, UN, NATO and OECD)
- Establishing a national cyber security R&D policy and encouraging the development of national technologies
- Taking steps to increase scientific studies conducted in universities on the subject
- Taking steps to cultivate human resources (in other words, training national cyber security experts)
- Taking steps to increase cyber security capabilities of institutions and security forces
- Establishing independent centers in institutions that would do cyber security penetration tests
- Making legislative reforms

The document argued that a Turkish National Cyber Emergency Response Team (TC-SOME) should be established to provide training to and coordination among other CERTs in critical infrastructure and public and private organizations. It also recommended the establishment of a central national cyber threat and vulnerability research laboratory that would monitor malicious software and inspect national and international cyber security software. The document made a specific reference to backdoors, built-in malware, and other vulnerabilities that may be present in imported hardware and called for the development of national hardware as well as a national Operating System (OS), search engine, and web browser.[33] It also suggested the creation of a Cyber Security Excellence Network under the auspices of the Undersecretariat for Defense Industries to conduct and coordinate research and development on cyber security.

The Turkish Information Security Association's draft document became one of the first reports to place a strong emphasis on national critical infrastructure.[34] In the report, critical infrastructure was defined as "structures that, damages to or the destruction of which would hamper the continuity of public services and public order and; the partial or complete loss of their functionality would have detrimental effects on public health, safety, security and on economic activity and on the effective and efficient functioning of the government."[35] The report categorized the structures related to the following sectors as critical infrastructure: IT; energy; financial; health; foodstuffs; water; transportation; defense; public security; and nuclear, biological, and chemical facilities. In addition, it suggested that all institutions with critical infrastructure should be involved in annual national cyber security exercises and that all IT that run critical infrastructure belonging to government and private institutions should meet the Information Security Management System standards (TS ISO/IEC 27001) by the end of 2013.

2.2.4. The Cyber Security Council

The first step in the path the report has drawn was taken on 20 October 2012 with Cabinet Decision No. 2012/3842 on the Implementation, Management and Coordination of National Cyber Security Efforts. The cabinet decision established the Cyber Security Council "in order to determine the precautions that will be undertaken regarding cyber security, approving, implementing and coordinating plans, programs, reports, regulations, guidelines and standards."[36] The Council is headed by the Minister of Transport, Maritime Affairs and Communications and includes undersecretaries from the Ministries of Foreign Affairs, Internal Affairs, National Security, UDH, as well as the Undersecretary of Public Order and Security, the Undersecretary of National Intelligence Agency, the Head of the Turkish General Staff Communications, Electronics and Information Systems Department, the Head of BTK, the President of TÜBİTAK, the Head of the Financial Crimes Investigation Board, the President of Telecommunication and Communication (TİB), and other high-level staff of ministries and public organizations determined by UDH.

With Cabinet Decision No. 2012/3842, the Ministry of Transport, Maritime Affairs and Communications were given the following tasks:[37]

- Prepare the policies, strategies and action plans to provide National Cyber Security.
- Prepare regulations and guidelines to ensure that the security and privacy of information and data belonging to government agencies and organizations is maintained.
- Monitor, verify the effectiveness and test the creation of technical infrastructure on national cyber security in government agencies and organizations.
- Take action towards securing national information technologies, communications infrastructure and systems and databases, determining critical infrastructure and creating systems to track, intercept and prevent cyber threats and attacks against them, setting up related centers, and inspecting, running and continuously fortifying these systems.
- Encourage the development, production and use of national cyber defense tools and national solutions in providing national cyber security.
- Plan, coordinate and implement the education, hiring and advancement of necessary and sufficient amount of expert personnel to agencies and positions of critical importance to national cyber security.
- Cooperate with other countries and international organizations in the framework of this decision
- Adopt education and awareness raising measures on national cyber security
- Determine regulations and guidelines for persons and institutions that work on the field of education, testing and generating solutions on information security, and give security documentations.
- Undertake the secretariat functions of the Cyber Security Council.

The following year the Cyber Security Council released the country's first National Cyber Security Strategy and 2013-2014 Action Plan, which became effective with Cabinet Decision No. 2013/4890 dated 25 March 2013.[38] The action plan defined critical infrastructure as follows:

"The infrastructures which host the information systems that can cause,
- Loss of lives,
- Large scale economic damages,
- Security vulnerabilities and disturbance of public order at national level when the confidentiality, integrity or accessibility of the information they process is compromised."[39]

The action plan suggested that critical infrastructure is susceptible to cyber threats, since most critical services and infrastructure rely on IT systems to conduct their operations and are connected to the internet. It was noted that in addition to the systemic vulnerabilities of cyber space, the vulnerabilities in Turkey arose from lack of knowledge among the general populace, institutions, and high-level executives on matters of cyber security. Furthermore, the action plan pointed to the lack of IT infrastructure and IT experts, the absence of coordination, and the inadequacy of national and international legislation.

The 2013 - 2014 action plan added more actionable items to the recommendations put forth by the 2012 Workshop recommendation document and drafted plans for the enactment of 29 separate actions in total. This ambitious set of goals include a multiplicity of stakeholders, including government ministries, research institutions, the private sector and agencies tasked with ensuring the cyber security of the country. Critical infrastructures were given a significant emphasis within the action plan. Action number five covers information security management in critical infrastructures and puts TÜBİTAK in charge of determining critical infrastructure that might be directly threatened by cyber-attacks. TÜBİTAK will also conduct sectoral risk analysis of one of these critical infrastructures. Furthermore, public organizations responsible for regulating and auditing the critical sectors are put in charge of determining the methods of sectoral risk analysis and the requirements of sectoral emergency action plans, completing yearly risk analysis reporting activities, implementing the requirements of sectoral business continuity plans and sectoral security precautions.[40] Moreover, under action number 10 on the implementation of the software security program, TÜBİTAK is tasked with publishing a document on the fundamental rules of secure software development for use in critical infrastructures. TÜBİTAK will also have to prepare and submit to the Cyber Security Council feasibility studies on implementing and checking the technical requirements within critical infrastructure organizations (in the scope of the security assessments of the software developed for Critical National Infrastructure).[41]

In addition to strengthening critical infrastructure, some actionable items concern reinforcing resilience and minimizing the effects of contingencies. Under action number 16, UDH is tasked with developing and deploying a test infrastructure for detecting data loss for key public organizations. In action number 14, UDH is tasked with establishing business continuity and data backup systems. Furthermore, along with TÜBİTAK and the Turkish Standards Organization, it is tasked with the certification of products and service providers in the field of cyber security.

One of the highest priorities of the action plan is to build up the country's human capital. At least nine separate actions are devoted to fomenting knowledge and expertise on cyber security. For example, some of the action items suggest raising awareness by training IT experts, conducting cyber security exercises, hosting cyber events, and increasing the number of classes and departments on the issue. Furthermore, BTK is tasked with developing mechanisms for the detection, monitoring, and prevention of cyber threats, including the establishment of a honeypot system to detect threats under action number 11.

Another emphasis is on developing domestic technologies on cyber security by setting up R&D labs in universities; including cyber security as a priority subject among current project promotion systems; and conducting regular activities with the public and private sectors, NGOs, universities, and IT experts to participate in creating national products and solutions in the field of cyber security. The strategy document also points towards the shortcomings in national legislation and urges the Ministry of Justice and other relevant ministries and organizations to determine the needed regulations. Furthermore, it tasks the Turkish Language Association with creating a dictionary for cyber security terms.

2.2.5. National Cyber Incidents Response Center (USOM)

One additional outcome of the National Cyber Security Strategy and 2013-2014 Action Plan was the creation of a Cyber Incidents Response Center to identify threats, develop and share warnings. The strategy document called for the establishment of the National Cyber Incidents Response (USOM) team, "which will be available 24/7 to respond to the threats that may affect the country" and a sectoral Team for Responding to Cyber Incidents (SOME), which will "work under the coordination of USOM"[42] under the auspices of TİB. Furthermore, USOM is responsible for setting up sectoral SOMEs for critical infrastructure sectors and public organizations in addition to providing training and coordination for them.

On November 11, 2013, the Ministry of Transport, Maritime Affairs and Communication released the Communiqué on the Regulations and Guidelines for the Foundation, Missions and Activities of Cyber Incidents Response Teams[43]. The communiqué suggested that Ministries set up their institutional SOMEs based on their specific needs in a way that covers the divisions and related agencies. All other public institutions, subdivisions, related ministerial agencies, and private institutions could set up their own institutional SOMEs. The goal was to set up an institutional SOME for all ministries and other public institutions that have their own IT units, as well as all private companies that run critical infrastructure. By January 2015, 245 institutional SOMEs had been set up and were staffed with around 720 personnel.[44] UDH is in charge of coordinating the foundation of institutional SOMEs.

Critical sectors determined by the Cyber Security Council must have sectoral SOMEs, whereas sectoral SOMEs of regulatory and supervisory institutions are coordinated by BTK. So far, six critical sectors have been identified: banking and finance, transportation, electronic communication, water management, energy, and critical public services.[45] Public and private operators of critical infrastructure are also tasked with setting up institutional SOMEs, which will operate under sectoral SOMEs.

All SOMEs are required to work on a 24/7 basis and must report any potentially illegal activity to legal bodies and USOM immediately. Individual SOMEs are responsible for taking necessary precautions against cyber-attacks, setting up response and incident recording systems, and working towards securing the information of their respective institution. If an incident is beyond their capabilities to respond, they can ask sectoral SOMEs or USOM for assistance. Furthermore, USOM will provide training to SOMEs and may work directly with institutional and sectoral SOMEs if it deems necessary. The cooperation with international organizations and counterpart agencies will be carried out by USOM. In its current organizational structure, USOM comprises of five departments dealing with cyber incident reporting and communication, malware analysis, interagency coordination, software development, and international outreach.[46] Between the beginning of 2014 and January 2015, the organization has detected more than 1500 cyber incidents targeted at public institutions and the private sector.

