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