DEVELOPING AND VERIFYING A SET OF PRINCIPLES FOR THE CYBER SECURITY OF THE CRITICAL INFRASTRUCTURES OF TURKEY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS INSTITUTE
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BİLGE KARABACAK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

JUNE 2015

DEVELOPING AND VERIFYING A SET OF PRINCIPLES FOR THE CYBER SECURITY OF THE CRITICAL INFRASTRUCTURES OF TURKEY

Submitted by **BİLGE KARABACAK** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Information Systems, Middle East Technical University** by,

Prof. Dr. Nazife BAYKAL _____
Director, **Informatics Institute**

Prof. Dr. Yasemin YARDIMCI ÇETİN _____
Head of Department, **Information Systems**

Assoc. Prof. Dr. Sevgi ÖZKAN YILDIRIM _____
Supervisor, **Information Systems, METU**

Prof. Dr. Nazife BAYKAL _____
Co-Supervisor, **Information Systems, METU**

Examining Committee Members:

Prof. Dr. Soner YILDIRIM _____
Computer Education and Instructional Technology, METU

Assoc. Prof. Dr. Sevgi ÖZKAN YILDIRIM _____
Information Systems, METU

Assist. Prof. Dr. Erhan EREN _____
Information Systems, METU

Assoc. Prof. Dr. Hulisi ÖĞÜT _____
Business Administration, TOBB ETU

Prof. Dr. Ali Aydın SELÇUK _____
Computer Engineering, TOBB ETU

Date: 19.06.2015

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Bilge KARABACAK

Signature:

ABSTRACT

DEVELOPING AND VERIFYING A SET OF PRINCIPLES FOR THE CYBER SECURITY OF THE CRITICAL INFRASTRUCTURES OF TURKEY

Karabacak, Bilge

Ph.D., Department of Information Systems
Supervisor: Assoc. Prof. Dr. Sevgi Özkan Yıldırım
Co-supervisor: Prof. Dr. Nazife Baykal

June 2015, 181 pages

Critical infrastructures are vital assets for countries as a harm given to critical infrastructures may affect public order, economic welfare and/or national security. Today, cyber systems are extensively used to control and monitor critical infrastructures. Therefore, cyber threats have the potential to adversely affect the order of societies and countries. In this PhD study, the root causes of the susceptibility of the critical infrastructures of Turkey to the cyber threats are identified by analyzing the qualitative data with the grounded theory method. The extracted root causes are verified by two experts. The set of principles for the cyber security of the critical infrastructures are determined by introducing the root causes to six experts in a five-phased Delphi survey. A state-level cyber security maturity model to measure the readiness level of the critical infrastructure protection efforts is developed by using the set of principles. Because maturity criteria are grounded on the root causes of the susceptibility to cyber threats, the maturity model is named Vulnerability Driven National Cyber Security Maturity Model. The readiness level of the critical infrastructure protection efforts of Turkey is measured by the participation of ten former/current government officials in the maturity survey. The root causes, the set of principles, and the results of the maturity survey are compared with the relevant studies of the academia, non-profit organizations and governments.

Keywords: Cyber Security, National Security, Critical Infrastructures, Critical Infrastructure Protection, Maturity Model, Grounded Theory, Delphi Survey

ÖZ

TÜRKİYE'NİN KRİTİK ALTYAPILARININ SİBER GÜVENLİĞİ İÇİN PRENSİPLERİN GELİŞTİRİLMESİ VE DOĞRULANMASI

Karabacak, Bilge

Doktora, Bilişim Sistemleri
Tez Yöneticisi: Doç. Dr. Sevgi Özkan Yıldırım
Ortak Tez Yöneticisi: Prof. Dr. Nazife Baykal

Haziran 2015, 181 sayfa

Kritik altyapılardaki sorunlar toplum düzenini, ekonomiyi ve/veya ulusal güvenliği etkileyebildiği için kritik altyapılar ülkeler için hayati varlıklardır. Günümüzde, kritik altyapıları kontrol etmek ve izlemek için siber sistemler yoğun olarak kullanılmaktadır. Bu nedenle, siber tehditler toplumların ve ülkelerin düzenlerini kötü yönde etkileyebilecek potansiyele sahiptirler. Bu doktora çalışmasında, Türkiye'deki kritik altyapıların siber tehditlere yönelik hassasiyetinin kök sebepleri sözel verinin temellendirilmiş kuram metoduyla analiz edilmesi sonucu bulunmuştur. Kök sebepler iki uzmanın katılımı ile doğrulanmıştır. Kök sebepler beş fazlı olarak düzenlenen bir Delfi anketi ile altı uzman ile paylaşılmış ve anket sonucunda kritik altyapıların siber güvenliği için prensipler elde edilmiştir. Elde edilen prensipler kullanılarak bir ülkenin kritik altyapı koruma çalışmalarının olgunluk seviyesini ölçmek üzere ulusal bir siber güvenlik olgunluk modeli önerilmiştir. Olgunluk modeli kök sebeplere dayandığı için Açıklık Tabanlı Ulusal Siber Güvenlik Olgunluk Modeli olarak adlandırılmıştır. Türkiye'nin kritik altyapı koruma çalışmalarının seviyesi on adet eski/hâlihazırdaki kamu çalışanının katıldığı bir olgunluk anketi ile ölçülmüştür. Kök sebepler, prensipler ve olgunluk ölçüm sonuçları konuyu ele alan akademik çalışmalar, kurumsal raporlar ve hükümet çalışmaları ile karşılaştırılmıştır.

Anahtar Kelimeler: Siber Güvenlik, Ulusal Güvenlik, Kritik Altyapılar, Kritik Altyapıların Korunması, Olgunluk Modeli, Temellendirilmiş Kuram, Delfi Anketi

To Selcen, Betül, Sibel

ACKNOWLEDGMENTS

I express my gratitude to my advisor, Dr. Sevgi Özkan Yıldırım, my co-advisor, Dr. Nazife Baykal, and my committee members, Dr. Soner Yıldırım and Dr. Erhan Eren, for their continuous support throughout this long and tough journey. I will never forget their guidance and encouragement. Without their supervision and constant help this thesis would not have been written. I extend my gratitude to the professionals and officials who contributed to the research by sharing their knowledge and experience. Finally, my research would not have been possible without the invaluable data of the project funded by the Ministry of Development of Turkey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND DEFINITIONS

APT	:	Advanced Persistent Threat
ASPI	:	Australian Strategic Policy Institute
BRSA	:	Banking Regulation and Supervision Agency
CCDCOE	:	Cooperative Cyber Defence Centre of Excellence
CCSMM	:	Community Cyber Security Maturity Model
CERT	:	Computer Emergency Response Team
CI	:	Critical Infrastructure
CIP	:	Critical Infrastructure Protection
CIPP		Critical Infrastructure Protection Program
CoBIT	:	Control OBjectives for Information and related Technology
Critical Infrastructure Owner	:	A private or governmental organization that is in the charge of operating a critical infrastructure facility. The terms "critical infrastructure owner" and "critical infrastructure operator" are used interchangeably in the thesis.
CSIRT	:	Computer Security Incident Response Team
DDoS	:	Distributed Denial of Service
DHS	:	Department of Homeland Security
DoS	:	Denial of Service
ECL	:	Electronic Communications Law
EMRA	:	Energy Market Regulatory Authority
EO	:	Executive Order
EU	:	European Union
FISMA	:	Federal Information Security Management Act
GAO	:	Government Accountability Office
GCI	:	Global Cybersecurity Index
GLBA	:	Gramm–Leach–Bliley Act
GSM	:	Global System for Mobile communications
GTM	:	Grounded Theory Method
HIPAA	:	Health Insurance Portability and Accountability Act
ICT	:	Information and Communications Technologies
ICTA	:	Information and Communications Technologies Authority

IEC	:	International Electrotechnical Commission
ISACA	:	Information Systems Audit and Control Association
ICS	:	Industrial Control Systems
ISO	:	International Organization for Standardization
IT	:	Information Technology
ITU	:	International Telecommunication Union
NATO	:	North Atlantic Treaty Organization
NCSecMM	:	National Cybersecurity Management System
NCSR	:	National Cyber Security Review
NGO	:	Non-Governmental Organization
NIST	:	National Institute of Standards and Technology
OECD	:	Organization for Economic Co-operation and Development
Regulatory Authority	:	A public institution which audits the critical infrastructure operators in a critical sector and prescribes rules and regulations for them.
SCADA	:	Supervisory Control and Data Acquisition
UK	:	United Kingdom
UNESCO	:	United Nations Educational, Scientific and Cultural Organization
US	:	United States
USA	:	United States of America

CHAPTER 1

1 INTRODUCTION

Introduction consists of prologue, background and statement of the problem, researcher's motivation and significance of the study, research objective, research questions, assumptions, limitations, delimitations, internal threats, and organization of the thesis.

1.1 Prologue

Critical infrastructures are vital assets for the public safety, economic welfare and/or national security of countries (Alcaraz & Zeadally 2015). Today, cyber systems are extensively used to control and monitor critical infrastructures (Abou El Kalam et al. 2009). Therefore, cyber security is an important item on the national security agenda of countries (Young 2012). Academia have an increasing interest in the protection of critical infrastructures as well (Ten 2008; Apostolakis & Lemon 2005; Eusgeld et al. 2009; Little 2002; Johansson & Hassel 2010). Having been studied by governments and academics within last five years, the measurement of the state-level cyber security maturity has proved to be a popular topic. There are some national-level maturity assessment studies (ITU 2014; Hathaway 2013; Tobias Feakin & Woodall 2014; BAH 2011; White 2012; Kettani & Debbagh 2009). However, none of the reviewed studies is dedicated to the maturity assessment of the critical infrastructure protection efforts of countries. Instead, they evaluate the existence of the best national level cyber practices in diverse disciplines, ranging from cyber-crime response to privacy protection.

In this PhD thesis, a state-level cyber security vulnerability assessment is performed at the first step. Secondly, a state-level cyber security maturity model is proposed to measure the resilience of the critical infrastructure protection efforts of a level. The maturity model is developed through the use of the vulnerabilities extracted at the first part of the study.

1.2 Background of the Problem

Any physical or cyber infrastructure is called critical infrastructure if a damage to that infrastructure has a harmful effect on the economy of a country, on social order and/or national security (USA 2001). The term of Critical Infrastructure was first used at the Executive Order of President of the US in 1996 (The White House 1996). The Executive Order identifies two types of threats against critical infrastructures; physical threats and cyber threats.

The interest of the countries in critical infrastructures has continuously been growing. Because the harm given to critical infrastructures adversely affects the society, national security, and economy, governments bear the responsibility to protect critical infrastructures (Jayawickrama 2006). More than fifty countries have prepared and enacted national cyber security policies or strategies in the last decade (NATO CCDCOE 2015). The protection of the critical infrastructures against cyber threats is a leading goal in these strategies.

The interest of the academia in the critical infrastructures has been increasing as well. The studies on the security of the critical infrastructures can be categorized into five perspectives (Lopez et al. 2007; Adar & Wuchner 2005). These perspectives from highest (policy) level to lowest (tactical) level are as follows:

1. National and international security (Developing policies and strategies)
2. Business and sectorial security
3. Organizational security
4. The security of the information processing and information technologies
5. Physical security

Some studies may cover only one perspective while some others may cover more than one. In fact, critical infrastructure protection is an interdisciplinary research topic thanks to the diversity of the critical sectors and the nature of the cyber systems (Lopez et al. 2007).

Governments mainly carry out studies within the scope of the first perspective. The academic studies on the first perspective are generally performed by the social scientists from such disciplines as international affairs and public policy (Harrop & Matteson 2013; Assaf 2008; Dunn-Cavelty & Suter 2009).

The most of the academic research focus on the availability of the infrastructures. In the view of availability, there are prominent studies that analyze and model the interdependencies among the infrastructures, and they usually propose mathematical models to prevent cascading failures (Johansson & Hassel 2010; Svendsen & Wolthusen 2007; Rinaldi et al. 2001). These studies can take place in the second perspective.

There are fewer academic studies that specifically concentrate on cyber threats compared to the studies that consider all type of threats from a reliability perspective. The academic studies that cover security related issues are generally risk analysis studies that propose models designed to analyze all kinds of threats including physical and cyber ones. (Baiardi et al. 2009; Crowther 2008; Kjølle et al. 2012; Flammini et al. 2008; Luiijf et al. 2011; Haimes et al. 2002; Michaud 2005; Adler & Fuller 2007). The studies in this category can be placed in either second or third perspective.

There are considerable amount of studies that propose countermeasures and protection models for SCADA networks. These studies generally focus on the technical details of the networks such as the usage of data diodes and access control systems (Igure et al. 2006; Ten 2008; Weiss 2010). These studies can be positioned in the fourth or fifth perspectives.

This PhD study is primarily under the first perspective; however, it covers some parts from the second perspective as well.

1.3 Statement of the Problem

First of all, critical infrastructures are the targets of the cyber threats, as stated in the background of the problem. State-level policies and strategies play an important role in tackling with the cyber threats and managing the cyber security of the infrastructures (Healey & Pitts 2012). The studies that analyze the vulnerabilities of the infrastructures can help determine state level policies and strategies (Lin 2012). There is a limited number of academic studies that focus on the state level critical infrastructure vulnerabilities, the reason for which may be the sensitivity constraints on the critical infrastructure information (DHS 2005; Dunn-Cavelty & Suter 2009; US-GAO 2013; Goldman & Valdez 2004; Reiter & Rohatgi 2004).

Secondly, the decision-makers in governments and organizations may benefit from the results of the cyber security maturity assessment studies. They evaluate the current situation and decide what to do next by looking at the current maturity level (DHS 2014). For organizations, there are a number cyber security maturity assessment studies which are developed by academia or governments (Adler 2013; Lessing 2008; Miron & Muita 2014; Eshlaghy & Pourebrahimi 2011; Karokola et al. 2011; Butkovic & Caralli 2013). However,

there is a limited number of studies that measure the state level cyber security maturity. Moreover, there is currently no academic study that measures the maturity level of the critical infrastructures protection efforts of a country.

This PhD study combines the concept of the state-level vulnerability analysis and maturity assessment in a single pot. Firstly, the root causes of the susceptibility of the critical infrastructures to the cyber threats are extracted by analyzing the data of a state-sponsored project through Grounded Theory Method. Secondly, the set of principles are determined by using expert opinion in a five-phased Delphi survey. Thirdly, a state-level cyber security maturity model is developed by applying the set of principles.

1.4 Researcher's Motivation and Significance of the Study

The researcher participated in the state-sponsored project named "Information Security Management in Critical Infrastructures", between January 2012 and December 2013. Each critical sector was examined in terms of the usage of information technologies, and the problems associated with the technology. The project demonstrated that cyber systems were significantly used in the sectors of energy, telecommunications, finance, government, transportation as well as the water management in Turkey. The project also showed that critical infrastructures had significant vulnerabilities associated with the cyber systems. The motivation of the researcher is to discover the root causes of the vulnerabilities that were identified in the state-sponsored project.

The following list underlines the points that render this PhD study significant:

1. Critical infrastructures are vital assets for public safety, economic welfare and/or national security of the countries. Having been considered as an important part of the national security, cyber security of the critical infrastructures is a critical agenda item of the countries, as observable from their cyber security strategies.
2. The measurement and improvement in security can be accomplished through the utilization of maturity models. A maturity model is a benchmark against which the current level of capability is evaluated. Goals and priorities for improvement can be set by using maturity models.
3. The number of the academic studies that propose national level cyber security maturity assessment is limited. The studies in the literature are usually performed by nonprofit organizations, international organizations, and government agencies. Most studies in the literature do not focus on maturity measurement of a specific country; they rather score and rank a number of countries. No academic study on the maturity assessment of the critical infrastructures protection efforts of a country has been prepared until now. Therefore, proposed maturity model is the first academic study that measure the maturity of the critical infrastructure protection efforts of a country.
4. The most important shortcoming of the current studies is their maturity criteria. Their criteria are grounded on the best practices. The criteria for a maturity model that would be more useful for the policy-makers should be grounded on the realistic and credible data on critical infrastructures.
5. Being a former government official, there was an opportunity for the researcher to interview the critical infrastructure operators of Turkey, and to reach the data on its critical infrastructures. The researcher effortlessly reached ten current/former government officials to conduct the maturity survey as well.
6. As a cyber security expert with fifteen years of experience, the researcher contacted with the experts without any difficulty. Two experts performed the verification of

the root causes. Six experts participated in the Delphi survey to extract the set of principles for the security of the infrastructures.

7. With this PhD research, the researcher contributed to the literature:
    a. By extracting the root causes of the susceptibility of the critical infrastructure to cyber threats.
    b. By determining the set of principles for the security of the critical infrastructures.
    c. By proposing a national-level cyber security maturity model that measures the cyber resilience of the critical infrastructures.
8. Grounded Theory Method, a developmental research technique, was used to extract the root causes. The researcher was the main participant in the research.
9. Delphi survey was used to determine the set of principles. The researcher undertook a passive role during the survey.
10. The researcher proposed a maturity model by taking the shortages of the current maturity literature into account. The model is developed to assess the maturity level of the critical infrastructure protection efforts of a country.
11. Government officials from various countries may benefit from the list of the root causes and the principles, and the maturity model.

1.5 Research Objective and Research Questions

The objectives of the research are:

1. To extract the root causes of the susceptibility of the critical infrastructure to cyber threats,
2. To determine the set of principles for the cyber security of the critical infrastructures,
3. To develop a national-level cyber security maturity model.

The research method for the data analysis is the Grounded Theory Method, which is an interpretative and qualitative research method. GTM is not a hypothesis testing, it is rather a theory generation from data by performing structured analysis. In GTM, the research question is the phenomenon to be studied (Strauss & Corbin 2008). The phenomenon to be studied is as follows:

The results of the state-sponsored project showed that:

1. Cyber systems are used significantly in critical infrastructures
2. There are a number of vulnerabilities that originate from cyber systems

In this PhD study, the researcher discovers the possible root causes of the susceptibility of the critical infrastructures of Turkey to cyber threats. The phenomenon can be written in research question as “What are the possible root causes of the susceptibility of the critical infrastructures of Turkey to cyber threats?”

The second research question is “What are the set of principles to mitigate these root causes?”

1.6 Assumptions, Limitations, Delimitations, and Internal Threats

It is assumed that interviewees, experts and government officials have responded accurately during the interviews, the verification of the extracted theory, Delphi survey, and the application of the maturity model.

Extracted from the data by using GTM, the root causes are bound by the opinions of the interviewees, the gathered documents, and the theoretical sensitivity of the researcher.

The maturity criteria and weight values of criteria are depended on the opinions of the experts who have participated in Delphi survey.

The national cyber security maturity level of the Turkey, which is calculated in a pilot survey, is depended on the answer choices of the government officials. It is noteworthy to state that the calculated maturity level of Turkey is not an officially produced and recognized value.

For this study, the critical infrastructure sectors, determined in the second meeting of the Cyber Security Council of Turkey, are selected as the critical sectors. The analyses are performed by using the gathered data from these sectors.

As the disciplines of cyber crime fighting, military cyber operations and privacy protection are not directly associated with the cyber security of critical infrastructures (Klimburg 2012), they are left out of scope of this PhD thesis.

The vulnerabilities associated with the physical security of the critical infrastructures are left out of scope of the PhD thesis.

The interviewees might have avoided giving correct and complete information as not to be responsible for disclosing problems and vulnerabilities. At the beginning of each interview, it was assured that the interviewee and his/her organization would remain anonymous and no vulnerabilities that may be associated with the organization would be written within the thesis. Conducting interviews with nine different organizations from six sectors can be a mitigating factor for this threat.

1.7 Organization of the Thesis

The contents of each chapter are shown in Table 1-1.

Table 1-1: Organization of the Thesis

Chapter	Title	Content
Chapter 1	Introduction	Prologue, background and the statement of the problem, the motivation of the researcher, the significance of the study, research objective, research questions, assumptions, limitations, delimitations
Chapter 2	Literature Review	Critical review of the literature, comparisons of the national cyber security maturity models
Chapter 3	Research Design	Data collection methods, research population and sampling strategies, the details of application of GTM, Delphi survey, role of the researcher and trustworthiness of the research
Chapter 4	Findings	The findings of the data analysis with GTM, the discussion of the root causes, the findings of the Delphi Survey, the comparison of the proposed model with the literature, the application results of the maturity survey
Chapter 5	Conclusions	Discussion of the findings in the light of different regulation perspectives, contributions to the literature, implications for future research

CHAPTER 2

2 LITERATURE REVIEW

Literature review starts with the definition and the history of the critical infrastructures. It continues with the taxonomy of the cyber threats against critical infrastructures. Some national efforts on the protection of critical infrastructures are detailed. Literature review also contains the summary of the regulatory approaches for critical infrastructures, along with the application details in Turkey. Finally, six maturity models for the national level cyber security measurement are summarized and compared.

2.1 Definition and History of Critical Infrastructures

Any physical or cyber infrastructure is called critical infrastructure, if a damage to that infrastructure has a harmful effect on the economy of the country, social order and/or national security (USA 2001). The term of critical Infrastructure is first used within the Executive Order 13010 in 1996 (The White House 1996). The purpose of the order was to introduce the term "Critical Infrastructure Protection", to define the problem and to establish interim commissions to recommend comprehensive strategies and amendments to the existing laws. The executive order mentioned two types of threats against critical infrastructures: physical threats and cyber threats. Although critical infrastructures existed long before the Internet prevalence and widespread use of cyber technologies, the Critical Infrastructure Protection is defined as an important governmental term because of the dominant use of cyber systems in infrastructures. The first of the two reasons for this phenomenon is that cyber systems welcome a novel type of threats; cyber threats. Cyber threats are asymmetric in nature; an attacker can hide himself easily, and compared to the conventional threats, cyber threats are extremely cheap and prevalent. Therefore, cyber threats easily and effortlessly pave the way for harmful attacks against critical infrastructures. There is a number of materialized cyber attacks against critical infrastructures, like nuclear plants, electrical grids, sewing infrastructures, flight control systems and harbors (Condron 2007; Farwell & Rohozinski 2011). As a result, cyber resilience of the critical infrastructures forms a prominent portion of the national security efforts of the countries. Secondly, cyber systems caused or increased interdependencies among critical infrastructures. These interdependencies are considered the main cause of the cascading failures (Little 2002; Eusgeld et al. 2011). That means, a problem in one infrastructure may result in a subsequent failure in another. As an example, a problem in the telecommunications infrastructure may have a weakening effect on the finance infrastructure, as witnessed in the Russian hackers' attacks to Estonian networks in 2007 (Ottis 2008). Therefore, countries started to take critical infrastructure protection more seriously.

Today, cyber systems are vastly used in the monitoring and controlling of critical infrastructures. SCADA systems, used in controlling energy and water management systems, are the examples of such cyber systems. Smart grids, smart transportation systems and remotely controllable local gas distribution systems have been emerging as the vital parts of the modern society. Apart from SCADA systems, some critical infrastructures are completely dependent on the conventional cyber systems. For instance, the banking and finance infrastructure depends considerably on the conventional information technologies.

The daily operations of banking and finance companies are totally depended on their huge server parks and network infrastructures. Telecommunications infrastructure is completely composed of cyber systems. In other words, cyber systems created a new critical infrastructure called telecommunications. Without telecommunications infrastructures, the modern society cannot be maintained. Because of the new service models like cloud computing, Internet can be regarded as a critical infrastructure. The attacks to the Estonian networks in 2007 demonstrated how much the well-being of a country is depended on the Internet infrastructure.

Although the Internet is physically distributed, it is logically single. Therefore, the Internet brings physically such detached things as people, organizations and states together in the same medium. Therefore, everyone share the same medium with cyber attackers, but with different motivations; ranging from cyber criminals to state sponsored hackers. Today, some of the critical infrastructures are connected to the Internet (Lopez et al. 2007). The infrastructures that do not have any direct connection to the Internet are usually connected to the internal production networks of organizations. Hence, critical infrastructures are connected to the Internet after passing one hop (Igure et al. 2006).

The use of cyber systems in critical infrastructures is a necessity without doubt. For some infrastructures, Internet connection is a rigid requirement to serve citizens and/or customers suitably. The critical infrastructure operators benefit from cyber systems for the efficient and cost effective management of the critical infrastructures. For states, however, cyber systems must be used in accordance with some specific policies due to the attack potential of cyber threats. At this point, Critical Infrastructure Protection Program comes to the scene. The importance of the critical infrastructures necessitates the state level coordination of security efforts according to the some rigid policies, strategies and procedures (Harrop & Matteson 2013). This hierarchical set of rules is called CIPP. CIPP is the national and coordinated efforts to keep the critical infrastructures protected from both cyber and physical threats (Assaf 2008). A number of countries, including developing ones, have critical infrastructure protection programs. Some developed countries, like the US, have been working on this subject for decades. Most of the developed countries have started to prepare programs within last five to ten years. Today, countries give an important place to cyber threats in their CIPPs. In developed countries, CIPP is an important part of the national security efforts. In other words, national security officials take cyber security into account because of the widespread use of cyber systems and their vulnerable nature (Nicholson et al. 2012). This consideration is materialized with the CIPP.

2.2 Critical Infrastructures and Cyber Threats

Cyber threats against critical infrastructures can be categorized in four main groups, which area hacktivism, cyber crime, cyber espionage, and cyber war (Prichard & MacDonald 2004). However, there is no clear-cut distinction among these groups, as shown in Figure 2-1. These categorized cyber threats can intersect with each other in many different ways. A member of a hacktivist group may get into a cyber crime activity. The same group may take part in a coordinated cyber war or cyber espionage. A cyber act can be categorized or perceived as both cyber war and hacktivism. As an example, while a country can consider a cyber incident as cyber war, another can consider the same act as hacktivism.

When critical infrastructures are taken into consideration, cyber espionage and cyber war are much more harmful than hacktivism and cyber crime. The number of cyber espionage and cyber war activities is lower, compared to the number of cyber crime and hacktivist attacks. When the economic damage and national security are the main concerns, the impact level of cyber espionage occurs to be very high, compared to the impact level of other threat types

(Kshetri 2005). Although cyber espionage attacks are low in number, they cause losses of intellectual property, which has a great value for a country. Although cyber crime activities are large in number, the loss is limited to credentials and money. As far as the public safety is concerned the impact level of cyber war is high compared to the impact level of other threat types. Cyber war can affect the availability of SCADA systems and corporate networks.

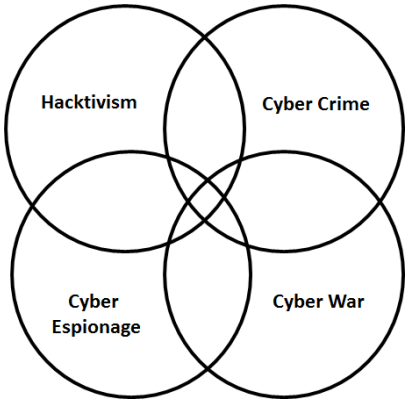


Figure 2-1: Four Types of Cyber Threats against Critical Infrastructures

According to "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", an industry can be defined as "critical" if a damage or unauthorized access to that system could reasonably

a) Result in the interruption of life-sustaining services,
b) Cause catastrophic economic damages or
c) Cause severe degradation of national security (USA 2001).

By using the damage classification above, the prominent effects of the four threat categories on critical infrastructures are shown in Table 2-1 (Kshetri 2005; Lewis 2002; Prichard & MacDonald 2004; Hinde 1998) . Although there is no crystal-clear classification and correlation between threat and impact types, Table 2-1 shares the notion that cyber espionage and cyber war are much more harmful than cyber crime and hacktivism.

Table 2-1: Threat Categories versus Impact Types

Threat Type	Impact Type
Hacktivism	The interruption of life-sustaining services
Cyber Crime	Economic damages
Cyber Espionage	Economic damages Severe degradation of national security
Cyber War	The interruption of life-sustaining services Economic damages

2.2.1 Hacktivism

Hacktivists create opportunistic attacks against weak targets. The power of hacktivists comes from their number: Hacktivism is the activity of a group of hackers. For instance, the hacker group 'Anonymous' is a hacktivist group. The main purpose of hacktivists is not to make money: they rather protest something. For example, they protest the governmental restrictions on the Internet and they attack at the websites of public organizations.

Hacktivists usually perform Denial of Service attacks. A DoS attack can be defined as purposefully flooding the bandwidth or resources of a targeted system with a huge number of legitimate service requests. Hacktivists usually target the availability of networks and systems by performing DoS attacks. In addition to DoS attacks, hacktivists try to deface websites, especially the ones of public organizations. They do not usually try to deface a specific website for a long time. Instead, they search for a specific vulnerability on a number of websites and deface all of the websites with specific vulnerabilities in their search scope. Hacktivist use botnets or contact with the owner of botnets to perform DDoS attacks to guarantee the unavailability of networks and systems.

2.2.2 Cyber Crime

In contrast with hacktivists, the main purpose of cyber criminals is to make money. Cyber criminals are individuals. They usually do not act in groups like hacktivists. They steal credit card information, bank account credentials and passwords. Banking and finance are the target critical sectors for cyber criminals. Compared to other threat types, cyber crime does not have a prominent effect on critical infrastructures.

2.2.3 Cyber Espionage

Cyber espionage is basically the act of stealing documents from the networks of foreign countries (Lewis 2002). The loss of confidentiality is the major consequence of cyber espionage. The term Advanced Persistent Threat is used within the context of cyber espionage. According to the Mandiant, a famous information security company, APT is a group of sophisticated, determined and coordinated attackers that have been systematically compromising US government and commercial computer networks for years. The vast majority of APT activity observed by Mandiant has been linked to China (Mandiant 2013).

According to the Department of Defense Strategy for Operating in Cyberspace, an amount of intellectual property larger than kept in the Library of Congress is stolen every year from the networks maintained by the US businesses, universities, and government departments and agencies (DoD 2011).

US - China Economic and Security Review Commission prepared a report for the Congress in 2008. According to the report, China has an active cyber espionage program and its cyber warfare is so sophisticated that the United States may not be able to counteract or even detect the efforts (USCESRC 2008).

2.2.4 Cyber War

Cyber war is the coordinated attacks on the specific critical sectors of a country. Every critical sector is a potential target for cyber war. Most of the cyber security experts think that Stuxnet virus marks the beginning of real cyber war. Discovered in June 2010, the Stuxnet virus targeted the availability of Iranian nuclear energy infrastructure (Farwell & Rohozinski 2011; Langner 2011). According to the American media, the US officials secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, and according to the participants in the program, that significantly expanded America's first sustained use of cyber weapons (Sanger 2012; Kahn 2013). The cyber attacks against the availability of Estonian and Georgian websites and network infrastructures are the other examples of cyber war. Although Russia did not undertake those attacks as a government, the coordinated attacks were performed by Russian people. Cyber war aims more than the availability of systems and networks. For instance, discovered after Stuxnet, a virus called Duqu affected the confidentiality of Iranian energy infrastructure. Because of the similarities they bear, it is considered that the source of Duqu and Stuxnet was the same. Duqu provided services, which include information stealing capabilities, for

the attackers (Bencsáth & Pek 2012). The latest discovered malware is called Flame, Flamer or Skywiper. According to New York Times, Flame appears to be part of the state-sponsored campaign that spied on and eventually set back Iran's nuclear program in 2010 (Perlroth 2012).

When the Turkish media reports of the last three years are analyzed, it is easily seen that there is a dominance of the public services and the energy sectors in the news associated with the cyber security breaches. As an example, it is reported by the Minister of Energy that one of the possible reasons for the country-wide electricity blackout in March 31th, 2015 was a cyberattack against electricity transmission infrastructure (Melvin 2015). Operated by the government, the electricity transmission infrastructure was attacked in October 2014 by the hacker group Redhack, which alleged to erase 1.5 million debt of the citizens; however it was refuted by the Ministry of Energy (DHA 2014). According to the Bloomberg, the part of Baku-Tbilisi-Ceyhan pipeline in eastern Turkey was blasted by a cyber attack in 2008 (Robertson & Riley 2014).The hacker groups Redhack and Anonymous launched successful website defacement and denial of services attacks against internet services of various governmental organizations, including Ministry of Interior, Ministry of Foreign Affairs, Security General Directorate, and Higher Education Council.

2.3 Efforts of Governments and Organizations

Cyber security is an evolving topic. Cyber security was almost only a technical subject two decades ago, when cyber systems were used solely by a small academic and bureaucratic community. As the time passed, the engagement of the organizations in the cyber systems increased. Internationally recognized security management standards are thus developed and adopted by organizations. As the proliferation of the Internet continued, countries started to consider cyber security a vital parameter of national security. Therefore cyber security has been considered as the fifth war-fighting domain by countries (Andress & Winterfeld 2013). Countries started to prepare national cyber security strategies in this era. Especially after the alleged Russian hackers' attacks on Estonian cyber infrastructure in 2007 and the Stuxnet incident in 2011, they increased national coordination activities in order to secure infrastructures and prompt response capabilities against adversaries. These events triggered and accelerated national cyber security strategy preparation processes (Tatar et al. 2014). According to the webpage of NATO's Cooperative Cyber Defence Centre of Excellence, more than fifty countries have national cyber security strategies (NATO CCDCOE 2015). When the mandates in the national cyber security strategies are taken into account, Critical Infrastructure Protection is seen to have a dominance over other functions. Because cyber threats are quite prevalent and advanced today, the priority for those countries is ensuring the cyber resilience of the critical infrastructures. There are a number of cyber incidents sponsored by conflicting states. Therefore, it is vital for countries to have secure, resilient and robust critical infrastructures in terms of cyber security. Such infrastructures can be accomplished by preparing strategies and action plans that contain the action items intended to reach this goal.

Presidential Policy Directive – 21 defines cyber resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents". Therefore, cyber resilience can be concisely defined as the robustness of a country against cyber attacks. It is the preparedness efforts of a country for a cyber war. Therefore, cyber resilience is something parallel to the defensive actions of a state (Harrop & Matteson 2013). The offensive strategies and efforts cannot be regarded within the cyber resilience efforts of a state. Hence, there is a strong relationship between critical

infrastructure protection programs and cyber resilience. A critical infrastructure protection program is the prominent effort to have a cyber-resilient country and society.

As stated earlier, the US has been the first country that used the term Critical Infrastructure. The US also takes place in the forefront of the studies on critical infrastructure protection. The following paragraphs summarizes the efforts of the US.

2.3.1 National Infrastructure Protection Plan

National Infrastructure Protection Plan is the central document of the current critical infrastructure protection program of the US (DHS 2013). The subtitle of the plan is "Partnering for Critical Infrastructure Security and Resilience". As the subtitle implies, the National Infrastructure Protection Plan highlights the partnership of public and private entities. The aim of the plan is to establish the collaboration and cooperation routines in order to achieve secure and resilient infrastructures. National Infrastructure Protection Plan is released pursuant to the Presidential Policy Directive-21 (The White House 2013b).

The national plan is a detailed call to action and a document that explains the details of a risk management framework. Risk management is the core process for critical infrastructure security and resilience; and it is fully integrated with the National Infrastructure Protection Plan since achieving resilience is directly related to the successful risk management process (DHS 2013). The proposed risk management framework has five steps. These steps are as follows.

1) Set goals and objectives
2) Identify infrastructures
3) Assess and analyze risks
4) Implement risk management activities
5) Measure effectiveness

According to the framework, physical, cyber, and human elements of critical infrastructures should be considered through all steps of the framework. Entire risk management framework is accompanied by information sharing mechanisms. Information sharing is used as a feedback mechanism to convey the results of measurement of effectiveness. All of the steps of risk management framework is explained in this section. The link between these steps and the items of call to action are shown with call-out boxes. National Infrastructure Protection Plan does not urge critical infrastructure operators to use this framework. Rather, risk management framework is an "organizing construct" for different types of infrastructures.

The call to action section of the National Infrastructure Protection Plan is a detailed action plan which is formed to enhance national critical infrastructure security and resilience. This section refers to all of the critical infrastructure partners and stakeholders, whether public and private entities. The basic themes of the call to action section are the sector or cross-sector collaboration, cooperation, partnership and information sharing among different types of partners and stakeholders. The details of the collaboration, cooperation, partnership and information sharing activities and routines are given in this section. The call to action has twelve actions to advance national efforts. All of these actions are linked to the national goals by using call-out boxes, which were given in second section of National Infrastructure Protection Plan.

National Infrastructure Protection Plan is comprised of the list of the partners and stakeholders, from federal government agencies to private sector entities, of the critical infrastructure protection community. The document also lists the roles, responsibilities and capabilities of these stakeholders. These appendices are extremely useful for the experts who

try to understand the organizational structure of the US in terms of critical infrastructure protection.