In many ways, USOM is a good candidate for being the primary governmental agency in charge of protecting critical infrastructure and managing cyber security crises in Turkey. However, USOM does not have the necessary coordination authority that is required to direct other governmental bodies and agencies. Yet, comprehensive communication, cooperation, coordination and the application of new policies are necessary to manage most of the cyber security crises that may envelop the country. It can be seen that the national SOME was not designed to perform such a function.

On the other hand, most of the critical infrastructure runs on industrial control systems, including SCADA, which are crucial to industrial processes, including energy distribution, water treatment, transportation, chemical, government, defense, and food. Securing these ICS systems requires specific expertise,which involves the ability to discern sectoral differences . This particular expertise demand, forces various states to establish Industrial Control Systems Computer Emergency Response Teams (ICS-CERT). Turkey has no ICS-CERT that would focus on the protection of critical infrastructure.

2.2.6. Prime Ministry Disaster & Emergency Management Authority (AFAD)

On the other hand, the role of cyber crisis management and critical infrastructure protection have been delegated to the Prime Ministry's Disaster and Emergency Management Authority (AFAD) with Law No. 5902. As dictated by this law, AFAD's duty is to coordinate all institutions and organizations that take part in managing disasters both before and after the disasters and to develop policies regarding these issues. AFAD created an action plan that categorized disasters into two major groups: natural disasters and technological disasters. Critical infrastructure protection and cyber security are listed under technological disasters. In its critical infrastructure protection plan, AFAD designated the following 12 institutions and ministries as key members of the process: Ministry of Interior; Ministry of Environment and Urbanization; Ministry of Energy and Natural Resources; Energy Market Regulatory Authority; Ministry of Health; Ministry of Transport, Maritime Affairs and Communication; Turkish Atomic Energy Authority; Ministry of Science, Industry and Technology; TÜBITAK; General Command of Gendarmerie; Undersecretariat of Public Order and Security; and Hacettepe University. AFAD published "2014-2023 Critical Infrastructure Protection Road Map Document" to define the fundamental steps of the protection process. The document listed the necessary steps and their fulfillment dates as such:[47]

- To determine responsible authorities.
- To determine the authority in charge of coordination, and to outline criteria for determining critical infrastructure sectors (CIS) on a division of labor level.
- To prepare draft regulations concerning harmonization with European Union directives, to determine critical infrastructure based on the effects of scope, magnitude and time, and increasing protective precautions.
- To effectively protect critical infrastructure, and the communication, coordination and cooperation with all relevant stakeholders at the national or EU level.
- To make operator security plans regarding CIS.
- To appoint security liaison officers.
- To create and implement training programs.
- To prepare a Plan for Critical Infrastructure Protection to safeguard critical infrastructure at the national level.
- To integrate to the practices of EU Critical Infrastructure Warning Information Network (CIWIN) that could promote the development of appropriate precautionary measures through the sharing of best practices and instant threats and alarms in a safe manner.
- Reporting.

In the road map document, 2016 has been declared as the earliest and 2018 as the latest date of fulfillment. The road map document does not clarify how AFAD will manage cyber security crises.

2.3. Cyber Defense Mechanisms of the Armed Forces

After the cyber-attacks against Estonia and Georgia, the number of cyber-attacks against the Turkish government and private entities increased, leading the government to take steps towards defining cyber-attacks as a threat by creating a national cyber security strategy. The Turkish National Security Council defined cyber security as a threat and included the term in Turkey's military strategy, named the "Red Book." Meanwhile, NATO, on May 17, 2010, presented its new strategy to its member states, also defining cyber security as an emerging threat.[48]

It was also at this time that the decision to establish the Cyber Security Command, also known as Turkey's cyber army, was taken. The Command that aimed to protect the country against cyber-attacks, was planned to operate as a special branch within the General Staff in cooperation with TÜBİTAK and the Middle East Technical University.

Subsequently, with the formation of the Cyber Security Council, the Turkish Armed Forces (TSK) established the Cyber Defense Center Presidency in June 2012. Although this branch was far from establishing a Cyber Command, it could be considered a good start as a CERT center that would assist TSK and its branches. After the announcement of a National Cyber Security Strategy, TSK declared the formation of Cyber Defense Command in 2013 and defined its tasks as follows;

1. To protect all systems of TSK in the cyber space.
2. To respond to cyber incidents 24/7.
3. To participate in national and NATO exercises.
4. To organize training and awareness raising activities in the TSK.
5. To test and conduct routine cyber security inspections in the networks used by onTSK.

The Communications and Information Systems (MEBS) Support Command was complemented by the establishment of the TSK Cyber Security Command Center Directorate in June 2012. Later, the Directorate was reorganized into the MEBS and Cyber Security Command in August 2013.[49] Reportedly, the MEBS and Cyber Security Command operates with roughly 30 personnel and is headed by a Colonel ranked officer and works on a 24/7 basis, primarily responding to cyber-attacks and testing TSK networks and systems.[50]

It can be gathered that the TSK has a very different approach to cyber command compared to that of the global approach. Judging by subsequent reports in Turkish media, it can be seen that the Command is also gathering intelligence to protect the infrastructure of TSK. In line with the assessment made by a member of the Cyber Security Command, it can be understood that TSK has structured its cyber security management in three layers.[51] At the top of this hierarchy rests TSK Cyber Defense Management Board, which is responsible for policy and decision-making processes. In the second layer is TSK Cyber Security Command, which runs the cyber units of the Turkish General Staff, navy, army, air force, coast guard as well as the gendarmerie, which comprise the third tier.

The main problem of military cyber operations that TSK is running is its attempt to respond to asymmetrical attacks with a symmetrical and hierarchical structure. TSK is facing similar problems due to its engagement strategies that are focused on land, sea, and air domains. In order to overcome these challenges and pose a stronger stance, TSK has to design a new structure and develop new strategies that could dynamically respond to hybrid threats. In this context, the fact that the responsibilities of TSK Cyber Command and its role in the national

cyber defense architecture is not clearly defined is posing itself as another complicating factor. In addition to this ambiguity, it can be said that TSK is also underestimating the role of third party contractors and social engineering. However, it is possible for hackers to access information and references pertaining to the particular hardware and software that TSK uses through contractors. The personnel management policy of TSK may also be preventing the Cyber Defense Command to accumulate experience. In order to compete with the private sector and retain experienced cyber security personnel in the command, TSK has to reevaluate its personnel management policy as well as the payments and benefits that it provides. In the long run, TSK has to consider how to attract young and gifted minds to its service.

Moreover, in 2014 Turkish Armed Forces prepared a Project Definition Document on Cyber Security, which was approved by the Minister of National Security. According to this document, TSK will only procure Turkish-made software and hardware for Cyber Command, but these software and hardware would also have to be compatible for use in joint exercises with NATO.[52] Cyber Command took part and coordinated Turkey's participation in NATO's Cyber Coalition 2014 exercise that took place on November 17-21, 2014.[53] Furthermore, the document stated that the size of the Communications and Cyber Security Command would be expanded to reach 80 personnel.[54]

2.4. Cyber Defense Structure of the Turkish National Police (TNP)

The Turkish National Police (TNP) set up its first Computer Crimes and Information Security Council in April 1998. This council paved the way for the establishment of the Informatics Crimes Study Group on March 1999 to outline informatics crimes, study existing domestic and international regulations, distinguish amongst various types and means of IT criminal activity, and assign tasks to directorates within the TNP.[55] Even before this group was founded, however, the TNP had been dealing with cyber-crimes, including the country's very first case of criminal prosecution of a blog post in 1997. In this case, the defendant criticized police brutality on a blog post and was reported by an individual to the TNP – the defendant was later arrested by one of the TNP's counter terrorism units.[56] The defendant was later prosecuted for "openly insulting and lampooning the state's security forces" under Turkish Penal Code Article 159/1.

In 2011, the TNP established a department, called Combating IT Crimes (renamed Combating Cyber Crimes Department in February 2013), for fighting against cyber-crimes. The unit was recently mentioned in the Turkish media for allegedly outsourcing extralegal wiretapping and tracing activities to an Italian company called Hacking Team.[57] According to reports, the TNP contacted the company initially in 2011 and has continued to renew its contract over the years with the latest renewal executed on February 2015.[58] It is reported that the TNP has thus far paid the company €440,000 and received hardware, training, and remote control and data injection software.

2.5. Intelligence and Counter-intelligence

The ambiguity of cyber space affects security concepts as well. Terms such as, cyber espionage, cyber spying, and cyber intelligence are used interchangeably due to their similar connotations. In fact, they all depend on similar vectors of attack and technology. Yet it is challenging to

definitively determine whether the perpetrator of a cyber-attack is a state or a non-state actor. Some states take advantage of the fact that cyber space is ambiguous and unowned. The main aspect of cyber intelligence is collecting information through cyber means to address cyber security threats.

In Turkey, the National Intelligence Service (MIT) is one of the units responsible for collecting the necessary intelligence to prevent cyber security threats. The "Law Amending the Law on State Intelligence Services and the National Intelligence Agency" (Law No. 6532, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun), which gave MIT mandate on this area, entered into force on April 26, 2014. In the new law, the responsibility of MIT is redefined as:

> "To deliver the produced intelligence to relevant institutions on Foreign Intelligence, National Defense, Counter-terrorism, international crimes and cyber security topics by using all types of technical intelligence, human intelligence via utilizing relevant tools, methods and systems with the process of collecting, recording and analyzing pertinent information, document, news and data."[59]

Although there is no public information regarding how the amendment clearly changed the organizational structure of MIT, recent job opening announcements have provided clues about the new division of labor. By looking at the MIT job openings page, it can be gathered that MIT is seeking experts in the following fields: Signal Analysis and Applications, Crypto and Crypto Analysis, Cyber Activities,[60] Satellite Communication, GIS, Audio-Visual Processing, Telecommunications Systems, Software Development, Communication Software Development, Hardware Development, Mobile Application Development, System Management, Network Management, Database Management, Information Security and Internet Technologies, System Analysis, Mechanical System Design, System Support and Training, Data Processing. All these expertise requests show that MIT is preparing its organizational structure for a cyber intelligence framework.