2.3.2 Presidential Policy Directive – 21

The name of Presidential Policy Directive-21 is Critical Infrastructure Security and Resilience, which can be regarded as the initiator of the critical infrastructure protection efforts of the US in recent years. Presidential Policy Directive -21 emphasize the physical and cyber threats equally. The directive says that "it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats."

Presidential Policy Directive - 21 is the stimulus of the National Infrastructure Protection Plan. It specifies the organizational structure, roles and responsibilities for critical infrastructure protection. Presidential Policy Directive - 21 divided the critical infrastructures into sixteen sectors and identified Sector-Specific Agencies for them.

Here, it is important to share some remarkable points of the Presidential Policy Directive - 21. The "interconnectedness and interdependency" of critical infrastructures are emphasized in the directive. The directive draws attention to interconnectedness and interdependency to underline the importance of coordination, collaboration and partnership. The directive also mentions "effective partnerships with critical infrastructure owners and operators". It is said that "this partnership is imperative to strengthen the security and resilience of the Nation's critical infrastructure". Presidential Policy Directive – 21 accentuates the importance of international cooperation and the promotion of research and development activities as well.

Three strategic imperatives for critical infrastructure security and resilience are:

1) "Refining and clarifying functional relationships across the Federal Government"
2) "Enable effective information exchange"
3) "Implement an integration and analysis function" (The White House 2013b).

From these excerpts, it can be understood that the protection efforts have to take interdependencies, relationships and partnership into account. These are the prerequisites to a successful CIPP. These prerequisites are not technical countermeasures, rather they can be regarded as the non-technical soft skills of a state. Soft skills denote that they are related to the security culture and years -even decades- may be required for such skills to be internalized.

2.3.3 Executive Order – 13636

Executive Order – 13636 is released simultaneously with Presidential Policy Directive – 21 (The White House 2013a). Presidential Policy Directive – 21 covers both physical and cyber security of the critical infrastructures whereas EO – 13636 is dedicated only to cyber security. The title of EO is "Improving Critical Infrastructure Cybersecurity". It is noteworthy to state that EO – 13636 is released after the delay of US Cybersecurity Act in Senate in the summer of 2012.

EO – 13636 assigns duty to the Federal Government to coordinate with critical infrastructure operators to improve information sharing and to collaboratively develop and implement risk-based approaches to cybersecurity (DHS 2013).

Some of tasks that are assigned by EO to Federal Agencies are stated below:

1) Increasing the volume, timeliness, and quality of cyber threat information shared with the US private sector entities (Responsible bodies: Attorney General, the Secretary of Homeland Security, the Director of National Intelligence)

2) Expanding the Enhanced Cybersecurity Services program (voluntary information sharing program) to all critical infrastructure sectors in order to assist the owners and operators of critical infrastructures in protecting their systems (Responsible bodies: the Secretary of Homeland Security, the Secretary of Defense)
3) Developing a Cybersecurity Framework (Responsible body: National Institute of Standards and Technology Director) This framework is prepared by the participation of representative of public and private organizations and released (NIST 2014).
4) Reviewing the preliminary release of Cybersecurity Framework (Responsible bodies: Sector-Specific Agencies, Department of Homeland Security, Office of Management and Budget)
5) Preparing a report for the President, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. (Responsible body: Secretary of Defense)
6) Using a risk-based approach to identify critical infrastructure, reviewing and updating the list of identified critical infrastructure on an annual basis (Responsible bodies: the Secretary of Homeland Security)

2.3.4 Nationwide Cyber Security Review

Nationwide Cyber Security Review was performed by the US Department of Homeland Security in 2011, after Congress directed the DHS to assess the cybersecurity of all levels of the government. Among the 162 State and local government officials, forty-four State representatives participated in the NCSR survey. There are fifty-seven survey questions, which are distributed among 12 control areas. The control areas are composed by the help of the standards like ISO 27001, ISO 27002, NIST SP800-30 and CoBIT. The control areas are consistent with the famous US security management legislations like FISMA, HIPAA and GLBA. The control areas are as follows:

1. Malicious Code
2. Physical Access Control
3. Logical Access Control
4. Security Testing
5. Incident Management
6. Business Continuity
7. Personnel and Contracts
8. Information Disposition
9. Security Program
10. Security within Technology Lifecycle
11. Risk Management
12. Monitoring and Audit Trails

There is a control maturity model, which consists of six levels:

1. Ad-hoc (Tier-1)
2. Documented policy (Tier-2)
3. Documented standards/procedures (Tier-2)
4. Risk measured (Tier-3)
5. Risk treated (Tier-3)
6. Risk validated (Tier-3)

There is a three-level tier structure according to these levels. Therefore, based on their answers, survey respondents fall into one of the tier levels. It should also be noted that the answers to the survey questions are selected from these six levels.

The respondents of the survey were grouped into three distinct types, which are State, State Agency (agencies responsible for IT services, revenue services, health services and transportation services) and Local Government (municipalities, counties). The survey results were published in March of 2012. The detailed results show the answers separated according to the respondent types.

Although NCSR is not designed to evaluate a nation's cyber security preparedness or to determine a maturity level of cyber security, it may show the overall situation of a state, based on the answers.

2.4 Development of Policies for Protection of Critical Information Infrastructures

An OECD publication named Development of Policies for Protection of Critical Information Infrastructures compares the development of policies for the protection of critical infrastructures in seven developed countries (OECD 2007a).

The comparative study of OECD shares some of the good practices of cyber security. It is stated that these good practices are critical to the successful implementation of information security in public and private organizations. Some of these good practices are listed as follows:

1) Clear policy and objectives for cyber security have to be set at the state level.
2) The adopted approach for cyber security have to be consistent with the culture of all the participants, whether public or private.
3) The state administration have to support and commit to the cyber security studies.
4) Risk assessment and management processes have to be internalized in order to identify the requirements of cyber security.
5) Information sharing has to be substantiated effectively among all of the participants.
6) All relevant policies and standards have to be distributed to all of the participants.
7) Required training and education facilities have to be performed.
8) Measurements have to be conducted to improve persistently and continually.

Based on the good practices, some components are examined by OECD to compare the critical infrastructure protection studies of seven developed countries. It is claimed that governments take these components into account while implementing critical infrastructure programs. These components are:

1) A national strategy
2) Legal foundations
3) Incident response capability
4) Industry-government partnerships
5) A culture of security
6) Information sharing mechanisms
7) Risk management approach

Some of the good practices and components that are listed in OECD report can be regarded as the parameters of cyber maturity.

2.5 Regulatory Approaches for Critical Infrastructure Protection

The academic articles that study the different approaches for enforcing regulations on critical sectors are summarized in this section.

There are two perspectives on the regulation of the critical infrastructures in terms of cyber security. This situation can sometimes be viewed as a dilemma for the governments (Orlowski 2001). On one side, some security experts and government officials think that

regulations are imperative to protect the critical infrastructures. On the other side, private sector executives claim that regulations are the obstacles in front of the innovations in cyber security. Executives assert that we should cooperate instead of regulate. The disputes increase in line with the infrastructure ownership of the private sector.

The dilemma was experienced in the proposal of the Cybersecurity Act of 2012 in the US. The original version of the act imposed mandatory security standards on critical infrastructure owners. It also involved information sharing with the military. Private sector criticized the proposal for these obligations. As the result of the critiques, the proposal was altered to reflect changes as the voluntary participation of private sector and stronger government incentives (Hiller & Russell 2013). In spite of these changes in favor of the private sector, Cybersecurity Act of 2012 failed to pass US Senate, although it was endorsed by White House (Kelly 2012). After the dispute of Cybersecurity Act of 2012, Executive Order 13636 was released by White House in In February 2013 (The White House 2013a). The title of the EO was "Improving Critical Infrastructure Cybersecurity". The main theme of the EO was to increase the public-private partnership. It assigned duties to federal agencies in sharing cyber threat information with private sector, in coordinating with critical infrastructure owners and in collaboratively developing and implementing risk-based approaches to cybersecurity (DHS 2013).

According to the current EU rules, among all critical sectors, only telecommunications sector has to adopt security measures and report significant security incidents (European Commission 2013b). EU is on the way to impose government provisions on several critical infrastructure sectors of the member countries. On February 2013, European Commission prepared a proposal for a directive "concerning measures to ensure a high common level of network and information security across the Union" (European Commission 2013a). The directive has not been approved yet. If it is approved by the European Council and Parliament, Member States will have to implement the Directive within 18 months (European Commission 2013b). As the strongest motive of its latest proposal, European Commission reminds the previous cyber security gaps that resulted from the voluntary nature of the past efforts. If the proposal is approved, critical infrastructure operators (from the sectors ranging from energy to healthcare) and public administrators will be required to assess the risks they face and to adopt appropriate and proportionate measures to ensure network and information security. These entities will also be required to report incidents with a significant impact on core services provided to competent authorities (European Commission 2013a). As a result, the directive will apply to the critical infrastructures owned by the private sector as well (Hiller & Russell 2013).

Hiller and Russell state that countries struggle to find the best strategy and regulation for the critical infrastructures owned by the private sector (Hiller & Russell 2013). The authors compare the approaches of the US and EU in terms of the cyber security rules on the private sector. According to the authors, the US follows a voluntary approach for the private sector, whereas the EU adopts a relatively mandatory approach. This conclusion confirms the latest developments in the US and EU.

The approach of Australia resembles the approach of the US. According to the Wilson, Australian government has a deliberate non-regulatory approach for CIP. The liability of the protection of the infrastructure is left to the owners of the infrastructures (Wilson 2014). The legal situation is the same for the Australian National Broadband Network, the largest infrastructure project in the Australian history. There is no security strategy associated with the national broadband network. Instead of the government rules for the protection of the infrastructures, Public-Private Partnerships, as a cost-effective partnering with Non-

Government Organizations, would produce positive outcomes for cyber resilience (Cook 2010).

Dunn-Cavelty and Suter emphasize the importance self-regulating and self-organizing networks for the CIP policy. They argue that the role of the government should be far from close supervision and immediate control; the government should rather coordinate and motivate these networks for the CIP tasks. In their article, they contrast the neoliberal governance theory and the network governance approach and argue that neoliberal governance theory is not suitable for the security-focused CIP policy because it aims to increase the efficiency.

Assaf does not see the regulation issue of the critical infrastructures as a dilemma. Rather, he considers it a choice of governments. According to him, there are two basic models for CIP: the national security model and the business continuity model (Assaf 2008). Assaf shares an illuminating regulatory continuum to demonstrate the seven different options; from highest government intervention to the lowest. He compares the US and Israel in terms of their governmental interventions in cyber security regulations of critical infrastructures. The US adopts the business continuity model with the exceptions in energy and chemistry sectors whereas Israel adopts the national security model.

According to the Luiijf and Klaver, no single governance model for CIP is applicable to all countries. The regulation of CIP in a country depends on its legal system, the trust level between government and private sectors, and its historical and cultural background (Luiijf & Klaver 2004). Hence, Luiijf and Klaver corroborate the idea of Assaf. Luiijf and Klaver also mention the importance of the cooperation and collaboration efforts in both national and international domains. They also emphasize the internationally harmonized CIP efforts for multinational operators.

Orlowski also points out the regulatory approaches for the multinational infrastructures. According to Orlowski, there are two types of regulations for the CIP: protective security and criminal laws. Protective regulations should be the last resort for the free market economies. Countries with such economies should cooperate instead of regulate because they may impose different regulations on critical infrastructures according to their constitutional powers. These differences result in inconsistencies at cross-border management, especially for multinational corporations. On the other hand, fighting against cybercrime is the area where a commonly accepted regulation is needed (Orlowski 2001). Convention on Cybercrime, also known as Budapest Convention, is an international treaty to fight against cybercrime by urging the harmonization of the domestic laws (European Council 2001). It is signed by 33 countries: 32 members of European Council and the US.

Table 2-2 summarizes the provision approaches of three countries and the EU according to the articles reviewed. The US and Australia adopt the market provision, which means minimum supervision of the government. However, energy and chemistry sectors are more strictly supervised by the US federal agencies. Israel adopts the government provision; that is, strict supervision of the market by the government. EU recently attempted to shift the paradigm from market to government provision. However, as a result, the approaches on the CIP regulation is a hot topic in the developed world. The strict government intervention and regulations on the CIP efforts is not considered as a suitable option by the academia and governments of developed countries. A number of academic studies that propose security management models for CIP originates in such countries. This topic can be summarized by the following questions: Which is suitable? Regulation or Innovation? These articles focus on the importance of the cooperation, innovation, and non-regulation over regulations.

Table 2-2: Provisional Approaches of Three Countries and EU

	Government Provision	Market Provision
US*		✔
EU	✔	
Israel	✔	
Australia		✔

** Except for energy and chemistry sectors*

2.6 Regulations of Turkey for Critical Infrastructures

In this section, the regulations of Turkey related with the cyber security and critical infrastructure sectors are resumed.

The statute 2011/2237 on Military Forbidden Zones and Security Zones mentions the requirements of the physical security of energy, manufacturing, water management, transportation, telecommunications, intelligence, and military facilities, without using the term critical infrastructure (Turkish Cabinet 2011). The aforementioned statute does not include any articles about the cyber security.

Cyber Security Council of Turkey was established in October 2012, with the members from eleven governmental organizations. After the second meeting of the council in June 2013, the telecommunications, energy, water management, public services, transportation, and finance sectors were designated as national critical infrastructures of Turkey. However, the decision remained in the minutes of the meeting, without changing the existing regulations or creating a new one in Turkey (Kaska & Trinberg 2015).

Turkey has regulatory authorities for the energy, telecommunications and finance sectors. The related agencies are autonomously managed. The government in force can appoint only some members of the boards of these agencies.

Until the amendments in December 2014, there were no cyber security or information security-related articles in the statutes of the energy sector. Energy Market Regulatory Authority amended the license regulations of the electricity, natural gas, and petroleum markets in December 2014. According to the amendments, electricity production, transmission, and distribution facilities, natural gas transmission and distribution facilities, and petroleum refineries were required to establish ISO 27001 compliant information security management systems for information processing departments (EMRA 2014a; EMRA 2014b; EMRA 2014c).

Publishing a legal annunciation, Information and Communications Technologies Authority urged the operators to comply with the ISO 27001 in telecommunications sector in October 2010. The authority released a new and more stringent regulation for ISO 27001 compliance in July 2014 (ICTA 2014).

Banking Regulation and Supervision Agency published several legislations for the finance sector. In January 2008, BSRA published a legal annunciation on the information security management of the banks. The annunciation contains the provisions about information security risk management, management liabilities, internal audit, outsourcing rules, separation of the duties and several other controls (BRSA 2007). Another regulation sets the rules for the information systems audits of the banks by the independent external auditors (BRSA 2010).

In February 2014, Electronic Communications Law was amended to reflect the cabinet decisions dating back to October 2012 (Turkish Cabinet 2014). By these amendments;

a) Cyber Security Council was defined in ECL. The president of the Cyber Security Council was appointed as the Minister of Transport, Maritime Affairs and Communications. One of the responsibilities of the Cyber Security Council was to approve the list of the critical infrastructures.
b) The cyber security roles of the Ministry of Transport, Maritime Affairs and Communications (Ministry) were defined. One of the responsibilities of the ministry was to determine the critical infrastructures, their owners and locations.

As the critique of the Turkish organizational structure and the legislation; Turkey lacks an overarching critical infrastructure protection program that handles cyber and physical security together. By considering the establishment of a security zone around the facilities, the decree 2011/2237 considers only the physical security. The recent amendments to ECL assign some responsibilities to the Ministry and Cyber Security Council only on cyber security. The term "critical infrastructure" was used explicitly in the amendments. However, the amendments hold neither a definition nor a list of the critical infrastructures. Therefore, they are far from setting up a holistic critical infrastructure protection program. There is neither legislative nor organizational connection between the decree 2011/2237 and the amendments to ECL.

The recent amendments to ECL assigned some roles to the Ministry, but not the required authority. As an example, the Ministry did not have the power to audit the public organizations and the critical sectors, in context of cyber security. According to the civil law system, a role that is assigned to a governmental authority by a law has to be elaborated with lower level statutes. By this way, the details of the applications of the law are specified in detail. The recent amendments to ECL have not been detailed by using lower level statutes so far.

2.7 Maturity Models for Cyber Security

Measurement is an important instrument for the continuous improvement of security. Something that is not measured cannot be managed and thus improved. The maturity measurement of the cyber security efforts of a country is a rarely-studied topic in the academic literature, and similarly the maturity measurement of the critical infrastructure protection efforts of a country has not been studied in the academic literature. It is because the confidentiality constraints limit the availability of the data and limited data in this area affect the number and content of the academic studies. The number of governmental studies about this topic is limited, too. The measurement of the national level cyber security effort is quite challenging, compared to the measurement of information security within an organization. The first of the three prominent reasons for the fact is that, cyber security is a new and challenging topic for countries. Secondly, the scope of the national level cyber security is quite wide due to the horizontal usage of cyber system by all the sectors. Thirdly, as cyber security has several dimensions, including policy-level, technical, international, legislative, and organizational, it is quite difficult to evaluate the different dimensions in the same pot. Most of the studies in the literature do not propose a dedicated, country-oriented model; rather they score and rank countries.

Six studies on national cyber security maturity assessment are summarized and compared in this section. Cyber security is the main focus in four studies, and in two of them is considered as the parameter of the cyber power of the countries. Two studies are performed by academics; whereas four studies are performed by international / regional organizations or governments.

2.7.1 The Community Cyber Security Maturity Model

The Community Cyber Security Maturity Model is a government-funded academic study that includes a holistic cyber security program with five maturity levels (White 2012). The model includes guidance on how to step forward onto the higher maturity levels. The CCSMM checks the existence of various best cyber security practices to determine the maturity level; however, the article did not share a pre-defined and detailed list of the countermeasures that corresponds to each maturity level. Besides, the upper levels of the model are not fully developed, because "no community is currently at that level" (White 2012). The CCSMM can be adapted according to the requirements of different types of targets. The targets of the CCSMM can be organizations, communities, states and even individuals. The list of the countermeasures may differ according not only to the level of maturity but also the type of the target. The model is applied to eleven communities within five states of the US, but the details of the studies are not shared. As far as understood from the presented article, there is currently no state-level application of the model.

The CCSMM is a three dimensional maturity model. First dimension of the CCSMM is five maturity levels, extending from initial to vanguard. The second dimension is the type of the body for which maturity model can be applied. The model can be applied to an organization, a community or a state. The third dimension of the model is the countermeasures that build the model. Determined for this dimension, four countermeasure domains are cyber security awareness, information sharing, processes and procedures to handle cyber events, and test and evaluation of the cyber security countermeasures.

As of 2011, the model have been implemented in five states within the US. It is stated that the CCSMM model will evolve and improve as it is applied by the states. As of the publication date of the article, the upper two levels of the model have not been constituted; and the application will occur "as a natural outcome as states and communities advance in the model" (White 2011).

2.7.2 National Cyber Security Management System

National Cybersecurity Management System provides guidance with which a state or region can measure its current security status (Kettani & Debbagh 2009). NCSecMM is a holistic security program like the CCSMM. It includes an application framework, roles and responsibilities matrix, an implementation guidance, and a maturity model. It is basically an adaptation of ISO 27000 series standards and CoBIT framework countermeasures to the national context. The maturity level of each process is measured separately according to a five-level maturity model adapted from CoBIT framework. The model is not applied in a national context yet. NCSecMM framework includes thirty-four cyber security processes in five groups. The headings of the some of the processes in five groups are as follows:

1. Strategies and Policies
    a. National Cyber Security Strategy
    b. Lead Institutions
    c. National Cyber Security Policies
2. Implementation and Organization
    a. National Cyber Security Council
    b. National Cyber Security Authority
    c. National CERT
    d. National Experts and Policymakers
    e. International Expertise
3. Awareness and Communication

a. Leaders in Government
b. National Awareness
c. Research and Development
d. Cyber Security Culture for Business

4. Compliance and Coordination
    a. Private Sector Cooperation
    b. Incident Handling
    c. International Compliance and Cooperation
5. Evaluation and Monitoring
    a. National Cyber Security Observatory
    b. National Cyber Security Assessment
    c. National Cyber Security Governance

2.7.3 Cyber Readiness Index

Cyber Readiness Index was proposed by the former acting senior director for cyberspace at the National Security Council of the US. By using the publicly available data resides at the governmental websites of the countries, the cyber security efforts of thirty-five countries were assessed according to the best practices specified by the author. The maturity levels of each country are not represented quantitatively or qualitatively. The study is concluded as "no country is cyber ready" (Hathaway 2013). The author of the study explains the goal of the study as "to spark international discussion and inspire global interest in addressing the economic erosion from cyber insecurity that is holding back more robust economic growth".

With the aim of determining whether a country is cyber ready or not, five state level domains are proposed. The titles of each domain and the criteria for each title are given below:

a) National cyber security strategy
    i. The existence of strategy
    ii. The existence of budget allocated to strategy
    iii. The participation and engagement of private sector in national cyber security strategy
b) The existence of operational Computer Security Incident Response Team
    i. The existence of tested emergency and recovery plans that take the infrastructure dependencies into account
    ii. The exchange of national contact details of different networks such as governmental / regulatory bodies and critical infrastructure operators
    iii. The existence of information sharing and alert system
c) The commitment (by country) to protect against cyber crime
    i. The existence of the studies to determine the monetary loss of cybercrime
    ii. Threat assessment
    iii. Establishment of criminal offenses
    iv. Reviewing existing laws
    v. Capacity building mechanisms.
d) The existence of information sharing mechanisms
    i. The existence of cross sector incident-information sharing during and after incidents
    ii. The existence of rapid reaction mechanism
    iii. The use of unclassified intelligence data
    iv. The existence of situational awareness mechanism
    v. The existence of the cross sector incident management and coordination mechanism that take the interdependencies into account

e) The existence of investments and funding of research activities
    i. The existence of budget allocated for cyber security research
    ii. The existence of the national funding for universities
    iii. The ratio of the operational products that emanates from research activities
    iv. The existence of the universities that offer degree in cyber security or information security
    v. The existence of the government incentives for innovation
    vi. The commitment to the internationally accepted interoperability and security standards
    vii. The commitment to protect intellectual property

2.7.4 Global Cybersecurity Index

Global Cybersecurity Index is proposed by International Telecommunication Union to figure the cyber security maturity levels of 104 countries (ITU 2014). The maturity level of a country is figured by evaluating the existence of seventeen criteria within five domains, which were determined at Global Cybersecurity Agenda of ITU (ITU 2007).

The domains and the respective criteria are as follows:

a) Legal Measures
    i. Criminal legislation
    ii. General cyber security regulation / compliance
b) Technical Measures
    i. National Computer Security Incident Response Teams
    ii. Government-approved standardization studies
    iii. Personal certification studies
c) Organizational Measures
    i. Clear polices
    ii. Cyber security governance
    iii. Responsible agency for the implementation of cyber security
    iv. National benchmarking in the light of nationally adopted standards
d) Capacity Building
    i. Standardization development studies
    ii. Professional manpower development
    iii. Individual certification
    iv. Agency certification
e) Cooperation
    i. Intra-state cooperation activities
    ii. Intra-agency cooperation activities
    iii. International cooperation activities
    iv. Public-private partnership practices

The goals of the study are stated as the following:

1) Promote government strategies at a national level
2) Drive implementation efforts across industries and sectors
3) Integrate security into the core of technological progress
4) Foster a global culture of cybersecurity

ITU published a conceptual framework that shows both the explanations of the criteria and the readiness calculation methodology. The parameters were converted into survey questions

to measure the maturity level. For each parameter, three possible answers were created. A country gets zero point for no action, one point for a partial action, and two points for a comprehensive one.

There were primary and secondary data sources. The primary data source was the relevant national stakeholders. The secondary data source was the publicly available sources.

There were more than one type of data collection. First of all, the data were collected by using the online questionnaire in the webpage of the project. The second way was contacting with the relevant national stakeholders, as stated by ITU. Internal databases of ITU and publicly-available resources were used as the third data source.

The maturity level of a country is represented by the normalized values between zero and one. There were twenty-nine different maturity levels, which means that a number of countries were represented by the same maturity level. As stated by the ITU, "the index has a low level of granularity since it aims at capturing the cybersecurity preparedness of a country and not its detailed vulnerabilities". At final report of the study, the countries were ranked from the highest to the lowest maturity level.

A total number of 104 countries were scored and ranked in the study. However, the data of 90 countries were based on the internal databases of ITU, and publicly-available resources, which means only fourteen countries provided data specifically for the study.

2.7.5 Cyber Maturity in the Asia–Pacific Region

Prepared by Australian Strategic Policy Institute, the report "Cyber Maturity in the Asia–Pacific Region" includes the cyber maturity analysis of fourteen Asia-Pacific region countries, along with the UK and US (Tobias Feakin & Woodall 2014). The study does not concentrate solely on cyber security. Cyber security is considered as a dimension of the general cyber maturity of the countries. The evaluation criteria along with the weights are determined by the help of the experts from the government, private sector, and academia. Countries are assessed and scored according to the publicly available data about the countries. The maturity assessment results are converted into percentages and the countries are sorted from the highest to the lowest percentage values. ASPI analyzed the cyber maturity of 14 Asia-Pacific countries. It also included the UK and US as the benchmark.

Cyber maturity assessment is performed according to four key topics and associated subtopics as follows:

1. Governance
    a. The existence of organizational structures for cyber issues, like policy, security, critical infrastructure protection, crime, consumer protection
    b. The existence of legislation
    c. The engagement in international discussion on cyberspace
    d. The existence of cyber assistance service like CSIRT
2. Military Application
    a. The role of the military in cyberspace, cyber policy and cyber security
3. Digital Economy and Business
    a. The existence of dialogue between government and industry
    b. The extent of digital economy in economic activity
4. Social Engagement.
    a. The existence of public awareness, media coverage
    b. The percentage of population with internet connectivity.

As seen from the listed criteria, some of them are related to cyber security while some of them are not. These criteria are determined in a workshop with the participation of government officials, private sector representatives and academic experts. After the identification of the criteria, they are scored by experts, between one and ten. The final weight value for a specific criterion is calculated by experts by taking the arithmetic average of weights assigned to it. After weighting the criteria, five answer choices are determined for each criterion. The answer choices are weighted between one and ten. After the indication of the weight values for questions (criteria) and the associated answer choices, countries are assessed and scored. The results are converted into percentages and the countries are sorted from the highest score to the lowest.

The cyber-maturity assessments and evaluations are made based on the information in the public domain and open-source material. It is a regional cyber maturity metric within this study, and planned to conduct annually.

2.7.6 Cyber Power Index

Cyber Power Index is created by Booz Allen Hamilton to score and sort the cyber powers of nineteen G20 countries, except EU (BAH 2011). Cyber security is not the main focus of the study, it is rather a dimension of the cyber power of the countries. The weight values of the criteria and the answer choices are determined by the expert members of a peer panel. The main sources of data for country evaluations were Economist Intelligence Unit, UNESCO, ITU, and World Bank.

Cyber power is evaluated according to the four criteria:

1. Legal and regulatory framework
    a. Government commitment to cyber development
    b. Cyber protection policies
    c. Cyber censorship
    d. Political efficacy
    e. Intellectual property protection
2. Economic and social context
    a. Educational levels
    b. Technical skills
    c. Openness of trade
    d. Degree of innovation in the business environment
3. Technology infrastructure
    a. Access to ICT
    b. Quality of ICT
    c. Affordability of ICT
    d. Spending on IT
    e. Number of secure servers
4. Industry application
    a. Smart grids
    b. E-health
    c. E-commerce
    d. Intelligent transportation
    e. E-government

The weight values of for these subcategories and thus the categories are settled by the expert members of a peer panel in May 2011. The weights are created for answer choices for each subcategory as well. Cyber security is the topic of the cyber protection policy subcategory within the legal and regulatory framework category. The existence and the details of cyber

enforcement authority, cybersecurity laws, cybercrime response, international cybersecurity committees and cybersecurity plan are evaluated. Cyber power index of nineteen countries are measured and the countries are sorted from the highest to the lowest maturity.

2.7.7 Comparison and Critiques of the Maturity Models

Table 2-3 summarizes six models according to their various properties. The CCSMM and NCSecMM devise country-level cyber security maturity assessment models. Other four studies perform country scoring and sorting. Among them, Cyber Readiness Index and Global Cybersecurity Index concentrate solely on cyber security. The scopes of other two studies (Cyber Maturity in the Asia–Pacific Region and Cyber Power Index) are wider than cyber security, which means that cyber security is just a parameter of the broader topic: cyber power.

It is notable that, none of the studies is specifically dedicated to the maturity assessment of the critical infrastructure protection efforts of a country

Table 2-3: Summary of the Maturity Studies

Name of the study	Developed by	Brief description	Main theme	Evaluation criteria are determined by using	Country evaluations are performed according to
The Community Cyber Security Maturity Model	Gregory B. White, The University Texas at San Antonio (Academia)	A holistic security program for organizations, communities, and states and maturity model for determining cyber security postures of them.	Cyber security	Not specified	Data provided by government officials
National Cybersecurity Management System	Kettani & Debbagh (Academia)	A holistic security program for countries, including framework, maturity model, roles assignment and implementation guide.	Cyber security	ISO 27002, ITU documents	Country-level evaluation is not performed
Cyber Readiness Index	Hathaway Global Strategies, LLC (Private organization)	Country scoring (35 countries)	Cyber security	Not specified	Publicly available data

Name of the study	Developed by	Brief description	Main theme	Evaluation criteria are determined by using	Country evaluations are performed according to
Global Cybersecurity Index	ITU (International agency)	Country scoring and sorting (104 countries)	Cyber security	Global Cybersecurity Agenda (ITU 2007)	Internal databases of ITU and publicly-available resources (90 countries) Data acquired from national stakeholders for the study (14 countries)
Cyber Maturity in the Asia–Pacific Region	Australian Strategic Policy Institute (NGO)	Country scoring and sorting (18 countries)	Cyber power	Expert opinion	Publicly available data
Cyber Power Index	Booz Allen Hamilton (Private Organization)	Country scoring and sorting (19 countries)	Cyber power	Not specified	Publicly available data, international organizations, Economist Intelligence Unit

First of all, the maturity criteria of the models are not the same. Therefore, the maturity level of a country may differ among models. As an example, the maturity level of Turkey in Global Cybersecurity Index study is 64.7%, ranking seventh among twenty-nine different scores, while it is 30.4% in Cyber Power Index, ranking fifteenth among nineteen countries.

Because national cyber security and critical infrastructure protection are important agenda items for the countries, some maturity criteria exist in the countries even with low level maturities. As an example, the national CSIRT organization was specified as a maturity / readiness criterion in five of the models. However, most countries today –even underdeveloped ones- have national CSIRTs. Therefore, it may not be a true criterion for the cyber maturity of a country. A country can effortlessly claim the establishment of national CSIRT by registering itself to some of the international CSIRT databases. However, whether a government provides budget, personnel, and trainings is more essential than the registration to the international databases. The later processes show that the country attributes importance to cyber security. Therefore, specifying the details of the trivial maturity criteria may be a sound practice during the development of a maturity model. The selection of the trivial maturity criteria may even result in unexpectedly high scores for especially underdeveloped countries.

The second criticism for the current models is about the method of specifying the maturity criteria and the application of the maturity model. The basic constructs of a maturity model are its maturity criteria. If the criteria are determined by analyzing the actual security posture of a country, the current situation and progress can be observed more realistically by using the maturity model. The models that evaluate the maturity of the national level cyber security efforts are limited not only in number but also in content. The maturity evaluations in the current literature are performed by applying the following two steps consecutively:

1) A set of criteria is determined by using usually the best practices or publicly available sources. (Please refer to the fifth column of Table 2-3)
2) The countries are evaluated according to the publicly available data or sometimes by using the questionnaires. (Please refer to the sixth column of Table 2-3)

In order to increase the accuracy level of a maturity model, the criteria of the maturity model should be grounded on the actual data and vulnerabilities of the country. Following to the preparation of the maturity model, the measurements should be performed by the relevant government officials. These customizations will definitely increase the accuracy of the maturity model. Hence, the model will be more beneficial for the countries in both the evaluation of the current cyber security postures and in the identification the requirements of the prospective studies.

In this PhD research, the researcher performed these customizations by using the data of the state-sponsored project and by contacting with government officials. Secondly, rather than the measurement of the state-level cyber security, the researcher proposed a maturity model which is specific to the critical infrastructure protection efforts of a country, because critical infrastructure protection is the common and one of the most vital agenda items in the national cyber security strategies of the countries (Klimburg 2012).

CHAPTER 3

3 RESEARCH DESIGN

This chapter contains the sections of several issues regarding the research design. These are research motivation, research question, methodical details of GTM, motive of selecting GTM as research method, details of research data, interval validity issues, details of Delphi survey, research population, sampling methods, role of the researcher, trustworthiness of the research and finally research ethics.

3.1 Introduction

The PhD study has three main outputs. Firstly, the root causes of the susceptibility of the critical infrastructures to cyber threats are extracted. Secondly, the set of principles for the cyber security of the critical infrastructure of Turkey are extracted by using the root causes. Thirdly, a national level cyber security maturity model is devised by using the set of principles.

Therefore, the PhD study was basically a three-phased research. At the first phase, a qualitative data analysis was performed by using the GTM to extract the root causes from the data. At the second phase, Delphi survey was performed by using the outputs of the first phase to find the set of principles. At the third phase, based on a simple linear additive evaluation model, a maturity model was developed by using the views of the experts at Delphi survey. The overview of the research process along with the inputs and outputs is shown Figure 3-1.

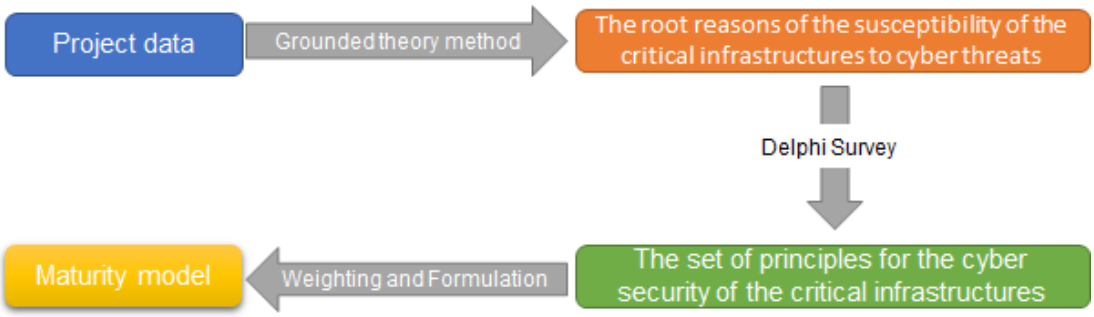


Figure 3-1: Research Process (General View)

The details of the research is shown in Figure 3-2. The three phases of the research are explicitly shown with dashed lines in this figure. GTM is composed of four consecutive recursions, a saturated theory was extracted after these recursions. The Delphi Survey consists of five consecutive rounds. After the Delphi survey, a maturity model was devised by using the linear additive model. Finally, an unofficial application of the model was performed as well.

3.2 Research Motivation and Research Questions

The researcher participated in the state-sponsored project named “Information Security Management in Critical Infrastructures” between January 2012 and December 2013. The vulnerabilities that stem from the usage of the cyber systems were analyzed in the project. The results of the project showed that critical infrastructures had significant vulnerabilities

related with the cyber systems, in spite of recent national efforts such as the establishment of Cyber Security Council and the national CSIRT organization.

The research motivation of the GTM is to discover the possible root causes of the susceptibility of the critical infrastructures to cyber threats. The research question is "What are the possible root causes of the susceptibility of the critical infrastructures of Turkey to cyber threats?"

The second research question is "What are the set of principles to mitigate these root causes?" This question is answered through the conduction of Delphi survey.

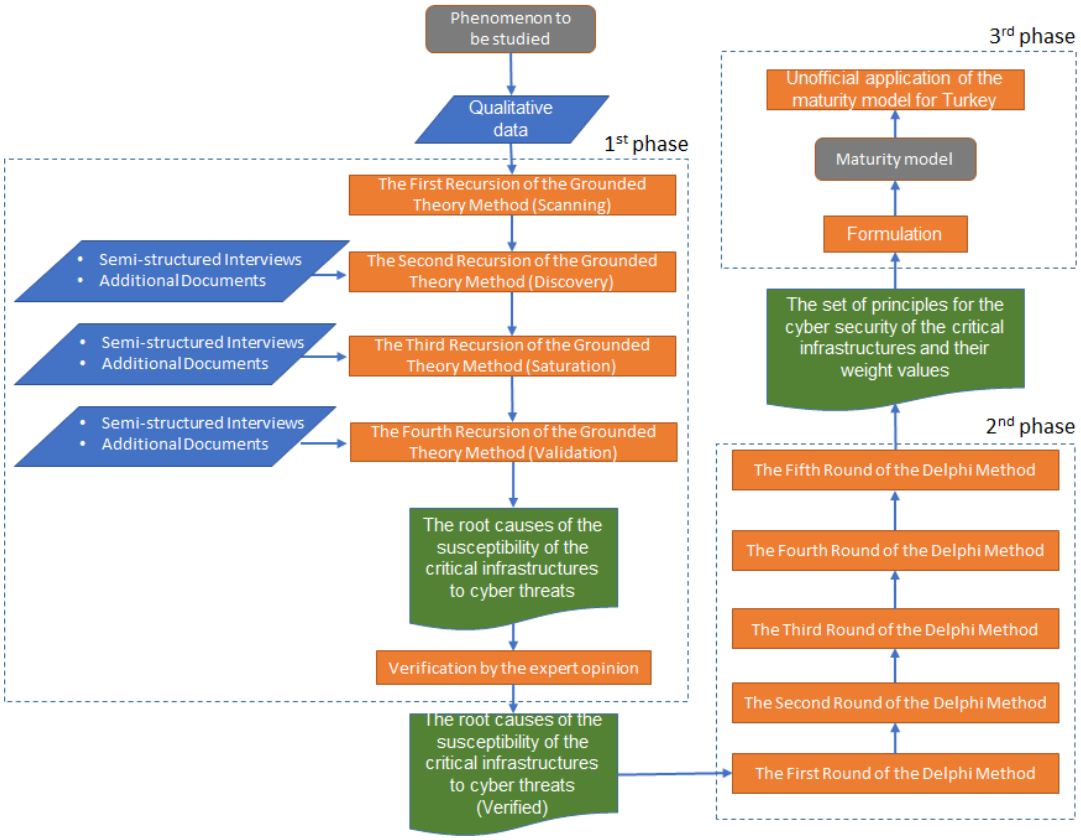


Figure 3-2: Research Process (Detailed View)

3.3 Grounded Theory Method

A number of qualitative data were gathered for the PhD research. The data were analyzed using Grounded Theory Method, a qualitative data analysis method. The qualitative data were rigorously coded, codes were categorized and categories were compared in order to extract the theory inside the data, the root causes of the susceptibility of the critical infrastructures to cyber threats.

GTM is an interpretive, qualitative and inductive data analysis method, which is proposed and used by two sociologists, Glaser and Strauss in 1967. It is the discovery of the theory through the analysis of data (Strauss & Corbin 2008). GTM provides a detailed, rigorous, and systematic method of data analysis (Jones & Alony 2011). In GTM, the researcher does not begin with a hypothesis that has to be proved or disproved, but he begins "with an area of study and allows the theory to emerge from the data" (Strauss & Corbin 2008). In GTM, the research question is a statement that identifies the phenomenon to be studied. The results of the assessments within the project of "Information Security Management in Critical

Infrastructures" showed that cyber systems were used significantly in the sectors of the energy, telecommunications, finance, government services, transportation, and water management. The project also showed that critical infrastructures are susceptible to cyber threats because of their inherent vulnerabilities. These vulnerabilities are paving the way for the successful cyber attacks. In this research, the phenomenon of the susceptibility of the critical infrastructures to cyber threats were analyzed. The root causes of the susceptibility were extracted as the theory.

3.3.1 Suitability of the Grounded Theory Method

There were several reasons for the selection of GTM as the data analysis method. First of all, GTM is particularly suitable when "the topic of interest has been relatively ignored in the literature or has been given only superficial attention" (Goulding 2002). The topic of the possible root causes of cyber security vulnerabilities of the critical infrastructures of Turkey has been studied in neither the national nor the international literature. Secondly, GTM is suitable for studying social issues (Jones & Alony 2011; Glaser & Strauss 1967). Cyber security is a horizontal area that intersects a number of social disciplines, like public administrations, regulations and international security policies. Because the researcher aims to find the "root causes" of the cyber security vulnerabilities of the critical infrastructures of Turkey, he has to analyze the topics in social nature rather than technical issues. Thirdly, GTM is suitable for the analysis and interpretation of complex and multifaceted phenomena (Orlikowski 2002; Charmaz 2000). During the data analysis, the researcher took the organizational, sectorial and country level cyber security countermeasures into account. The researcher had to consider not only technical countermeasures, but also the non-technical ones. He dealt with the complex correlations among the vulnerabilities. GTM provided a structured roadmap in analyzing the complex phenomena. Fourthly, GTM is a proven method for its appropriateness to develop new theories from broad and diverse sets of complex data (Glaser & Strauss 1967). During the data analysis, the researcher had to deal with hundreds of documents of different types, from questionnaires to legislation texts, from media reports to independent evaluation ones. Well-defined coding steps helped much in dealing with the vast amount of diverse data. Lastly, the first phase of the research, to some extent, falls under the discipline of management information systems. GTM fits well into the information systems research, because information systems cover not only information technology, but also procedures and peoples (Fernández & Lehmann 2011). There are a number of information systems researches that are performed by using GTM (Rodon & Pastor 2007; Matavire et al. 2010; Hansen & Kautz 2005).

There are two basic schools of GTM, namely Glaserian school and Straussian school (Jones & Alony 2011). In Glaserian School, the researcher has an empty mind at the beginning. He asks neutral questions and lets the theory emerge. As a result, the researcher is in a passive role. In Straussian School, the researcher has a general idea of the phenomenon to be studied. He forces the theory by using structured questions. As a result, the researcher is in an active role. In this research, Straussian school was adopted. The researcher has a considerable amount of knowledge on the subject area. He does not have an empty mind. He directs the research until the extraction of the theory.

3.3.2 Research Data

The data belonging to six critical sectors were analyzed in this PhD study. The six critical sectors were energy, telecommunications, finance, transportation, water management, and government services, which were resolved in the second meeting of the Cyber Security Council of Turkey in June 2013.

The project data were composed of interview texts and various kinds of official documents. Data collection and interviews were performed until theoretical saturation. Nine semi-structured interviews were performed with the critical infrastructure owners. Interviews provided the focused, in-depth and rich data on the phenomenon under analysis. The interviews included open-ended questions about the general security posture, threats, potential vulnerabilities, applied countermeasures, and weaknesses of the interviewed organization and the critical sectors. The questions were reshaped according to the emerging categories and themes, and they were regarded as the initiators and catalyzers of the long lasting and evolving interviews. The interviewees were mid-managers and employees of the information processing departments. Table 3-1 shows the distribution of the interviewed organizations according to the sector and organization types.

Table 3-1: Distribution of the Interviewed Organizations

Critical Sector	Interviewed organization (Public)	Interviewed organization (Private)
Energy	1	1
Telecommunications	1	1
Finance	1	1
Transportation	1	0
Water Management	1	0
Government Services	1	0
Total	6	3

As to increase the robustness and reliability of the study, interviewed critical infrastructure operators were determined for each sector according to the dominance of the governmental or private organizations in that sector. Table 3-2 summarizes the situation of the ownership for each sector. Table 3-2 is created by using the public information sources like websites of the regulatory authorities and critical infrastructure operators. There is no official statistical data on the ownership of the critical infrastructure operators.

Water management and transportation sectors are substantially operated by the governmental organizations in Turkey. The semi-structured interviews are performed with governmental organizations for these sectors. The energy, telecommunications, and finance sectors are operated by both private and governmental organizations. Therefore, for these sectors, both types of the organizations are interviewed.

Table 3-2: Summary of the Ownerships of the Critical Infrastructure Operators

Critical Sector	Ownership
Energy	Electricity production: %38 government (EUAS 2015) Electricity transmission: government (TEIAS 2015) Electricity distribution: private (TEDAS 2015) Natural gas transmission: government (BOTAS 2015) Natural gas distribution: In privatization. (Ankara: private, Istanbul: government) Petroleum production: %73 government (TP 2015) Petroleum transmission: government (BOTAS 2015) Petroleum refinery: private (TUPRAS 2015)

Critical Sector	Ownership
Telecommunications	Two GSM operators: Private One GSM operator: %88,99 of shares are owned by Turk Telekom Turk Telekom: %55 of the shares are privatized (Turk Telekom 2015) Satellite and cable television: government
Finance	Stock exchange, treasury, central bank: government Banks: %6 government (Wiki 2015b)
Transportation	The prominent airway, railway and seaway operators are owned by government.
Water management	Government
Government services	Government

Three hundred and nine documents associated with ninety one different governmental or private organizations were gathered. Most of these organizations were critical infrastructure owners from energy, telecommunications, finance, transportation, water management and government services sectors. There were also documents belonging to the regulatory authorities and the ministries.

The distribution of the organizations according to the sector type and ownership is shown in Table 3-3.

Table 3-3: Distribution of the Organizations according to the Sector and Owner

Critical Sector of the Organization	Private	Governmental	Total
Energy	6	12	18
Telecommunications	5	7	12
Finance	8	10	18
Transportation	5	7	12
Water Management	3	3	6
Government Services	0	25	25
Total	27	64	91

The collected documents were classified in five groups. These are:

a) Minutes of meeting
b) Independent evaluation report
c) Regulation text
d) Organizational report
e) New and media report

Minutes of meeting are the notes taken during the state-sponsored project. The researcher took a written consent from the project manager. Performed by the independent third parties, independent evaluation reports are information security audit and analysis results of the critical infrastructure owners. Regulation texts are the laws and statues that regulate the activities of critical infrastructures operators. Regulation texts provide insight into the security views and practices of the organizations. Organizational reports are the documents prepared by the organizations such as annual activity reports, annual plans, and strategic plans. Organizational reports were downloaded from the websites of the organizations. These reports contain valuable information on the cyber security perceptions of the organizations. News and media reports are media excerpts related with the critical infrastructures. The

researcher collected the news related with the critical infrastructures of Turkey between 2011 and 2014. News and media reports include valuable information on threats, the opinions of the experts and the government officials.

As shown in Table 3-4, minutes of meetings and independent evaluation reports are restricted documents, which are not available publicly; whereas regulation texts, organizational reports, and news and media reports are publicly available documents. Table 3-4 shows the source of the documents as well.

Table 3-4: Confidentiality of the Gathered Documents

Document Type	Confidentiality	Source
Minutes of Meeting	Restricted	State sponsored project
News and Media	Publicly available	Newspapers and Internet media
Regulation Text	Publicly available	Official websites of the organization Official Gazette State sponsored project
Organizational Report	Publicly available	Official websites of the organizations State sponsored project
Independent Evaluation Report	Restricted	State sponsored project

The distribution of the collected documents according to the critical sector type is shown in Table 3-5.

Table 3-5: Distribution of the Documents

Critical Sector / Document Type	Energy	Telecommunications	Finance	Transportation	Water Management	Government Services	TOTAL
Minutes of Meeting	20	3	5	2	3	13	46
News and Media Report	15	9	3	4	2	41	74
Regulation Text	12	9	5	3	2	8	39
Organizational Report	18	7	2	3	4	14	48
Independent Evaluation Report	21	11	16	14	6	34	102
TOTAL	86	39	31	26	17	110	309

3.3.3 Internal Validity by Using Data Triangulation

The triangulation obtained by using different sources of data for the internal validity of the research was performed in this PhD study (Kaplan & Duchon 1988). The triangulation of the data improved the reliability and validity of the study. The data triangulation can be regarded as a means of completeness of the research as well (Adami & Kiger 2005). By triangulating data, the research relied on the multiple sources of evidence and the construct validity is ensured (Thai et al. 2012). Therefore, unbiased data were used in data analysis. The triangulation of data from different sources helped the researcher to avoid potential analytical errors and omissions (Kaplan & Duchon 1988). Therefore, the researcher tried to

reduce the weaknesses of each individual data source (Thai et al. 2012). Table 3-6 shows the sources of the collected data. Internal means that the data are produced by the analyzed organizations. External means that the data are produced by the independent third party organizations. News and media along with independent evaluation reports are external to the organization. Organizational reports are internal documents.

Table 3-6: Sources of the Documents

Document Type	Prepared by
Minutes of Meeting	Internal / External
News and Media	External
Regulation Text	Internal / External
Organizational Report	Internal
Independent Evaluation Report	External

Regulation texts can be either internal or external. If it is prepared by the critical infrastructure operator itself, it is internal. If it is prepared by a higher order authority such as regulatory authority, it is external. Directives, instructions, circulars are internal regulations, whereas laws are external to the most of the critical infrastructure operators.

Minutes of meetings can be either internal or external as well. Minutes of meetings were created by the researcher including the opinions of the third parties. However they also contain the opinions of the organizations.

3.3.4 Application Details of the Grounded Theory Method

In Straussian GTM, there are three consecutive steps which are open coding, axial coding and selective coding. The qualitative data were coded, and codes were categorized in open coding step. Categories are the basic headings under which extracted codes are clustered. Categories were compared to find the themes in axial coding step. Redundant, obvious, and irrelevant themes were eliminated to refine the theory in the selective coding step. Selective coding is the integration of different categories in order to build a theory (Thai et al. 2012). A single run of three steps was not enough to obtain a saturated theory. GTM is the recursive process of data collection, data coding, comparative analysis, and theoretical sampling until theoretical saturation (Glaser & Strauss 1967; Goulding 2002; Locke 1996; Strauss & Corbin 2008). The details of the application of the GTM for the PhD research is shown in Figure 3-3. Data analysis performed in four recursions. Only open coding step was conducted in the first recursion. In the following three recursions, all three consecutive coding steps were conducted.

It is important to emphasize the theoretical sampling processes between the recursions. Because GTM is a process of discovery rather than hypothesis testing, theoretical sampling was performed instead of statistical sampling (Denscombe 2010; Strauss & Corbin 2008). In theoretical sampling, the unsaturated theory of initial recursions guides the data collection processes of the next recursion. The type of data, critical sector, interview questions, and organization for the next recursion were determined according to the results of the current recursion during the data analysis. The researcher decided the new resources of data, reshaped the interview questions according to the theoretical sampling. This process was performed until theoretical saturation. Theoretical saturation is the point where new data does not change the discovered theory (Shannak 2009).

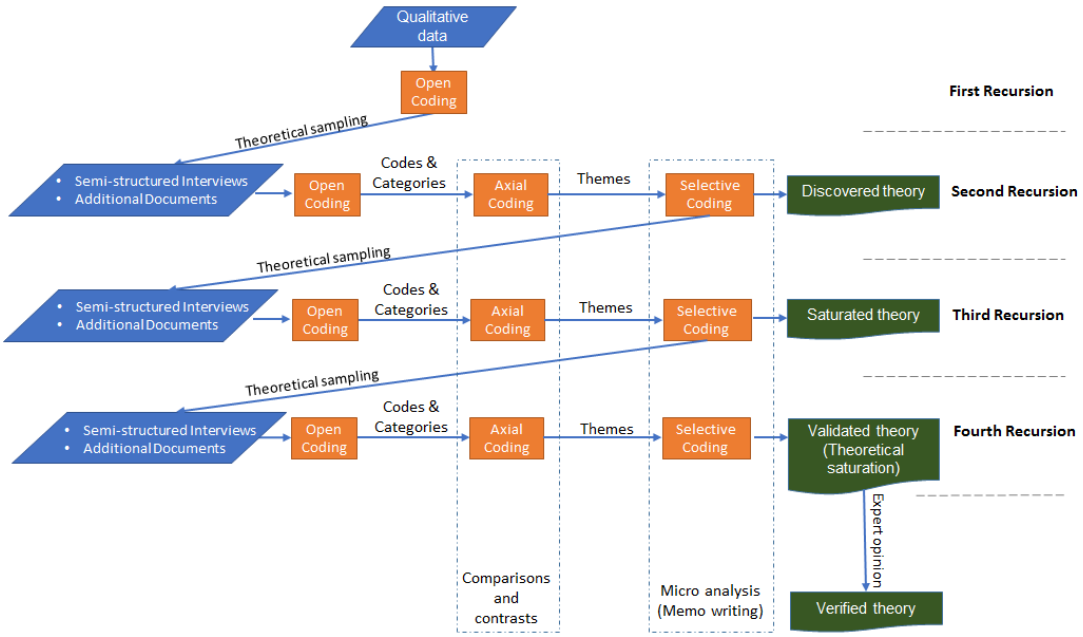


Figure 3-3: Details of the Grounded Theory Method

As shown in Figure 3-3, first open coding started with an initial set of data. The results of the first open coding process guided the second recursion in terms of both sector type, organization type and the document collections. The first set of codes, categories, and themes were created during the second recursion. A theory was discovered after the second recursion. Second recursion guided the third recursion by performing the theoretical sampling again. A saturated theory was obtained after the third recursion. The purpose of the fourth recursion was to validate the saturated theory by performing the last coding based on new interviews and documents. The validated themes were the root causes of the susceptibility of the critical infrastructures to cyber threats. After the last recursion, the root causes were verified by the participation of two experts. During the axial coding steps of all recursions, comparisons and contrasts among and within categories were performed to extract the meaningful themes. During the selective coding steps, the researcher performed micro analysis, meaning that the researcher prepared memos in order to find the repetitions and eliminate the redundant, irrelevant, and trivial themes.

The researcher exhibited the results of previous recursions to the participants of the semi-structured interviewees at the next recursion to acquire the reactions like acceptance, rejection, and comments (Thai et al. 2012). The results were substantially accepted by the interviewees with minor comments.

3.4 Delphi Survey

The second important output of the thesis was the development of the set of cyber security principles for critical infrastructures. The researcher had the opportunity of contacting with the experts to develop a set of principles for the cyber security of the critical infrastructures. The set of principles was determined by conducting a Delphi survey. Besides the set of principles, the weight values of the principles were determined by the Delphi survey. The arithmetic averages of the individual weight values were used in the maturity measurement.

The Delphi survey as a research method was quite compatible with the task of determining the set of cyber security principles and weight values. The objective of the Delphi survey is to obtain the consensus of the opinions of a group of experts (Dalkey & Helmer 1962). The

Delphi technique is a widely used and accepted method for gathering the opinions of the experts (Hsu & Sandford 2007).

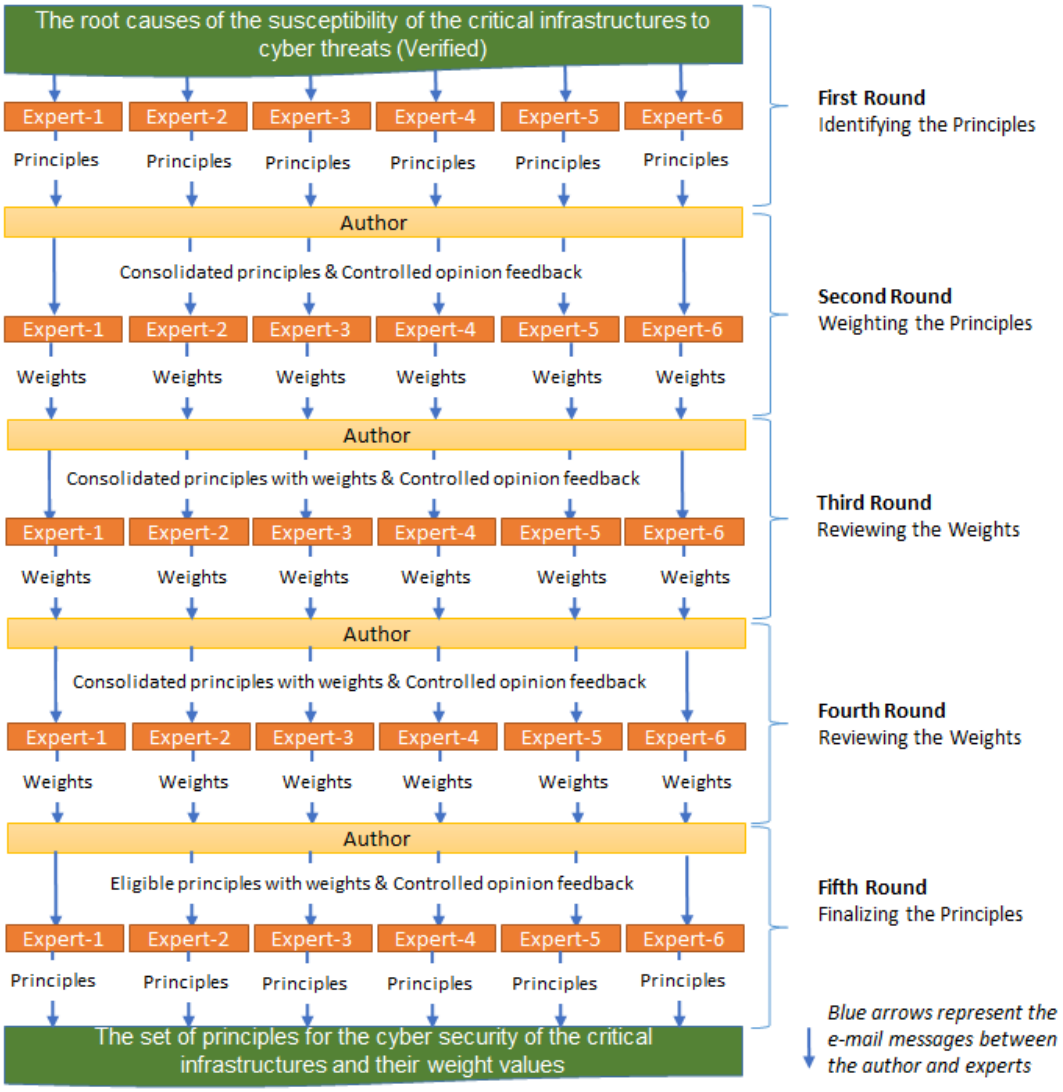


Figure 3-4: Detailed Flowchart of the Delphi Survey

The flowchart of the Delphi survey is given in Figure 3-4. The researcher provided experts the extracted root causes of the susceptibility to cyber threats. A five-round Delphi survey was conducted with controlled opinion feedback of the researcher between the rounds. The e-mails were sent to experts separately. So that the experts remained anonymous to express their opinions freely without any biases or refrainment (Chan et al. 2001). As the result of the Delphi survey, a convergence of the opinions of six experts was gathered. It seems notable that the set of principles were determined by six experts, not by the researcher. The role of the researcher in Delphi Survey was to consolidate the answers and send back to experts along with the controlled opinion feedbacks. The researcher provided the necessary instructions and warning between the rounds as feedback.

3.5 Creation of a Maturity Model and Pilot Application of the Model

For organizations, there are a number cyber security maturity assessment studies, which are developed by academia or government (Adler 2013; Lessing 2008; Miron & Muita 2014;

Eshlaghy & Pourebrahimi 2011; Karokola et al. 2011; Butkovic & Caralli 2013). However, there is a need for models that measure the state-level maturity.

After determining the set of principles and their weight values, a maturity model was proposed by using the linear additive evaluation model.

An unofficial pilot application of the maturity model was performed for Turkey by the participation of ten government or former government officials. The maturity model and application details were given in the next chapter.

3.6 Research Population

During the research, there were several points where sampling has to be performed. Table 3-7 shows the all points of the research at which the sampling was performed.

Table 3-7: Summary of the Sampling Process

Research Process	Target Population	Sampling Method
The semi-structured interviews (The first phase of the research)	All of the critical infrastructure operators	Convenience sampling & Theoretical sampling
The collection of the documents (The first phase of the research)	All of the critical infrastructure operators	Theoretical sampling & Convenience Sampling
The verification of the theory with expert opinion (The first phase of the research)	All of the experts that studies critical infrastructure security	Convenience Sampling
Delphi survey (The second phase of the research)	All of the experts that study critical infrastructure security	Convenience Sampling
The application of the maturity model for Turkey (the third phase of the research)	All of the related government official	Convenience Sampling

The target population of the first phase of the research was all of the critical infrastructure operators in all the critical sectors. There are more than 300 critical infrastructure operators in six different sectors in Turkey. It was infeasible to study the entire population due to the time and cost constraints. In order to ensure reliable observation and analysis, a wholly representative sample from the population was selected, by performing both theoretical and convenience sampling methods. As a consequence, the documents that belong to 91 different organizations were gathered. 71 of the organizations were critical infrastructure operators. The distribution of the organizations according to the areas of activity are shown in Table 3-8.

Table 3-8: Distribution of the Organizations According to the Areas of Activity

Organization type	Total Number
Critical infrastructure operators	71
Ministries and regulatory authorities	15
Research institutes and non-profit organizations	5
Total	91

The organizations for the semi-structured interviews were determined by using theoretical sampling. According to the results of the data analysis in a recursion, the organizations were

determined for the next recursion. The current situation and interim results of the data analysis guided the researcher to the selection of the organizations. The process of theoretical sampling may also be called as purposeful sampling, because the samples were selected purposefully by the researcher (Coyne et al. 1997).

The documents were collected by using both theoretical sampling and convenience sampling. The results of the previous recursion guided the researcher to gathering the documents for the current recursion.

The researcher collected conveniently accessible and proximate documents rather than barely reachable and obtainable ones. This is where the convenience sampling begins. Because the cyber security of the critical infrastructure is a confidential topic, not all of the organizations in target population were willing to document sharing. Therefore, the documents provided by the voluntary organizations were accepted. However, the researcher took the following factors into consideration for the convenience sampling.

a. The type of the document
b. The belonging organization type (governmental or private)
c. The belonging sector type

Therefore, the researcher gathered the documents to obtain a uniform distribution in terms of the above-mentioned factors.

The researcher studied with two experts for the verification of the theory. Six experts participated in the Delphi Survey. Ten government officials participated in the application of the maturity survey of Turkey. The experts were selected by convenience sampling. Because the researcher has fifteen years of experience in cyber security field and cyber security community is already a closed and small community, he is acquainted with the most of the experts and government officials in Turkey. Therefore, the researcher easily identified and reached the experts and officials for these three studies.

The selection of the experts for the verification was performed according to the criteria in Table 3-9.

Table 3-9: Sampling Details for the Verification of the Theory

Criteria	Value	Reason
The number of the years of experience in cyber security	At least five years of experience	At least five years of experience in cyber security is necessary to obtain the required insight for the assessment and verification of the extracted theory.
Job description	The participation of the national level cyber security efforts	Because the scope of the PhD study is national level cyber security, experts who participated in the national level cyber security are required to verify the root causes.

The selection of the experts for the Delphi survey was performed in accord with the criteria in Table 3-10.

Table 3-10: Sampling Details for the Delphi Survey

Criteria	Value	Reason
The number of the years of experience in cyber security	At least five years of experience	At least five years of experience in cyber security is necessary to determine the set of principles.

Criteria	Value	Reason
Job description	The knowledge of the domain of the critical infrastructures	The knowledge of the concept of critical infrastructures, and critical infrastructure protection is required to determine the set of principles.
Job divergence	At least one participant from government At least one participant from private sector At least one participant from academia	The job divergence of the participants enables the acquisition of the different point of views.

The selection of the government officials for the application of the maturity model was performed in line with the criteria in Table 3-11.

Table 3-11: Sampling Details for the Application of the Maturity Survey

Criteria	Value	Reason
The number of years of experience in cyber security	At least one year of experience	At least one year of experience in cyber security is necessary to assess the current situation of Turkey.
Job description	The knowledge of the domain of national cyber security	The existence of knowledge of national cyber security is required to assess the current situation of Turkey.

3.7 Role of the Researcher

The researcher has fifteen years of cyber security experience, which provides some advantages for this PhD study. First of all, it helped much in accessing the experts and officials in different parts of the PhD research. It also assisted in reaching documents. Secondly, it increased the theoretical sensitivity of the researcher. The researcher has the knowledge of the current literature on the critical infrastructure protection, and the latest efforts of the countries. That knowledge increased the theoretical sensitivity of the researcher. By this way, the researcher was sensitive about the criticality of the data in developing the theory at the first phase of the research: data analysis with GTM. The researcher had the insight in the selection of the organizations, interviewees, and collection of the documents. That insight accompanied the researcher throughout the four recursions of the first phase of the research. By theoretical sensitivity, the researcher had the ability to interpret the data, to understand the complex situations, and to omit the irrelevant pieces from the analysis. The researcher was already familiar with the research setting, which covers the organizations like critical infrastructure operators, ministries and regulatory authorities. Therefore, the researcher started his PhD research with some pre-knowledge about the phenomenon and the organizations in mind. This situation helped the researcher to perform the required delimitations. In this research, theoretical samplings between the recursions of the first phase were the points where delimitations were performed. During the Delphi survey, opinion feedbacks, which were also another means of delimitations, were given to the experts between the rounds.

On the other hand, the experience of the researcher may also be a disadvantage for the PhD study (Creswell 2012; Malterud 2001). The discovered theory at the end of the first phase of the research may be influenced by the researcher's experience. The experience and knowledge of the researcher, in other words, his theoretical sensitivity may be a bias factor for the first phase of the research. The constant comparisons during axial coding steps were important gadgets to eliminate any bias. Challenging the interim conclusions with the new data helped to eliminate the bias (Strauss & Corbin 2008). The verification phase at the end of the first phase of the PhD study was another important gadget to check the existence of any bias. Two experts checked the extracted theory in detail and made some corrections. The Delphi Survey was performed by six experts, with minor contributions of the researcher. Therefore, the disadvantages that might originate from the experience of the researcher were debilitated by incorporating the experts into the PhD research.

3.8 Trustworthiness of the Research

Several validity and reliability measures were applied to secure the trustworthiness and the robustness of the research and findings.

A data analysis, which is performed by GTM, can be evaluated according to four aspects (Strauss & Corbin 2008). These aspects are:

a) The reliability, validity, and credibility of the data,
b) The credibility of the theory,
c) The reliability, validity, and credibility of the data analysis process,
d) Back-traceability from the theory to the data.

At the first phase of the research, the triangulation of the data by using different sources of the data was performed. Therefore, the possible weaknesses of a single data source were eliminated. Secondly, the researcher exhibited the interim results to the participants of the semi-structured interviews to receive the reactions like acceptance, rejection, and comments (Thai et al. 2012). The researcher shared each transcript with the participants to check for the accuracy as well. These were the means of the construct validity of the research.

The researcher collected data and made interviews until theoretical saturation. This type of actions increased the reliability and repeatability of the study.

Research steps are auditable by the documentation of coding steps. These audit trails ensure the credibility of the theory (Sandelowski & Barroso 2002).

The first step of the data analysis was the selection of the sample population. The researcher showed the details of the selecting sample in the PhD thesis. The researcher also wrote memos which show the impressions of the researcher. Constant comparison and theoretical sampling processes continuously evolved the theory. All of these steps can be observed in the thesis document.

At the end of the first phase of the research, the extracted theory was verified by two experts. The experts checked the theory and accepted it with minor changes that did not change the meaning of the theory. At the second phase of the research, the Delphi survey was performed by the participation of six cyber security experts, who have twelve years of experience on average. Some of them have PhD degrees. These peer examination processes also increased the internal reliability of the PhD research.

3.9 Research Ethics

Interviewees of the semi-structures interviews were aware of their rights, such as rejecting the participation and giving up at any time. Interviewees also knew their rights to control the data that were produced as the result of interviews. The control of data included the deletion of the data as well. They also knew their rights to review the results of the interviews, to ensure that their statements had been accurately represented.

The data were anonymized during data analysis by using coding steps. Therefore, none of the interviewees could be identified through their responses.

The PhD topic intersects with the national security. The research data and the codes contain a mass amount of vulnerabilities associated with critical infrastructures. Because of the confidentiality constraints, no organization name was exposed in the thesis. Any vulnerability information that might be used to trace back to the specific organizations was anonymized during the preparation process of the thesis. Therefore, any explicit or implicit relationships between the vulnerabilities and the organizations were removed.

The most of the data (all of the confidential documents) were gathered by using the authorization obtained by the state sponsored project. The written and signed consent of the project manager was obtained at the beginning of the research.

The research data were kept safe during the research. Nobody had access to it apart from the researcher. At the end of the PhD research, the data were permanently deleted.

CHAPTER 4

4 FINDINGS

Forth chapter contains step-by-step application details and findings of the three-phased research.

4.1 First Phase of the Research: Grounded Theory Method

As stated at the third chapter, qualitative data analysis with GTM was a recursive process with four recursions. The research process of the GTM was shown in Figure 3-3 in the previous chapter. The qualitative data analysis was repeated four times until the theoretical saturation. After each recursion, the theoretical sampling was performed for the next recursion based on the interim results of the previous one.

At the first recursion, only open coding step was performed. At next three recursions, open coding, axial coding and selective coding steps were performed. At the second recursion, extracted codes started to cluster around categories. Relationships emerged after constant comparisons among categories, and these relationships yielded themes, which were fundamental constructs of the theory. At two subsequent recursions, the categories and themes are saturated and validated with minor changes.

Table 4-1 contains the summary of the recursions in the first phase of the research.

Table 4-1: Details of the Four Recursions of the Data Analysis

	First Recursion	**Second Recursion**	**Third Recursion**	**Fourth Recursion**
Analyzed documents	Publicly available documents (regulation texts, news & media reports, organizational reports)	Internal documents (independent evaluation reports, minutes of meetings) Publicly available documents (regulation texts, organizational reports)	Internal documents (independent evaluation reports, minutes of meetings) Publicly available documents (regulation texts, organizational reports)	Internal documents (independent evaluation reports, minutes of meetings) Publicly available documents (regulation texts, organizational reports)
The number of analyzed documents	109	76	86	38
The sector of the interviewed organization*	-	Energy (G) Water management (G) Finance (P)	Government services (G) Transportation (G) Telecommunications (G, P)	Energy (P) Finance (G)

	First Recursion	Second Recursion	Third Recursion	Fourth Recursion
Interview questions	-	Initial set of open-ended interview questions	Reshaped and detailed interview questions	Same questions as the previous recursion
Coding steps	Open coding	Open coding Axial coding Selective coding	Open coding Axial coding Selective coding	Open coding Axial coding Selective coding
Evolution of the Theory	No theory discovered	Discovery of a theory (unsaturated)	Saturation of the theory	Validation of the theory

* G: Governmental organization, P: Private organization

4.1.1 First Recursion: Scanning

At the first recursion, data analysis was performed by using publicly available documents, which were regulation texts, news - media reports, and organizational reports. The goal of the first recursion was to understand the environment in which critical infrastructures operate, and to minimize the possible biases of researchers for the next recursion (Thai et al. 2012). In the first recursion, only open coding was performed. All of the collected data from all sectors were read and prominent pieces of the data were labelled so that the codes would be extracted. The content of the data was limited. So, extracted codes were not enough to create categories and to perform axial coding. However, the first recursion provided important information on the general security postures of the critical sectors. When the documents were analyzed during the first recursion, energy and water management sectors drew the attention of the researcher as the critical infrastructure operators of these sectors had minimum amount of cyber security or information security paragraphs in their organizational reports and regulations. In addition, there were some remarkable pieces of news associated with the problems of these sectors as well.

Table 4-2 shows the distribution of the coded documents according to the type of the documents. The researcher coded 109 documents at the first recursion.

Although the documents were high in number, the number of codes extracted from these document was relatively low. It was because most of these documents were not cybersecurity-oriented. For example, in some of the documents, less than five codes were extracted.

Table 4-2: Distribution of the Analyzed Documents at the First Recursion

Document type	Number of documents
News and media report	74
Regulation text	21
Organizational report	14
Total	**109**

After the open coding process at the first recursion, it was decided that the energy and water management sectors were to be the focus because of the low number of security related codes in regulations and organizational reports and high number of security incident related codes in the news and media reports. The semi-structured interviews were arranged with the

operators within these sectors. An operator from finance sectors was also arranged to make comparisons with a sector that seems more secure than these sectors according to the codes.

4.1.2 Second Recursion: Discovery

All three coding steps of the data analysis were performed in the second recursion. Therefore, the researcher discovered a theory at the end of the second recursion. However, the discovered theory was probably unsaturated because there were still critical sectors for which no interviews were performed.

4.1.2.1 Data: Documents and Interviews

In the second recursion, the number of coded documents is seventy-six. The distribution of the documents according to the sectors and document types are shown in Table 4-3 and Table 4-4 respectively.