After the amendment to Law no. 6532, then Prime Minister Erdogan started the re-organization process of the TIB and assigned the task to MIT. Indeed a candidate supported by MIT, Ahmet Cemalettin Celik, a former member of MIT, was appointed as the Chairman. Celik's assignment suggests that TIB and MIT are closely cooperating on cyber security issues like cyber monitoring. However, it cannot be said that this alleged collaboration increases cyber security awareness or entails actual cyber defense activities.

2.6. Recent Developments

At the end of 2013, Turkey was shaken by a corruption scandal unearthed by leaked tapes and phone conversations. During the subsequent months, an ample amount of voice recordings – including those recorded in a highly sensitive top-level meeting at the Foreign Ministry – were released, and the probes to discover their origins spread to TÜBİTAK and BİLGEM by the beginning of 2014. A considerable amount of TÜBİTAK employees, including the Deputy President of TÜBİTAK and Head of BİLGEM, Hasan Palaz, lost their jobs. In his book regarding the probe, Palaz argues that in the first quarter of 2014, 80 percent of all administrators were purged or pressured to leave TÜBİTAK for political reasons.[61] By 2015, the number had reached more than 1,000 scientists and researchers. In other words, a quarter of all TÜBİTAK employees were gone. Palaz argues that this has resulted in a considerable loss of capability and expertise on the side of TÜBİTAK. As a matter of fact, in March 2015, BİLGEM rejected the request of a court to analyze four hard discs that were presented as

evidence in an illegal organization case on the grounds that the "organization did not have proficient and suitable personnel to analyze the evidence due to the high level of reshuffling of the personnel in the last six months."[62]

On February 6, 2014, Parliament approved an omnibus bill, Law No. 6518.[63] The bill included several changes to Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications, dated May 4, 2007.[64] With the new omnibus bill, TİB was put in charge of coordinating – under the scope of national cyber security activities – content, area, and service providers, and other related agencies and institutions on the issue of detecting and preventing cyber-attacks. Furthermore, the omnibus law made changes to the Electronic Communication Law No. 5809, dated November 5, 2008.[65] With these changes, BTK became responsible for "fulfilling the tasks on the fields of cyber security and internet domains given by the Cabinet, UDH and/or the Cyber Security Council through the use of TİB or any other of its units."[66] With Article 106 of the omnibus law, the Cyber Security Council was tasked with approving policies, strategies, and action plans on cyber security. The Cyber Security Council became responsible for making the necessary decisions on the effective implementation of these policies, strategies and action plans throughout the country, finalizing decisions on suggestions for determining critical infrastructure, determining the institutions and agencies that would be exempt from all or some of regulations on cyber security, and fulfilling other tasks set forth by the law. The amendment suggested that the guidelines and procedures on the workings of the Cyber Security Council were to be determined upon regulations put forth by the Office of the Prime Minister.

TİB gradually gained more authority and responsibility in the realm of cyber security. An amendment passed in March 2015 gave TİB the right to control the removal of content and prevention of access to web pages "in cases where the delay of a decision could endanger the protection of the right to life, the protection of the life and private property of the people, the protection of national security and public order, prevention of crime or the preservation of the public health, upon demand by the Prime Ministry or ministries dealing with national security and the protection of the public order, prevention of crime or the preservation of public health."[67] In this process, after TİB decides to remove content or block access to a page, it notifies the related access, content, and area providers, who then must take action within four hours. According to the law, failure to comply with TİB's request results in an administrative penalty ranging from 50,000 to 500,000 TL ($19,000-190,000 USD).

TİB must also report its decision, within the first 24 hours after taking it, to a penal court of peace, and the civil judge has to decide upon the matter within 48 hours after receiving TİB's pledge. If the judge does not agree with TİB's decision, the ban is automatically lifted. On the other hand, if the judge agrees with TİB's decision to ban access to content or web pages, then content, service, and access providers must present "the information necessary to reach the culprits of the crime" to legal authorities upon the request of the judge, otherwise face administrative penalties.[68] Access providers have to obtain all the necessary hardware and software to comply with TİB's decisions on their own and must take preventive measures against alternative access methods to banned publications.[69] The law established an Access Providers Union (ESB – Erişim Sağlayıcıları Birliği in Turkish), in which participation is mandatory to facilitate compliance with the law and TİB's decisions. Members of the union are required to obtain all hardware and software needed to comply with TİB's decisions. In sum, with the amendments in 2015, TİB gained the authority to suspend access to content and web pages rapidly, as well as strong financial and legal deterrents to ensure compliance.

3. Non-Governmental Actors: Local Hacker Groups And Their Motivations

Turkish hackers play a role in international cyber-attacks. However, there is no study on the profile of these groups for future reference. The capabilities of Turkish hackers are critical in evaluating domestic cyber threats in Turkey. In recent years, states have voiced support for changing the Internet infrastructure as we are accustomed to now, by blocking connectivity and permitting the use of intranet connections.

The following characteristics describe the typical profile of Turkish hackers:

- Age between 14 to 45 years old but majority between 18 to 25 years old
- Mostly high school or university graduates and not all studied computer science
- New hackers learn skills from hacker forums and mostly use basic hacking tools
- 92% male, 8% female
- Mostly from middle or lower income level families
- Prefer to use Social Engineering[70] and Reverse Engineering[71]
- Small group interested in satellite data sniffing, intelligence, etc.[72]

In Turkey, several hacker groups began to emerge following the civilianization of the Internet. This section will focus on seven of those groups: Ayyıldız, RedHack, B3yaz Hacker, Turk Hack Team, Cyber Warrior (Akıncılar), Türk Güvenliği, and PKK Hack Team.

3.1 Ayyıldız Team

According to their website, the Ayyıldız Team was formed in 2002. The group listed its mission under seven points:

> "1. To protect the Republic of Turkey and its all public institutions against all attacks.
> 2. To stop the websites on satanism, pornography, and any site that tries to change the constitutional regime.
> 3. To provide technical support to websites and systems which are valuable to public service.
> 4. To protect the websites ending in gov.tr, pol.tr, edu.tr, bel.tr
> 5. To organize anti-propaganda activities to protect the reputation of the Republic of Turkey.
> 6. To respond forcefully to the verbal, written, and active attacks against the Republic of Turkey with the approval of the group's board of governors.
> 7. To publish declarations to raise the awareness level of the public."[73]

There were 13,579 notifications on Zone-H website[74] on the cracking activities of Ayyıldız Team. In one of the defaced websites, which was also recorded by Zone-H, the Ayyıldız Team introduced itself as Turkey's Cyber Army, with the following note:

> "We are Turkey's Cyber Army.
>
> Homeland to the enemy to the cold, snow, winter fighting in the virtual world how to fight for the sake of the motherland.
>
> I never tired. We do not ever give up. Support each other, we are always a good day bad day.

> Turkishness against our religion, and having bad ideas all states will open a virtual war.
> Get ready for a virtual war on bad ideas, if you continue this! Anyone not afraid!
> Where necessary, to give the answer!
>
> AYYILDIZ TEAM
> TURKEY'S CYBER ARMY"[75]

As seen in these lines and in the principles, Ayyıldız is a self-declared patriotic hacker community that mostly cooperates or works in parallel to state goals.[76] However, six members of the Ayyıldız Team were detained for blackmailing the site owners. Ayyıldız Team denied the membership of these persons. But still there is some suspicion about the groups' activities and connections with criminal activities.[77] In addition to these speculations, Ayyıldız Team mostly presents a pro-state standing with its attacks. Particularly, the recent defense of Ayyıldız Team against the Anonymous mass attack campaigns to Turkey also demonstrates that the former does not constitute a threat to Turkey's prospective nuclear power plant's cyber security.[78]

3.2. RedHack

RedHack is one of the most notorious hacker groups in Turkey. In one of its interviews, the group leader claimed that RedHack was established in May 1997.[79] RedHack explains its ideology as using hacking for an equal, just and non-exploitative world.[80] RedHack also formulates its position as "...at the disposal of any organization that targets the [fascist] order.[81]"

Zone-H website has several records of web defacements attributed to RedHack, starting in 2008.[82] The hacking group began to garner more attention after its first attack to the Ankara Police Department's website and with the subsequent distribution of classified documents to the public.[83] The group gained popularity after its intensified attacks to the government offices following the Gezi Park Protests in 2013.[84] After another attack, RedHack released the e-mail accounts and password information of police officers within Ankara Police Department. In addition to these attacks, RedHack defaced the websites of Turkish Police, Turkish Football Federation, National Intelligence Organization, Türk Telekom, and Air Forces Command, Turkish Airlines, Higher Education Council, Ministry of Foreign Affairs and published various classified documents such as ID card of diplomatic mission members and classified communication between governmental offices that it captured.[85]

RedHack has the capacity to cooperate with international hacker groups. In 2013, RedHack and Anonymous worked together to execute the attack on the Israeli Intelligence Service's (MOSSAD).[86]

3.3. B3yaz Hacker

This hacker group uses a modification of the Turkish word for *white*, or *beyaz*, in its name in reference to white hackers (i.e. non-malicious hackers) who report vulnerabilities to manufacturers in order to make online systems more secure.. On its website, the group announces that its staff is ready for Pentest[87] requests. This is the only example in Turkey where a hacker group offers its hacking capabilities for a proper Pentest service. Since the penetration testing depends on trust, firms prefer to hire trustworthy private security companies, which can guarantee the protection of sensitive information regarding the firm.