A set of publicly available documents and restricted documents were analyzed and coded. The restricted documents were independent evaluation reports and minutes of meetings. They contained a number of valuable information on the vulnerabilities, cyber threats, the practices of organization, and the reflections of current legislative frameworks. These documents were richer than the regulation texts, news and the organizational reports, which were publicly available.

Table 4-3: Distribution of the Documents According to the Sector Type

Critical sector	The number of documents associated with the critical sector
Energy	43
Water management	15
Finance	18
Total	**76**

Table 4-4: Distribution of the Documents According to the Document Type

Document type	Number of documents
Regulation text	7
Organizational report	16
Minutes of meeting	21
Independent evaluation report	32
Total	76

There were two types of independent evaluation reports, which were penetration test and information security management evaluation reports. Penetration test reports were technical, whereas other reports were not. Penetration test reports contained technical and technological aspects while the content of information security management evaluation reports along with minutes of meetings were nontechnical. They contained vulnerabilities and threats that were associated with organizational processes. Information systems have three perspectives, which are technology, management and organization (Laudon & Laudon 2015). The researcher covered all three aspects of information system by analyzing these reports during the coding processes.

At the second recursion, the organizations for semi-structured interviews were determined. The selection was performed by using theoretical sampling, which was based on the results of the first recursion. Because energy and water management sectors seemed problematic in terms of cyber security, the researcher decided to make semi-structured interviews with two

governmental critical infrastructure operators from these sectors at the second recursion. Apart from the two sectors, a private organization from finance sector was selected for the interview. When the codes of the first recursion are reviewed, the finance sector is considered much more resilient against cyber threats than energy and water management sectors. The purpose of including a financial organization in the interviews was to make comparisons and contrasts during the axial coding phase, namely to check whether the discovered problems exist in the finance sector.

Table 4-5 summarizes the properties of the semi-structured interviews. The energy and water management operators were governmental organizations; whereas the finance organization was private sector. The water management sector is totally operated by the governmental organizations. In energy sector, there are prominent private sector operators. However, at the first round of data analysis, it was seen that their cyber security posture is much less problematic compared to the governmental operators. Therefore, governmental operators were chosen for the energy sector.

Table 4-5: Properties of the Interviewees of the Second Recursion

Interviewee	Sector	Type
Interviewee - 1	Energy	Governmental organization
Interviewee - 2	Water management	Governmental organization
Interviewee - 3	Finance	Private organization

4.1.2.2 Open Coding

The second recursion started with the open coding of the documents listed in Table 4-4. As open coding progressed, the extracted codes started to cluster around categories in this recursion

The list of emerged categories at the end of open coding of second recursion is shown in Table 4-6.

Table 4-6: List of the Categories before the Interviews in the Second Recursion

No	Categories
1	Vulnerabilities
2	Countermeasures
3	Outsourcing
4	Audit
5	Security culture
6	Personnel
7	Security standards
8	Collaboration
9	Regulation
10	Regulatory authority
11	Leadership
12	Interdependence
13	National software
14	National governance

During the open coding of these documents, two categories, Vulnerabilities and Countermeasures, emerged quickly along with the other codes and categories. These two categories, sub-categories and associated codes for each sub-categories are shown in Table 4-7.

Table 4-7: Codes of the Vulnerabilities and Countermeasures Categories

Category	Subcategory	Selected Codes
Vulnerabilities	Nontechnical vulnerabilities	Password sharing Shared accounts Accounts with no password Limited technical training Limited awareness training Single point of failure Damaged backup facilities Equipment shortage Remote access of vendors Uncertainty Unconsolidated huge systems Very old systems Management problems in sectorial level Disorderliness
	Technical vulnerabilities	No Backup DDoS Limited log capability Limited capacity for logs
Countermeasures	Nontechnical countermeasures	Limited USB storage usage Security roadmap Prioritization of countermeasures Awareness trainings
	Technical countermeasures	Access control Firewalls Intrusion Detection and Prevention Systems Antivirus Patch management Secure configuration Cryptographic solutions Physical security Facility backup Data backup Identity management Data loss prevention Passwords Hardening Monitoring systems Biometric systems Log management Technical trainings Database security

As it is seen from Table 4-7, both categories have two subcategories: technical and nontechnical. For the Vulnerabilities category, there was an excess of non-technical vulnerabilities over technical vulnerabilities. For Countermeasures category, there was an excess of technical countermeasures over nontechnical ones. Although a number of countermeasures were extracted from the various kind of documents, they might not be considered as the signs of security. If there are limited or problematic organizational security

practices, these countermeasures might not be used effectively. They even might be the sources of the new vulnerabilities because of the improper usage. The problems at tactical level might be the result of limited or absent rules at the policy level (von Solms & (Basie) von Solms 2006). Therefore, by taking these two categories into consideration, the researcher shifted his attention towards the higher level problems instead of technical level problems for the semi-structured interviews.

Before starting the semi-structured interviews with the organizations, the prepared survey questions at the beginning of the research were reviewed and changed according to the results of the comparisons of the Vulnerabilities and Countermeasures categories, and the focus of the questions were changed to reflect the organizational, policy and even national level aspects more.

The questions of the semi-structures surveys are listed below. All of the questions were open-ended. They did not have multiple-choice answers. The respondents were allowed to answer the questions freely without much disturbance. The requested information was qualitative rather than quantitative.

Question list:

1. What are prominent cyber security problems? What is your idea on the reasons of these problems?
2. Do you think that the technical countermeasures are effective? If not, why?
3. What do you think about cyber threats? Do you think that you may face but not realize? Why?
4. What do you think about the security standards? Are they useful or just a burden for the organizations?
5. Do you outsource your IT and security services? Why? How?
6. Do you perform IT audit? Is it regular? What do you think about audit process? Is it useful?
7. Do you have a relationship with a regulatory authority? Could you please explain the details?
8. Are you dependent on other critical sectors and associated organizations? Is there any other critical infrastructure that depends on you?
9. Let's talk about security culture. Do you have a security culture as the organization? What kind of security behaviors do your personnel, managers and IT staff have?
10. Do you cooperate with other organizations, people, government agencies, and training institutions?
11. Do you need any regulations for cyber security? Do you believe in the effectiveness of regulations?
12. What is the source of the software you use? (Foreign country, Turkish) Does it matter for you? Does a software developed by a Turkish company make any difference?
13. What about the quality and number of IT and security personnel?
14. Do you need any leadership in cyber security?
15. What do you think about the role of the governments and national security officials in the security of the critical infrastructures? Should they be involved or isolated?

Because of the characteristics of the semi-structured survey, these questions were regarded as the initiators and catalyzers of the long lasting and evolving interviews.

Each interview lasted around two hours. The interviews were conducted face to face. The interviewees were mid-managers who work in information processing departments. They

had responsibilities for cyber security and were acting as bridges between the technical personnel and the higher level managers.

Sound recording was not permitted during interviews. Nevertheless, the researcher was allowed to take notes. The transcripts were the most valuable source of information for the research.

After finishing all of the semi-structured interviews, open coding was conducted more thoroughly. It is noteworthy to state that, Vulnerabilities and Countermeasures categories emerged at first during the open coding; however, they were mostly merged into other categories as coding process continued after interviews. The codes belonging to these categories were distributed among the other categories such as leadership problems, outsourcing problems, collaboration problems and regulation problems. The situation was the same for the countermeasures category. Therefore, Vulnerabilities and Countermeasures categories, which came into sight at the open coding, were used to update the questions of semi-structured interviews and they finally merged with other categories.

Some of the codes are shared to show and explain the research process and the findings. A list for the extracted codes is not given in the thesis because of the space and confidentiality constraints.

The final list of categories at the end of the open coding is listed in Table 4-8.

Table 4-8: List of the Categories after the Open Coding in the Second Recursion

No	Categories
1	Outsourcing
2	Audit
3	Security culture
4	Personnel
5	Security standards
6	Collaboration
7	Regulation
8	Regulatory authority
9	Leadership
10	Interdependence
11	National software
12	National governance

The sample transcripts of three interviewees are written for each category below. All transcripts are accompanied with the extracted sample codes. It is noteworthy to state that the selected transcripts are peculiarly selected from interview texts as they contain valuable input for comparisons. These transcripts are enough to show how the comparisons are made in axial coding.

For the Outsourcing category:

Interviewee-1:

English (Translated): *"We of course outsource the critical IT services. We pay the firm for that and receive/expect for the services. The work must be permanent, that's the point. That's why we don't want to intervene with the outsourced services. As long as all is fine, you shouldn't question the practices. There is no need to ruin the ongoing mechanism."*

Turkish (Original): *"Kritik BT hizmetlerini tabi ki dışardan alıyoruz. Biz firmaya parasını veririz. Sonra da hizmet bekleriz. Bizim için önemli olan işlerin sürmesidir. Bu nedenle firmaya da fazla karışmak istemeyiz. İşler düzgün olduktan sonra sen ne yaptın diye fazla sorulmaz. Çalışan düzeni bozmaya gerek yok."*

Extracted codes: Outsourcing of IT services, outsourcing behavior, the importance of business continuity

Interviewee-2:

English (Translated): *"We outsource IT services from the firms we already know and trust. It is quite hard when you have to work with an unfamiliar firm. I wish we also had rules and principles for the outsourcing of the IT services."*

Turkish (Original): *"Dışarıdan BT hizmet alırız. Güvendiğimiz, bildiğimiz firmalardan almaya çalışırız. Bilmediğimiz firma ile uğraşmak zor. Keşke bize dışarıdan hizmet alımı konusunda kurallar belirli olsa."*

Extracted codes: Outsourcing of IT services, no outsourcing rules

Interviewee-3:

English (Translated): *"We do outsourcing. But, we also have procedures of strict audits. In other words, we already have outsourcing rules and established penal sanctions for the firms."*

Turkish (Original): *"Dışardan hizmet alımı yapıyoruz. Bu konu bizde çok sıkıdır. Zaten bu konu ile ilgili kurallar da belirlenmiştir. Firmaların ne yapıp ne yapamayacağı ve cezai yaptırımlar bellidir."*

Extracted codes: Outsourcing of IT services, outsourcing rules, sanctions to third parties

Note: For the governmental organizations, there are some problems with outsourcing practices. They do not have the rules obliged on them (Regulation, Regulatory authority). Also they trust the third party firms without grounds (Security culture). It is important to try to find the reasons for these differences between governmental and private organizations. The possible reasons are sought in the axial coding.

Categories to be compared with: Security culture, Regulation

For the Audit category:

Interviewee-1:

English (Translated): *"There is a partial IT audit, which, I think, is not sufficient. First of all, standards must be set, or to put it another way, the problem of which standards to apply should be resolved. We have a lot work to do, but we cannot start anyhow."*

Turkish (Original): *"BT denetimi kısmen var. Ama yeterli olduğunu düşünmüyorum. Bu konuda öncelikle standartların oluşması lazım veya hangi standartların kullanılacağının belirlenmesi lazım. Yapacak işimiz çok; ama başlayamıyoruz."*

Extracted codes: Insufficient IT audit, IT audit standards, IT audit is not a priority

Interviewee-2:

English (Translated): *"There is no IT audit. But we do maintain our work properly as we work with competent firms."*

.

Turkish (Original): *"BT denetim süreci yok. Ama işlerimizi düzgün yapıyoruz. Çalıştığımız firmalar yetkin firmalar."*

Extracted codes: No IT audit, no awareness on IT audit

Interviewee-3:

English (Translated): *"Obliged by the regulations, an audit is a process of established standards. Regular and official IT audits are conducted. A considerable part of those audits are performed and reported by competent audit firms."*

Turkish (Original): *"Denetim yönetmelikler çerçevesinde zorunlu tutulan ve standartlarının oluşturulduğu bir süreçtir. Düzenli ve resmi BT denetimleri yapılır. Bu denetimlerin önemli bir kısmı yetkili denetçi firmalar tarafından yapılır ve raporlanır."*

Extracted codes: IT audit regulation, IT audit standards, regular and formal IT audit, external

Note: Like the outsourcing category, there is a considerable difference between governmental and private organizations in terms of both the practices and the perception of the audit. There is limited security awareness in governmental organizations. Regulation and regulatory authorities may cause considerable differences in audit process. In the axial coding phase, required comparisons will be performed to examine this phenomenon.

Categories to be compared with: Security culture, Regulation

For the Security culture category:

Interviewee-1:

English (Translated): *"We have to develop a security culture, and in that sense, we have a long way to go."*

Turkish (Original): *"Güvenlik kültürünü oluşturmamız lazım. Bu konuda alınacak çok mesafemiz var."*

Extracted codes: The lack of security culture

Interviewee-2:

English (Translated): *"The users may share their passwords. Some users don't even have their own ones. Password sharing is common even in the IT department."*

	Turkish (Original): *"Kullanıcılar şifrelerini paylaşır. Hatta bazı kullanıcılarda şifre bile yok. Bilgi işlemde bile şifre paylaşımı var."* Extracted codes: Password sharing, no passwords
Interviewee-3:	
	English (Translated): *"Security is considered a significant process it is a part of the business we manage. We cannot overlook that fact. The business is dependent on the financial data and monetary issues anyhow."* Turkish (Original): *"Güvenlik önemli bir süreç olarak görülüyor. Yapılan işin bir parçası da güvenlik. Güvenliği göz ardı edemeyiz. İş sonuçta finansal bilgilere ve paraya dayanıyor."* Extracted codes: Security is the part of business, business value of security
The security awareness level is quite low in the governmental operators. Business-oriented security culture is observed for the financial institutions. The concept of security culture is directly related with the profile of the personnel. Also, the contribution of the regulation and regulatory authorities to the security culture is checked. Categories to be compared with: Regulation, Personnel	

For the Personnel category: Interviewee-1:	
	English (Translated): *"We have a sufficient number of personnel. But, it is hard to say that they are efficient and productive. The personnel who are good at any type of work are very few while the unqualified employees are far higher in number."* Turkish (Original): *"Personel sayımız yeterli olsa da verimli bir personel altyapımız yok. Her işe koşturan az sayıda personel var, bir de kalitesiz çok sayıda personel var."* Extracted codes: Unqualified personnel, efficient usage of personnel
Interviewee-2:	
	English (Translated): *"We cannot employ qualified people, and even if we do, they are sure not to accept to be recruited for that amount of salary. We cannot pay higher salaries for the qualified personnel as we operate on certain rules and regulations as a governmental organization."* Turkish (Original): *"Kaliteli personel bulamıyoruz, bulsak da vereceğimiz maaşa gelmezler. Kaliteli personele yüksek maaş veremiyoruz. Sonuçta kamu kurumu olarak belli kanunlara göre iş yapıyoruz."* Extracted codes: Low salaries, governmental organization, unqualified personnel
Interviewee-3:	

English (Translated): *"We have a sufficient infrastructure of personnel and but at some points, we need more employees. Qualified personnel is always on demand. Finding qualified employees is a country-wide problem as they are very few."*

Turkish (Original): *"Personel altyapımız yeterli ama bazı noktalarda da personele ihtiyacımız oluyor. Kaliteli personel her zaman ihtiyaç. Ülkemizde genel olarak kaliteli personel sıkıntısı var. Yetişmiş eleman çok az."*

Extracted codes: Qualified personnel is required, the need for qualified personnel

All of the organizations need qualified personnel. However, governmental organizations have problems with the recruitment of the qualified personnel because of the regulations. Also the possible problem of the lack of qualified personnel

Categories to be compared with: Regulation, National governance

For the Security standards category:

Interviewee-1:

English (Translated): *"There is no institutional risk management, either. We don't operate in compliance with a security standard as we are not lawfully bound by one. We once considered adopting ISO 27001, but later we thought it would be hard to convince the top management for the application of the standard and to implement it and so, it had to remain as a plan. We, the IT department, seem responsible for the security. Yes, we are in fact, but we don't have any authorities over it."*

Turkish (Original): *"Kurumsal bir risk yönetimi de yapılmıyor. Herhangi bir güvenlik standardına göre çalışmıyoruz. Kanuni olarak uymak zorunda olduğumuz bir standart da yok zaten. Bir ara ISO 27001 alalım mı diye düşündük; sonrasında başlatmak yönetimi ikna etmek zor geldi. Düşünce planında kaldı. Güvenliğin sorumlusu biz (bilgi işlem) olarak görülüyor. Sorumluyuz ama yetkimiz yok."*

Extracted codes: No risk management, Standards are not obliged by law, adoption of international standard, convincing top management for the adoption of standards, the lack of due care of management

Interviewee-2:

English (Translated): *"The security standards exist and we are aware of how critical they are, but have no practices. We cannot initiate the process for ISO 27001. We are not sure whether we can persuade the management, either. The standard must be obliged by a higher authority. Only by this way we can convince the managers, to whom we cannot explain the importance of IT investments. The management must be responsible and decide for security-based issues but such a practice is nonexistent within our organization."*

Turkish (Original): *"Güvenlik standartları var. Öneminin farkındayız ama uygulamamız yok. ISO 27001 konusunda ilk adımı atamıyoruz. Yönetimi ikna*

edebileceğimiz noktasında emin değiliz. Bir üst kurumun bunu şart koşması gerekir. Yöneticileri ancak bu şekilde ikna edebiliriz. Biz yöneticilere IT yatırımını anlatamıyoruz. Güvenlik konusunda yönetimin sorumlusu olması ve karar alması gerekir ama maalesef bize böyle bir pratik yok."

Extracted codes: convincing top management for the adoption of standards, the lack of awareness of top level management, obligation of standards by regulatory authority, the lack of due care of management

Interviewee-3:

English (Translated): *"There are both COBIT based audit standards and some security standards designated by the regulations and reports. You have to establish you own institutional standard by combining the utilizable parts of COBIT, ITIL and 27001."*

Turkish (Original): *"COBIT bazlı oluşturulmuş denetim standartları var. Ayrıca yönetmelik ve tebliğlerde belirlenmiş bazı güvenlik standartları var. COBIT'i, ITIL'ı, 27001'i alıp işinize yarayacak bölümlerini bir araya getirip kurumsal standardınızı oluşturmanız gerekir."*

Extracted codes: customized standard, obligation of standards by law

Security standards are customized, adopted and obliged in the finance sector. The situation is completely negative for other sectors. Security standards category intersects with the ones of regulatory authority, regulations and security culture.

Categories to be compared with: Regulation, Security culture

For the Collaboration category:

Interviewee-1:

English (Translated): *"We generally act on our own and do not have external connections. We occasionally attend the IT and security occasions. We try to solve the security problems by ourselves, we search in the forums for the solutions, for instance. We do not cooperate with the private sector, either, apart from the times when they undertake a post as part of the projects."*

Turkish (Original): *"Genelde kendi halimizdeyiz. Dışarıyla pek bağlantımız yoktur. Arada bir BT ve güvenlik etkinlikleri olduğu zaman katılırız. Bir güvenlik problemi olduğu zaman kendi başımıza çözmeye çalışırız. İnternet'ten falan forumlara bakarız. Özel sektör ile işbirliğimiz de yok; projeler kapsamındaki iş yaptırma ilişkisi dışında."*

Extracted codes: Isolated organization, no cooperation, no partnership with private sector

Interviewee-2:

English (Translated): *"We are not in touch with the other organizations. We learn everything by ourselves. Thus, common platforms for information sharing would be highly beneficial. And we do not cooperate with the private sector in areas like R&D etc."*

Turkish (Original): *"Diğer kurumlarla temasımız yok. Kendimiz öğreniyoruz. Ortak bilgi paylaşım platformları falan çok iyi olur. Özel sektör ile ar-ge vs. kapsamında bir birlikteliğimiz yok."*

Extracted codes: No cooperation, no information sharing, no partnership with private sector

Interviewee-3:

English (Translated): *"There is no settled culture of cooperation and collaboration in the sector. When a problem with the security arises, we try to resolve it by ourselves. Maybe there are some other organizations who have experienced the same problems before, so if there were a pool of information, we would benefit from that to solve out the deficiencies. In the sector, there is a top-down structure of directives. So, the obligations by the regulatory authority are conducted. We work with the private sector in projects, but we have no cooperation."*

Turkish (Original): *"Sektörde pek işbirliği, ortak bir şeyler yapma kültürü yok. Bir güvenlik olayı meydana gelince kendi başımıza çözmeye çalışırız; belki daha önce başına gelip çözen kurumlar vardır, bir bilgi havuzu olsa faydalanırız. Sektörde tepeden aşağıya doğru bir direktif yapısı var. Düzenleyici kurumun getirmiş olduğu zorunluluklar yerine getirilir. Özel sektör ile beraber sık sık proje yapıyoruz. Ama proje, bir işbirliğimiz yok."*

Extracted codes: No cooperation culture in sector, regulatory authority does not promote cooperation, no partnership with private sector

The lack of collaboration and cooperation is a common problem for all three sectors. The reasons for this situation are attempted to be extracted. After the recursions, it was seen that this was a root problem itself.

Categories to be compared with: Regulation, Security culture

For the Regulation category:

Interviewee-1:

English (Translated): *"Regulations are important, but in the sector we do not have any legal regulations for the cyber security issues. There must be, in fact. The basic and minimum standards must also be obliged by the law."*

Turkish (Original): *"Kanuni düzenlemeler önemli, ancak bizim sektörde siber güvenlik konusunda yasal düzenleme yok. Olması lazım. Kanunlarla belli başlı temel asgari standartların da belirlenmesi lazım."*

Extracted codes: the lack of regulations, the obligation of minimum standards

Interviewee-2:

English (Translated): *"The parts pertaining to information security and cyber security are left blank in the legislation. It is impossible to talk about cyber security in a legal context when even information security issues are not included in the legislation."*

Turkish (Original): *"Mevzuatta bilgi güvenliği veya siber güvenlik boş bırakılmış. Zaten siber güvenlik çok yeni bir kavram bilgi güvenliği bile yer almıyorken siber güvenlikten kanunlar seviyesinde hiç bahsedemeyiz."*

Extracted codes: the lack of regulations

Interviewee-3:

English (Translated): *"There are highly detailed sectorial regulations for the security issues. Everything including the report format is detailed in the sectorial legislations. Legal legislations prove significant in the proper maintenance of the sector."*

Turkish (Original): *"Güvenlik konusunda sektörel kanuni düzenlemeler var, oldukça detaylı. Rapor formatına kadar sektörel mevzuatta belli. Yasal mevzuat sektörün düzgün işlemesi için önemli."*

Extracted codes: the detailed set of regulations, sectorial regulations

There is a considerable gap between the legislative infrastructure of finance sector and the other sectors. The possible adverse effects of this situation and also its effects on the security practices within the sectors will be analyzed.

Categories to be compared with: Regulatory authority, Security standards

For the Regulatory authority category:

Interviewee-1:

English (Translated): *"An auditing and regulatory institution renders critical in that it lays down the rules and supervises their implementation. In the sector, we have an auditing institution, which supervises over the market, but not the cyber security. The institution doesn't have a proper and clear regulation for that."*

Turkish (Original): *"Denetleyici ve düzenleyici kurum kuralların tepeden konulup takip edilmesi noktasında önemli. Bizim sektörde denetleyici kurum var. Ama piyasa unsurlarını denetler, siber güvenlik konusunda etkin değil. Net bir regülasyonu yok."*

Extracted codes: the lack of cyber security supervision

Interviewee-2:

English (Translated): *"The water sector does not resemble to the other ones like energy, finance or telecommunications. Of course, water management is very important, the service is distributed among all the citizens, but the sector doesn't have a firm market approach. Thus, in the sector, there has been no regulatory authority that is similar to those of the other mentioned sectors. In the absence of a regulatory authority, every organ acts independently, which is not favorable."*

Turkish (Original): *"Su sektörü gibi bir sektör ülkemizde yok. Enerji, finans, Telekom gibi değil. Tamam, su yönetimi önemli; tüm vatandaşlara hizmet veriliyor ama bir piyasa yaklaşımı yok. Bu nedenle düzenleyici kurum da diğer*

saydığım sektörler manasında yok. Düzenleyici kurum olmayınca herkes bağımsız, bu aslında pek de iyi bir durum değil."

Extracted codes: no regulatory authority

Interviewee-3:

English (Translated): *"The regulatory authority has adopted a crucial position for security. It both determines the rules and audits their conduction process. It sets the rules with its experts in a balanced and experienced manner. And sectorial standards are formed in this way."*

Turkish (Original): *"Düzenleyici kurum güvenlik konusunda çok önemli bir pozisyonda. Hem kuralları koyar, hem uygulanıp uygulanmadığını denetler. Ayrıca kuralları da oldukça dengeli koyar. Bu konuda uzmanları vardır. Sektörel standartlar belirlenmiş olur."*

Extracted codes: the sectorial rules, the audit according to the rules, the sectorial standards

The current situation with the regulatory authority is completely parallel to the situation of regulations. It is expected that there are strong relationships between the existence of regulatory authority and audit standardization.

Categories to be compared with: Leadership, National governance

For the Leadership category:

Interviewee-1:

English (Translated): *"Of course we need leadership in security. In face of a security problem, we are all alone. We don't have anyone to consult. It is the regulatory authority which is to undertake the leadership position."*

Turkish (Original): *"Güvenlik konusunda liderliğe elbette ihtiyacımız var. Bir güvenlik problemi olunca tek başınayız. Soracağımız kimse yok. Liderliği yapacak kurum düzenleyici kurumdur."*

Extracted codes: the leadership of regulatory authority

Interviewee-2:

English (Translated): *"Leadership matters a lot. For the security issues, there must be a body of authority which shows the way to proceed in. It is the responsibility of the government to seriously deal with the security issue and establish the institutional structures. And the leadership must belong to the top."*

Turkish (Original): *"Liderlik önemli bir konu. Birilerinin güvenlikte nasıl ilerleneceğini göstermesi gerekir. Devletin bu güvenlik işine ciddi şekilde eğilip kurumsal yapıları oluşturması gerekir. Liderlik ise en tepeden başlamalı."*

Extracted codes: the leadership of state-level actors on cyber security

Interviewee-3:

English (Translated): *"I think, the regulatory authority in the sector has assumed the leadership as well. But, more space must be allocated within the sector for more cooperative opportunities and the regulatory authority may then act as the pioneer, as something beyond legislation setting and auditing."*

Turkish (Original): *"Sektördeki düzenleyici kurum gerekli liderliği bence yapıyor. Ama sektörde biraz daha işbirliği fırsatları yaratmalı, etkinliklerde belki öncülük yapabilir. Kural belirle ve denetlemenin ötesinde bir şey."*

Extracted codes: the leadership of regulatory authority, enabler of cooperation

There is a relationship between leadership and regulatory authorities. For the sectors that have regulatory authorities; interviewees set this relationship. The interviewee from the water management sector talks about the higher level leadership as "state-level leadership".

Categories to be compared with: Regulatory authority

For the Interdependence category:

Interviewee-1:

English (Translated): *"Many sectors are dependent on the energy sector. Energy is the source of everything. Until now, there has been no serious energy cut based problems that have also affected other infrastructures. Even if there may happen wide-scale cuts, it wouldn't matter much as long they do not last long as all large institutions have their own energy production infrastructures. This is another subject for further analyses, of course in the leadership of the high level state institutions."*

Turkish (Original): *"Pek çok sektör enerji sektörüne bağımlıdır. Enerji can suyudur. Şu ana kadar kesintilerden dolayı diğer altyapıları da etkileyen ciddi bir sıkıntı yaşanmadı. Gerçi geniş çaplı kesintilerde bile çok uzun süreli olmadığı müddetçe sıkıntı yaşanmayabilir. Çünkü örneğin büyük kurumların kendi enerji üretim altyapıları var. Bu konuda üzerinde analizler yapılması gereken bir konu. Tabi üst düzey devlet yapılarının önderliğinde."*

Extracted codes: Redundancy of the energy supply, the state leadership to make analysis

Interviewee-2:

English (Translated): *"No institution is dependent on us. We do not depend on another one either. It doesn't affect us anyway even when the electricity is cut off as we have generators as part of our infrastructure."*

Turkish (Original): *"Bize bağlı yer yoktur. Biz de bağlı değiliz. Elektrik gitse de etkilenmeyiz. Altyapımızda jeneratörler var."*

Extracted codes: Interdependency is not a concern

Interviewee-3:

English (Translated): *"When we cannot provide services, only the service takers will be adversely affected, not the other infrastructures. Our systems are*

directly connected to the energy infrastructure, but we also have our own spare energy infrastructure."

Turkish (Original): *"Bizim hizmet veremez duruma gelirsek bizden hizmet alanlar etkilenir. Altyapı manasında diğer altyapılar etkilenmez. Bizim sistemlerimiz doğrudan enerji altyapısına bağlıdır ama yedekli enerji altyapılarımız var."*

Extracted codes: Interdependency is not a concern

Interdependency is not a concern in general. However, the interdependency issue is checked at next recursions.

Categories to be compared with: National governance

For the National software category:

Interviewee-1:

English (Translated): *"National software is a critical topic. The use of foreign software is widely common in the energy systems. The energy sector is fully under the dominance of foreign companies. But we cannot handle the problem of foreign software on our own. The state must also be involved in the issue and must encourage the use of a national software in multiple aspects and must offer some warranties for that."*

Turkish (Original): *"Milli yazılım önemli bir konu. Enerji sistemlerinde çok ciddi yabancı yazılım kullanılıyor. Sektör tamamen yabancıların hakimiyetinde. Yabancı yazılım hakimiyeti sadece bizim kırabileceğimiz bir konu değil. Devletin el atması, milli yazılımı her yönüyle teşvik etmesi ve bazı garantiler vermesi gerekir."*

Extracted codes: the dominance of foreign companies, a difficult topic, a national governance issue

Interviewee-2:

English (Translated): *"We would like to work with national software firms. But how much we can work only with our sources, in isolation from the outer world, is another matter. We use the certain products, like many other countries. The systems shouldn't be facing problems when a national software is obliged."*

Turkish (Original): *"Yerli yazılım firmaları ile çalışmak isteriz. Ama küresel dünyada ne derece izole olunacak o da ayrı mesele. Pek çok ülke belli başlı ürünleri kullanıyor, biz de kullanıyoruz. Milli yazılım olacak diye sistemlerde de sıkıntı olmaması gerekir."*

Extracted codes: dependence to foreign software, a difficult topic, not a priority

Interviewee-3:

English (Translated): *"National software is a difficult topic. We benefit from the operating systems and the databases used by all other countries. We pay for annual maintenance support for those operating systems and databases. They have penal mechanisms for the problems that are not solved on time as the*

finance sector does not tolerate any negligence. Frankly, we have not national software topic in our agenda. But if it is implemented as a governmental policy, there might be a transition process that covers many years and various stages. But anyhow, that would be very tough ..."

Turkish (Original): *"Milli yazılım çok zor bir konu. Tüm dünyanın kullandığı veri tabanlarını, işletim sistemlerini kullanıyoruz. Bunlara yıllık destekler satın alıyoruz. Zamanında çözüm olmayınca ceza mekanizmaları var. Finans sektörü gevşeklik kabul etmez. Milli yazılım olmaması gibi bir problemimiz ve gündemimiz yok açıkçası. Ama bu konuda bir devlet politikası olursa aşama aşama ve uzun yılları içine alacak şekilde bir geçiş düşünülebilir. Ama çok zor bir konu yine de ..."*

Extracted codes: dependence to foreign software, not a priority, a difficult topic

Developing software by a national firm is important for national security. However, this is very difficult to actualize.

Categories to be compared with: National governance

For the National governance category:

Interviewee-1:

English (Translated): *"I think that there is no awareness of the protection of the national cyber security infrastructures or critical infrastructures of the state from cyber threats. But I wish there were, as this lack is the beginning point of all other deficiencies. There has been some improvements in the area, but I think they weren't sufficient. Anyhow, I hope more improvements will come up."*

Turkish (Original): *"Devletimizin ulusal siber güvenlik veya kritik altyapıların siber tehditlerden korunması adına yeterli bir farkındalığının olduğunu düşünmüyorum. Keşke olsa. Bu eksiklik bence pek çok eksikliğin de kaynağı. Son yıllarda bazı gelişmeler oldu ama hem yeterli olmadığını düşüyorum hem de umarım devamı gelir diyorum."*

Extracted codes: Unawareness at state level, the lack of governance is the source of the other problem

Interviewee-2:

English (Translated): *"I think the leadership topic is quite parallel to this one. The state must undertake the leadership task. And only then we will be able to achieve the objectives which we now cannot reach."*

Turkish (Original): *"Daha önce konuştuğumuz liderlik başlığı ile bu başlığı paralel görüyorum. Devletin liderlik yapması gerekir. Şu an tek başına başaramadığımız pek çok şeyi ancak o zaman başarabiliriz."*

Extracted codes: the leadership of government is important, the key to the success

Interviewee-3:

English (Translated): *"There is certainly a leadership and governance on a sectorial basis. There are some country-wide developments, either. But when we compare the security level of the finance sector with those of other sectors, only Telekom has a similar position. As far as I know, the rest of the sectors do not have a structure like ours. Among the sectors you have mentioned, there are even ones with no regulatory authorities. In this respect, it becomes obligatory to take steps for the formation of a national governance."*

Turkish (Original): *"Sektörel olarak düşündüğümüz zaman kesinlikle bir liderlik, bir yönetişim var. Ülke bazında da bazı pozitif gelişmeler var. Ama finans sektöründeki güvenlik seviyesi ile diğer sektörleri karşılaştırdığımız zaman, sadece Telekom sektörünün benzer durumda olduğunu görüyorum. Diğer geri kalan tüm sektörlerde benim bildiğim kadarıyla bizdeki gibi bir yapı yok. Hatta ismini saydığınız diğer sektörler içerisinde denetleyici kurumu olmayan sektörler de var. Bu durumda ulusal yönetişim adına ciddi adımlar atılması gerektiği aşikar."*

Extracted codes: Problems at national governance, problematic sectors

All of the interviewee agree on the need of national governance framework to make improvement in cyber security of critical infrastructures.

Categories to be compared with: Regulatory authority, Regulation, Personnel

Please note the list of categories under the heading "Categories to be compared with", under each group of transcript. These categories were created after performing sufficient coding on the transcripts of the interviews. After the coding of the transcripts, some inherent dependencies and especially "cause and effect relations" among categories are realized. Table 4-9 show the categories to be compared at the axial coding step.

Table 4-9: Compared Categories

Compared Categories	Outsourcing	Audit	Security culture	Personnel	Security standards	Collaboration	Regulation	Regulatory authority	Leadership	Interdependence	National software	National governance
Outsourcing			X				X					
Audit			X				X					
Security culture				X	X	X	X					
Personnel							X					X
Security standards							X					
Collaboration							X					
Regulation								X				X
Regulatory authority									X			X
Leadership												
Interdependence												X

Compared Categories	Outsourcing	Audit	Security culture	Personnel	Security standards	Collaboration	Regulation	Regulatory authority	Leadership	Interdependence	National software	National governance
National software												X
National governance												

4.1.2.3 Axial Coding

During the axial coding phase, comparisons and contrasts were carried out among and within the categories. Comparisons among different sectors and comparisons between different organizations types (governmental vs. private) were performed as well. Relationships among categories emerged and these relationships yielded themes, which means some remarkable cyber security problems were clustered around these categories. These themes were the basic constructs before reaching a theory.

Table 4-10 shows the first comparison over eleven categories between governmental critical infrastructure owners and private infrastructure owners. According to the table below, the security practices in private sectors are much more mature in terms of outsourcing, audit, security culture, personnel and standards. The private sector has a regulatory authority and associated regulations. The regulatory authority supervises cyber security.

Table 4-10: Comparison of the Governmental and Private Critical Infrastructure Operators

	Governmental	Private
Outsourcing	Improper outsourcing practices	Proper outsourcing practices
Audit	No audit / limited audit	Periodical / formal / external audit
Security culture	Do not have a clear security culture	Created a security culture
Personnel	Cannot recruit qualified staff	Has qualified staff; however, the lack qualified staff is a general problem
Security standards	No standards No risk management	Established standards Due care of the top level management
Collaboration	No apparent cooperation routines	No apparent cooperation routines
Regulation	No regulation	Established sectorial regulation
Regulatory authority	No regulatory authority / regulatory authority with no cyber supervision	Regulatory authority with cyber supervision
Leadership	Vital. Should be performed by regulatory authority / top level state officials	Vital. Should be performed by regulatory authority

	Governmental	Private
Interdependence	Not a concern	Not a concern
National software	Challenging issue, not a priority	Challenging issue, not a priority
National governance	Must be done	Must be done

Table 4-11 shows the compared categories and the results of each comparison in this recursion. The table also shows the extracted themes, based on the comparisons at the last column.

Table 4-11: Comparisons and the Resulting Themes

Compared Categories	Comparison Results	Themes
Regulation versus Regulatory authority	The lack of a regulatory authority results in the deregulation of the sector.	The lack of sectorial regulations The lack of regulatory authorities for some sectors
Regulation versus Audit, Security culture, Personnel, Security Standards,	The operators in a sector with no or minimum cyber security regulations have problems with security. These problems are: a) The lack of audit practices or minimum audit practices b) Limited security culture c) Limited awareness level of employees (including managers) d) Operating and outsourcing without security standards e) The lack of management responsibility on cyber security f) No risk management	Limited security culture in organizations Limited security awareness level of employees Operating without security standards No regular and formal IT audit Problematic contract management practices and granting full access rights to third party companies Limited information security governance No or partial internalization of information security management within the organizations
Security culture versus Collaboration, Regulation Collaboration versus Regulation	Collaboration is an enabler of the cyber security; however, the practices like collaboration and cooperation are limited. There is no relation between collaboration and regulation. Collaboration is a matter of culture. Partnership and collaboration with private sector do not exist.	No collaboration culture Limited public and private cooperation

Compared Categories	Comparison Results	Themes
Security culture versus Outsourcing, Audit, Personnel, Security standards Regulation versus Audit, Outsourcing, Security Standards	Because security is somehow related with the culture, the existence of audit rules, outsourcing rules and security standards may not increase the level of security.	-
National governance – Personnel, Leadership, National software, Interdependence, Regulation, Regulatory authority	The lack of national governance has some negative effects on cyber security. Such as: a) Qualified personnel is limited because of the limited national capacity building efforts b) The lack of leadership in cyber security c) The lack of studies such as amendments to the laws, creation of policies on national software development, or national infrastructure interdependence studies d) The lack of diffusion of the cyber security into the critical sectors in terms of regulatory authority and regulations	The lack of national governance Limited capacity building efforts The lack of leadership in cyber security The adverse effects of some laws on the cyber security of critical infrastructures The lack of diffusion of the cyber security into the critical sectors

The themes at last column of Table 4-11 are written in the list below. This list is analyzed in selective coding, next step of the data analysis.

1. The lack of sectorial regulations
2. The lack of regulatory authorities, for some sectors
3. Limited security culture in organizations
4. Limited security awareness level of employees
5. Operating without security standards
6. No regular and formal IT audit
7. Problematic contract management practices and granting full access rights to third party companies
8. Limited information security governance
9. No or partial internalization of information security management within the organizations
10. No collaboration culture
11. Limited public and private cooperation
12. The lack of national governance

13. Limited capacity building efforts
14. The lack of leadership in cyber security
15. The adverse effects of some laws on the cyber security of critical infrastructures
16. The lack of diffusion of the cyber security into the critical sectors

4.1.2.4 Selective Coding

During the selective coding phase, memos are written by the researcher in order to find repetitions, redundancies and to eliminate irrelevant and trivial themes. Memos are the researcher's record of analyses, thoughts, interpretations, questions, and directions for further data collection (Strauss & Corbin 2008). Memos also provided some important inputs for theoretical sampling.

Table 4-12 shows the list of themes after selective coding, along with the themes before the selective coding for the comparison purposes.

Table 4-12: Themes after the Axial and Selective Coding in the Second Recursion

Before Selective Coding (After Axial Coding)	**After Selective Coding (Discovered Theory)**
The lack of sectorial regulations	The lack of sectorial authorities for cyber security
The lack of regulatory authorities, for some sectors	
The lack of diffusion of the cyber security to the critical sectors	
Limited security culture in organizations	The lack of legislation that may create security culture and collaboration
No collaboration culture	
Limited security awareness level of employees	Limited security awareness level of employees
Operating without security standards	*Discarded after writing memos.*
No regular and formal IT audit	No regular and formal IT audit
Problematic contract management practices and granting full access rights to third party companies	Problematic contract management practices and granting full access rights to third party companies
No or partial internalization of information security management within the organizations	Risk management process is not conducted by the critical infrastructure owners.
Limited information security governance	Limited information security governance practices
Limited public and private cooperation	Limited public and private cooperation
The lack of national governance	The lack of national governance
The lack of leadership in cyber security	
Limited capacity building efforts	Limited capacity building efforts
The adverse effects of some laws on the cyber security of critical infrastructures	The adverse effects of some laws on the cyber security of the critical infrastructures

The list of themes after selective coding is as follows:

1. The lack of sectorial authorities for cyber security
2. The lack of legislation that may create security culture and collaboration
3. Limited security awareness level of employees
4. No regular and formal IT audit

5. Problematic contract management practices and granting full access rights to third party companies
6. Risk management process is not conducted by the critical infrastructure owners
7. Limited information security governance practices
8. Limited public and private cooperation
9. The lack of national governance
10. Limited capacity building efforts
11. The adverse effects of some laws on the cyber security of the critical infrastructures.

4.1.2.5 Theoretical Sampling for the Third Recursion

It was seen at the second recursion that the critical infrastructure operators in the finance sector conducted more mature and concrete security practices, compared to the other operators in water management and energy sectors. The water management sector does not have a regulatory authority. The energy sector has a regulatory authority with no/minimum supervision on cyber security.

At first glance, the non-existence of regulatory authority can be considered a root cause for cyber security problems. In the similar manner, the non-existence of regulations can be regarded a root cause as well. The first two root causes were written to show these two phenomenon.

Nevertheless, the most important input to the third recursion was to check the role of the regulations and regulatory authorities for cyber security. A theoretical question as the following arises at that point: "Is the supervision of cyber security by law/regulations feasible or not?" As a result, five focused and detailed questions based on the core problems discovered in the second recursion were added for the next recursion.

Because of the results of the second recursion, governmental critical infrastructures were preferred for the interviews of the third recursion because it was seen in the second round that the cyber security problems of the critical infrastructures of Turkey mainly emanate from governmental organizations. Four interviews were performed in the third recursion. Three of the interviews were performed with governmental organizations.

4.1.3 Third Recursion: Saturation

Like in the second recursion, all the three coding steps of the data analysis were performed at the third recursion. The sectors, the critical organizations and the new interview questions were determined by making theoretical sampling at the end of the second recursion. The researcher reshaped the theory that was discovered at the second recursion. The researcher also observed saturation in the theory at this recursion.

4.1.3.1 Data: Documents and Interviews

In the third recursion, there were eighty-six coded documents. The distribution of the documents according to the sector and the document types are shown in Table 4-13 and Table 4-14 respectively.

As in the second recursion, a set of publicly available documents and restricted documents were analyzed and coded. The restricted documents were independent evaluation reports and minutes of meetings. These documents were richer than the regulation text, news and organizational reports, which are publicly available data. As in the second recursion, there

were two types of independent evaluation reports, which were penetration test reports and information security management evaluation reports.

Table 4-13: Distribution of the Documents According to the Sector Type

Critical sector	The number of documents associated with the critical sector
Government services	51
Transportation	17
Telecommunications	18
Total	**86**

Table 4-14: Distribution of the Documents According to the Document Type

Document type	Number of documents
Regulation text	8
Organizational report	14
Minutes of meeting	14
Independent evaluation report	50
Total	86

For the third recursion, the organizations from the government services, transportation and telecommunications sectors were selected as the result of the theoretical sampling. Three out of four organizations were governmental organizations. Table 4-15 summarizes the properties of the semi-structured interviews. Transportation and one of the telecommunications operators were governmental organizations; whereas the other telecommunications organization was from the private sector. The most part of the transportation sector is operated by the governmental organizations. In other words, there is a dominance of the governmental organization in the transportation sector. In the telecommunications sector, there are prominent private sector operators.

Table 4-15: Properties of the Interviewees of the Third Recursion

Interviewee	Sector	Type
Interviewee – 4	Government services	Governmental organization
Interviewee – 5	Transportation	Governmental organization
Interviewee – 6	Telecommunications	Governmental organization
Interviewee – 7	Telecommunications	Private organization

The work done in the third recursion was to perform data analysis in a different set of data and to compare the results with the ones of the previous recursion as to reach a theoretical saturation.

4.1.3.2 Open Coding

The third recursion started with the coding of eighty-six documents. After reading and coding these documents, it was seen that, cyber security practices within the telecommunications sector were more mature, in contrast with the government services and the transportation sectors

Interviews were performed following the coding of the documents. Each interview lasted around two hours. Like the interviews of the previous recursion, they were face to face. The

interviewees were mid-managers working within information processing departments. Sound recording was not permitted during interviews. The researcher was free to take notes.

The new interview questions for the third recursion to elaborate the role of the regulations and regulatory authorities for cyber security on this issue were:

1. Do you think that the regulations on cyber security will be sufficient to improve the cyber security of the critical infrastructures?
2. What is your opinion on the role of regulatory authority in improving cyber security?
3. Is there a preventive law against collaboration?
4. Could you please compare top-down supervision and bottom-up approach? Which one is more valuable?
5. How can a security culture be created for organizations?

After finishing all of the semi-structured interviews, open coding continued on the transcripts of the interviews. Some of the transcripts related with the new questions are placed below. The transcript about other questions is not placed in the thesis because of the space constraints.

Interviewee-4: Do you think that the regulations on cyber security will be sufficient to improve the cyber security of the critical infrastructures
English (Translated): *"Laws may affect the security based issues and in my opinion, security cannot be attained through the laws. The sense of security must be the result of an inner consideration. It is not possible to proceed farther by the help of external forces. This issue is related to the proper conduction of work and business ethics, it is a matter of settled practice. Laws can only set the necessary regulations, but they cannot create what is nonexistent."* Turkish (Original): *"Kanunların ve yasaların güvenliğe belli bir etkisi olabilir ama ben güvenliğin kanun ile sağlanacağını düşünmüyorum. Güvenlik denen şey biraz da içten gelecek. Dışarıdan zorlamayla nereye kadar? Düzgün iş yapmakla, iş ahlakıyla ilgisi olan bir konu. Bir alışkanlık meselesi. Kanunlar sadece gerekli düzenlemeyi yapar ama olmayan şeyi oluşturamaz."* Extracted codes: No direct relation between regulations and security, security culture
Interviewee-4: What is your opinion on the role of regulatory authority in improving cyber security?
English (Translated): *"The existence of a regulatory authority is not by itself enough. There are some sectors which own a regulatory authority but no security applications. I don't want to mention the names now."* Turkish (Original): *"Sadece düzenleyici kurumun varlığı tek başına güvenlik için elbette yeterli değil. Öyle sektörler var ki, düzenleyici kurumu var. Ama güvenlik uygulaması yok. Şimdi örnek vermeyeyim."* Extracted codes: No direct relation between regulatory agency and security
Interviewee-5: Is there a preventive law against collaboration?
English (Translated): *"Laws neither inhibit nor promote cooperation or participation, which should only be internally and inherently encouraged."*

Turkish (Original): *"İşbirliği, katılımcılık gibi şeyleri engelleyen kanun olmaz. Bunlar teşvik edilen şeylerdir. Ancak bunlar engellenmediği gibi kanunla da teşvik edilmez."*

Extracted codes: No relation between collaboration and security

Interviewee-6: Could you please compare top-down supervision and bottom-up approach? Which one is more valuable?

English (Translated): *"I guess bottom up approach would create long lasting/permanent results. Even if the top down imposition may create positive result in the short term, what is crucial is the efforts by the down."*

Turkish (Original): *"Bence güvenlikte aşağıdan yukarıya yaklaşım daha kalıcı sonuçlar doğurur. Yukarıdan aşağıya bir şeyleri empoze etmenin kısa vadede pozitif sonuçlar olsa da asıl olan aşağıdakilerin çalışmalarıdır."*

Extracted codes: The value of bottom up approaches for security

Interviewee-7: How can a security culture be created for organizations?

English (Translated): *"The establishment of a security culture within organizations is an important subject. Overall national security would rise considerably when all or at least the critical organizations would form a security culture. An external force might increase security but the rest will be the responsibility of the organization itself. In our sector, telecommunications, some information security rules are dictated by the regulatory authority. But I know that many organizations, and ours as well, want to take the easiest and shortest way out. We pass through the auditing process with a seeming culture of security, but whether we are actually secure or not is a matter of question."*

Turkish (Original): *"Kurumlarda güvenlik kültürünün oluşması önemli bir konu. Bunu tüm kurumlar başarsa veya en azından kritik kurumlar başarsa ulusal güvenlik ciddi oranda artar. Dışarıdan ne yapılacağı söylenmesi güvenliği artırır ama güvenlik kültürünün oluşması için biraz da kurumun kendisinin bir şeyler yapması gerekir. Bizim sektörde (elektronik haberleşme) bazı bilgi güvenliği kuralları düzenleyici kurum tarafından dikte ediliyor. Ama ben biliyorum ki bazı kurumlar hatta bizim kurum da dahil işin kolayına kaçabiliyor. Göstermelik bazı şeyler ile denetimlerden geçiyoruz ama güvenlik oluyor muyuz soru işareti."*

Extracted codes: Organizational culture, inefficiency of the regulatory agency

4.1.3.3 Axial Coding

At the axial coding phase, eleven themes that were determined after the selective coding of the second recursion was compared with new data. Table 4-16 shows the results of the comparison. Three themes are discarded according to the results of the comparisons. Two themes emerged, and they were supported by the data of the second recursion as well.

Table 4-16: Themes before and after the Axial Coding in the Third Recursion

No	The Discovered Theory of the Second Recursion	The Discovered Theory after the Axial Coding in the Third Recursion
1	The lack of sectorial authorities for cyber security	Discarded
2	The lack of legislation that may create security culture and collaboration	Discarded
3	Limited security awareness level of employees	Discarded
4	No regular and formal IT audit	IT audit is not performed regularly and formally.
5	Problematic contract management practices and granting full access rights to third party companies	The improper relationship practices with product/service providers
6	Risk management process is not conducted by the critical infrastructure owners	Risk management process is not conducted by the critical infrastructure owners.
8	Limited information security governance practices	Limited information security governance practices
9	Limited public and private cooperation	Private sector is not perceived by the government as an important stakeholder in the national cyber security efforts.
10	The lack of national governance	The lack of national governance
11	Limited capacity building efforts	The number of cyber security experts is limited.
12	The adverse effects of some laws on the cyber security of the critical infrastructures	Some laws have adverse effects on the cyber security of the critical infrastructures.
13	-	The culture of collaboration is very limited. (Emerged at the third recursion)
14	-	Security is not considered as a design construct by the critical infrastructure owners. (Emerged at the third recursion)

The first two themes were discarded because of the results of the interviews in this recursion. There were some indications on the relationship of regulation and security in the second recursion. The same was true for the relationship between regulatory authority and security. However, the data of the previous recursion was not enough to come to a conclusion in these relationships. In this recursion, some specific interview questions were asked. The sample transcripts in the table above demonstrate some ideas of the interviewees. In axial coding, comparisons were performed for these categories. These two themes were dropped according to new data introduced as it was concluded that the lack of either regulation or regulatory authority was not the root causes of cyber security problems.

For the third theme in the table, the limited security awareness level of employees was an obvious problem. However, this was not a root cause for the national cyber security of the critical infrastructures. There were no supporting data in this recursion for this previously-emerged theme.

The themes at the thirteenth and fourteenth rows emerged at this recursion. Although there were some supporting data in the second round, these two themes did not emerge. At the third recursion, newly introduced codes supported these two themes.

4.1.3.4 Selective Coding

After open coding and axial coding, selective coding step started. The list of the root causes (themes) before starting the selective coding is given in Table 4-17.

Table 4-17: Themes after the Axial Coding in the Third Recursion

Root Causes
IT audit is not performed regularly and formally.
The improper relationship practices with product/service providers.
Risk management process is not conducted by the critical infrastructure owners.
Limited information security governance practices.
Private sector is not perceived by the government as an important stakeholder in the national cyber security efforts.
The lack of national governance
The number of cyber security experts is limited.
Some laws have adverse effects on the cyber security of the critical infrastructures.
The culture of collaboration is very limited.
Security is not considered as a design construct by the critical infrastructure owners.

Again memos were written in selective coding. The memos for the third recursion were useful especially in re-wording the root causes more precisely and clearly.

At third recursion, the saturation of the extracted theory was observed because there were not considerable changes in the extracted themes. The newly emerged themes were already supported by the data of the second recursion. It was seen that the general posture of cyber security, the types of vulnerabilities, and the threats that were associated with the sectors were similar. The important difference among sectors was the higher security maturity of the private sector. This phenomenon was observed in the last two recursions. The root causes of the cyber security problems of the critical infrastructures were seen to be generally associated with the governmental critical infrastructure operators.

The list of the themes (Saturated theory) after the selective coding is shown in Table 4-18.

Table 4-18: Saturated Theory after the Selective Coding in the Third Recursion

Root Causes (Saturated Theory)
Cyber security of critical infrastructures is not perceived as a problem at the state level.
The culture of collaboration is very limited.
Private sector is not perceived by the government as an important stakeholder in the national cyber security efforts.
Civil servants laws have adverse effects on the cyber security of the critical infrastructures.
The number of cyber security experts is limited.

Root Causes (Saturated Theory)
The improper relationship practices with product/service providers.
IT audit mechanism does not exist within critical infrastructure owners.
The managers of the critical infrastructure owners do not perceive the information security as an area of responsibility.
Risk management process is not conducted by the critical infrastructure owners.
Security is not considered as a design construct by the critical infrastructure owners.

The most of the themes (root causes) in the saturated theory were rewritten after selective coding, without changing the meaning. Some of the changes were performed to reflect more generalized concepts, and some to detail the problem for better explanation.

4.1.3.5 Theoretical Sampling for the Fourth Recursion

The interviews at the fourth recursion were performed with the set of questions of the third recursion. No new interview question was introduced after the third recursion. Two interviews were arranged for the fourth recursion. The sectors of the interviews were energy and finance, which were already interviewed in the second recursion. The researcher took the validation requirement into consideration for the fourth recursion. Because the theory was saturated in the third recursion, the task to be fulfilled in the fourth recursion was to validate the saturated theory. The effective way of validating the theory was to turn back to the sectors of second recursion and to analyze and compare the previous data again, based on the completely new data.

4.1.4 Fourth Recursion: Validation

The saturation of the theory was observed at the third recursion. The purpose of the fourth recursion was to confirm the saturation and so validate the theory after performing new coding tasks in a completely different data set. As in previous two recursions, all three coding steps of the data analysis were performed at the fourth recursion. At the end of the fourth recursion, the researcher observed the validation of the theory.

4.1.4.1 Data: Documents and Interviews

In the fourth recursion, the number of coded documents is thirty-eight. The distribution of the documents according to the sector and document types are shown in Table 4-19 and Table 4-20 respectively.

On contrary to the second and third recursions, the documents from all sectors were coded to make validation.

Table 4-19: Distribution of the Documents According to the Sector Type

Critical sector	The number of documents associated with the critical sector
Energy	13
Finance	8
Telecommunications	4
Transportation	4
Government Services	9
Total	**38**

Table 4-20: Distribution of the Documents According to the Document Type

Document type	Number of documents
Regulation text	3
Organizational report	4
Minutes of meeting	11
Independent evaluation report	20
Total	38

For the fourth recursion, as the result of the theoretical sampling, the organizations from the energy and finance sectors are selected for interviews. The organization from the energy sector was private. The organization from the finance sector was governmental. Table 4-21 recapitulates the properties of the semi-structured interviews.

Table 4-21: Properties of the Interviewees of the Fourth Recursion

Interviewee	Sector	Type
Interviewee – 8	Energy	Private organization
Interviewee – 9	Finance	Governmental organization

In the fourth recursion, the data analysis in a different set of data was performed. The purpose of this recursion was to check whether the findings were similar to those of the previous recursion and compare the results as to obtain a theoretical saturation.

The researcher started the fourth recursion by coding thirty-eight documents. The researcher performed semi-structured interviews and continued coding the transcripts of the interviews. The results of the data analysis at the fourth recursion exposed that fourth recursion confirmed the results of the third recursion. Hence, the data analysis process was finalized with the validation of the theory.

Table 4-22 shows the list of themes (theory) after the third and fourth recursions comparatively. There were some minor changes in wordings to reflect the ideas more clearly. The completely new data did not change the themes, but rather rendered them stronger. What was done at the axial and selective coding steps at the fourth recursion was to confirm the saturated theme.

Table 4-22: Saturated and Validated Theories

Theory (Saturated)	Theory (Validated)
Cyber security of critical infrastructures is not perceived as a problem at the state level.	Cyber security of critical infrastructures is not perceived as a problem at the state level.
The culture of collaboration is very limited.	The culture of collaboration and cooperation is very limited.
Private sector is not perceived by the government as an important stakeholder in the national cyber security efforts.	The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.
Civil servants laws have adverse effects on the cyber security of the critical infrastructures.	The laws of public procurement and civil servants have adverse effects on the cyber security of the governmental critical infrastructure owners.
The number of cyber security experts is limited.	The number of cyber security experts is limited.

Theory (Saturated)	Theory (Validated)
The improper relationship practices with product/service providers.	The improper relationship practices with product/service providers.
IT audit mechanism does not exist within critical infrastructure owners.	IT audit mechanism does not exist within critical infrastructure owners.
The managers of the critical infrastructure owners do not perceive the information security as an area of responsibility.	The managers of the critical infrastructure owners do not perceive the information security as an area of responsibility.
Risk management process is not conducted by the critical infrastructure owners.	Risk management process is not conducted by the critical infrastructure owners.
Security is not considered as a design construct by the critical infrastructure owners.	Security is not considered as a design construct by the critical infrastructure owners.

4.1.5 Verification of the Theory by Using Expert Opinion

After the saturation and validation of the theory, it was verified with two cyber security experts. Both experts have master's degrees and over ten years of professional experience in cyber security. The first expert was one of the researchers who undertook responsibility in the action items of national cyber security strategy and action plan, which were related with critical infrastructures protection. He contributed to the cyber security studies at national level such in such areas as the preparation of national cyber security strategy, the guidance document of sectorial and organizational computer security incident response teams, and national critical infrastructure protection plan. He was managing a new project about geography and population, based profiling and risk analysis of national critical infrastructures. He also took part in the adaptation of the internationally recognized standards to the national context. He was currently working at a governmental research organization. The second expert had ten years of experience in cyber security. He also took part in national level cyber security studies. He was one of the professionals who took part in the establishment of National Computer Incident Security Response Team. He contributed to the preparation of the national cyber security strategy and action plan. He prepared national level policy documents on incident response mechanisms and organizations to tackle state sponsored cyber threats. The verification based on the expert opinion lasted for three weeks. Three face to face meetings were performed. Here it should be noted that two experts never met during the verification process to prevent any bias. The researcher was the mediator between two experts. The mediator role lasted until experts met at the same point. Apart from the face to face meetings, a number of e-mail correspondence and phone conversations were done with the experts over three weeks' period. Verification with experts was an iterative process, during which, root causes did not change in meaning. However, they were evolved by some amendments for better meanings. Both experts underlined the security problems in the governmental organizations. Their views were parallel to the findings of the research. The term "governmental critical infrastructure owners/operators" was added to the five root causes to demonstrate that the root causes were observed specifically in the governmental organizations. As a result two experts and the researcher agreed on the final list shown at the second column of the Table 4-23.

Table 4-23: Validated and Verified Theories

Theory (Validated)	Theory (Verified)
Cyber security of critical infrastructures is not perceived as a problem at the state level.	The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.
The culture of collaboration and cooperation is very limited.	The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.
The laws of public procurement and civil servants have adverse effects on the cyber security of the governmental critical infrastructure owners.	The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.
The number of cyber security experts is limited.	The number of qualified cyber security experts is limited.
The improper relationship practices with product/service providers.	The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.
IT audit mechanism does not exist within critical infrastructure owners.	The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.
The managers of the critical infrastructure owners do not perceive the information security as an area of responsibility.	The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.
Risk management process is not conducted by the critical infrastructure owners.	The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.
Security is not considered as a design construct by the critical infrastructure owners.	Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.

Table 4-24 shows the evolution of the theory from the first discovery to the verification by expert opinion.

Table 4-24: Evolution of the Theory from Discovery to Verification

Recursion-2 (Discovered Theory)	**Recursion-3 (Saturated Theory)**	**Recursion-4 (Validated Theory)**	**Verified Theory by Expert Opinion**
The lack of national governance	Cyber security of critical infrastructures is not perceived as a problem at the state level.	Cyber security of critical infrastructures is not perceived as a problem at the state level.	The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.
The lack of legislation that may create security culture and collaboration	The culture of collaboration is very limited.	The culture of collaboration and cooperation is very limited.	The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.
Limited public and private cooperation	Private sector is not perceived by the government as an important stakeholder in the national cyber security efforts.	The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.
The adverse effects of some laws on the cyber security of the critical infrastructures	Civil servants laws have adverse effects on the cyber security of the critical infrastructures.	The laws of public procurement and civil servants have adverse effects on the cyber security of the governmental critical infrastructure owners.	The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.
Limited capacity building efforts	The number of cyber security experts is limited.	The number of cyber security experts is limited.	The number of qualified cyber security experts is limited.
Problematic contract management practices and granting full access rights to third party companies	The improper relationship practices with product/service providers.	The improper relationship practices with product/service providers.	The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.

Recursion-2 (Discovered Theory)	Recursion-3 (Saturated Theory)	Recursion-4 (Validated Theory)	Verified Theory by Expert Opinion
No regular and formal IT audit	IT audit mechanism does not exist within critical infrastructure owners.	IT audit mechanism does not exist within critical infrastructure owners.	The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.
Limited information security governance practices	The managers of the critical infrastructure owners do not perceive the information security as an area of responsibility.	The managers of the critical infrastructure owners do not perceive the information security as an area of responsibility.	The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.
Risk management process is not conducted by the critical infrastructure owners.	Risk management process is not conducted by the critical infrastructure owners.	Risk management process is not conducted by the critical infrastructure owners.	The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.
-	Security is not considered as a design construct by the critical infrastructure owners.	Security is not considered as a design construct by the critical infrastructure owners.	Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.
The lack of sectorial authorities for cyber security	-	-	-
Limited security awareness level of employees	-	-	-

4.1.6 Findings of the First Phase of the Research

The prominent finding of the first phase of the research was ten root causes of the susceptibility of the critical infrastructures to cyber threats. The root causes are as follows:

1) The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.
2) The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.
3) The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.
4) The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.
5) The number of qualified cyber security experts is limited.
6) The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.

7) The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.
8) The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.
9) The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.
10) Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.

The first root cause is associated with the state-level perception of cyber security. Cyber security is not considered as a vital part of the national security by the national security authorities. This root cause might be the underlying reason for the other extracted root causes. In this aspect, this root reason can be regarded as a core theme among the other extracted themes.

Cyber security is a horizontal area because of the ubiquitous use of the cyber systems. Therefore, cyber security is the common problem of all organizations in all critical sectors. This fact requires effective collaboration and cooperation activities to cope with the cyber threats as the threats to a sector will probably be the same to other sectors as well. In the same way, threat information exchange is crucial to counteract cyber threats before they actually occur. In Turkey, owing to the privacy and confidentiality constraints, organizations usually keep away from information sharing. Thus, the culture of cooperation, collaboration and information sharing is quite tenuous. There are no incentives by regulatory authorities to encourage the information sharing within the sectors. The practices of information sharing, collaboration and cooperation have to be flourished for resilient infrastructures.

The government authorities and the most of the critical infrastructure operators are not aware of the private sector's potential. The private sector is not regarded as an important stakeholder to reach the cyber security goals, it is rather kept outside of the cyber security agenda. In Turkey, the private organizations did not participate in the preparation process of national cyber security strategy and action plan. There is no private sector representative in Cyber Security Council of Turkey, which, as a fact, affects the national cyber security adversely. For example, public-private partnership cannot be achieved. The public-private partnership is an accelerative force for cyber resilient societies. It is an important instrument for the security of the critical infrastructures (Kelly & Hunker 2012; Rak 2002).

Most of the interviewees in governmental organizations asserted the problems which originate from Turkish Public Servant's Law and Turkish Public Procurement Law. Both laws are comprehensive regulations that shape the core employment and procurement processes of the governmental organizations. The strict articles of the Public Servant's Law prevent the employment of the qualified personnel in the governmental organizations. The strict conditions of the Public Servant's Law bring some problems with the procurements for the governmental organizations as well.

There is a limited number of qualified cyber security experts in Turkey. This is a widespread problem, in fact, the problem of the whole country. It affects all sectors in a way. There are limited efforts regarding human capital to increase the cyber capacity of the country. For example, there is a low number of universities that offer cyber security programs. The training facilities in Turkey are also insufficient in terms of both their number and quality.

The last five root causes are directly associated with the governmental critical infrastructure operators. The lack of IT audit, preliminary security design, information security risk management, and due care of management are related with the inappropriate information

security management culture and practices within the governmental organizations. After the interviews with the critical infrastructure owners, it was seen that business oriented formal and regular risk management was not conducted. The decisions on risk levels and countermeasure procurements were taken in an ad-hoc manner. The insufficiency of the relationship management practices with product/service providers is common among governmental operators. This problem creates considerable cyber security challenges.

The comparisons between applied countermeasures and vulnerabilities within all sectors showed that:

1) There is no correlation between the existence and sophistication of the technical countermeasures and inherent vulnerabilities.
2) Organizations lack in the security processes, which are related to the security culture.

According to the Computer Security Institute, a professional membership organization in US, 60% - 80% of all the network misuse is perpetrated by the people inside the organizations (Peltier et al. 2005). The state-of-the art technical countermeasures will not be effective unless the personnel support the countermeasures by understanding the logic behind their implementation. A cultural change is required to achieve the integration of information security into the organizational culture (Woodhouse 2007).

Technology is a means of improving of security; however, the human factor is the real determinant that ensures security. People's behavior is an essential parameter for the design, implementation, and maintenance of the security controls (Colwill 2009).

The comparisons among the six sectors and between the governmental and private organizations showed that:

1) Independent of the sectors, private organizations are more mature, compared to the governmental organizations. The most of the extracted root causes are mainly associated with the governmental organizations.
2) Therefore, if a sector is dominated by the private organizations, the general security posture of the sector is more mature; and vice versa.
    a. The security maturity of a sector does not mainly originate from the sectorial security practices. While a governmental operator in the finance sector had relatively poor security practices, a private operator in the energy sector had state-of-the art security practices.
    b. Telecommunications and finance sectors are more mature compared to the others because of the private sector dominance in these sectors.
    c. Energy, water management, government, and transportation sectors are less mature due to the government dominance and recently-completed privatizations.
3) Although private organizations are more mature; the root causes are observed in private organizations as well.

Seven out of ten root causes are associated with especially governmental operators. These root causes contain the term "government" explicitly in their definitions. As it can be seen from Table 3-2 in section 3.3.2, the considerable amount of the critical infrastructures are operated by governmental organizations. Therefore, the root causes considerably and negatively affect the critical infrastructures of Turkey. Table 4-25 shows the prevalence of the root causes in governmental and private organizations.

Table 4-25: Appearance of the Root Causes in the Governmental and Private Operators

The Ownership of the CI Operators / Root Causes	Governmental	Private
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	N/A	N/A
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	✔	✔
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	✔	✔
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	✔	-
The number of qualified cyber security experts is limited.	✔	✔
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	✔	~
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	✔	-
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	✔	~
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	✔	~
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	✔	-

✔ : Fully observed; ~: Partially observed; - : Not observed

4.2 Second Phase of the Research: Delphi Survey

The purpose of the second phase of the research was to determine the set of principles for the cyber security of the critical infrastructures of Turkey. The set of principles were determined by a Delphi survey. The input to the Delphi survey was the extracted theory which was the output of the first phase of the research. At the beginning of the second phase, the root causes were introduced to the experts, and they were requested to determine the principles that could be remedies for the root causes of the susceptibility.

The second output of the Delphi survey was the weight values of the principles. The weight values were used to measure the maturity percentage in the proposed national level cyber security maturity model.

The Delphi survey lasted for three weeks. Nine experts were invited to participate in the Delphi survey. However, two of the experts refused to participate in because of their previously-arranged schedules. And one expert was very late to participate in the survey, and thus, his opinions could not be included in the subsequent rounds of the survey. Therefore, the Delphi survey was conducted with six experts to determine the principles associated with the root causes.

The properties of the participants of the Delphi survey are shown in Table 4-26. Two experts with ten and fifteen years of experience in cyber security were from the private sector. Two experts with five and fourteen years of experience were from a governmental research

institute in cyber security. Two experts with fifteen years of experience both were from academia.

Table 4-26: Profile of the Participants of the Delphi Survey

Expert	Years of Experience	Affiliation
Expert-1	14	Government
Expert-2	15	Academia
Expert-3	5	Government
Expert-4	15	Academia
Expert-5	15	Private sector
Expert-6	10	Private sector

To ensure the anonymity, the Delphi survey was conducted by sending e-mails to the six experts separately (Okoli & Pawlowski 2004). The survey had five consecutive rounds. Controlled opinion feedback was supplied by the researcher to the respondents between the rounds (Hsu & Sandford 2007). The details of the rounds of the Delphi survey are given in Appendix A: Details of the Delphi Survey.

4.2.1 First Round: Identifying Principles

At the first round, ten root causes were sent to the experts. Some of the root causes were clarified. The experts were requested to determine principles, from one to three in number, for each root cause by considering the following proposition: "The proposed principle is a sign or countermeasure. If it exists, the effect of the root cause descends, the root cause vanishes or the root cause does not exist". The set of principles determined by each individual is listed in Appendix A: Details of the Delphi Survey. After gathering responses from the experts, the researcher took the repeated principles into consideration and consolidated them. A total of seventy-nine unique principles were obtained. The researcher consolidated the principles into a single document before the second round for the weighting.

4.2.2 Second Round: Weighting Principles

The answers of the experts were consolidated into a single document and sent back to the experts at the second round in which the experts were requested to weight the principles.

According to the Table 4-27, a principle could be regarded as "recognized" by the expert if s/he assigns it a weight value other than zero, or it could be discarded if it is assigned zero. Therefore, three Likert scales were used for the "recognized" principles. Three Likert scales are considered suitable to assess the importance of the principle. Because the national level cyber maturity is assessed, there is not much data on the application details of a specific principle at national level so as to use, for example, a five Likert scale. As an example, a study of the US Department of Homeland Security that measures the cybersecurity capabilities at the national level use a three Likert level to represent the level (DHS 2014).

At this round, the experts were encouraged to assign zero weights to the principles. It was said that the maturity model would include only the most vital principles. This was an important feedback given to the experts at this round.

Table 4-27: Reference Table for the Weight Values of the Principles (W_m)

W_m	Explanation
0	The principle is duplicate, nonsense, confusing, unrelated, imprecise (careless), too detailed or too technical.
1	The lack of the principle can be compensated by other principles to some extent. The country improves its critical infrastructure protection effort more slowly than expected.
2	The maturity principle is important on its own. The lack of the principle cannot be compensated by other principles. The lack of criterion indicates an obvious problem for the critical infrastructure protection. The critical infrastructures will not be resilient at some parts.
3	The lack of the maturity criterion indicates a major problem for the critical infrastructure protection efforts of the country because of the dependencies of the other criteria on this criterion. The country cannot improve the cyber resilience of the critical infrastructures.

4.2.3 Third Round: Reviewing Weights

The scores of six experts were collected into a single document and sent back to the experts at the third round in which the experts were allowed to review and change their scores by looking at the scores of the other anonymized experts. For the controlled opinion feedback, the arithmetic average of the weight values of all principles were sent back to the experts at the beginning of the third round. A distribution chart that shows the frequency of each average weight value was sent as well.

4.2.4 Fourth Round: Reviewing Weights

At the fourth round, the action in the third round was repeated. However, the principles were sorted according to their arithmetic averages from the highest to the lowest before sending the document to the experts. Each expert was requested especially to concentrate on the principles which s/he graded zero point when the average score of the principles is more than one. If a principle got zero point from at least one expert, it would be regarded as the disagreement of the experts and discarded although its average was high because group consensus is vital in Delphi survey (Chan et al. 2001). As controlled opinion feedback, if an expert insisted on the zero value, a reason for insistence was requested.

After the fourth round, a significant consensus of experts on the weights of the principles was reached. The weight values of the experts were converged into each other, compared to the results of the second and the third rounds. After the second round, there were seventeen principles with weight values below one, as seen in Figure 4-1. The number of principles with highest values was relatively low.