B3yaz Hacker's attacks can be divided into two groups. The first group of attacks is conducted to inform websites of their vulnerabilities. The second group of attacks are against websites that host content that are against the group's moral values. On Zone-H, there are several records under B3yaz.org, B3yaz, B3yazHacker, which contain 540 defacements in total on different websites with most of the attacks taking place in 2015. After inspecting the capabilities of B3yaz Hacker group, it is possible to say that it is not a treat to the nuclear power plants and critical infrastructure of Turkey.

3.4. Turk Hack Team

Turk Hack Team is one of the most organized and well known hacker groups in Turkey, which was established in 2002. [88] Its website is one of the most organized websites amongst hacker groups, including sections ranging from history to theater, training to e-books. The design of the website shows that the administration of Turk Hack aims to form a community and train it via the website. Throughout the last decade, the group has kept its nationalistic stance, but now includes more religious undertones. The members define the group as "Muslims who love their homeland."

The group's self-declared mission consists of the following:

1. To halt the websites which publish items contrary to the Turkish language, religion, beliefs, customs, ethics, and values.
2. To popularize the idea that hacking is not an action for fun but rather a goal.
3. To assist righteous, ethical, and helpful websites on technical issues for free.
4. Turk Hack Team works for the Turkish nation.
5. To aid Turk Hack members who accept these terms on any condition.[89]

The Turk Hack Team claims that they control one of the largest botnets in operation. In Zone-H website, there are many records of Turk Hack Team with slightly different spellings, which obstructs the comprehension of its precise capabilities. However, Turk Hack Team's leader Zorrokin's recent attack to the website of the Holy See, just after the Pope's declaration on Armenian issue, gives some ideas about its qualifications and potentials.[90] The group's most recent attack was against The New York Times after it published an article critical of the Turkish president right before the Turkish parliamentary elections (07 June 2015). The attack stopped homedelivery.nytimes.com, es.nytimes.com, blog.nytimes.com, app.nytimes.com, register.nytimes.com and harmed the hosting server.[91] Following the attack, the Turk Hack Team attacked The Guardian following the publishing of an article criticizing the Turkish president, causing limited disruption to the newspaper's website and server.[92] All of these attacks give clues about the group's capabilities. The pro-government tendency of the group renders it unlikely to pose a threat to the planned nuclear power plant in Turkey.

3.5. Cyber Warrior (Akıncılar)

Cyber Warrior, also known as Akıncılar[93] (Turkish for "Raiders"), is a group that was established in 1999 with the name illegal-port. Later, they restructured this group under the name Cyber Warrior. The group's hierarchy mirrors that of the military. In one of the early recruitment calls of the group, Cyber Warrior's defined itself as a way of brotherhood.[94]

The group listed the qualifications it seeks in its members as the following[95]:

- Devoted to our religion, traditions and customs.
- Turkish nationalists.
- Thoseready to be part of the Cyber Warrior brotherhood.
- New members should not curse at, or use slang when communicating with other team members. If one swears at one of us, he swears at all of us.

The Cyber Warrior website claims that the group was active during the Turkish Internet law (No. 5651[96]) preparation period, which could infer that it is close to Turkish decision makers or the political elite. After the legislation of Turkey's cyber security (5651), the group rephrased its mission, consistent with the Internet Law:

- The group will fight against satanic and pornographic content that attacks its faith and moral values and confuses pure minds on the Internet. All websites that bear a negative effect on public conscious as well as those that are against Turkey are included in this category.
- The group will technically support the institutions, websites, and groups that share the ideas listed in underneath its mission, without expecting any repayment.
- The group will not attack any websites or groups insofar as they do not attack its values.[97]

The group also elaborated on its tasks under the organization section of its website:

- The Cyber Warrior team has no ideological or political attachment to any association, institution, organization, or political party.
- Any new member accepted to the group will be assigned a position commensurate with his/her skills.[98]

In several of its online forums, the Cyber Warriors claim that it did not attack any website in Turkey.[99] This behavior change of Cyber Warrior group seems consistent with the claim that the group has connections with the Turkish police in different levels.[100] Zone-H has 7,895 defamation records for this group. The Cyber Warriors has attacked Israel, Egypt, Austria, and Armenia, among others.[101]

All available evidence shows that the group has strong relations with the state.[102] The HP Cyber Security Research Cyber Risk Report 2015 categorized it as a state-sponsored hacker group based on the following evidence:

> "Members of the hacker team Akıncılar, part of the Cyber Warrior team threat actor group, were commended by the Turkish police for their attacks against RedHack and other entities perceived as a threat to Turkish or Islamic ideals. Several actors in Akıncılar are also on the management team of the Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği (Information Security and Counter Cyber Crime Association), which has provided free information security support to gov.tr and pol.tr domain names and has submitted sensitive information to government entities.
>
> In April 2012, representatives from Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği (Information Security and Counter Cyber Crime Association), including the group's manager Gökhan Şanlı, participated in a meeting on stopping access to certain websites in Turkey and intellectual property rights at Çankaya Köşkü, the Turkish equivalent of the White House. Şanlı, who uses the alias Doktoray, manages the Cyber Warrior forums. The now deceased Halit Uygur, who used the alias Dogukan, was a key figure in Cyber Warrior TIM and was also a key figure in the Ministry of National Education in Istanbul."[103]

The activities of the Cyber Warrior group show that it is most likely not to be considered a threat to Turkish nuclear power plants.[104] However, any change in the political climate can alter the group's behavior and position. It would be prudent for the Turkish government to follow the activities of the group to prevent unexpected attacks.

3.6. Türk Güvenliği

Türk Güvenliği, Turkish for Turkish Security, was established in 2006 by Agd_Scorp, a famous hacker and current leader of Türk Güvenliği. Türk Güvenliği became known internationally after a series of attacks on fuse.microsoft.com, The Register[105] and Vodafone. The Guardian described the group's activities as follows:

> "A Turkish hacker group diverted traffic to a number of high-profile websites including the Telegraph, UPS, Betfair, Vodafone, National Geographic, computer-maker Acer and technology news site the Register on Sunday night, putting unwary users at risk of having passwords, emails and other details stolen."[106]

After the attacks, The Guardian interviewed the group, which elevated the international reputation of the group.[107] At the time of research, Türk Güvenliği's website was not active, but Agd_Scorp had a manifesto on Pastebin[108] website in which he briefly clarified his approach:

> "Freedom, is what you must fight for. The world may not know me. But, people in the underground know who I am, and some people, know of my work.
>
> I always had a dream on hacking large organizations on the internet. After a early time, my dreams did came true.
>
> I've hacked Google, Microsoft, MSN, NATO, Nintendo, Sony, NASA, Kaspersky, Avast, AOL, Pentagon, TrendMicro, CocaCola, Peugeot, UNESCO, .mil domains, Yahoo, Playstation Network, UPS, National Geographic, Telegraph, The Register, spam.org, resellerclub.com, eNom and even fbijobs.gov & interpol.com."[109]

Zone-H recorded 225 defacements for Türk Güvenliği[110] and 424 for Agd_Scorp.[111] In the beginning, the group mainly used SQL injection techniques[112] but improved its skills and methodology. Because Türk Güvenliği's ideology is not clear, it is difficult to predict its moves; however, in one instance, the group responded to Syrian Electronic Army's (SEA) phishing attacks against various Turkish governmental sites. The SEA also leaked several Turkish official documents on its website. As a response, Türk Güvenliği hacked SEA's website and left a message that included Quran verses.[113] The attack to SEA's website and the message that it left proved the group's nationalist tendencies. As a nationalist group, Türk Güvenliği does not constitute a threat to Turkish nuclear cyber security.

3.7. PKK Hack Team

PKK Hack Team is a branch of the Kurdistan Workers' Party also known as Partiya Karkerên Kurdistanê (PKK). The PKK was founded as a Marxist-Leninist organization before turning into an primarily Kurdish nationalist movement over the course of the 1980s and 1990s. There is limited information on the PKK Hack Team regarding its online activities. The earliest news about its activity goes back to 2006, in which two hackers defaced 2,307 governmental and non-governmental sites and placed its signatures.[114] Police detained two pro-PKK hackers. In 2008, one of the PKK hackers was captured by the Turkish police during a routine search in Diyarbakir, Turkey. Police stopped the hacker on suspicion of a stolen

laptop that he was carrying and later found encrypted confidential information; documents; passwords; malware code by the name of Poison Ivy; and video recordings of the General Staff, the National Intelligence, and Gendarme of Turkey. After a subsequent search of the hacker's house, the police confiscated 924 CD-ROM's, 57 DVD's, 22 Hard disks, and two laptops. The investigation ended with the detainment of the PKK courier who was carrying this information to PKK headquarters.

During the interrogation, the hacker confessed that he obtained all this information by planting his own malware into pornographic sites and infiltrated the computers of the intelligence service and army staff using this vulnerability.[115] This hacker's skills and the PKK Hack Team's organizational skills astonished the law enforcement officials. In 2011, Turkish police conducted operations to stop PKK hackers in Şanlıurfa, Hakkari, Batman, and Gaziantep.

The PKK Hack Team has two different records in the Zone-H website. In one of them, the PKK Hack Team clocked in 279 defacements[116], the other registry has 241 defacements according to the Zone-H website.[117] Before the June 2015 elections, the rising tension between HUDAPAR and PKK in Eastern Turkey[118] boosted the conflict in cyber space.[119] These clashes introduced a new hacker group, the T. A.K. (Teyrenbazên Azadiya Kurdistan – Kurdistan Freedom Hawks) Hack Team.[120] This group mostly targeted Twitter accounts and kept a low-profile.[121] To sum up, all pro-PKK hacker teams constitute a risk to nuclear power plants. They can cooperate with other hacker groups to organize an attack. Moreover, the PKK and PKK Hack Team can use their hybrid capabilities to inflict more harm to the facilities. They are the only group with the ability to utilize both kinetic and cyber-attacks to paralyze critical infrastructure. Therefore, both the public and private sectors must follow the group closely.

4. Conclusion: Ankara's Plans for the Future

It may be argued that the Turkish cyber-crime scene is in fact invaded due to intense activities of a multitude of actors. The fourth quarter of 2014 alone witnessed attacks originating from 199 countries or regions. China, USA, Taiwan and Russia take the lead amongst the origins of cyber-attacks against Turkey.[122]

Ultimately, it can be seen that Turkey is subject to an increasing wave of cyber-crimes.[123] In terms of the number of cyber-crimes committed, Turkey is placed as the 9th country (out of 20) to face the highest number of attacks. Turkey experiences 3 percent of the total global malicious computer activity. Regarding malicious codes, Turkey ranks the 15th. In the ranking for the origin of the attacks, Turkey holds the 12th position. The country is placed as the 5th for zombie spam and 24th for phishing web site hosts.[124] In the evaluation of a report prepared on this subject, Turkey is the 8th regarding distributed-denial-of-service attacks for the second quarter of 2014.[125] In conclusion, the information and data presented in this section demonstrate that, in terms of cyber-attacks, the level of threat that Turkey is exposed to should carefully be considered. "37 times more Sality and 1.6 times more Zeus Gameover infections per 1,000 users than Germany, a country of similar population size but almost double the number of Internet users."[126]

The information at hand suggests that cyber criminals "exploit the weakest targets first".[127] From a potential attacker's point of view, what matters most while picking the targets is the relative level of security that a certain country or a sector in a certain country has. For this, an attacker ensures that his/her initiative is low-cost and that the financial, political or other returns match expectations. These prospects are obviously higher to fulfill in weaker targets compared to stronger ones.

Seeking to establish a roadmap of the country's cyber security program for the next five years, the Ministry of Development released a draft plan for 2014-2018 entitled "Information Society Strategy and Action Plan." The Plan lists five ambitious courses of action to bolster Turkey's cyber security capabilities.[128] The first two calls for the creation of the National Information Security Law – which has been under consideration since the beginning of the 2000's – and the ratification of the Law on the Protection of Personal Data by the end of 2015. The third recommended course of action is the completion of a Strategy on Combating Cyber Crime and Action Plan in 2016. The main responsible party for this task would be the Turkish National Police, Ministry of Justice, Ministry of the Interior, Ministry of Foreign Affairs, Gendarmerie General Command, Ministry of Transport, Maritime Affairs and Communication, and Presidency of Telecommunication. [129] The fourth action order is to raise awareness about best practices of Internet safety. The final action item listed in the draft document is the foundation of courts specialized in IT crimes by the end of 2015.

Although Turkey has gradually increased its capabilities and presence in cyber space, this has not been realized at the same level across the board – resulting in making significant leaps in some aspects while stagnating in others. Nevertheless, the last few years have seen a rise in the number of governmental institutions dealing with cyber security and Turkish security forces have put an additional focus on dealing with cyber threats. Furthermore, politicization of some issues has served to be a complicating factor in Turkey's ambitions to augment its capabilities in the cyber realm, as exemplified by the failure to ratify key draft laws, and the loss of considerable human capital at TÜBİTAK. As a result, Turkey continues to lag behind its key

allies and rivals in terms of its preparedness for cyber security.

Open source information on the capabilities of hacker and cracker groups operating in Turkey is limited. Anti-nuclear groups, institutions and individuals that may turn into cyber criminals (referred to as lone wolves) are amongst those facts that may pose a threat to Turkey's nuclear facilities. Among these are local actors like Redhack, and terrorist groups such as, PKK affiliated PKK Hack Team that are driven by political aims. In this context, an interesting point regarding the Turkish cyber-crime world is the variety of rival groups that conduct activities deemed appropriate or inappropriate by the state, based upon their standing and relations with state institutions and political authority. The most known and best-fitted example to this is the rivalry between the self-declared Marxist socialist group Redhack and Australia-originated Ayyıldız Team, with an ethos to protect Turkey's public institutions and defend the country's interests.

Such a distinction is not acceptable for agencies and institutions tasked with defending Turkey's critical infrastructure. Though they may function under different names to conduct cyber "operations", it must be noted that the motives, priorities and aims of these groups may change in time and according to developments. As such classifying these groups according to their political stances and priorities and treating them accordingly would undoubtedly increase cyber security vulnerabilities. Furthermore, there are examples of ad hoc partnerships formed from time to time between different criminal or terror networks based on converging interests. In this context, the potential for rival states to support these groups or conduct hostile cyber attacks directly under the guise of these organizations complicates the threat environment for Turkey. Finally, given that nuclear energy plants are projects that involve international partners, the prospect for cyber attacks that target the vulnerabilities and interests of Turkey's partners should not be overlooked.

1- Libicki, M. C. (2009) "Cyberdeterrence and Cyberwar" Rand Corporation

2- International Telecommunications Union (Geneva) (2014) "Percentage of Individuals Using the Internet 2000-2013", http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls, Accessed on 9 November, 2015.

3- Bloomberg (2013, April 23) "Top Ten Hacking Countries"

4- Turkish Grand National Assembly (Türkiye Büyük Millet Meclisi), "Law on Amending Certain Clauses of the 765- dated Turkish Penal Code" (765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun), Law No. 3756 Date of approval: 6.6.1991 (Official gazette publication: 14.6.1991, No: 20901) http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf also see: http://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d18/c061/b127/tbmm180611270516.pdf, Accessed on 16 July, 2014.

5- Türk Ceza Kanunu (Turkish Penal Code) (2004, September 26) Law no. 5237

6- Dokurer, S. (2002) "Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri" (Informatics Crimes in our country and Means of Combating them) EGM Bilgi İşlem Daire Başkanlığı Bilişim Suçları Büro Amirliği, http://bilisimsurasi.org.tr/dosyalar/17.doc, Accessed on 23 September, 2014.

7- The first article on the definition of terror, with the amendment in 15 July 2003, reads: "Terrorism is any kind of act done by one or more persons belonging to an organization with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish State and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat."

8- These include item 113 on obstructing the right to access public services, 142 on qualified theft (which refers to the use of IT systems specifically in 142.2.e), 151 and 152 on damaging property and qualified ways of damaging property, 170 on deliberately endangering public security, 213 on threats with the aim of creating fear and panic among the general public, and arguably, article 172 on spreading radiation and article 173 on causing explosions with the use of atomic energy.

9- Şentürk, H. et al. (2012), "Cyber Security Analysis of Turkey" International Journal of Information Security Science Vol.1, No. 4

10- Official Gazette of the Republic of Turkey, (2006, June 28) No: 26242, "Bilgi Toplumu Stratejisi Eylem Planı" (Information Society Strategy Action Plan) (2006-2010)", http://www.resmigazete.gov.tr/eskiler/2006/07/20060728- 7.htm, Accessed on 16 July, 2014.

11- Ibid.

12-) T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü (Republic of Turkey Prime Ministry General Directorate of Laws and Regulations) (2008, 22 April) "Kişisel Verilerin Korunması Kanunu Tasarısı", (Protection of Personal Data Draft Law) http://www2.tbmm.gov.tr/d23/1/1-0576.pdf, Accessed on 18 July, 2014.

13- Accessed from the Republic of Turkey Prime Ministry's web page on 21 June 2014 from: http://www.basbakanlik.gov.tr/Handlers/FileHandler.ashx?FileId=1167

14- T.C. Başbakanlık (Republic of Turkey Prime Ministry) (2002, August) "e-Türkiye Girişimi Eylem Planı (TASLAK)" (e-Turkey Initiative Action Plan (DRAFT)).

15- Aksakal, A. (1999) "Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı", (National Information Security Structure and Roles, Draft Law) Journal of Turkish Librarianship Vol. 13 No. 4 pp. 438-457

16- "Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı", (Directorate General for Information Technology and Coordination) (2010, May), "Kritik Altyapıların Korunması" (Protection of Critical Infrastructure)

17- Law No. 5651 Article 10.6 (Amendment made on 6 February 2014 - 6518/95) Accessible from: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

18- TÜBİTAK-BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (National Research Institute

of Electronics and Cryptology) web page, "Tarihçe" (History). Accessed on 16 July, 2014 at: http://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

19- TÜBİTAK-BİLGEM's webpage "History". Accessed on 16 July, 2014 from: http://bilgem.tubitak.gov.tr/en/kurumsal/history

20- TÜBİTAK Siber Güvenlik Enstitüsü (TÜBİTAK Cyber Security Institute) web page, "Tarihçe" (History). Accessed on 16 July, 2014 from: http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

21- TÜBİTAK-BİLGEM's webpage "History". Accessed on 16 July, 2014 from: http://bilgem.tubitak.gov.tr/en/kurumsal/history

22- Şentürk, H. et al. (2012), "Cyber Security Analysis of Turkey" International Journal of Information Security Science Vol.1, No. 4

23- Ibid.

24- TÜBİTAK-BİLGEM's webpage "History". Accessed on 16 July, 2014 from: http://bilgem.tubitak.gov.tr/en/kurumsal/history

25- Ibid.

26- Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" International Journal of Information Security Science Vol.1, No. 4

27- Bekdil, B. E. (2013, December 1) "Cybersecurity an Emerging Market in Turkey" Defense News

28- Presentation at Institutional SOME Event on 30 January 2015 organized by USOM and TUBİTAK in Ankara, last accessed at https://www.usom.gov.tr/faydali-dokuman/15.html on 14 April 2015.