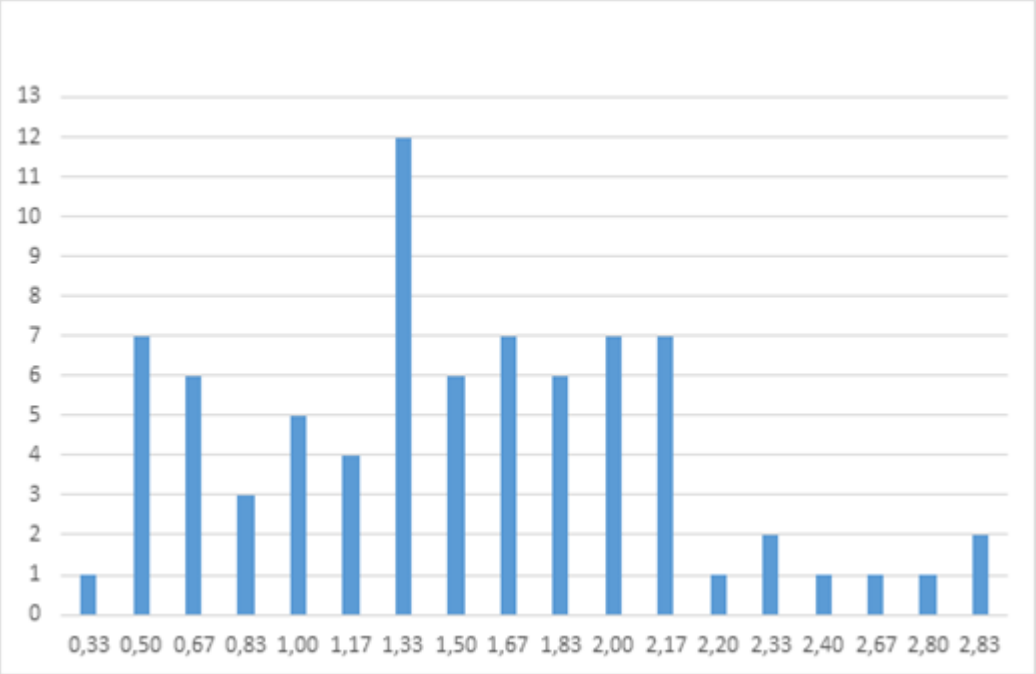


Figure 4-1: Distribution of the Average Weights after the Second Round

After the third round, the distribution of the average weight values changed, as in Figure 4-2. A more uniform distribution was obtained. Both the number of principles with higher averages and the ones with average weight less than one increased.

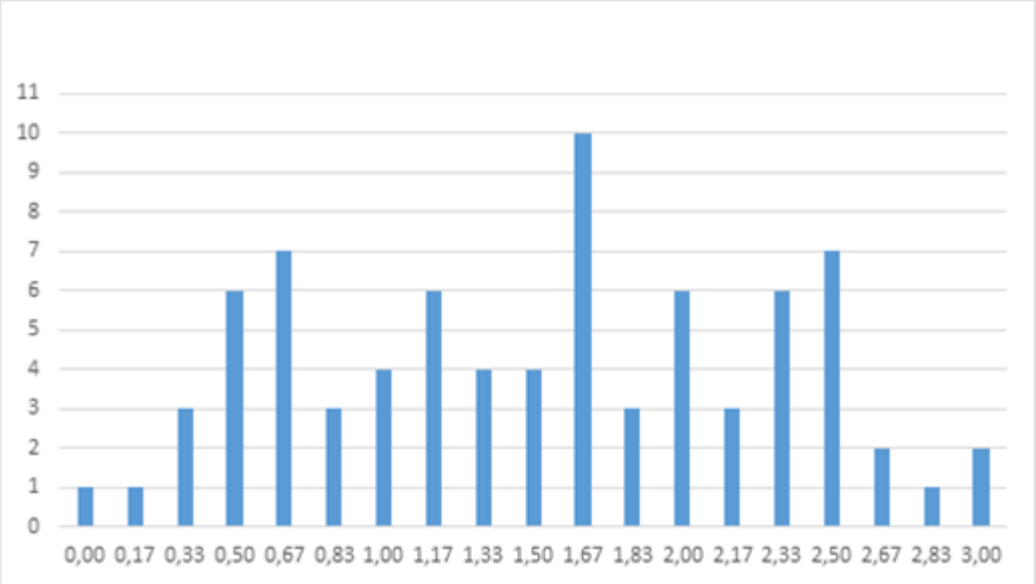


Figure 4-2: Distribution of the Average Weights after the Third Round

The distribution of the weight values after the fourth round is shown in Figure 4-3. Again, the number of principles with relatively higher and lower weight values increased after the fourth round.

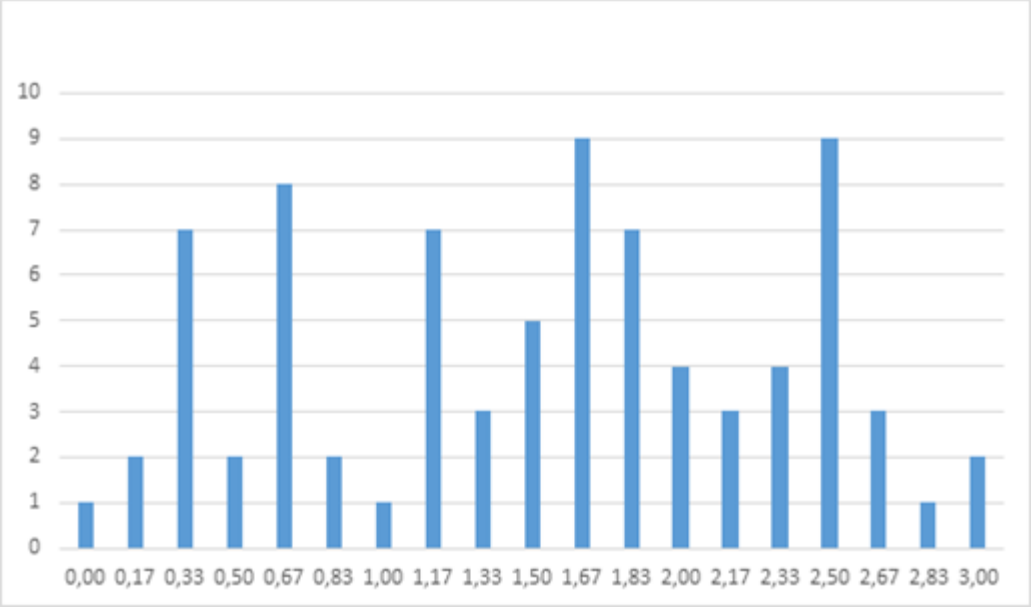


Figure 4-3: Distribution of the Average Weights after the Fourth Round

It is important to obtain the most reliable consensus of the opinions of the experts in Delphi surveys (Chan et al. 2001). Therefore, only the principles, which did not get zero point from any of the experts by the end of the fourth round, were selected as the potential criteria of the maturity model. Although there were fifty-eight principles with average weights between one and three, only forty-one of them got non-zero weights from the six experts by the end of fourth round of Delphi survey.

4.2.5 Fifth Round: Finalizing Principles

A final round of Delphi survey was performed to obtain a final list of the principles as some of the principles were close in meaning. There were both some detailed and general principles for the same topic. The experts were requested to decide on whether to eliminate these principles. The consensus of the experts were required in the elimination of a principle. It means that a principle would be eliminated only if all experts agreed on elimination. As a result, only one principle was omitted at the fifth round. Therefore, forty principles were selected as the criteria of the maturity model at the end of the fifth round. The final list of the principles with weight values are shown in Table 4-28. At the fifth round of the Delphi survey, the experts were requested to review the English translations of the principles as well. It is notable that, at the fifth round, weighting of the principles was not performed.

4.3 Third Phase of the Research: Developing the Maturity Model

Maturity models might help the national security officers in taking accurate decisions on national security and in directing the investments by looking at the current snapshot (DHS 2014; ITU 2009). A national level cyber security maturity model, which measures the state level preparedness of the critical infrastructures protection efforts, was proposed to assess the current cyber security posture.

4.3.1 National Cyber Security Maturity Model

The proposed maturity model was grounded on the set of principles determined in the Delphi Survey. Because the set of principles are grounded on the root causes of the susceptibility to cyber threats, the proposed maturity model was called Vulnerability Driven National Cyber Security Maturity Model.

Table 4-28 shows the list of the principles along with the associated root causes, and their weight values set after the fifth round of the Delphi Survey. The weight value of each principle was the arithmetic average of the individual scores of the six experts for that principle. These weights values were used in the formula of the maturity model. The principles were set as the maturity criteria for the proposed maturity model.

Table 4-28: List of the Principles Determined After the Delphi Survey

Root causes of susceptibility to cyber threats	**Principles (Maturity Criteria)**	**Average Weight Value (W_m)**
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	1) A Critical Infrastructure Protection Program (CIPP) that considers cyber threats	2,5
	2) The management of the CIPP by a governmental organization which has responsibilities for the national security as well / the communication between CIPP and national security bodies	2,5
	3) The existence of a consultant who provides technical, regulatory and diplomatic cyber security consultancy for the head of the state	1,67
	4) Budget allocated to critical infrastructure protection efforts	2,5
	5) Regulatory agencies that set cyber security regulations and check their applications for each critical sector	1,83
	6) A CSIRT organization dedicated to the protection of critical infrastructures	2
	7) A national cyber security strategy that considers the cyber security of critical infrastructures as part of national security	2,17
	8) Nation-wide risk analysis and risk management activities which cover all critical sectors / sector-wide wide risk analysis and risk management activities	2,5
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	9) A public-private partnership program which is developed and supported by the government	2,33
	10) Regulations that specify the inner - inter sector information sharing and cooperation principles	2
	11) Sector based CSIRTs that have information sharing responsibilities determined by the regulations	1,5
	12) The existence of an internationally recognized National CSIRT that performs international cooperation with other CSIRTs	2
	13) A technical infrastructure to fulfill the inner - inter sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers)	1,67

Root causes of susceptibility to cyber threats	Principles (Maturity Criteria)	Average Weight Value (W_m)
	14) A National CSIRT that handles the warnings of cyber incidents related to critical infrastructures by coordinating with the relevant sectorial CSIRTs and critical infrastructure owners when needed	1,83
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	15) Government policies and strategies that position private sector as a key player in national cyber security efforts	2,5
	16) The participation of the private sector in the preparation of the national or sectorial cyber security strategies	2
	17) Permanent seat for the private sector in the national boards like the cyber security council	1,33
	18) Government leadership for innovation, research & development activities, and the identification of the priority areas in cyber security by the government	2,33
	19) The extensive participation of the private sector in the national cyber security exercises	1,5
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	20) Critical review and update of the existing legislation that may affect critical infrastructures (especially for the needs of the governmental critical infrastructure operators)	2,5
	21) Making amendments to the regulations to hire outsourced personnel / qualified government officials with higher salaries / contracted personnel in governmental critical infrastructures	2,5
The number of qualified cyber security experts is limited.	22) National capacity building plans and strategies	2,5
	23) Preference of the internationally accepted certificate owners in the recruitments by critical infrastructure owners	1,67
	24) Qualified and sufficient number of cyber security training institutions (private, academic or governmental) that support/train the personnel of critical infrastructure operators	1,83
	25) Cyber security and IT curriculum for all levels of the education, from elementary schools to universities	2,33
	26) Special positions for cyber security experts in critical infrastructure operators	1,67
The relationship management practices	27) National / sectorial products and service procurement standards or rules for critical infrastructure operators	2,67

Root causes of susceptibility to cyber threats	Principles (Maturity Criteria)	Average Weight Value (W_m)
with the product/service providers are insufficient in governmental critical infrastructure operators.	28) The establishment of a system for the eligibility certifications of the IT companies to provide IT services for critical infrastructure operators	2,17
	29) Security standards for the IT products to be used by critical infrastructure operators	1,83
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	30) National or sectorial regulations that enforce the internal / external audit for critical infrastructure operators	2,67
	31) Regular cyber security audits performed by the regulatory authorities of the sectors for critical infrastructure operators	3
	32) Experienced IT auditors who are employed within the internal audit units of critical infrastructure operators	1,67
	33) Sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities	1,83
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	34) Regulations that render top level management of critical infrastructure operators responsible for cyber security	2,83
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	35) Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process	3
	36) Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners	2,17
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	37) Minimum security countermeasures that are obliged by regulations for critical infrastructure owners	2,5
	38) Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators	2,33
	39) Sector-specific technical guidance documents for the secure design, set-up and operation of the networks of critical infrastructure operators	1,5
	40) Sectorial or national security standards that set out the best security practices for each critical sector	1,83

Vulnerability Driven National Cyber Security Maturity Model is a survey-based maturity assessment method. The other numerical value that was used in the national level cyber

security maturity evaluation was the value of each answer choice selected by the survey participants. The existence of each principle would be checked by the survey participants according to the three answer choices based on the three Likert scale, as shown in Table 4-29. A country gets zero point for very limited or no action, one point for the partial action, and two points for the comprehensive action. Table 4-29 was the evaluation table used at a similar study, Global Cybersecurity Index (ITU 2014). Global Cybersecurity Index is the most similar study to the proposed maturity model among other studies in terms of its content. Global Cybersecurity Index is the only study that scores countries according to their cyber security efforts only. Therefore, the same evaluation table is selected to make more reliable discussions and comparisons after the application of the model.

Table 4-29: Weight Values of the Answer Choices

A_m	Explanation
0	No action or very limited action
1	Partial Action
2	Comprehensive Action

Before conducting the maturity survey, the forty maturity criteria (m) are converted into the questions (W_m). For each question, three answer choices (A_m) are written under the question based on the Table 4-29. The survey sheet is given at Appendix B: Maturity Survey.

Formula 1 shows the maturity model associated with the legend. The maturity calculation is performed based on a simple linear additive evaluation model. The numerator of the fraction in Formula 1 represents the maturity percentage evaluated by a single participant. The final maturity level is the arithmetic average of the opinions of all participants.

$$Maturity\ Level = \frac{\sum_p \left(\frac{\sum_m W_m \times A_m}{\sum_m W_m \times 2} \times 100 \right)}{p} \quad (1)$$

where;
p: The total number of the survey participants
m: The total number of the maturity criteria (principles) (m=40)
W_m: The weight of the principle "m" (See Table 4-28)
A_m: The weight of the selected answer choice for the principle "m" (See Table 4-29)
Maturity Level: The cyber security maturity percentage of critical infrastructure protection efforts of the evaluated country

The maturity level is presented as percentage values which are more flexible and meaningful for the government officials compared to the Likert scale in presenting maturity level. Cyber Power Index and Cyber Maturity in Asia-Pacific Region studies also use percentage values to represent the maturity level (BAH 2011; Tobias Feakin & Woodall 2014). Both studies measure the maturity of cyber capabilities of various countries and they are intended to be read by policy makers.

4.3.2 Application of the Maturity Model for Turkey

A maturity survey was performed with ten participants (p) who are working in the governmental organizations or are former government officials. They participated in the national cyber security efforts such as the preparation and review of the national strategy, the participation of the nation cyber security exercises and the preparation of the national level

cyber security statues. The results of the survey do not officially represent the maturity level of Turkey because the survey was not officially conducted.

A maturity survey would produce the most accurate results when it was answered by the related government officials. Most of the country level maturity surveys were answered by the experts and according to the publicly available data about the countries. Publicly available data may be misleading because the real preparedness level and the intent of the government can only be known by the appropriate government officials.

Table 4-30 shows the results of the maturity survey. Table 4-30 also shows the individual maturity percentages. The cyber security maturity percentage of the critical infrastructure protection efforts of the Turkey is 22.27 percent.

Table 4-30: Results of the Pilot Application of the Maturity Survey for Turkey

Participant (p)	**Individual Maturity Percentage** $\frac{\sum_m W_m \times A_m}{\sum_m W_m \times 2} \times 100$	**Maturity Level (Average Maturity Percentage)** $\frac{\sum_p \left(\frac{\sum_m W_m \times A_m}{\sum_m W_m \times 2} \times 100 \right)}{p}$
p=1	24,01%	20,85%
p=2	28,30%	
p=3	14,20%	
p=4	20,03%	
p=5	28,50%	
p=6	21,59%	
p=7	10,99%	
p=8	22,28%	
p=9	21,02%	
p=10	17,61%	

It is worthy of note that the maturity percentage of Turkey was 64.7% in the GCI of ITU. Turkey got the seventh highest point among the twenty-nine levels in ITU's Global Cybersecurity Index survey study. The considerable difference between the maturity levels of two studies may emanate from the details of the analysis. Vulnerability Driven National Cyber Security Maturity Model checks the details of the organizational structures, CSIRTs, and the regulatory infrastructure etc. However GCI checks the existence of these structures and it does not detail the survey. As an example, GCI checks whether National and Sectorial CSIRTs are legally mandated and also National CSIRT's ability to gather its own intelligence. However, the following detailed criteria are checked for CSIRTs in the proposed model:

a) A CSIRT organization dedicated to the protection of critical infrastructures
b) Sector based CSIRTs that have information sharing responsibilities determined by the regulations
c) The existence of an internationally recognized National CSIRT that performs international cooperation with other CSIRTs
d) A technical infrastructure to fulfill the inner - inter sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers)

e) A National CSIRT that handles the warnings of cyber incidents related to critical infrastructures by coordinating with the relevant sectorial CSIRTs and critical infrastructure owners when needed

The scope of the proposed model is the cyber security posture of the critical infrastructures. However, the scope of the GCI is the general cyber security efforts of the countries. This may be the other reason for the difference of the results.

The other study that scores Turkey is Cyber Power Index performed by Booz Allen Hamilton with a maturity percentage of 30.4%. Turkey was the fifteenth among nineteen countries. This percentage value is close to the percentage of unofficial application of the proposed model. The theme of the Cyber Power Index was broader than cyber security. There are four different categories in Cyber Power Index. The criteria related with cyber security –as well as the ones not related with cyber security- are under the legal and regulatory framework category. The maturity level of Turkey is 49,2% in this category. However, the ranking of Turkey for this category does not change despite relatively higher maturity. Again, the details of the analysis may be a reason for the difference of the maturity percentages. The principles of the Cyber Power Index are not detailed like the principles of GCI. Secondly, the other criteria in the legal and regulatory framework such as intellectual property protection may be another reason for the relatively higher maturity level.

Although the maturity model is based on the data specific to Turkey, it can produce accurate results for the countries that have certain similarities with Turkey in terms of organizational and legislative properties. Before conducting the survey, the weight values of the criteria can be reviewed and changed by the experts in that country.

CHAPTER 5

5 CONCLUSIONS

The conclusion chapter has five sections, which are comparison of the extracted theory with the literature, comparison of the set of principles with the criteria of the other maturity models, suggested list of principles, regulatory approaches for the mitigation of the root causes, and the implications for future research.

There were two research questions for the PhD research. These were:

1) What are the possible root causes of these vulnerabilities?
2) What are the set of principles to mitigate these root causes?

The first and the second research questions were discussed in the section 5.1 and in the section 5.2 respectively.

5.1 Comparison of the Extracted Theory with the Literature

Academic studies, the reports of the Turkish government and the international/regional organizations, Turkish regulations, and the official webpages of the government agencies of Turkey were reviewed to find the appropriate materials that may confirm the extracted root causes. The literature that analyzes the cyber security efforts of Turkey is quite limited. Most of the found studies are conducted by Turkish citizens. This section contains the comparison of the current literature with the findings.

Ten root causes, which were the reasons of the susceptibility of the critical infrastructures to the cyber threats, were as follows:

1. The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.
2. The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.
3. The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.
4. The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.
5. The number of qualified cyber security experts is limited.
6. The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.
7. The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.
8. The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.
9. The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.
10. Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.

There are several findings in the literature that confirm the first root reason. As opposed to the developed countries in which the organizations with national security responsibilities have a central role in cyber defense, the cyber security coordinator body of Turkey does not have any national security responsibility (Ikitemur 2014). The webpage of the national CSIRT does not contain any security recommendation or bulletin specific to the critical infrastructures (TR-CERT 2015). According to the eighth action item of National Cyber Security Action Plan, an international cyber security exercise had to be organized by the end of May 2014 (Ministry of Telecommunications 2013). However, no exercise was organized either at that date or later. The national cyber security action plan spanned between the years 2013 and 2014. Currently, there is no action plan in effect. Cyber Security Council of Turkey was established at the end of 2012 by the Cabinet decision (Senturk et al. 2013). The council has not gathered for the last fifteen months. At the meeting of the Cyber Security Council in June 2013, the critical infrastructure list of Turkey was updated. The decision remained in the meeting record and has not yet been part of a regulation (Kaska & Trinberg 2015).

For the second root reason; there are currently no sectorial level CSIRTs or no CSIRT specific to Industrial Control Systems like ICS-CERT of USA, although it was obliged at the fourth action item of the obsolete national cyber security action plan of Turkey. CSIRTs share various pieces of information with other CSIRTs, ISPs, Law Enforcement Agencies and any other related parties (Cichonski et al. 2012) The successful CSIRT operations depend on the collaborative and cooperative activities. The lack of security-specific organizations like CSIRT is one of the primary causes of the lack of information sharing, collaboration and cooperation. According to the e-government studies report of OECD, only 10-25% of the respondents from central and municipal government collaborate with other public sector organizations (OECD 2007b). According to the same report, nearly 50% of respondents emphasize that the complexity of regulations prevents the collaboration. The legislative infrastructure has not changed since 2007. There is no public-private partnership model, as stated in the article that analyzes the cyber security structure of Turkey (Senturk et al. 2013). According to the same article, government and privately owned critical infrastructure owners should cooperate.

For the third root reason; the contribution of the private sector to the national cyber security efforts is minimum (Ikitemur 2014). As an example, the cyber security council of Turkey does not have a member who represents the private sector, as the Cabinet Decision and Electronic Communications Law amendments deal with the cyber security issues from a public point of view (Turkish Cabinet 2012; Turkish Cabinet 2014). The national cyber security strategy and action plan were prepared by a governmental research organization. As written in the webpage of the governmental research agency that prepared the strategy, exposure draft was shared only with the related governmental organizations (CSI 2013). Only six of the forty participants of the national cyber security exercise, organized in 2011, were private organizations (ICTA & TUBITAK 2011). Among thirty OECD countries, Turkey ranks the twenty-sixth among thirty countries in 2013 in terms of gross domestic spending on research and development (OECD 2013). This statistic may be regarded as an indicator of the limited power of the private sector in Turkey.

For the fourth root reason; all of the interviewees from governmental critical infrastructure owners emphasized the adverse effect of the civil servants law on the employee quality. Three of the interviewees stated the adverse effect of the public procurement law on the security of critical infrastructure owners. As stated by all governmental interviewees, there are three prominent problems with the civil servants law. Firstly, it grants job guarantee according to the article 125 (Republic of Turkey 1965). Secondly, it lacks the performance evaluation based on technical performance. Thirdly, high salaries for successful personnel

cannot be granted according to the article forty-three. As a result, qualified personnel look for jobs with higher salaries and usually find a favorable job. Governmental critical infrastructure owners cannot purchase the desired software/hardware because of the public procurement law which urges tendering for almost all needs of the organizations.

For the fifth root reason; Ministry of Development of Turkey recently published a report, which analyzes the problems of the information society. According to the report, available human resources do not meet the requirements of the employers in the information technology sector. According to 58% of the participants of a survey made by an employers' association, the qualified workforce deficit is the most important problem of the sector (Ministry of Development 2013). According to the presentation made by the authorized government official in 2014, there is no cyber security doctoral program in Turkish universities. There are master programs in only six universities among 196 universities (Ministry of Telecommunications 2014).

For the sixth root reason; the State Supervisory Council, which works on behalf of Turkish Presidency, examined the security postures of six governmental critical infrastructure owners in 2013. According to the confidential audit report, the owners of the information systems of the organizations are mostly private organizations "in practice", because of the granted permissions to control and monitor the critical systems (Turkish Presidency 2013). The same report points out the problems with the authorization procedures of the service provider personnel, security clearance procedures, access management processes, and nondisclosure agreements. To summarize, critical infrastructure owners do not comply with the cyber security principles when procuring services or products from third party firms. According to another study that contains the results of eight information security management projects within governmental organizations, the managers of the governmental organizations and the chiefs of the information processing departments may fallaciously think that "information security management can and should be achieved by the consulting firm" (Karabacak & Ozkan 2010).

For the seventh root reason; the report of the State Supervisory Council emphasizes the lack of internal audit procedures and processes. According to the report, some of the critical infrastructure owners do not have internal audit units (Turkish Presidency 2013). The report of the national cyber security exercise in Turkey points out the inherent audit problems of the participant organizations (ICTA & TUBITAK 2011). Fourteen critical infrastructure owners from the telecommunications, finance, and government services participated in the national cyber security exercise.

For the eighth root reason; according to the results of information security management projects within eight critical governmental organizations, the top level managers do not feel themselves responsible for information security (Karabacak & Ozkan 2010). Five of the analyzed organizations were critical infrastructure owners. Therefore, due care principles of information security were violated (Solms & Solms 2004). According to the article the enterprise wide information security was delegated to the head of the information processing department by the top level managers (Karabacak & Ozkan 2010). Therefore, information security governance principles are not obeyed by critical infrastructure owners, meaning that information security is not seen as a part of corporate governance and business strategy (von Solms & von Solms 2006; Von Solms & Von Solms 2005).

For the ninth root reason; the lack of the information security management systems was the first finding of the national cyber security exercise (ICTA & TUBITAK 2011). According to the exercise report, organizations do not perform a risk analysis process; which is the

essential part and the starting point of the risk management process (Stoneburner et al. 2002).

For the tenth root reason; according to the national cyber security exercise report, some participants of the exercise did not consider security as a main design principle in the system design stage (ICTA & TUBITAK 2011). The similar problem was stated in the audit report of the State Supervisory Council (Turkish Presidency 2013). The report recommends the consideration of the security requirements at the design phase.

Table 5-1 shows the root causes, which are implicitly stated by the aforementioned studies. Six of the root causes are implied by thirteen different studies; only two of them are from the academia.

Table 5-1: Implicitly Stated Root Causes

Root Cause	Discussed By
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Implicitly discussed in a PhD thesis (Ikitemur 2014) Implied in the webpage of TR-CERT (TR-CERT 2015) Implicitly stated by a NATO report (Kaska & Trinberg 2015)
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited	Implicitly stated in an OECD report (OECD 2007b) Implicitly stated in the article (Senturk et al. 2013)
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Implicitly discussed in a PhD thesis (Ikitemur 2014) Implied in the Turkish regulations (Turkish Cabinet 2014; Turkish Cabinet 2012) Implied in the webpage of governmental organization (CSI 2013) Implied in the report of cyber security exercise (ICTA & TUBITAK 2011) Implicitly stated by an OECD report (OECD 2013)
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Implied in the Turkish Civil Servant's Law (Republic of Turkey 1965)
The number of qualified cyber security experts is limited.	Implied by a ministry report (Ministry of Development 2013) Implied in a presentation of a government official (Ministry of Telecommunications 2014)
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	Implied in the report of cyber security exercise (ICTA & TUBITAK 2011)

Table 5-2 shows the root causes, which are explicitly stated by other studies. Four of the root causes are explicitly stated by three different studies; only one of them is from the academia, which is an article of the researcher and his advisor. As a result, this PhD thesis brings ten

root causes together as the result of the analysis of the project data. This fact also points out to the significance of the study.

Table 5-2: Explicitly Stated Root Causes

Root Causes	Discussed By
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	Explicitly stated in a report of Turkish Presidency (Turkish Presidency 2013) Implicitly discussed in an academic article (Ozkan & Karabacak 2010)
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	Explicitly stated in a report of Turkish Presidency (Turkish Presidency 2013) Explicitly stated in the cyber security exercise report (ICTA & TUBITAK 2011)
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	Explicitly discussed in an academic article (Ozkan & Karabacak 2010)
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	Explicitly stated in a report of Turkish Presidency (Turkish Presidency 2013) Explicitly stated in the cyber security exercise report (ICTA & TUBITAK 2011)

5.2 Comparison of the Principles with the Criteria of the other Maturity Models

According to the National Cyber Security Framework Manual prepared by NATO's Cooperative Cyber Defence Centre of Excellence, there are five mandates for national cyber security strategies (Klimburg 2012). These mandates can be defined as national level cyber security functions of a country. These are:

1. Military Cyber Operations
2. Counter Cyber Crime
3. Intelligence/Counter-Intelligence
4. Cyber Security Crisis Management and Critical Infrastructure Protection
5. Internet Governance and Cyber Diplomacy

The scope of this PhD thesis is the fourth mandate in the report of NATO, as stated a delimitation in the introduction chapter of the thesis. The extracted root causes are all about the vulnerabilities of the critical infrastructures. The set of principles are for the protection of critical infrastructures. Finally, the purpose of the proposed maturity model is to assess the maturity of the critical infrastructure protection efforts of a country. Any principle that may be considered within any mandate other than critical infrastructure protection is out of scope of the PhD thesis. Such principles (criteria) that belong to other mandates are excluded from Table 5-3.

Maturity models are compared in terms of their maturity criteria. Before making comparisons, similar criteria are generalized to produce a maturity theme for comparability purposes. However, some criteria that elaborate on certain technical topics are not

generalized to produce a theme; comparisons are performed over these criteria. Table 5-3 shows maturity themes and criteria which are related with critical infrastructure protection and denoted by at least one maturity model. The numbers in the parentheses at the first column of Table 5-3 are the sequence numbers of the relevant principles of the proposed model. Please refer to Table 4-28 for the list of principles along with the sequence numbers.

Proposed maturity model provides thorough and multiple criteria for the CSIRT organization, national level organization, capacity building, cyber security legislation, audit and risk management concepts.

First ten criteria or class of criteria are commonly used in the maturity models along with the proposed method. Next six criteria are less commonly used in other maturity models. The following nine criteria are unique to the proposed model. Next five criteria are not included in the proposed model although they are included in other models. Public awareness is a commonly used criterion; however it is not used in the proposed model. The reason for that may be the peculiarity of the proposed model to governmental critical infrastructure protection efforts.

Table 5-3: Comparison of the Maturity Models in terms of the Maturity Criteria

Maturity Models / **Maturity Themes / Maturity Criteria**	Proposed Model	The CCSMM	NCSecMM	Cyber Readiness Index	Global Cybersecurity Index	Cyber Maturity in the A-P Region	Cyber Power Index
Cyber security organization / coordination (2, 5)	X		X	X	X	X	X
National CSIRT organization (12, 14)	X	X	X	X	X	X	
Public - private partnership (9)	X		X	X	X	X	X
International cooperation / international engagement (12)	X		X	X	X	X	X
Regulations related with the cyber security (30, 34, 35, 38)	X		X		X	X	X
Cyber security program / strategy / plan / policy (1, 7)	X		X	X	X	X	X
Information sharing and cooperation (10, 11, 13, 14)	X	X	X	X	X		
Certification, training, promoting higher education, capacity building (22, 23, 24, 25, 26)	X	X	X	X	X		
Innovation, research and development programs (18)	X		X	X	X		

Maturity Models / Maturity Themes / Maturity Criteria	Proposed Model	The CCSMM	NCSecMM	Cyber Readiness Index	Global Cybersecurity Index	Cyber Maturity in the A-P Region	Cyber Power Index
Audit, performance evaluation, exercises, benchmarking to measure cybersecurity development (30, 31, 32)	X	X	X		X		
Participation and engagement of private sector (15, 16, 17, 19)	X		X	X			
Adoption of the information security governance routines by critical infrastructure owners (34)	X		X		X		
Adoption of (internationally approved) standards to critical infrastructure owners (29, 36, 40)	X			X	X		
Risk analysis and management for critical infrastructure operators (35)	X		X				
Critical review of and amendments to the existing laws (20, 21)	X			X			
Budget dedicated to cyber security / National funding for research (4)	X			X			
Critical infrastructures focused CSIRT and Sector based CSIRTs (6, 11)	X						
Nation-wide / sector-wide risk analysis and management processes (8)	X						
National / sectorial product and service procurement standards or rules (27, 38)	X						
Sector-specific technical guidance documents for the secure design, set-up and operation of the networks (39)	X						
Certification scheme of IT companies for eligibility to provide IT services for critical infrastructure operators (28)	X						
Cyber security consultant (cyber czar) of the president / prime minister of the country (3)	X						

Maturity Themes / Maturity Criteria \ Maturity Models	Proposed Model	The CCSMM	NCSecMM	Cyber Readiness Index	Global Cybersecurity Index	Cyber Maturity in the A-P Region	Cyber Power Index
Minimum security countermeasures that are obliged by regulations for critical infrastructure owners (37)	X						
Sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities (33)	X						
Technical infrastructure to fulfill the inner - inter sector information sharing needs (13)	X						
Public awareness		X	X		X	X	
Situational awareness mechanisms				X			
The existence of rapid reaction mechanism				X			
Identification of the appropriate experts and policymakers within government, private sector and university			X				
Persuade national leaders			X				

5.3 Suggested List of Principles

Some principles underline general matters, whereas some others deal with more detailed matters. At this section of the thesis, a suggested list of principles are suggested. While creating the suggested list:

a) Some principles are grouped together to have a more general meaning (29th, 36th, and 40th principles)
b) Some principles are grouped under another principle that has more general meaning (16th, 17th, and 19th principles are grouped under 15th principle; 21st principle is positioned under 20th principle; 31th principle is positioned under 30th principle)

The following thirty-three principles can be used in maturity measurements as well. The weight values of the consolidated principles can be selected as either arithmetic average of the principles or the highest weight value of the combined principles.

- A Critical Infrastructure Protection Program (CIPP) that considers cyber threats (1)

- The management of the CIPP by a governmental organization which has responsibilities for the national security as well / the communication between CIPP and national security bodies (2)
- The existence of a consultant who provides technical, regulatory and diplomatic cyber security consultancy for the head of the state (3)
- Budget allocated to critical infrastructure protection efforts (4)
- Regulatory agencies that set cyber security regulations and check their applications for each critical sector (5)
- A CSIRT organization dedicated to the protection of critical infrastructures (6)
- A national cyber security strategy that considers the cyber security of critical infrastructures as part of national security (7)
- Nation-wide risk analysis and risk management activities which cover all critical sectors / sector-wide wide risk analysis and risk management activities (8)
- A public-private partnership program which is developed and supported by the government (9)
- Regulations that specify the inner - inter sector information sharing and cooperation principles (10)
- Sector based CSIRTs that have information sharing responsibilities determined by the regulations (11)
- The existence of an internationally recognized National CSIRT that performs international cooperation with other CSIRTs (12)
- A technical infrastructure to fulfill the inner - inter sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers) (13)
- A National CSIRT that handles the warnings of cyber incidents related to critical infrastructures by coordinating with the relevant sectorial CSIRTs and critical infrastructure owners when needed (14)
- Government policies and strategies that position private sector as a key player in national cyber security efforts (15)
    - The participation of the private sector in the preparation of the national or sectorial cyber security strategies (16) / Permanent seat for the private sector in the national boards like the cyber security council (17) / The extensive participation of the private sector in the national cyber security exercises (19)
- Government leadership for innovation, research & development activities, and the identification of the priority areas in cyber security by the government (18)
- Critical review and update of the existing legislation that may affect critical infrastructures (especially for the needs of the governmental critical infrastructure operators) (20)
    - Making amendments to the regulations to hire outsourced personnel / qualified government officials with higher salaries / contracted personnel in governmental critical infrastructures (21)
- National capacity building plans and strategies (22)
- Preference of the internationally accepted certificate owners in the recruitments by critical infrastructure owners (23)

- Qualified and sufficient number of cyber security training institutions (private, academic or governmental) that support/train the personnel of critical infrastructure operators (24)
- Cyber security and IT curriculum for all levels of the education, from elementary schools to universities (25)
- Special positions for cyber security experts in critical infrastructure operators (26)
- National / sectorial products and service procurement standards or rules for critical infrastructure operators (27)
- The establishment of a system for the eligibility certifications of the IT companies to provide IT services for critical infrastructure operators (28)
- National or sectorial regulations that enforce the internal / external audit for critical infrastructure operators (30)
    - Regular cyber security audits performed by the regulatory authorities of the sectors for critical infrastructure operators (31)
- Experienced IT auditors who are employed within the internal audit units of critical infrastructure operators (32)
- Sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities (33)
- Regulations that render top level management of critical infrastructure operators responsible for cyber security (34)
- Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process (35)
- Minimum security countermeasures that are obliged by regulations for critical infrastructure owners (37)
- Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators (38)
- Sector-specific technical guidance documents for the secure design, set-up and operation of the networks of critical infrastructure operators (39)
- Security standards for the IT products to be used by critical infrastructure operators (29) / Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners (36) / Sectorial or national security standards that set out the best security practices for each critical sector (40)

5.4 Regulatory Approaches for the Mitigation of the Root Causes

The policy-level issues of critical infrastructure protection as an academic topic is mostly studied in the developed countries like United States, European Union Members, and Oceanian countries. In terms of developing policies and strategies, the governments of the developed countries are ahead of the governments of the less developed ones Secondly, the critical infrastructures are mostly owned and operated by private entities in the developed countries. For example, the percentage of private sector ownership of infrastructures in the US is eighty-five percent (de Bruijne & van Eeten 2007).