29- Bilişim Dergisi, "2. Ulusal Siber Güvenlik Tatbikatı Yapıldı" (2nd National Cyber Security Drill has been Executed) Vol.151 p:148-151 http://www.bilisimdergisi.org/s151/

30- The report comes with the disclaimer that it does not represent the views of the Authority. Please see Unver, M. et al. (2009, May), "Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler" (Cyber Security Provision: Current Situation in Turkey and Measures to be Taken), Bilgi Teknolojileri ve İletişim Kurumu

31- Sabah (2010, October 28) "Kırmızı Kitap'a MGK'dan vize" (Visa for Red Book from the National Security Council)

32- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (Republic of Turkey Ministry of Transport, Maritime Affairs and Communication, Information Security Foundation), (2012, June), "Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için" (National Cyber Security Strategy: For a strong and leading Turkey in 2023's cyber space)

33- One such attempt is the Pardus project, a Linux based OS initially developed by a group of developers sponsored by TÜBİTAK UEKAE and made its first release in December 2005. European Commission ISA Joinup (2008, Nov 27) "A new kid on the block: The Turkish Pardus Linux Distribution" Some of the users of Pardus included the Ministry of National Defense – which reportedly saved $2 million by switching to Pardus – and the Social Security Institution. NTVMSNBC (2009, April 14) "MSB, Pardus ile 2 milyon dolar tasarruf etti" (Ministry of National Defense saved 2 million dollars with Pardus) NTVMSNBC (2009, April 13) "SGK, Pardus'a göç etmeye hazırlanıyor" (Social Security Instutiton is preparing to migrate to Pardus). The project came to a halt in 2011, reportedly due to major losses in the work force following political shifts in TÜBİTAK. www.shiftdelete.net (2012, Feb 01) "Yerli Pardus'ta Sona Doğru" (Towards the end in national Pardus) Accessed on 9 September, 2014 from:http://shiftdelete.net/yerli-pardusta-sona-dogru-34654?p=1. After two years without any releases, the 2013 version of the OS was released. Upon announcing his government's program on August 2014, Prime Minister Davutoglu made a specific reference to Pardus, suggesting that the aim of the government was to disseminate Pardus to public and private institutions. Pardus Portal Web Page (2014, August) "PARDUS 62. Hükümet Programında Yerini Aldı!" (Pardus took its place in the 62th Government Programme!) Accessed on 9 September, 2014 from: http://www.pardus.org.tr/pardus-hukumet-programinda

34- An earlier document dated May 2010 penned by BTK staff inspects the various international definitions and legislations regarding critical national infrastructure and points to the lack of steps taken regarding CNI in Turkey.

Please see Ünver, M. et al. (2010, May) "Kritik Altyapıların Korunması" (Critical Infrastructure

Protection) Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, (Directorate General of Information Technologies and Coordination)

35- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (Republic of Turkey Ministry of Transport, Maritime Affairs and Communication, Information Security Foundation, (2012, June), Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için" (National Cyber Security Strategy: A strong and leading Turkey in 2023's cyber space) " pp.11-12

36- Bakanlar Kurulu Kararı (Council of Minister's Decision), 2012/3842 published in the Official Gazette no. 28447 dated 20 October 2012

37- Bakanlar Kurulu Kararı (Council of Minister's Decision), 2012/3842 #5.1.ç published in the Official Gazette no. 28447 dated 20 October 2012

38- Republic of Turkey Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013-2014 Action Plan" The document in English can be accessed from the NATO Cooperate Cyber Defence Centre of Excellence web page: http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf

39- Republic of Turkey Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013-2014 Action Plan" p.8

40- Republic of Turkey Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013-2014 Action Plan" p.28

41- Republic of Turkey Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013-2014 Action Plan" p.32

42- Republic of Turkey Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013-2014 Action Plan" p.19

43- "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" (Communique on the Foundation, Duties and Workings of Cyber Emergency Response Teams), published on the Official Gazette no. 28818 dated 11 November 2013

44- Presentation at Institutional SOME Event on 30 January 2015 organized by USOM and TUBİTAK in Ankara, last accessed at https://www.usom.gov.tr/faydali-dokuman/15.html on 14 April 2015.

45- BTK Web page "USOM-SOME" Accessed on 14 April 2015 from: http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usomsome.php

46- Ibid.

47- T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı (Disaster and Emergency Management Authority) (2014, Eylül) "2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi" (2014-2023 Critical Infrastructure Protection Road Map Document) Accessed on 30 November 2015 at: https://www.afad.gov.tr/Dokuman/TR/123- 20141010111330-kritikaltyapi-son.pdf

48-NATO, "Joint Press Conference with NATO secretary General Anders Fogh Rasmussen and Madeleine Albright, Chair of the Group of Experts", 17.05.2010, http://www.nato.int/cps/en/natolive/opinions_63696.htm (Accessed on 29 July 2015)

49- Sabah (2013, December 2) "TSK'dan siber savunma atağı" (TSK's cyber defense offensive)

50- Radikal (2013, January 21) "TSK'da Siber Savunma Merkezi Başkanlığı kuruldu" (TSK Cyber Security Command established)

51- Emre Soncan, "Security Units patrolling online against cyber attacks and crises", Today's Zaman, 24.02.2013, http://www.todayszaman.com/national_security-units-patrolling-online-against-cyber-attacks-and-crimes_307094.html (Accessed on 3 August 2015)

52- Radikal (2014, May 27) "TSK'da siber ordu için önemli adım" (An important step at TSK for the cyber army)

53- Presentation at Institutional SOME Event on 30 January 2015 organized by USOM and TUBİTAK in Ankara, last accessed at https://www.usom.gov.tr/faydali-dokuman/15.html on 14 April 2015.

54- Haber7.com (2013, December 5) "TSK'ya Siber Savunma Komutanlığı" (Cyber Security Command at TSK) Accessed on 26 August 2014 from: http://www.haber7.com/guncel/haber/1102379-tskya-siber-savunma-komutanligi

55- Türkiye Bilişim Şurası web page (2002, Feb 19) "Bilişim Suçları Çalışma Grubu" (Informatics Crimes Study Group) Accessed on 15 September 2014 from: www.bilisimsurasi.org.tr/dosyalar/9.doc

56- "İlkiz, F. (2001, Dec 05) "İnternet Ortamındaki Yayınlarda İki Olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar Üzerine Görüşler" (Two Incidents and Convictions on Internet Publications and Opinions on Legal Studies) Accessed from Türkiye Bilişim Şurası web page on 20 September 2014 from: www.bilisimsurasi.org.tr/dosyalar/45.doc

57- Radikal (2015, July 12) "'Hacker skandalı'nda ilginç ortaklık MHP kasetlerine kadar uzandı" (The interesting partnership at the hacker scandal has expanded to the MHP casettes)

58- Hürriyet (2015, July 9) "Polise faturalı hackerlık hizmeti" (Billed hacker service to the police)

59- The Official Gazette, "Law Amending the Law on State Intelligence Services and the National Intelligence Agency" (Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanunu, no. 6532", No 28983, 17 April 2014, http://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm (Accessed on 23 July 2014)

60- This a strange expertise area that Turkish Intelligence Service asked. The title is not giving exact definition of the area.

61- Palaz, H. (2015, March) "Ömrümü Yedin Bay Böcek!" Cinius Publications pp.184-185

62- Radikal (2015, March 08) "TÜBİTAK'ta dijital analiz yapacak eleman kalmamış!" (TÜBİTAK has run out of staff that makes digital analyses!)

63- "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" (Act No. 6518 dated 6 February 2014 to amend the Decree having force of Law concerning the Organization and Duties of the Ministry of Family and Social Policies and to some Laws and Decrees having force of Law), Official Gazette no.28918 dated 19 February 2014

64- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (Law on the Arrangement of Publications on the Internet and Combating Crimes through these Publications No. 5651) 04 May 2007

65- 5809 sayılı Elektronik Haberleşme Kanunu (Law no. 5809 on Electronic Communication) 05 November 2008, Official Gazette no. 27050 dated 10 November 2008

66- "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" (Act No. 6518 dated 6 February 2014 to amend the Decree having force of Law concerning the Organization and Duties of the Ministry of Family and Social Policies and to some Laws and Decrees having force of Law) Article 103, Official Gazette no.28918 dated 19 February 2014

67- Law No. 5651 Article 8/A (Amendment made on 27 March 2015 - 6639/29) Accessible from: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

68- Law. No. 5651 Article 10 (2007, May 4) Official Gazette No. 26530 dated 23 May 2007

69- Law No. 5651 Article 6/Ç (Amendment made on 6 February 2014 - 6518/89) Accessible from: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

70- "Social Engineering: A deceptive process in which crackers "engineer" or design a social situation to trick others into allowing them access to an otherwise closed network, or into believing a reality that does not exist. To crack computer systems, crackers often employ their well-honed social engineering skills. A robust sample of social-engineering case studies can be found in Kevin Mitnick's book The Art of Deception." Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, p. 293.

71- Reverse-engineering: Involves analyzing a computer system to identify its components and their relationships. Then, the parts of the system are put together in a different form or at some other abstraction level. Reverse-engineering is often done to redesign a system for increased maintainability or to produce system replicas without having access to the original design. Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, p. 269.

72- Ufuk Eriş, "Türkiye'de Kırıcı (Hacker) Kültürü" (Hacker Culture in Turkey), Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Unpublished PhD dissertation, November 2009, pp. 141-200.