Developing countries like Turkey are mostly underway of the privatization of the infrastructures. For example, the largest and national telecommunications company of Turkey was privatized in 2005 (Turk Telekom 2015). Share transfer agreements between government and private organizations that are responsible for electricity distribution were completed as of August 2013 (TEDAS 2015). The approximate situation of the critical infrastructure ownership of Turkey was shown in Table 3-2 at section 3.3.2. Despite the

ongoing privatizations, there are still a considerable weight of the government ownership of the critical infrastructures in Turkey.

The regulation of critical infrastructures has been discussed for at least one decade. However, it is still a hot topic for the academia and the governments. The strict government intervention and regulations to CIP efforts are not considered as a suitable option by the academia and governments in the developed countries. In these countries, there are a number of academic studies that propose security management models for CIP. This topic can be summarized by a question: "Which is suitable- Regulation or Innovation?" The section 2.5 of the literature review summarizes the academic studies that seek answers to this question. These articles focus on or emphasize the importance of the cooperation, innovation, and non-regulation rather than emphasizing the importance of the regulations. The idea of non-regulation is accepted in a wider way in the developed countries, although there are still clear objections by some security experts and government officials (Wiki 2015a).

Although the developed world discusses the topics like innovation, non-regulation, business continuity, voluntary approaches, and network governance, the developing countries like Turkey should be prudent while considering these options. As opposed to the developed world, the approaches close to the deregulation of the infrastructures may not be a sound option to establish effective CIP policies for the developing countries like Turkey. The findings of the PhD research corroborate the situation as discussed in this section.

Currently, there is no or very limited disputes in Turkey on the intervention of the government in the critical infrastructure protection, as opposed to the developed countries. Two factors may result in or contribute to this phenomenon. Firstly, there is a considerable weight of governmental critical infrastructure owners in Turkey. If the proportion of the private sector ownership increases as a result of the privatization and globalization processes in the forthcoming years, some disputes on government intervention may emerge. Secondly, Turkey has a civil law system as opposed to the US and the commonwealth countries that have common law system. In civil law system; the rules have to be in written forms, which are structured in a hierarchy of norms. Therefore, well-defined and complete set of regulations may be necessary for Turkey because of the law system. The similar needs may emerge for the countries that resemble Turkey in terms of law system and critical infrastructure ownerships.

Table 5-4 summarizes six critical sectors of Turkey in terms of ownership status, the existence of regulatory authority, and the existence of cyber security regulations. It is seen that the sectors that are dominated by private operators are the most thoroughly-regulated critical sectors in Turkey. These sectors have regulatory authorities as well. The critical sectors that are dominated by the government have neither cyber security regulations nor associated regulatory authorities. Therefore, it can be stated that the private sector in Turkey is controlled by regulatory authorities in a strict manner.

The telecommunications and finance sectors have the most complete, mature and oldest regulations for information security and cyber security. The data analysis process of this PhD thesis showed that there was a salient supremacy and maturity of the cyber security practices in finance and telecommunications sectors compared to the other "government-dominated" ones.

Table 5-4: Summary of the Critical Sectors

Critical Sector	Prominent Ownership	Has Regulatory authority?	Has cyber security regulation?
Energy	Government / Private sector	Yes	Limited
Telecommunications	Private sector	Yes	Comprehensive
Finance	Private sector	Yes	Comprehensive
Transportation	Government	No	No
Water management	Government	No	No
Government services	Government	No	Limited

At first sight, the main problem of the Turkey can be regarded as the normlessness or deregulation of the certain sectors like energy, transportation, water management, and government services. As Turkey has a civil law system, written regulations can be considered as imperatives to ensure an acceptable level of cyber security practices within these sectors. However, as stated in section 4.1.6 where the findings of the first phase of research were shared:

1) Independent of the sectors, private organizations are more mature compared to the governmental organizations. The most of the extracted root causes are mainly associated with the governmental organizations.
2) The security maturity of a sector does not mainly originate from the sectorial security practices. A governmental operator in the finance sector had poor security practices. A private operator in energy sector had state-of-the art security practices.

As a result, if a sector is dominated by the private organizations, the general security posture of the sector is more mature; and vice versa. Therefore, cyber security problems may not originate from the missing cyber security practices in certain sectors; cyber security problems may rather be associated with the type of organization (government or private). Therefore, the organizational dynamics like security culture and human factors may be more effective for the improvement of security.

In the data analysis of the PhD study, most of interviewees also emphasized the prominence of the establishment of a security culture instead of enacting rules and regulations for the cyber security of the infrastructures.

The focus on the rules and regulations was more obvious in the Delphi survey. Security experts agreed on the following rules and regulations.

a) Critical review and update of the existing legislation that may affect critical infrastructures (especially for the needs of the governmental critical infrastructure operators)
b) Making amendments to the regulations to hire outsourced personnel / qualified government officials with higher salaries / contracted personnel in governmental critical infrastructures
c) National or sectorial regulations that enforce the internal / external audit for critical infrastructure operators
d) Sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities
e) Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners

f) Minimum security countermeasures that are obliged by regulations for critical infrastructure owners
g) Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators

The experts agreed on the following principles that can be considered as a part of the establishment of a security culture rather than emphasizing regulations.

a) The existence of a consultant who provides technical, regulatory and diplomatic cyber security consultancy for the head of the state
b) A CSIRT organization dedicated to the protection of critical infrastructures
c) Nation-wide risk analysis and risk management activities which cover all critical sectors / sector-wide wide risk analysis and risk management activities
d) A public-private partnership program which is developed and supported by the government
e) The existence of an internationally recognized National CSIRT that performs international cooperation with other CSIRTs
f) A technical infrastructure to fulfill the inner - inter sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers)
g) A National CSIRT that handles the warnings of cyber incidents related to critical infrastructures by coordinating with the relevant sectorial CSIRTs and critical infrastructure owners when needed
h) Government policies and strategies that position private sector as a key player in national cyber security efforts
i) The participation of the private sector in the preparation of the national or sectorial cyber security strategies
j) Permanent seat for the private sector in the national boards like the cyber security council
k) Government leadership for innovation, research & development activities, and the identification of the priority areas in cyber security by the government
l) The extensive participation of the private sector in the national cyber security exercises
m) National capacity building plans and strategies
n) Preference of the internationally accepted certificate owners in the recruitments by critical infrastructure owners
o) Qualified and sufficient number of cyber security training institutions (private, academic or governmental) that support/train the personnel of critical infrastructure operators
p) Cyber security and IT curriculum for all levels of the education, from elementary schools to universities
q) Special positions for cyber security experts in critical infrastructure operators

It is important to note that, the number of the principles related with the regulations is less than the number of the above-mentioned principles which are related with the security culture. The opinions of the interviewees and experts can be summarized as follows:

i. Regulations can be considered as an important gadget for the improvement in security.
ii. However, security cannot be ensured just by regulations and rules.

iii. The incentives like cooperation, innovation, information sharing, and security culture should be taken into account while considering the regulations for critical infrastructures.

By taking the findings of the PhD research and the sectorial situation of Turkey into account, a hybrid CIP model can be adapted for Turkey. In this model, the enforcement of the incentives like cooperation, innovation, information sharing can be flourished by using regulations. This is what cyber security experts may imply in the Delphi survey. As an example, the following four principles combine regulation and security culture together.

a) Regulations that specify the inner - inter sector information sharing and cooperation principles
b) Sector based CSIRTs that have information sharing responsibilities determined by the regulations
c) Regulations that render top level management of critical infrastructure operators responsible for cyber security
d) Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process

It will not be wrong to say that regulations are the means of applying countermeasures of different kinds. However, it is important to find the answer for the question: "how to apply regulations?" Section 5.5.2 explains the details of future research topic.

5.5 Implications for Future Research

In this section, future research topics that originate from the PhD study are written. First research topic is about the modeling of the interdependencies that may exist among root causes. The second research topic is the specification of the regulation options. The third research topic is the development of a more comprehensive maturity model for measuring the national cyber security.

5.5.1 Modeling Interdependencies among Root Causes

There are some certain dependencies among the root causes. As an example, the participation of private sector in national cyber security efforts depends on the perception of the government of national cyber security. Some of the dependencies could be extracted from the data; however, there was not enough data in this research to extract the all dependencies among the root causes. Figure 5-1 shows the chart that show dependencies among the extracted root causes, which were determined by using the data analysis. It is important to note that the dependencies shown by dashed lines are not the certain and definite results of the data analysis. No dependencies were extracted from the data for the root causes 2 and 8. It should be noted that there might be more dependencies among root causes than the dependencies shown in the Figure 5-1.

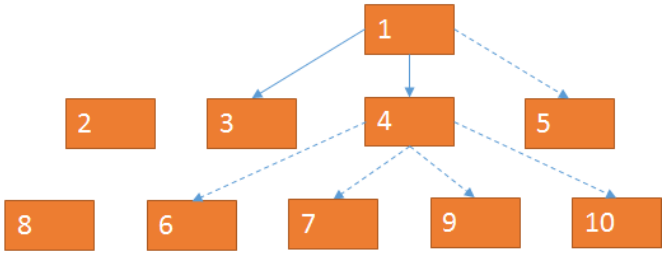


Figure 5-1: Ad-hoc Dependencies among the Root Causes

A new research can be performed to determine and model the dependencies among the root causes. However, this research will definitely necessitate to contact with the organizations to gather new data.

After the identification of the possible dependencies, the maturity model may be updated by adding a coefficient that represents the dependency. The more root causes are depended on a specific root cause, the larger weight values are assigned to the principles associated with that root cause. For example, three root causes are directly dependent on the root cause-1 and four root causes indirectly depends on the same root cause through root cause-4, a coefficient can be added to the maturity formula that augments the weights of the principles associated with the root cause-1.

5.5.2 Determining the Options for Regulations

Before detailing the future research topic, the list of principles that were related with regulations are given below:

a) Critical review and update of the existing legislation that may affect critical infrastructures (especially for the needs of the governmental critical infrastructure operators)
b) Making amendments to the regulations to hire outsourced personnel / qualified government officials with higher salaries / contracted personnel in governmental critical infrastructures
c) National or sectorial regulations that enforce the internal / external audit for critical infrastructure operators
d) Sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities
e) Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners
f) Minimum security countermeasures that are obliged by regulations for critical infrastructure owners
g) Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators
h) Regulations that specify the inner - inter sector information sharing and cooperation principles
i) Sector based CSIRTs that have information sharing responsibilities determined by the regulations
j) Regulations that render top level management of critical infrastructure operators responsible for cyber security
k) Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process

The question of how to apply these principles is the topic of the future research. When the regulations are taken into account, two approaches come to the forefront for the cyber security management of the critical infrastructures. These are:

1. Pure government/state provision of CIP
2. Pure market provision of CIP (Assaf 2008)

According to the government provision, regulations are imperative for the security of the infrastructures. Government provision is mostly supported by the national security officials and some academics. In market provision, regulations are seen as obstacles in front of innovation and cooperation. Market provisions are mostly demanded by the private sector owners. Government ownership is the most interventionist approach for the management of the critical infrastructures, whereas market is less interventionist (Assaf 2008).

It would be wrong to say that one approach is wrong and the other is right. Countries have different legislative infrastructures and organizational structures. The proportion of the private sector ownership of CI is different among countries as well. Countries may adopt different approaches according to their unique features.

Another important point is that there are more than two approaches for the cyber security management of the critical infrastructures. In fact, pure state provision and pure market provision are the two extreme points of a management scale. There are many grey areas in between. The following seven approaches can be listed as a regulatory continuum of critical infrastructures (Assaf 2008):

1. Government ownership
2. Command and control
3. Delegation to agency
4. Delegation to agency and negotiation
5. Enforced self-regulation
6. Voluntary self-regulation
7. Market

The decision on how to regulate critical infrastructures depends on the regulatory, organizational, and cultural aspects of the country. A future research on the cyber security regulation options of critical infrastructures will be planned. A focus group interview will be performed by the experts in different sectors. The following questions are planned to be answered by this research by taking the set of principles into account:

a) Which approaches are suitable for the governmental critical infrastructure operators?
b) Which approaches are suitable for the private critical infrastructure operators?
c) Are there differences/similarities between government and private infrastructures?
d) Are there differences/similarities among sectors?

The outputs of the research may also be useful for the developing countries that have similar regulatory and organizational infrastructures with Turkey.

5.5.3 Comprehensive Maturity Models

Information security is a mature domain for the organizations. It was already adapted by the organizations when most systems were standalone. There are a number of internationally recognized standards, frameworks, maturity models for information security that have been used for years (ISO/IEC 2013a; ISO/IEC 2013b; ISO/IEC 2010; ISO/IEC 2009; ISO/IEC 2008). As the organizations depended more on information technologies and these technologies were connected to the Internet, cyber security became a concern for organizations. Nevertheless, cyber security can be regarded as a subdomain of information

security from an organizational perspective (Wamala 2011), because the assets that have to be protected are the same for cyber security. The difference is the source of the threats in the context of cyber security. Cyber security is the prevention from the harm of cyber threats that come mostly from the Internet. Hence, information security standards, frameworks and models are also applicable to cyber security in the organizational context.

On contrary to organizational level, cyber security is a challenging domain for the countries. It has a number of dimensions –containing unresolved ones- at this level (Wamala 2011). There are a number of different types of domains that intersects with cyber security at the national level. The list includes but not limited to national security, counter espionage, organizational structures, legislative frameworks, privacy, and critical infrastructure protection.

The measurement is a mature topic in information security domain as well. The ninth chapter of ISO 27001 information security management standard is dedicated to the performance evaluation in which monitoring, measurement, analysis, evaluation, internal audit, and management review functions are described. There are a number of maturity assessment studies based on the standards in the academia (Susanto et al. 2012; Shamsaei et al. 2011).

From this point of view, two improvements on the proposed model can be studied in the future research. Firstly, a sectorial cyber security maturity model that makes use of the single maturity levels of critical infrastructure operators can be developed. This research implies the research on the organizational level maturity measurement as well. Nationwide Cyber Security Review of United States assesses the current security posture of one hundred and sixty-two agencies by using a questionnaire (DHS 2012). However, it does not convert the results of the questionnaire to a maturity value for the organizations. In this research, the following two questions will be answered.

a) How can the maturity level of each critical infrastructure owner be mathematically calculated?
b) How can the maturity level of the critical sector be calculated by using the individual maturity levels of the critical infrastructure owners?

The maturity criteria of the proposed model were the set of state-level principles. Instead of the measurement of the state level maturity by using predefined set of principles, it will be measured from a number of organizational maturity levels. This is in fact not an improvement in the proposed model; this is a completely different approach.

The other future research is again related with the maturity assessment. A process based maturity model may be developed to assess the national or sectorial level cyber security. The proposed maturity model may check not only the existence of a national/sectorial-level countermeasure but also its details of implementation based on the at least five level maturity scale as in the CoBIT framework (ISACA 2012). In the proposed model, the completion level of each principle was checked by using three possibilities; No action or very limited action, Partial Action, and Comprehensive Action. The maturity level was represented as percentage value. With this future work, the maturity level of each principle may be represented separately in a scale of at least five levels. The improved model may help the state representatives in assessing current cyber security posture more thoroughly.

REFERENCES

Abou El Kalam, A. et al., 2009. PolyOrBAC: A security framework for Critical Infrastructures. *International Journal of Critical Infrastructure Protection*, 2(4), pp.154–169.

Adami, M.F. & Kiger, A., 2005. The use of triangulation for completeness purposes. *Nurse Researcher*, 12(4), pp.19–29.

Adar, E. & Wuchner, A., 2005. Risk Management for Critical Infrastructure Protection (CIP) Challenges, Best Practices & Tools. *First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05)*, pp.90–100.

Adler, R.M., 2013. A dynamic capability maturity model for improving cyber security. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, pp.230–235.

Adler, R.M. & Fuller, J., 2007. An Integrated Framework for Assessing and Mitigating Risks to Maritime Critical Infrastructure. In *2007 IEEE Conference on Technologies for Homeland Security*. Woburn: IEEE, pp. 252–257.

Alcaraz, C. & Zeadally, S., 2015. Critical infrastructure protection : Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, pp.53–66. Available at: http://dx.doi.org/10.1016/j.ijcip.2014.12.002.

Andress, J. & Winterfeld, S., 2013. *Cyber warfare: Techniques, Tactics and Tools for Security Practitioners*, Elsevier.

Apostolakis, G.E. & Lemon, D.M., 2005. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk analysis : an official publication of the Society for Risk Analysis*, 25(2), pp.361–76.

Assaf, D., 2008. Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection*, 1(December), pp.6–14.

BAH, 2011. *Cyber Power Index: Findings and Methodology*, Available at: http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf.

Baiardi, F., Telmon, C. & Sgandurra, D., 2009. Hierarchical, model-based risk management of critical infrastructures. *Reliability Engineering & System Safety*, 94(9), pp.1403–1415.

Bencsáth, B. & Pek, G., 2012. Duqu: Analysis, detection, and lessons learned. In *ACM European Workshop on System Security (EuroSec)*.

BOTAS, 2015. About BOTAS. Available at: http://www.botas.gov.tr/index.asp [Accessed June 7, 2015].

BRSA, 2010. *The Statute on the Audit of Information Systems and Business Processes of Banks by Independent Auditors*, Turkey. Available at: http://www.resmigazete.gov.tr/eskiler/2010/01/20100113-4.htm.

BRSA, 2007. *The Statute on the Principles of the Information Security Management of the Banks*, Turkey. Available at: http://www.resmigazete.gov.tr/eskiler/2007/09/20070914-1.htm.

De Bruijne, M. & van Eeten, M., 2007. Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, 15(1), pp.18–29.

Butkovic, M.J. & Caralli, R.A., 2013. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale*, Pittsburgh.

Chan, A.P.C. et al., 2001. Application of Delphi method in selection of procurement systems for construction projects Application of Delphi method in selection of procurement systems for construction projects. *Construction Management and Economics*, 19(7), pp.699–718.

Charmaz, K., 2000. Grounded Theory: Objectivist and Constructivist Methods. In N. K. Denzin & Y. S. Lincoln, eds. *Handbook of qualitative research*. Sage Publications, pp. 509–535.

Cichonski, P. et al., 2012. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Gaither.

Colwill, C., 2009. Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, 14(4), pp.186–196. Available at: http://dx.doi.org/10.1016/j.istr.2010.04.004.

Condron, S.M., 2007. Getting It Right: Protecting American Critical Infrastructure In Cyberspace. *Harvard Journal of Law & Technology*, 20, pp.403–422.

Cook, D.M., 2010. Mitigating Cyber-Threats Through Public-Private Partnerships : Low Cost Governance with High- Impact Returns. In *Proceedings of the 1st International Cyber Resilience Conference*. Perth Western Australia, pp. 22–30.

Coyne, I.T., Dipn, H. & Rgn, R., 1997. Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing*, 26(3), pp.623–630.

Creswell, J.W., 2012. *Qualitative Inquiry & Research Design: Choosing Among Five Approaches* Third Edit., SAGE Publications.

Crowther, K.G., 2008. Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input–output model. *International Journal of Critical Infrastructure Protection*, 1(C), pp.53–67.

CSI, 2013. National Cyber Security Strategy and Action Plan. Available at: http://sge.bilgem.tubitak.gov.tr/tr/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani [Accessed March 30, 2015].

Dalkey, N. & Helmer, O., 1962. *An Experimental Application of the Delphi Method to the Use of Experts*, Santa Monica.

Denscombe, M., 2010. *The good research guide for small-scale social research projects* 4th ed., Open University Press.

DHA, 2014. Redhack: Hackledik... Enerji Bakanlığı: Tahsil ettik, bilgi kaybı yok. *Hurriyet*. Available at: http://www.hurriyet.com.tr/ekonomi/27582889.asp [Accessed April 21, 2015].

DHS, 2012. *2011 Nationwide Cyber Security Review: Summary Report*, Washington.

DHS, 2014. *Cybersecurity Capability Maturity Model White Paper*, Washington.

DHS, 2013. *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience*, Available at: http://www.dhs.gov/sites/default/files/publications/NIPP 2013_Partnering for Critical Infrastructure Security and Resilience_508_0.pdf.

DHS, 2005. *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*, US. Available at: http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf.

DoD, 2011. *Strategy for Operating in Cyberspace*, Washington. Available at: http://www.defense.gov/news/d20110714cyber.pdf.

Dunn-Cavelty, M. & Suter, M., 2009. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4), pp.179–187.

EMRA, 2014a. *The License Statute of Electricity Market*, Turkey. Available at: http://www.epdk.org.tr/documents/elektrik/mevzuat/yonetmelik/elektrik/lisans/Elk_Ynt_Lisans_Son_Hali1.doc.

EMRA, 2014b. *The License Statute of Natural Gas Market*, Turkey. Available at: http://www.epdk.org.tr/documents/dogalgaz/mevzuat/yonetmelik/dogalgaz/lisans/Dpd_Ynt_lisans_Son_Hali_19032015.doc.

EMRA, 2014c. *The License Statute of Petroleum Market*, Turkey. Available at: http://www.epdk.org.tr/documents/petrol/mevzuat/yonetmelik/petrol/lisans/PPD_YNT_Lisans_Son_190220151.docx.

Eshlaghy, A.T. & Pourebrahimi, A., 2011. Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity. *Computer and Information Science*, 4(1), pp.72–79.

EUAS, 2015. About EUAS, The Leader in Electricity Production. Available at: http://www.euas.gov.tr/Sayfalar/Hakkimizda.aspx [Accessed June 3, 2015].

European Commission, 2013a. *Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

European Commission, 2013b. Proposed Directive on Network and Information Security – frequently asked questions. Available at: http://europa.eu/rapid/press-release_MEMO-13-71_en.htm [Accessed June 9, 2015].

European Council, 2001. *Convention on Cybercrime*, Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Eusgeld, I. et al., 2009. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering & System Safety*, 94(5), pp.954–963.

Eusgeld, I., Nan, C. & Dietz, S., 2011. "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6), pp.679–686.

Farwell, J.P. & Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*, 53(1), pp.23–40.

Fernández, W.D. & Lehmann, H., 2011. Case Studies and Grounded Theory Method in Information Systems Research : Issues and Use. *Journal of Information Technology Case and Application Research*, 13(1), pp.4–15.

Flammini, F., Gaglione, A. & Mazzocca, N., 2008. Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. In *3rd International Workshop on Critical Information Infrastructure Protection*. Rome, pp. 180–189.

Glaser, B. & Strauss, A., 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Chicago: Aldine Publishing Company.

Goldman, K. & Valdez, E., 2004. Matchbox: secure data sharing. *IEEE Internet Computing*, (November-December), pp.18–24.

Goulding, C., 2002. *Grounded Theory: A Practical Guide for Management, Business and Market Researchers*, SAGE Publications Ltd.

Haimes, Y.Y. et al., 2002. *A Risk Assessment Methodology for Critical Transportation Infrastructure*, Richmond.

Hansen, B.H. & Kautz, K., 2005. Grounded Theory Applied - Studying Information Systems Development Methodologies in Practice. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*. Hawaii: IEEE, p. 264b.

Harrop, W. & Matteson, A., 2013. Cyber resilience : A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. *Journal of Business Continuity & Emergency Planning*, 7(1), pp.149–162.

Hathaway, M.E., 2013. *Cyber Readiness Index 1.0*, Cambridge.

Healey, J. & Pitts, H., 2012. Applying International Environmental Legal Norms to Cyber Statecraft. *I/S: A Journal of Law and Policy for the Information Society*.

Hiller, J.S. & Russell, R.S., 2013. The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law and Security Review*, 29(3), pp.236–245.

Hinde, S., 1998. Cyber wars and other threats. *Computers & Security*, 17(2), pp.115–118.

Hsu, C. & Sandford, B., 2007. The delphi technique: making sense of consensus. *Practical Assessment, Research & Evaluation*, 12(10), pp.1–8.

ICTA, 2014. *Statute of Network and Information Security in Telecommunications Sector*, Turkey. Available at: http://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm.

ICTA & TUBITAK, 2011. *National cyber security exercise 2011 final report*, Ankara.

Igure, V.M., Laughter, S. a. & Williams, R.D., 2006. Security issues in SCADA networks. *Computers & Security*, 25(7), pp.498–506.

Ikitemur, G., 2014. *Enhancing Cyber Security in Turkey Through Effective Public and Private Cooperation*. The University of Texas at Dallas.

ISACA, 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, Rolling Meadows.

ISO/IEC, 2013a. *ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements*, Geneva.

ISO/IEC, 2013b. *ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls*, Geneva.

ISO/IEC, 2010. *ISO/IEC 27003 Information technology — Security techniques — Information security management system implementation guidance*, Geneva.

ISO/IEC, 2009. *ISO/IEC 27004 Information technology — Security techniques — Information security management — Measurement*, Geneva.

ISO/IEC, 2008. *ISO/IEC 27005 Information technology — Security techniques — Information security risk management*, Geneva.

ITU, 2007. *Global Cybersecurity Agenda*, Available at: http://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf.

ITU, 2014. *International Telecommunication Union: Global Cybersecurity Index Conceptual Framework*,

ITU, 2009. *ITU National Cybersecurity/ CIIP Self-Assessment Tool*, Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf.

Jayawickrama, W., 2006. Managing Critical Information Infrastructure Security Compliance : A Standard Based Approach Using ISO/IEC 17799 and 27001. In R. Meersman, Z. Tari, & P. Herrero, eds. *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*. Montpellier: Lecture Notes in Computer Science, pp. 565–574.

Johansson, J. & Hassel, H., 2010. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering & System Safety*, 95(12), pp.1335–1344.

Jones, M. & Alony, I., 2011. Guiding the use of grounded theory in doctoral studies - An example from the australian film industry. *International Journal of Doctoral Studies*, 6, pp.95–114.

Kahn, L., 2013. Understanding Just Cause in Cyberwarfare. In F. Allhoff, N. G. Evans, & A. Henschk, eds. *Handbook of Ethics and War: Just War Theory in the Twenty-First Century*. Routledge, pp. 382–391.

Kaplan, B. & Duchon, D., 1988. Combining Qualitative and Quantitative Methods in Information Systems: A Case Study. *MIS Quarterly*, 12(4), pp.571–586.

Karabacak, B. & Ozkan, S., 2010. A Collaborative Process Based Risk Analysis for Information Security Management Systems. In E. L. Armistead, ed. *The Proceedings of the 5th International Conference on Information Warfare and Security*. Dayton: Academic Publishing Limited, pp. 182–192.

Karokola, G., Kowalski, S. & Yngström, L., 2011. Towards An Information Security Maturity Model for Secure e-Government Services : A Stakeholders View. *Proceedings of the 5th HAISA2011 Conference, London, UK*, pp.58–73.

Kaska, K. & Trinberg, L., 2015. *Regulating Cross-Border Dependencies of Critical Information Infrastructure*, Tallinn.

Kelly, B.B., 2012. Investing in a centralized cybersecurity infrastructure: why "hacktivism" can and should influence cybersecurity reform. *Boston University Law Review*, (1), pp.1663–1711.

Kelly, T. & Hunker, J., 2012. Cyber Policy : Institutional Struggle in a Transformed World. *I/S: A Journal of Law and Policy for the Information Society*, 8(2), pp.210–242.

Kettani, M.D.E.-C. El & Debbagh, T., 2009. NCSecMM: A National Cyber Security Maturity Model for an Interoperable "National Cyber Security" Framework. In D. Remenyi, ed. *9th European Conference on e-Government*. London: Academic Publishing Limited, pp. 236–247.

Kjølle, G.H., Utne, I.B. & Gjerde, O., 2012. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety*, 105(September), pp.80–89.

Klimburg, A. ed., 2012. *National Cyber Security Framework Manual*, Tallinn: NATO CCD COE Publication.

Kshetri, N., 2005. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11(4), pp.541–562.

Langner, R., 2011. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, 9(3), pp.49–51.

Laudon, K.C. & Laudon, J.P., 2015. *Management Information Systems: Managing the Digital Firm* 14th ed., Prentice Hall.

Lessing, M.M., 2008. Best practices show the way to Information Security Maturity. *6th National Conference on Process Establishment, Assessment and Improvement in Information Technology (ImproveIT 2008)*, pp.1–9.

Lewis, J.A., 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*, pp.1–12.

Lin, H., 2012. Thoughts on Threat Assessment in Cyberspace. *I/S: A Journal of Law and Policy for the Information Society*.

Little, R.G., 2002. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. *Journal of Urban Technology*, 9, pp.109–123.

Locke, K., 1996. Rewriting the discovery of grounded theory after 25 years? *Journal of Management Inquiry*, 5(3), pp.239–245.

Lopez, J., Alcaraz, C. & Roman, R., 2007. On the Protection and Technologies of Critical Information Infrastructures. In A. Aldini & R. Gorrieri, eds. *6th International School on Foundations of Security Analysis and Design*. Bertinoro, pp. 160–182.

Luiijf, E. a. M. & Klaver, M.H. a., 2004. Protecting a nation's critical infrastructure: the first steps. In *2004 IEEE International Conference on Systems, Man and Cybernetics*. pp. 1185–1190.

Luiijf, E., Ali, M. & Zielstra, A., 2011. Assessing and improving SCADA security in the Dutch drinking water sector. *International Journal of Critical Infrastructure Protection*, 4(3-4), pp.124–134.

Malterud, K., 2001. Qualitative research: Standards, challenges, and guidelines. *The Lancet*, 358(9280), pp.483–488.

Mandiant, 2013. *APT1: Exposing One of China's Cyber Espionage Units*, Available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Matavire, R. et al., 2010. Factors Affecting the Success of e-Government in a South African Context: a Grounded Theory Approach. *International Conference on Information Management & Evaluation*, pp.207–217.

Melvin, D., 2015. Power outage hits much of Turkey; officials won't rule out terrorism. *CNN*. Available at: http://edition.cnn.com/2015/03/31/middleeast/turkey-power-outage/ [Accessed April 21, 2015].

Michaud, D., 2005. *Risk Analysis of Infrastructure Systems: Screening Vulnerabilities in Water Supply Networks*.

Ministry of Development, 2013. *Bilgi Toplumu Stratejisinin Yenilenmesi Projesi: İhtiyaç Tespiti ve Öneriler Raporu*, Ankara.

Ministry of Telecommunications, 2013. *National Cyber Security Strategy and 2013-2014 Action Plan*, Available at: https://ccdcoe.org/sites/default/files/strategy/TUR_CyberSecurityEng.pdf.

Ministry of Telecommunications, 2014. *Ulusal Siber Güvenlik Çalışmaları*, Ankara.

Miron, W. & Muita, K., 2014. Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review*, (October), pp.33–39.

NATO CCDCOE, 2015. Cyber Security Strategy Documents. Available at: https://ccdcoe.org/strategies-policies.html [Accessed April 4, 2015].

Nicholson, a. et al., 2012. SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4), pp.418–436.

NIST, 2014. *Framework for Improving Critical Infrastructure Cybersecurity*, Gaithersburg.

OECD, 2007a. *Development of Policies for Protection of Critical Information Infrastructures*,

OECD, 2013. OECD Data. Available at: https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm [Accessed March 30, 2015].

OECD, 2007b. *OECD e-Government Studies: Turkey*, Paris.

Okoli, C. & Pawlowski, S.D., 2004. The Delphi method as a research tool: an example, design considerations and applications. *Information & Management*, 42(1), pp.15–29.

Orlikowski, W.J., 2002. Knowing in practice: Enacting a collective capability in distributed organizing. *Organization Science*, 13(3), pp.249 – 273.

Orlowski, S., 2001. Information management: Protecting critical information assets. *Computer Law and Security Report*, 17(3), pp.182–185.

Ottis, R., 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In *Proceedings of the 7th European Conference on Information Warfare*.

Ozkan, S. & Karabacak, B., 2010. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management*, 30, pp.567–572.

Peltier, T.R., Peltier, J. & Blackley, J.A., 2005. *Information Security Fundamentals*, CRC Press.

Perlroth, N., 2012. Researchers Find Clues in Malware. *New York Times*. Available at: http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html?_r=0 [Accessed June 1, 2015].

Prichard, J.J. & MacDonald, L.E., 2004. Cyber terrorism: A study of the extent of coverage in computer Security Textbooks. *Journal of Information Technology Education*, 3, pp.279–289.

Rak, A., 2002. Information Sharing in the Cyber Age : a Key to Critical Infrastructure Protection. *Information Security Technical Report*, 7(2), pp.50–56.

Reiter, M. & Rohatgi, P., 2004. Homeland Security. *IEEE Internet Computing*, (November-December), pp.16–17.

Republic of Turkey, 1965. *Civil Servants Law*, Turkey. Available at: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.657.pdf.

Rinaldi, B.S.M., Peerenboom, J.P. & Kelly, T.K., 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, (December), pp.11–25.

Robertson, J. & Riley, M.A., 2014. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. Available at: http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar [Accessed May 22, 2015].

Rodon, J. & Pastor, J. a, 2007. Applying Grounded Theory to Study the Implementation of an Inter-Organizational Information System. *Electronic Journal of Business Research methods*, 5(2), pp.71–82.

Sandelowski, M. & Barroso, J., 2002. Reading Qualitative Studies. *International Journal of Qualitative Methods*, 1(1).

Sanger, D.E., 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times*. Available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 [Accessed June 7, 2015].

Senturk, H., Cil, Z. & Sagiroglu, S., 2013. Cyber Security Analysis of Turkey. *International Journal of Information Security Science*, 1(4), pp.112–125.

Shamsaei, A., Amyot, D. & Pourshadid, A., 2011. A Systematic Review of Compliance Measurement Based on Goals and Indicators. In C. Salinesi & O. Pastor, eds. *CAiSE 2011 Workshops*. pp. 228–237.

Shannak, R.O., 2009. Grounded Theory as a Methodology for Theory Generation in Information Systems Research. *European Journal of Economics, Finance and Administrative Sciences*, 15(15), pp.32–50.

Von Solms, B. & Von Solms, R., 2005. From information security to...business security? *Computers and Security*, 24(4), pp.271–273.

Solms, B. Von & Solms, R. Von, 2004. The 10 deadly sins of information security management. *Computers & Security&*, 23, pp.371–376.

Von Solms, R. & (Basie) von Solms, S.H., 2006. Information Security Governance: A model based on the Direct-Control Cycle. *Computers and Security*, 25(6), pp.408–412.

Von Solms, R. & von Solms, S.H. (Basie), 2006. Information security governance: Due care. *Computers & Security*, 25(7), pp.494–497.

Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems*,

Strauss, A. & Corbin, J., 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, SAGE Publications.

Susanto, H., Almunawar, M.N. & Tuan, Y.C., 2012. A Novel Method on ISO 27001 Reviews: ISMS Compliance Readiness Level Measurement. *Computer Science Journal*, 2(1).

Svendsen, N.K. & Wolthusen, S.D., 2007. Connectivity models of interdependency in mixed-type critical infrastructure networks. *Information Security Technical Report*, 12(1), pp.44–55.

Tatar, U. et al., 2014. A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. In S. Liles, ed. *Proceedings of the 9th International Conference on Cyber Warfare and Security*. West Lafayette: Academic Conferences and Publishing International Limited, pp. 211–218.

TEDAS, 2015. About TEDAS. Available at: http://www.tedas.gov.tr/Sayfalar/Hakkimizda.aspx [Accessed June 5, 2015].

TEIAS, 2015. About TEIAS. Available at: http://www.teias.gov.tr/Hakkimizda.aspx [Accessed June 5, 2015].

Ten, C.-W., 2008. Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions On Power Systems*, 23(4), pp.1836–1846.

Thai, M.T.T., Chong, L.C. & Agrawal, N.M., 2012. Straussian Grounded-Theory Method: An Illustration. *The Qualitative Report*, 17(52), pp.1–55.

The White House, 1996. *Executive Order 13010 - Critical Infrastructure Protection*, USA: The White House.

The White House, 2013a. *Executive Order 13636—Improving Critical Infrastructure Cybersecurity*, USA: The White House.