73- Ayyıldız Tim Misyonu (Ayyıldız Team Mission), http://www.Ayyıldız.org/navigasyon.php?id=22 (Accessed on 21 September 2015)

74- Zone-H is one of the well-known archive of defaced websites. The site administration checks authenticity of defacements to prevent fake records. The hacker groups submit the proof of their defacement to Zone-H website. By this way, they are building up reputation and history of their activities. For further information, see; http:// http://www.Zone-H.org/

75- This English version may have been translated using translation software such as Google Translate. The direct translation from the Turkish version would be: "We are Turkey's Cyber Army. We fight for our homeland in the cyber world just as we fight against the enemy in the cold, in snow, in winter for our homeland. Never tires. We never give up. We support eachother, we are always together in its good days and bad days. We will wage virtual war against all states that have bad ideas against our religion and Turkishness. If you continue to have these bad ideas, get ready for a virtual war! We are not afraid of anyone! If need be, we will give the necessary answer! AYYILDIZ TEAM. TURKEY'S CYBER ARMY" Ayyıldız Team, "http://www.simos1.gr", Zone-H, http://www.Zone- H.org/mirror/id/13249689, 15 March 2011.

76- Ayyıldız – Tim, Görünmeyen Kahramanlar (Sanal Alemin Askerleri) (Ayyıldız – Team, Unseen Heroes [Soldiers of the Cyber Space], Ankara, 2008, p. 16.

77- Elvan Ezber, "Ayyıldız Tim'e Polisten Çete Baskını" (Police Raid to Ayyıldız Team). Radikal, 12 August 2011, http://www.radikal.com.tr/turkiye/Ayyıldız_time_polisten_cete_baskini-1059754; Elvan Ezber, "Ayyıldız Tim: Bekir K. ile bağlantımız yok" (Ayyıldız Team: We have no connections to Bekir K.). Radikal, 14 August 2011, http://www.radikal.com.tr/turkiye/Ayyıldız_tim_bekir_k_ile_baglantimiz_yok-1059928

78- Gamze Akkuş, "Anonymous resmi hedefe saldırdı. Ayyıldız Tim karşı atakla cevap verdi". (Anonymous attacked official targets. Ayyıldız Team retaliated with attacks) Hürriyet, 10 June 2011, http://www.hurriyet.com.tr/ekonomi/17996737.asp

79- "Kızılhack hedefimiz ezenler" (Kızılhack our aim is the oppressed), Atılım, 21 August 2006, http://web.archive.org/web/20100507133839/http://www.atilim.org/atilim/modules.php?name=Guncel&file=article&sid=16899 (Accessed 3 May 2015)

80- Ibid.

81- Ibid.

82- For further details; "RedHack Defacements", Zone-H, http://www.Zone-H.org/archive/notifier=RedHack/page=1 (Accessed 2 May 2015)

83- Serkan Ocak, "Ankara Emniyeti Çökertildi", (Redhack Crashed the Police) Radikal, 28 February 2012, http://www.radikal.com.tr/turkiye/ankara_emniyeti_cokertildi-1080108 (Accessed on 3 May 2015)

84- "RedHack Emniyeti hackledi mi?" (Did Redhack hack the Police?), Milliyet, 05.09.2013, http://www.milliyet.com.tr/RedHack-emniyet-i-hackledi-mi-/gundem/detay/1759446/default.htm (Accessed on 5 May 2015)

85- For further information on the chronology of the defacements, see; Burak Polat, Cemile Tokgöz Bakıroğlu, Mira Elif Demirhan Sayın. "Hacktivism in Turkey: The Case of RedHack", Mediterranean Journal of Social Sciences, Vol 4, October 2013.

86- Yiğit Turak, "RedHack özelinde Siber olaylar ve Siber Suçlar" (Cyber incidents and cyber crimes in the Redhack example), İstanbul Bilgi University, Unpublished Course Project for Cyber Crimes and its Practice in Turkish Law, http://www.yigitturak.com/wp-content/uploads/RedHack-Özelinde-Siber-Olaylar-ve-Siber-Suçlar.pdf (Accessed 11 May 2015)

87- Pentest is the short form of penetration testing. "Penetration Testing (general term): The process of probing and identifying security vulnerabilities and the extent to which they are used to a cracker's advantage. It is a critical tool for assessing the security state of an organization's IT systems, including computers, network components, and applications." Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, p. 243.

88- http://pastebin.com/mFFw5DqS (Accessed on 3 October 2015)

89- For Turkish version of the mission; see, http://www.turkhackteam.org/misyon.html (Accessed on 12 June 2015)

90- "Vatikan'a Turk Hack Team saldırdı", (Turk Hack Team attacked the Vatican) Aydınlık, 15 April 2015, http://www.aydinlikgazete.com/bilimteknoloji/vatikan-a-turk-hack-team-saldirdi-h67740.html (Accessed 15 May 2015)

91- "New York Times hacklendi" (New York Times was hacked), Sabah, 28 May 2015, http://www.sabah.com.tr/gundem/2015/05/28/new-york-times-hacklendi (Accessed 6 June 2015)

92- "Türk Hackerlardan Müdahale" (The Struggle of Turkish Hackers), Milliyet, 05 June 2015, http://www.milliyet.com.tr/turk-hackerlardan-the-guardian-gazetesine-istanbul-yerelhaber-824596/ (Accessed on 11 June 2015). Also see; http://www.turkhackteam.org/basin-duyurusu/1139755-guardian-operasyonu-ulusal-basinda.html

93- A special military unit in the Ottoman Empire that shocked the enemy with preliminary attacks and carried out reconnaissance missions in hostile territories.

94- http://board.tr.gladiatus.gameforge.com/index.php?page=Thread&threadID=8202

95- Ibid.

96- "The Turkish government enacted Law No. 5651, entitled Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication, in May 2007. The enactment of this law followed concerns about defamatory videos available on YouTube involving the founder of the Turkish Republic Mustafa Kemal Atatürk, combined with increasing concerns for the availability of child pornographic, and obscene content on the Internet, and websites which provide information about suicide, or about illegal substances deemed harmful or inappropriate for children." Yaman Akdeniz, (2010, January 11) Report of the OSCE Representative on Freedom the Media on Turkey and Internet Censorship, http://ec.europa.eu/enlargement/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censorship.pdf (Accessed on 10 November 2015)

97- http://www.cyber-warrior.org/Misyon.asp

98- Ibid.

99- "Cyber Warrior'u ekol yapan etkenler nelerdir?" (What are the factors that make Cyber Warrior an ecole?), haberseyret.com, 26 January 2014, http://haberseyret.com/haber/5319/cyber-warrioru-ekol-yapan-etkenler-nelerdir (Accessed on 01 June 2015)

100- "En makbul milliyetçi 'hacker' olan milliyetçi" (The most welcomed type of nationalist, is the nationalist 'hacker'), Agos, 18 June 2012, http://www.agos.com.tr/tr/yazi/1714/en-makbul-milliyetci-hacker-olan-milliyetci (Accessed on 29 May 2015)

101- "İsrail Sitelerini Hackleyen Türk Hacker" (The Turkish Hacker that Hacked Israeli Sites), http://www.dailymotion.com/video/xdk8lp_israil-sitelerini-hackleyen-turk-ha_tech (Accessed on 11 June 2015)

102- "Cyber Warrior Röportaj 1. Bölüm" (Cyber Warrior Interview Part 1), http://www.cyber- warrior.org/Forum/haberseyret-ile-Cyber-warrior-hk-roportaj_510091,0.cwx (Accessed on 02 June 2015); "Cyber Warrior Röportaj 2. Bölüm" (Cyber Warrior Interview Part 2), http://www.cyber-warrior.org/Forum/haberseyret-ile- cyber-warrior-hk-roportaj-2-bolum_510137,0.cwx (Accessed on 02 June 2015)

103- HP Security Research, "Cyber Risk Report 2015", p.11, http://www.asial.com.au/documents/item/113 (Accessed 11 June 2015)

104- For further details, see; "Cyber-Warrior'un basın sözcüsü XY: Emniyet'in 5 katı iş yapıyoruz" (Cyber Warrior's press officer XY: We do 5 times the work that the Police does), http://psikologdoctor.blogcu.com/unlu-turk-hackerdan- muthis-aciklamalar/2454785 (Accessed on 7 June 2015)

105- A British origin and well-known technology website.

106- Charles Arthur, "Turkish hacker group diverts users away from high-profile websites", The Guardian, 05 September 2011, http://www.theguardian.com/technology/2011/sep/05/turkish-hacker-group-diverts-users.(Accessed on 07 June 2015)

107- Charles Arthur, "Interviewed: the Turkish hackers whose DNS attack hit the Telegraph", The Guardian, 05 September 2011,

108- Pastebin is an online text repository.

109- Agd_Scorp, "Scorp's Manifesto", Pastebin, 11 September 2012, http://pastebin.com/TsqZpx5H (Accessed on 12 June 2015)

110- Turk Guvenligi, Zone-H, http://Zone-H.org/archive/notifier=TurkGuvenligi.info/page=1 (Accessed on 09 June 2015)

111- Agd_Scorp, Zone-H, http://Zone-H.org/archive/notifier=Agd_Scorp (Accessed on 09 June 2015)

112- SQL injection is a technique where malicious users can inject SQL commands into a SQL platform using website to control its database.

113- http://www.Zone-H.org/mirror/id/21545300

114- "PKK'lı hacker'lar 2307 siteyi çökertti" (PKK hacker crashed 2307 sites), Radikal, 27 December 2006, http://www.radikal.com.tr/turkiye/pkkli_hackerlar_2307_siteyi_cokertti-801430 (Accessed on 29 June 2015)

115- "Porno meraklisi istihbaratçılar PKK'nın hacker'ına çalışmışlar" (Intelligence officers interested in porn have played into the hands of PKK's hacker), Radikal, 27 November 2008, http://www.radikal.com.tr/turkiye/porno_meraklisi_istihbaratcilar_pkknin_hackerina_calismis-910264; "PKK'lı hacker'ın pişmanlığına Yargıtay'dan onay" (The Supreme Court approves the penitence of the PKK hacker), Radikal, 23 February 2011, http://www.radikal.com.tr/turkiye/pkkli_hackerin_pismanligina_yargitaydan_onay-1040911 (Accessed on 29 June 2015)

116- http://www.Zone-H.org/archive/notifier=pkkhackteam (Accessed on 21 September 2015)

117- http://www.Zone-H.org/archive/notifier=Pkk%20Hack%20Team (Accessed on 21 September 2015)

118- Turkish Hizbullah and its affiliate, the Free Cause Party (HÜDAPAR), engaged in several clashes with the PKK during the Oct. 7 protests across Turkey against the Islamic State (IS) siege of Kobani, across the border in Syria. The bloodiest clash between the two sides of the night caused the death of at least 10 people in the southeastern province of Diyarbakır. For further details, see,Metin Gürcan, "Kurd vs. Kurd: internal clashes continue in Turkey", AlMonitor, 09 October 2014, http://www.al-monitor.com/pulse/originals/2014/10/turkey-syria-kurds-kobani-pkk-kurdo- islamists.html# (Accessed on 11 November 2015) Read more: http://www.al-monitor.com/pulse/originals/2014/10/turkey-syria-kurds-kobani-pkk-kurdo- islamists.html#ixzz3rZvyedSY

119- "Hüdapar yöneticisinin hesabına hack" (Hüdapar administrator's account hacked), Özgür Gelecek, 11 February 2015, http://www.ozgurgelecek.net/guncel-haberler/13494-2015-02-11-16-01-45.html (Accessed on 30 June 2015)

120- https://twitter.com/tak_hacktim

121- "PKK yandaşı hackerlar Sözcü gazetesinin twitter hesabını hackledi" (PKK sympathizer hacked the twitter account of Sozcu newspaper), Mynethaber, 02 February 2015, http://www.mynet.com/teknoloji/pkk-yandasi-hackerlar-sozcu- gazetesinin-twitter-hesabini-hackledi-1687883-1; "PKK'lı hackerlar belediyenin hesabını hackledi" (PKK hackers hacked the account of the municipality), Cumhuriyet, 05.02.2015, http://www.cumhuriyet.com.tr/haber/turkiye/207781/PKK_li_hackerler_belediyenin_hesabini_hack_ledi.html (Accessed on 30 June 2015)

122- "The Most Hacker-Active Countries", InfoSec Institute, 5 August 2015, resources.infosecinstitute.com/the-most- hacker-active-countries-part-i/

123- Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları" (Cyber Crimes and Turkey's Cyber Security Policies), Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2, 2013, s.135 – 158.

124- For more see www.enigmasoftware.com/top-20-countries-the-most-cybercrime/.

125- Akamai, Q2 2015 State of the Internet – Security Report, www.stateoftheinternet.com/resources-cloud-security- 2015-q2-web-security-report.html.

126- Stefan Frei, Cyber Crime Threat Intelligence – Turkey, CSIS White Paper – July 2014,Copenhagen, 2014, www.csis.dk/downloads/Paper_-_Cyber_Threats_Turkey.pdf.

127- Ibid.

128- T.C. Kalkınma Bakanlığı (Ministry of Development) (2014, May) "2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı (Taslak)" (2014-2018 Information Society Strategy and Action Plan (Draft)) Accessible at: http://bilgitoplumustratejisi.org/tr/doc/8a94819842e4657b01464d5025b80002

129- The Ministry of Transport, Maritime Affairs and Communication has also released a strategic plan for 2014-2018, which reaffirms the aims designated by the 2013-2014 Action Plan but fails to go beyond them, please see T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Stratejik Planı 2014-2018

CYBER SECURITY AND NUCLEAR POWER PLANTS: INTERNATIONAL FRAMEWORK

Assoc. Prof. Ahmet Han

Advisor to the Rector and Faculty Member - Kadir Has University

Board Member - EDAM

Prof. Mitat Çelikpala

Dean, Graduate School of Social Sciences - Kadir Has University

1. Introduction

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

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

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

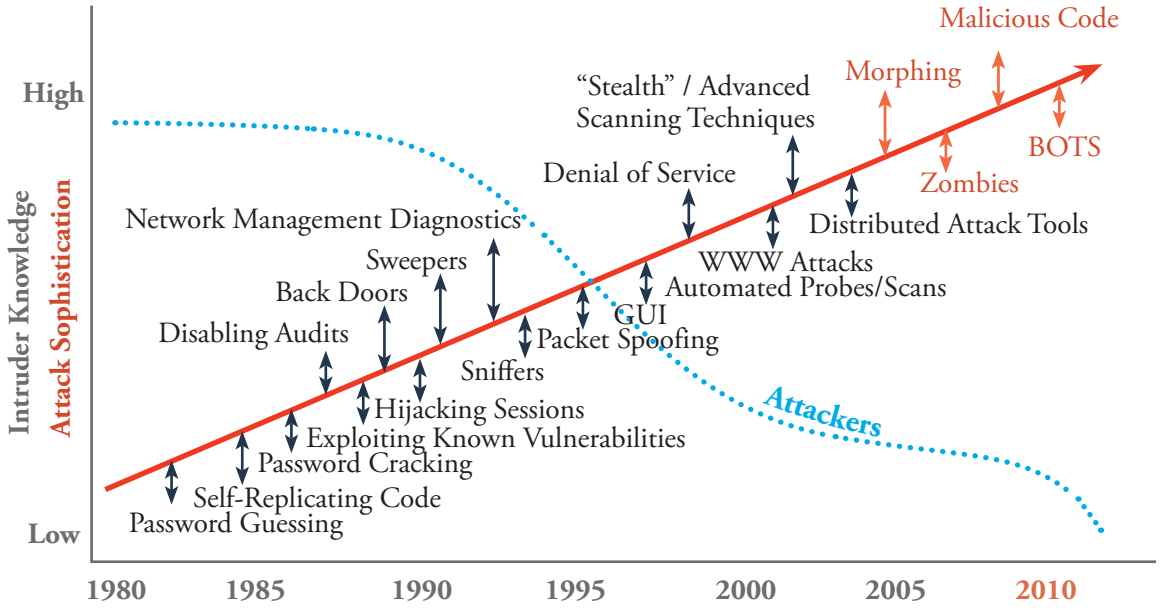
It can be seen that states and certain international organizations are attempting to generate a definition for cyber attack, which threatens the security of systems operating within cyber space. The U.S. Department of Defense (DoD) defines a cyber attack as "a hostile act using computer or related networks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

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

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

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

Figure 1. Sophistication and Proliferation of Cyber Attacks*



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

2.1. The Nature of the Beast: Cyber Attackers

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

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

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

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

Table 1. Internal Threats

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

Table 2. External Threats

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

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

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

3. Nuclear Power Plants and Critical Energy Infrastructure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Risk Management

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

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

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

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

establishment of a comprehensive security culture.

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

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

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

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

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

6. Inferences for Turkey

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

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

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

7. Conclusion

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

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

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

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

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

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

3- Ibid

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

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

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

7- Ibid. p. 34 - 35.

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

9- Ibid.

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

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

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

13- Ibid. p. 6

14- Ibid. pp. 5-6.

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

16- Ibid., pp. 40 – 42.

17- Ibid.

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

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

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

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

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

23- Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

38- Ibid., p.2

39- Ibid., p. 4.

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

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

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

43- Ibid.

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

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

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

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

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

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

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

50- Ibid, p.36.

51- Ibid., p.36.

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

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

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

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

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

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

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

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

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

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

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

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.

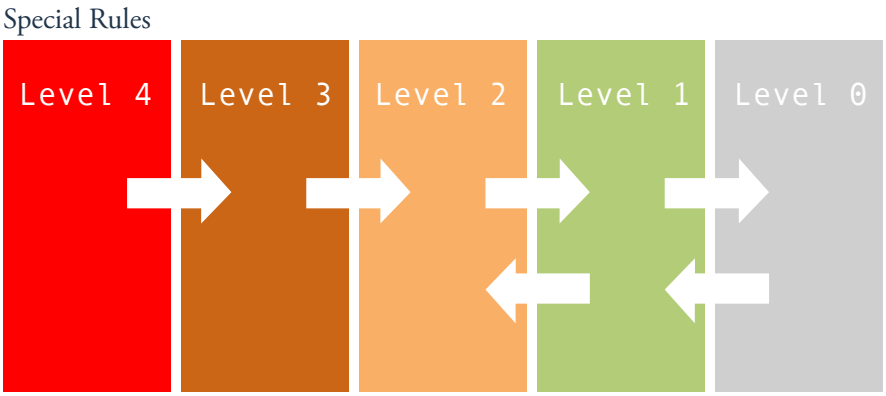
Nuclear power plant systems require hardware replacements and maintenance from time to time. The regulator has to organize how the operator will design the hardware support system. All new hardware should be tested and observed by national authority of test bed. Since the processes take time, the regulator 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)

The Centre for Economics and Foreign Policy Studies (EDAM) is an Istanbul based independent think-tank. EDAM's main areas of research are:

- Foreign policy and security,
- Turkey - EU relations,
- Energy and climate change policies,
- Economics and globalization,
- Arms control & non-proliferation,
- Cyber policy.

EDAM aims to contribute to the policy making process within and outside Turkey by producing and disseminating research on the policy areas that are shaping Turkey's position within the emerging global order. In addition to conducting research in these fields, EDAM organizes conferences and roundtable meetings. Additionally, EDAM cooperates with numerous domestic and international to conduct joint-research and publications.

A PRIMER ON CYBER SECURITY IN TURKEY AND THE CASE OF NUCLEAR POWER

ISBN: 978-9944-0133-7-6

The Centre for Economics and Foreign Policy Studies

Hare Sokak No:16,
Akatlar, 34335 Istanbul

Tel : 0212-352 1854

Email : info@edam.org.tr

www.edam.org.tr