The White House, 2013b. *Presidential Policy Directive /PPD-21, Critical Infrastructure Security and Resilience*, USA: The White House.

Tobias Feakin & Woodall, J., 2014. *Cyber Maturity in the Asia-Pasific Region 2014: Creating a Regional Cyber Maturity Metric*, Barton.

TP, 2015. About TPAO, Production. Available at: http://www.tpao.gov.tr/tp5/?tp=m&id=79 [Accessed June 5, 2015].

TR-CERT, 2015. Cyber Threat List. Available at: https://www.usom.gov.tr/tehdit.html [Accessed March 30, 2015].

TUPRAS, 2015. About, Refineries. Available at: http://www.tupras.com.tr/detailpage.tr.php?lPageID=831 [Accessed June 5, 2015].

Turk Telekom, 2015. About Türk Telekom. Available at: http://www.turktelekom.com.tr/tt/portal/TTHakkinda/KurumsalTanitim/Hakkinda [Accessed June 5, 2015].

Turkish Cabinet, 2014. *Aile ve sosyal politikalar bakanlığının teşkilat ve görevleri hakkında kanun hükmünde kararname ile bazı kanun ve kanun hükmünde kararnamelerde değişiklik yapılmasına dair kanun*, Turkey. Available at: http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.

Turkish Cabinet, 2011. *Regulation Amending the Regulation on Military Forbidden Zones and Security Zones*, Turkey. Available at: http://www.resmigazete.gov.tr/eskiler/2011/10/20111018-4.htm.

Turkish Cabinet, 2012. *Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar*, Turkey. Available at: http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm.

Turkish Presidency, 2013. *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*, Ankara.

USA, 2001. *USA Patriot Act*, USA. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

USCESRC, 2008. *USCC 2008 ANNUAL REPORT*, Available at: http://origin.www.uscc.gov/sites/default/files/annual_reports/2008-Report-to-Congress-_0.pdf.

US-GAO, 2013. *CRITICAL INFRASTRUCTURE PROTECTION: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, Washington.

Wamala, F., 2011. *ITU National Cybersecurity Strategy Guide*, Geneva.

Weiss, J., 2010. *Protecting Industrial Control Systems from Electronic Threats* First Edit., New York: Momentum Press.

White, G.B., 2012. A Grassroots Cyber Security Program to Protect the Nation. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. IEEE Computer Society, pp. 2330–2337.

White, G.B., 2011. The Community Cyber Security Maturity Model. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*. Waltham: IEEE, pp. 173–178.

Wiki, 2015a. Cyber Security Regulation. Available at: https://en.wikipedia.org/wiki/Cyber-security_regulation [Accessed June 14, 2015].

Wiki, 2015b. Türkiye'deki Bankaların Listesi. Available at: http://tr.wikipedia.org/wiki/T%C3%BCrkiye%27deki_bankalar_listesi [Accessed June 4, 2015].

Wilson, N., 2014. Australia's National Broadband Network – A cybersecure critical infrastructure? *Computer Law & Security Review*, 30(6), pp.699–709.

Woodhouse, S., 2007. Information Security: End User Behavior and Corporate Culture. *7th IEEE International Conference on Computer and Information Technology (CIT 2007)*, pp.767–772.

Young, M.D., 2012. United States Government Cybersecurity Relationships. *I/S: A Journal of Law and Policy for the Information Society*.

APPENDICES

Appendix A: Details of the Delphi Survey

The forms shown in Appendix A were sent to six experts separately by e-mail.

Round-1: Input

Held between 2012 and 2013, the project of "Information Security Management in Critical Infrastructures" aimed the determination of the dependency of the critical infrastructures of Turkey on information technologies, the diagnosis of the risks that result from the usage of information technologies and the identification of the required countermeasures for the reduction and termination of the risks. The project demonstrated that the critical infrastructures of Turkey were not resilient against cyber threats. The leading root causes were explained through the scientific method of qualitative data analysis. Ten root causes are detailed in the table below.

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.[1, 2]	
The number of qualified cyber security experts is limited.	
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.[3]	
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.[4]	
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	

[1] Many critical infrastructure operators uttered the following sentences: "We cannot have the qualified personnel within our organization for a long time", "We cannot pay higher salaries for them.

[2] Many critical structure operators said that they cannot purchase the products they want to and they have to be content with the unqualified products of the unqualified bidding companies.

[3] All critical infrastructure operators receive considerable amounts of services in the private sector but there have been no serious regulations pertaining to the cyber security rules to be obeyed before, during and after the reception of the services.(on country-wide, sectorial and institutional bases.) This situation also applies to the products sold. For instance, it is a very common case when the contractor firm with full authority can connect to the SCADA network of the critical infrastructure operator within the scope of warranty service, which is, as a practice, bound by no rules and logging mechanisms.

[4] The IT department owns the responsibility. And the aspects of a possible damage to be caused by the cyber threats cannot be seriously assessed and the necessary precautions cannot be taken in time.

Root causes of susceptibility to cyber threats	The set of principles
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	

A cyber security maturity model is to be designed on the cyber security principles which are derived from the root causes stated in the table above.

You are requested to suggest principles (ranging from one to three in number for each) for every root cause. The points that require attention are listed below.

1. The principle may indicate that a root cause doesn't exist or is not experienced in a country. (If the principle exists in a country, its root cause must also be nonexistent)
2. The principle may be a countermeasure that eliminates the root cause or a statistical parameter. It may cover a range of subjects that extend from legal measures and processes to organizational structures and budgets.
3. Please set at least one and at most three principles for each root cause.

Principles are the possible answers to the following kind of questions:

- Which principles in a country show that cyber security is internalized by that country?
- Which principles in a country show that cyber security is a self-sustaining effort at that country?
- Which principles in a country show that cyber security is positioned as an inseparable part of the national security by the government?

Round-1: Output

Expert-1

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Kritik altyapı sektörlerine yönelik siber güvenlik önlemlerini almaya zorlayıcı ve denetleyici mevzuat yok. Sadece bankacılık sektörü için BDDK nın kısıtlı regülasyonları var, onlar da uluslararası PCI standartları ile uyumluluk zorunluluğundan kaynaklandığını düşünüyorum. Kritik altyapıları düzenlemekten sorumlu üst kurullar (epdk, bddk v.s.) siber güvenlik konusunda yetkin değil, bünyelerinde siber güvenlikten anlayan personel bulunmuyor. Bulundurma konusunda da bir irade bulunmuyor. Bundan dolayı da bu konunun önemi anlayacak, anlatacak ve sonrasında bu konuda çalışmalar yapacak personel yok. Tüm kritik altyapı sektörlerinde BDDK nın yaptığına benzer, sektör spesifik siber güvenlik düzenlemeleri olmalı ve üst kurul bu düzenlemelerin yapılıp yapılmadığını denetlemelidir.
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	Sektörel ve ulusal bazda siber güvenlik konusunda bilgi paylaşım mekanizmaları Türkiye'de mevcut değildir. Örn: Amerika'da her sektör için bir bilgi paylaşım merkezi (ISAC-Information Sharing Center) tesis edilmiştir. Bu merkezler aracılığı ile sektör oyuncuları bilgi paylaşımında bulunabilmektedir. Türkiye'de de benzer merkezlerin oluşması ve çalışmaya başlaması gerekmektedir. Bunun için mevzuat ve teknik altyapının hazırlanması gerekiyor.
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Kritik altyapıların güvenliği konusunda uzmanlaşmış özel sektör firması ve personeli pek yoktur. Ek olarak özel sektörün bu alana girmeye teşvik edici faktörler (kar, bilinirlik, repütasyon vs.) yoktur. Özel sektörün çalışmalara katılması için devlet ve sektör işletmecileri tarafından maddi kaynak ayırılmalıdır.
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için düzenleme yapılması gerekiyor. Sözleşmeli personel çalıştırma imkanı olmalı. Böylece daha yüksek ücretlerle daha tecrübeli personel çalıştırılabilir. Ek olarak, outsource hizmet alımı ve personel kiralama için düzenlemeler olmalı. Böylece tecrübeli kişiler tam zamanlı olmasa da yarı zamanlı veya proje bazlı olarak kurumlara hizmet verebilmeli.
The number of qualified cyber security experts is limited.	Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi arttırılmalı. Bunun için devlet tarafından teşvik verilmeli ve kurumların çalışanları için belli bir eğitim kotası koyması sağlanmalı. Özellikle sektöre yönelik eğitim veren kurumların sayısı artmalı. Amerika'daki SANS benzeri özel kurumlar olmalı.

Root causes of susceptibility to cyber threats	The set of principles
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	İşletmeciler ve ürün/hizmet sağlayıcıların katılacağı sektör spesifik tatbikatlar ve konferanslar düzenlenmelidir. Bu organizasyonlarda iki tarafın bir araya gelerek "networking" yapması sağlanmalıdır.
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	Her sektör için üst kurul var ise, mevzuat ile denetim görevi verilmeli, kurul da bu denetimi düzenli olarak yapmalıdır. Denetim sonuçları işletmeciler için iş yapmasını etkilemeli, sonuçların iyi çıkmaması lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir.
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	Konunun önemine dikkat çekmek için yöneticilere odaklı bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) yapılmalıdır. Kurumda oluşacak siber olaylardan doğrudan kurum yöneticisini sorumlu tutan düzenleme (kanun, yönetmelik v.s.) getirilmelidir.
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	Kritik altyapı işletmecilerine yönelik risk yönetimi, BGYS konusunda regülasyonlar olmalı ve üst kurul bu regülasyona uyumluluk denetlenmelidir. Konunun önemine dikkat çekmek için bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) yapılmalıdır.
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmeli ve üst kurullar bunu denetlemelidir. Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar olmalıdır. Operatörler sistem kurar iken bu kılavuzlardan faydalanabilmelidir.

Expert-2

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı Siber tehditleri dikkate alan bir kritik altyapıların korunması programının (CIPP) varlığı Kritik altyapıları siber tehditlere karşı korumaktan sorumlu kurumun aynı zamanda ulusal güvenlik sorumlusu olması (ABD'de DHS örneği)

Root causes of susceptibility to cyber threats	**The set of principles**
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	Devlet tarafından geliştirilip desteklenen Public-private partnership programının varlığı Bilgileri gizliliğine göre sınıflandıran, bu sınıflandırmaya göre de paylaşımı ile ilgili kuralların belirlenmesinde rol oynayan bir veri koruma kanununun varlığı Sektör içi ve sektörler arası belirlenmiş bilgi paylaşım kurallarının varlığı
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Kritik altyapı programında özel sektöre verilmiş somut görevlerin varlığı Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Hâlihazırdaki yasaların kritik gözden geçirmesinin yapılması
The number of qualified cyber security experts is limited.	Ulusal seviyede kapasite geliştirme çalışmalarının varlığı
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı

Root causes of susceptibility to cyber threats	The set of principles
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	Kritik altyapı operatörlerinde güvenlik süreçlerinin varlığı

Expert-3

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Kamuda üst düzey yöneticiler siber güvenlik farkındalık eğitimi almıştır. Ulusal siber güvenlik stratejisinde kritik altyapılara yönelik düzenlemeler bulunmaktadır.
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	Ulusal CERT'ler kurulmuş ve uluslararası CERT'lerle işbirliği sağlanmıştır. CERT'ler yükümlülüğü kanun ve yönetmeliklerle tespit edilmiştir. Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır.
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Özel sektörü teşvik edici maddi çözümler (vergi muafiyeti, kamunun teknik imkânlarından ücretsiz faydalanma, ulusal siber güvenlik kurumlarından ücretsiz danışmanlık alınması vb.) yürürlüktedir.
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmıştır. (Yüksek maaş ve geniş imkanlar vb.) Kamu İhale Kanununda teknik satın almaları kolaylaştırıcı, kaliteli ürün alınmasını sağlayıcı düzenlemeler yapılmıştır
The number of qualified cyber security experts is limited.	Kamuda çalışmak üzere personel yetiştirme programları hazırlanmıştır. Bu programlardan mezun olan öğrencilerin uzun süreli (10 yıl vs.) zorunlu hizmet etmesi şart koşulmuştur. (TSK'da pilot eğitimi gibi) Personel sayısının yetersiz kaldığı durumlarda, yabancı memur ve işçi alımının önünü açacak yasal düzenlemeler yürürlüktedir. Bunun için klerans çıkarılması gibi güvenlik soruşturmaları devreye alınmıştır.

Root causes of susceptibility to cyber threats	The set of principles
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır. Ürün/hizmet sağlayıcılarını bilgilendirici ve katılım zorunluluğu olan eğitim/konferans/seminer vb. faaliyetler yapılmaktadır.
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir. Denetimlerin yapılması ve çıktılarının merkezi bir ortamda toplanıp düzenli olarak değerlendirilmesine imkan sağlayan teknik çözümler devreye alınmıştır.
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	Kritik altyapı işletmecilerinin tepe yöneticilerine bilgilendirme eğitimleri düzenli olarak verilmektedir. Bu yöneticilerin görev tanımlarında siber güvenlik sorumluluğu net olarak tanımlanmıştır.
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır.
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	Operatörlerin iş geliştirme ve tasarım süreçlerinde güvenlik farkındalığı düzenli olarak ölçülmektedir. Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır. Geliştirme yapacak personelin teknik olgunluğu ölçülmekte ve gerekli görüldüğünde zorunlu eğitime gönderilmektedir.

Expert-4

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması Ulusal güvenlik belgesinde kritik altyapıların güvenliğin yer alması Kritik altyapı güvenliğinin bir kurumun kanuni olarak sorumluluğunda olması ve ulusal güvenlikten sorumlu olan kurumla eşgüdüm mekanizmalarının oluşturulmuş olması
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması Sektör içi ve sektörler arası organizasyonlar (konferans, workshop vb) yapılması

Root causes of susceptibility to cyber threats	The set of principles
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Özel sektörün siber güvenlik kuruluna katılabilmesi Özel sektörü temsil eden sivil inisiyatif gruplarının var olması ve aktif faaliyetler yapması
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Devlette güvenlik uzmanı olarak çalışan memurların memnuniyet oranlarının belirli bir değerden yukarıda olması Devlette güvenlik uzmanı olarak çalışan memurların ürünlerden memnuniyet oranı
The number of qualified cyber security experts is limited.	Sadece siber güvenlik üzerine çalışan kişi sayısının oranının belirli bir değerden fazla olması Sertifikalı devlet çalışanlarının oranı Siber güvenlik tatbikatlarındaki takımların başarı durumu
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	İşletmecilerle ürün sağlayıcılar arasında güvenlikle ilgili sorunların iletildiği kanalların oluşturulup oluşturulmadığı Ürün güvenliği ile ilgili standartların belirli olması
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı IT denetim Planlarının varlığı Genel sektörel durumun ölçümlendiği bir bilgi toplama mekanizmasının varlığı ve işlerliği
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	Siber güvenlikle ilgili kurumsal sorumlu kişilerin belirlenmesi Kurumsal bilgi güvenliği politikasının varlığı Kurumsal yönetimsel toplantı tutanaklarında siber güvenlik ile ilgili kararların bulunması Yöneticilerin bir denetim mekanizması oluşturması Kurumsal siber güvenlik metriklerinin belirlenmiş olması, metriklerin hesaplanması ve raporlanması
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	Kurumlarda siber güvenliği de kapsayan tanımlı bir risk yönetim sürecinin var olması Risk yönetim süreci işletimiyle ilgili kayıtların varlığı
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	-

Expert-5

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Ulusal Siber Güvenlik Stratejisi kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendirmektedir Doğal gaz boru hatlarına yönelik 2007 yılında gerçekleştirildiği iddia edilen siber saldırı yetkili makamlar tarafından yeterince araştırılmamıştır. http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	Bilgi paylaşımı USOM üzerinden yapılmaktadır. 2015 Ocak ayında USOM 431 adet ihbar aldığını duyurmuştur. Bu ihbarlardan hangilerinin kritik altyapılarla ilgili olduğu açıklanmamıştır.
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Siber güvenlik tatbikatlarına özel sektörün katilimi sinirlidir. Özel sektör siber güvenlik önlemlerini ilave masraf olarak görmektedir. Yasal düzenlemeler özel sektörü gerekli önlemleri almaya zorlamakta yetersizdir. Özel sektör siber saldırılara ilişkin gerçek verileri paylaşmaktan imtina etmektedir.
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Kamu kurumlarında mevcut bilgi işlem personeli siber güvenlik konularıyla ilgili sorumluluk almaktadır. Siber güvenliğe ilişkin bir kadro bulunmamaktadır.
The number of qualified cyber security experts is limited.	Siber güvenlik eğitimi veren akademik kurumlar sinirli sayıdadır. Uluslararası geçerliliği olan sertifikalar kamu kurumları tarafından işe alımda tercih edilmemektedir.
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	Çoğunlukla güvenliğe ilişkin düzenlemeler yükleniciye ilave masraflar getirdiğinden, bütçe kaygısıyla sözleşmelerden son anda çıkarılması yoluna gidilmektedir.
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	-

Root causes of susceptibility to cyber threats	The set of principles
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	-
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	-
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	-

Expert-6

Root causes of susceptibility to cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) Üst düzey karar alıcıların (başbakan, bakan vb.) siber güvenlik danışmanı olması
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımını koordine etmek üzere bir kurumun görevlendirilmiş olması İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması Kritik teknolojilerin hızlı tedarik edilebilmesi için

Root causes of susceptibility to cyber threats	The set of principles
The number of qualified cyber security experts is limited.	Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planı vardır Siber güvenlik alanında insan kaynağı geliştirilmesini koordine etmekle görevli/sorumlu kurum ya da kurul gibi bir yapı vardır
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	Kritik altyapı işletmecilerinin dışardan hizmet aldıkları kuruluşlarla (IT hizmeti burada önemli, yemek/temizlik gibi hizmetler ilk etapta önemli değil) ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı Kritik altyapı işletmecilerinin ürün/hizmet sağlayıcıları ile bir araya gelebildikleri STÖ ler vardır
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi yapar
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	Kritik altyapı işletmecileri için ISO 27001 zorunluluğu vardır
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması

Round-2: Input

Root causes of the susceptibility to the cyber threats	The set of principles
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	1. Siber tehditleri dikkate alan bir kritik altyapıların korunması programının (CIPP) varlığı
	2. Ulusal güvenlikten sorumlusu kurum ve kuruluşların aynı zamanda kritik altyapıları siber tehditlere karşı koruma sorumlulukları olması (ABD'de DHS örneği) / Kritik altyapıların siber güvenliğinden kanunen sorumlu kurum ile ulusal güvenlikten sorumlu kurum ve kuruluşlar arasında eşgüdüm mekanizmalarının oluşturulmuş olması / Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) / Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması
	3. Üst düzey karar alıcıların (başbakan, bakan vb.) siber güvenlik danışmanı olması
	4. Kamuda üst düzey yöneticilerin siber güvenlik farkındalık eğitimi almış olması
	5. Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı
	6. Her bir kritik altyapı sektörü için oluşturulmuş siber güvenliği de sorumluluk alanı olarak tanımlamış denetleyici / düzenleyici kurum yapılanmasının varlığı
	7. Ülkedeki her bir kritik altyapı sektörü için BDDK'nın yaptığına benzer, sektör spesifik kanuni siber güvenlik düzenlemelerinin varlığı
	8. Kritik altyapıların ihtiyaçları dikkate alınarak kurulmuş bir CERT yapılanmasının varlığı (ABD'deki ICS-CERT örneği)
	9. Kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendiren bir ulusal Siber Güvenlik Stratejisinin varlığı
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	1. Devlet tarafından geliştirilip desteklenen public-private partnership programının varlığı
	2. Bilgileri gizliliğine göre sınıflandırmakta kullanılan, bu sınıflandırmaya göre de bilginin paylaşımı ile ilgili kuralların belirlenmesinde rol oynayan bir veri koruma kanununun varlığı
	3. Sektör içi ve sektörler arası belirlenmiş bilgi paylaşımı kurallarının varlığı / Bilgi paylaşımı ve işbirliği için mevzuat altyapısının varlığı / İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması
	4. Bilgi paylaşım yükümlülükleri kanun ve yönetmeliklerle tespit edilmiş kurumsal, sektörel CERT'lerin varlığı
	5. Kurulmuş bir Ulusal CERT'in varlığı ve bunun uluslararası CERT'lerle işbirliği sağlıyor olması.

Root causes of the susceptibility to the cyber threats	The set of principles
	6. Bilgi paylaşımı ve işbirliği için teknik altyapının varlığı / Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır. / Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi / Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması
	7. İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımını koordine etmek üzere bir kurumun görevlendirilmiş olması / Amerika'da her sektör için bir bilgi paylaşım merkezi (ISAC-Information Sharing Center) tesis edilmiştir. Bu merkezler aracılığı ile sektör oyuncuları bilgi paylaşımında bulunabilmektedir. Bu gibi merkezlerin varlığı,
	8. Sektör içi ve sektörler arası organizasyonların (konferans, workshop vb) varlığı
	9. Ulusal CSIRT (USOM) üzerinden yapılan bilgi paylaşımının varlığı
	10. Ulusal CSIRT'in kritik altyapılara yönelik yapılan ihbarları koordine etmesi, ilgili operatörlere eşgüdüm içerisinde çalışması
	11. Özel sektörün siber saldırılara ilişkin gerçek verileri paylaşmaktan imtina etmesini engelleyecek yasal düzenlemelerin varlığı
The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.	1. Özel sektörü siber güvenlik alanında önemli bir oyuncu yapacak politika ve stratejilerin varlığı
	2. Kritik altyapı programında özel sektöre verilmiş somut görevlerin varlığı
	3. Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması
	4. Özel sektörün siber güvenlik kurulu gibi yapılanmaların daimi üyesi olması
	5. Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması / Devlet tarafından öncelikli alanların belirlenmiş olması özel sektörün bu alanlara sevk edilmesi
	6. Özel sektörü teşvik edici maddi çözümler (vergi muafiyeti, kamunun teknik imkânlarından ücretsiz faydalanma, ulusal siber güvenlik kurumlarından ücretsiz danışmanlık alınması vb.) yürürlüktedir. / Özel sektörün çalışmalara katılması için devlet ve sektör işletmecileri tarafından maddi kaynak ayrılması
	7. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması
	8. Özel sektörü temsil eden sivil inisiyatif gruplarının var olması ve aktif faaliyetler yapması
	9. Ulusal siber güvenlik tatbikatlarına özel sektörün kapsamlı bir şekilde katılıyor olması

Root causes of the susceptibility to the cyber threats	The set of principles
	10. Özel sektörün siber güvenlik önlemlerini ilave masraf olarak görerek uygulamamasının önüne geçerek Yasal düzenlemelerin varlığı
The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.	1. Hâlihazırdaki önemli yasaların kritik gözden geçirmesinin yapılmış olması (critical review of the current laws)
	2. Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması / Sözleşmeli personel çalıştırma, outsource hizmet alımı ve personel kiralama için yapılmış düzenlemeler / Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmış olması (Yüksek maaş ve geniş imkanlar vb.)/ Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için yapılmış düzenlemeler
	3. Devlette güvenlik uzmanı olarak çalışan memurların memnuniyet oranlarının belirli bir değerden yukarıda olması
	4. Kritik teknolojilerin hızlı tedarik edilebilmesi için yasa değişikliği / Kamu İhale Kanununda teknik satın almaları kolaylaştırıcı, kaliteli ürün alınmasını sağlayıcı düzenlemelerin yapılmış olması
	5. Devlette güvenlik uzmanı olarak çalışan memurların ürünlerden memnuniyet oranı
The number of qualified cyber security experts is limited.	1. Ulusal seviyede kapasite geliştirme çalışmalarının varlığı / Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planının olması / Kamuda çalışmak üzere personel yetiştirme programları hazırlanmıştır. Bu programlardan mezun olan öğrencilerin uzun süreli (10 yıl vs.) zorunlu hizmet etmesi şart koşulmuştur. (TSK'da pilot eğitimi gibi)
	2. Siber güvenlik alanında insan kaynağı geliştirilmesini koordine etmekle görevli/sorumlu kurum ya da kurul gibi bir yapının varlığı
	3. Sadece siber güvenlik üzerine çalışan kişi sayısının oranının belirli bir değerden fazla olması
	4. Sertifikalı devlet çalışanlarının oranı / Uluslararası geçerliliği olan sertifikaların kamu kurumları tarafından işe alımda tercih edilmesi
	5. Siber güvenlik tatbikatlarındaki takımların başarı durumu
	6. Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi / Özellikle sektöre yönelik eğitim veren kurumların varlığı ve fazlalığı
	7. Eğitim veren yerler için devlet tarafından teşvik verilmesi
	8. Tüm eğitim seviyelerinde (ilkokuldan doktoraya) BT ve siber güvenlik konularında müfredatın olması / Siber güvenlik eğitimi veren akademik kurumlar yeterli sayıda olması
	9. Personel sayısının yetersiz kaldığı durumlarda, yabancı memur ve işçi alımının önünü açacak yasal düzenlemeler yürürlüktedir. Bunun için klerans çıkarılması gibi güvenlik soruşturmaları devreye alınmıştır
	10. Kritik altyapı operatörlerinde sadece siber güvenliğe ilişkin kadroların varlığı

Root causes of the susceptibility to the cyber threats	The set of principles
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	1. Özel sektörden kabul edilebilir hizmet alma standartlarının belirlenmesi / Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları
	2. Kritik altyapı işletmecilerinin dışardan IT hizmeti aldıkları kuruluşlarla ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı / ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır
	3. Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı
	4. Kritik altyapı işletmecilerinin ürün/hizmet sağlayıcıları ile bir araya gelebildikleri sivil toplum örgütleri vardır
	5. İşletmecilerle ürün sağlayıcılar arasında güvenlikle ilgili sorunların iletildiği kanalların oluşturulup oluşturulmadığı
	6. Ürün güvenliği ile ilgili standartların belirli olması
	7. Ürün/hizmet sağlayıcılarını bilgilendirici ve katılım zorunluluğu olan eğitim/konferans/seminer vb. faaliyetler yapılmaktadır. / İşletmeciler ve ürün/hizmet sağlayıcıların katılacağı sektör spesifik tatbikatlar ve konferansların varlığı
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı / Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir.
	2. Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar / Her sektörün üst kurulunun mevzuat ile denetim yapması
	3. İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı
	4. IT denetim Planlarının varlığı
	5. Genel sektörel durumun ölçümlendiği bir bilgi toplama mekanizmasının varlığı ve işlerliği
	6. Denetimlerin yapılması ve çıktılarının merkezi bir ortamda toplanıp düzenli olarak değerlendirilmesine imkan sağlayan teknik çözümler devreye alınmıştır.
	7. Denetim sonuçlarının ciddi yaptırımlarının olması (örneğin lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir)
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	1. Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı
	2. Kurumsal bilgi güvenliği politikasının varlığı
	3. Kurumsal yönetimsel toplantı tutanaklarında siber güvenlik ile ilgili kararların bulunması
	4. Kurumsal siber güvenlik metriklerinin belirlenmiş olması, metriklerin hesaplanması ve raporlanması
	5. Bu yöneticilerin görev tanımlarında siber güvenlik sorumluluğu net olarak tanımlanmıştır.

Root causes of the susceptibility to the cyber threats	The set of principles
	6. Konunun önemine dikkat çekmek için yöneticilere odaklı bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) / Kritik altyapı işletmecilerinin tepe yöneticilerine bilgilendirme eğitimleri düzenli olarak verilmektedir.
	7. Siber güvenlikle ilgili kurumsal sorumlu kişilerin belirlenmesi
	8. Yöneticilerin bir denetim mekanizması oluşturması
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı / Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır. / Kritik altyapı işletmecilerine yönelik risk yönetimi ve BGYS konularında yaptırım getiren kanuni düzenleme ve düzenleyici kurulun buna göre denetimi
	2. Kritik altyapı işletmecileri için ISO 27001 gibi bir güvenlik standardı zorunluluğu olması
	3. Kurumlarda siber güvenliği de kapsayan tanımlı bir risk yönetim sürecinin var olması
	4. Risk yönetim süreci işletimiyle ilgili kayıtların varlığı
	5. Konunun önemine dikkat çekmek için bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.)
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	1. Mevzuat ile zorunlu tutulan sektörel / ulusal minimum güvenlik önlemlerinin varlığı / Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır
	2. Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmesi / Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır.
	3. Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar
	4. Sektör bazlı güvenlik standartlarının oluşturulmuş ve yayınlanmış olması
	5. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması
	6. Operatörlerin iş geliştirme ve tasarım süreçlerinde güvenlik farkındalığı düzenli olarak ölçülmektedir.
	7. Geliştirme yapacak personelin teknik olgunluğu ölçülmekte ve gerekli görüldüğünde zorunlu eğitime gönderilmektedir.

Round -2: Controlled opinion feedback

I would like to ask you to grade the attached maturity criteria (including your own) determined by six experts. Could you please grade the criteria in accordance with the attached grading reference table? You are requested to give three points for the criteria (weights for the principles) that you consider the most important, and one point for the least and zero for the criteria that you would like to eliminate from the list. The elimination may be based on many reasons: Those criteria may be recurrent, irrelevant, illogical or too technically detailed etc. Please feel free to eliminate the criteria. You may give far more zero points than you do with the other grades. I even would like you to consider more on the zero-grade criteria as I am planning to have at most two or three criteria, in other words the most significant ones, for each root cause in my maturity model proposal. I would be glad to answer if you have any questions.

Note: If a totally new criterion come to your mind during weighing the existing criteria, please notice me as soon as possible as I will send it to the other experts in order to be graded in this round.

Score	Explanation
0	The principle is duplicate, nonsense, confusing, unrelated, imprecise (careless), too detailed or too technical.
1	The lack of the principle can be compensated by other principles to some extent. The country improves its critical infrastructure protection effort more slowly than expected.
2	The maturity principle is important on its own. The lack of the principle cannot be compensated by other principles. The lack of criterion indicates an obvious problem for the critical infrastructure protection. The critical infrastructures will not be resilient at some parts.
3	The lack of the maturity criterion indicates a major problem for the critical infrastructure protection efforts of the country because of the dependencies of the other criteria on this criterion. The country cannot improve the cyber resilience of the critical infrastructures.

Round-2: Output

Each expert weighted the principles separately. Please see the input of the Round-3 (below) for the individual weight values.

Round-3: Input

Root cause #	The set of principles	W1	W2	W3	W4	W5	W6
1	1. Siber tehditleri dikkate alan bir kritik altyapıların korunması programının (CIPP) varlığı	1	3	3	2	3	2
	2. Ulusal güvenlikten sorumlusu kurum ve kuruluşların aynı zamanda kritik altyapıları siber tehditlere karşı koruma sorumlulukları olması (ABD'de DHS örneği) / Kritik altyapıların siber güvenliğinden kanunen sorumlu kurum ile ulusal güvenlikten sorumlu kurum ve kuruluşlar arasında eşgüdüm mekanizmalarının oluşturulmuş olması / Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) / Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması	2	3	1	3	3	1
	3. Üst düzey karar alıcıların (başbakan, bakan vb.) siber güvenlik danışmanı olması	3	0	0	2	1	1
	4. Kamuda üst düzey yöneticilerin siber güvenlik farkındalık eğitimi almış olması	1	0	1	1	2	0
	5. Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı	3	3	0	2	3	1
	6. Her bir kritik altyapı sektörü için oluşturulmuş siber güvenliği de sorumluluk alanı olarak tanımlamış denetleyici / düzenleyici kurum yapılanmasının varlığı	0	3	2	3	1	1
	7. Ülkedeki her bir kritik altyapı sektörü için BDDK'nın yaptığına benzer, sektör spesifik kanuni siber güvenlik düzenlemelerinin varlığı	2	1	1	2	2	2
	8. Kritik altyapıların ihtiyaçları dikkate alınarak kurulmuş bir CERT yapılanmasının varlığı (ABD'deki ICS-CERT örneği)	3	0	2	3	2	1
	9. Kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendiren bir ulusal Siber Güvenlik Stratejisinin varlığı	3	0	2	3	3	1
	10. Sektör spesifik (sektörel) veya tüm kritik altyapıları içine alan risk yönetimi sürecinin veya teknik kılavuz, dokümantasyonun varlığı *(Introduced by Expert-1 as a result of the controlled opinion feedback)*	3	3	0	3	2	1
2	1. Devlet tarafından geliştirilip desteklenen public-private partnership programının varlığı	1	3	3	3	2	1
	2. Bilgileri gizliliğine göre sınıflandırmakta kullanılan, bu sınıflandırmaya göre de bilginin paylaşımı ile ilgili kuralların belirlenmesinde rol oynayan bir veri koruma kanununun varlığı	1	1	0	2	2	0

Root cause #	The set of principles	W1	W2	W3	W4	W5	W6
	3. Sektör içi ve sektörler arası belirlenmiş bilgi paylaşımı kurallarının varlığı / Bilgi paylaşımı ve işbirliği için mevzuat altyapısının varlığı / İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması	1	3	2	2	2	2
	4. Bilgi paylaşım yükümlülükleri kanun ve yönetmeliklerle tespit edilmiş kurumsal, sektörel CERT'lerin varlığı	2	1	1	1	2	2
	5. Kurulmuş bir Ulusal CERT'in varlığı ve bunun uluslararası CERT'lerle işbirliği sağlıyor olması.	2	2	1	3	3	1
	6. Bilgi paylaşımı ve işbirliği için teknik altyapının varlığı / Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır. / Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi / Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması	3	1	1	3	1	1
	7. İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımını koordine etmek üzere bir kurumun görevlendirilmiş olması / Amerika'da her sektör için bir bilgi paylaşım merkezi (ISAC- Information Sharing Center) tesis edilmiştir. Bu merkezler aracılığı ile sektör oyuncuları bilgi paylaşımında bulunabilmektedir. Bu gibi merkezlerin varlığı,	3	0	2	2	0	1
	8. Sektör içi ve sektörler arası organizasyonların (konferans, workshop vb) varlığı	2	0	0	1	1	1
	9. Ulusal CSIRT (USOM) üzerinden yapılan bilgi paylaşımının varlığı	2	1	1	0	3	1
	10. Ulusal CSIRT'in kritik altyapılara yönelik yapılan ihbarları koordine etmesi, ilgili operatörlere eşgüdüm içerisinde çalışması	2	0	1	3	2	1
	11. Özel sektörün siber saldırılara ilişkin gerçek verileri paylaşmaktan imtina etmesini engelleyecek yasal düzenlemelerin varlığı	0	0	1	3	2	2
3	1. Özel sektörü siber güvenlik alanında önemli bir oyuncu yapacak politika ve stratejilerin varlığı	1	3	3	3	2	1
	2. Kritik altyapı programında özel sektöre verilmiş somut görevlerin varlığı	0	2	2	0	2	2
	3. Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması	3	2	0	3	2	1
	4. Özel sektörün siber güvenlik kurulu gibi yapılanmaların daimi üyesi olması	2	2	1	0	1	2

Root cause #	The set of principles	W1	W2	W3	W4	W5	W6
	5. Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması / Devlet tarafından öncelikli alanların belirlenmiş olması özel sektörün bu alanlara sevk edilmesi	3	3	0	2	2	1
	6. Özel sektörü teşvik edici maddi çözümler (vergi muafiyeti, kamunun teknik imkânlarından ücretsiz faydalanma, ulusal siber güvenlik kurumlarından ücretsiz danışmanlık alınması vb.) yürürlüktedir. / Özel sektörün çalışmalara katılması için devlet ve sektör işletmecileri tarafından maddi kaynak ayrılması	3	0	1	0	1	1
	7. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	1	0	0	1	1	1
	8. Özel sektörü temsil eden sivil inisiyatif gruplarının var olması ve aktif faaliyetler yapması	0	0	0	3	0	1
	9. Ulusal siber güvenlik tatbikatlarına özel sektörün kapsamlı bir şekilde katılıyor olması	1	1	0	3	2	1
	10. Özel sektörün siber güvenlik önlemlerini ilave masraf olarak görerek uygulamamasının önüne geçerek Yasal düzenlemelerin varlığı	0	0	2	0	2	1
4	1. Hâlihazırdaki önemli yasaların kritik gözden geçirmesinin yapılmış olması (critical review of the current laws)	2	3	1	0	1	0
	2. Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması / Sözleşmeli personel çalıştırma, outsource hizmet alımı ve personel kiralama için yapılmış düzenlemeler / Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmış olması (Yüksek maaş ve geniş imkanlar vb.)/ Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için yapılmış düzenlemeler	3	2	3	0	2	3
	3. Devlette güvenlik uzmanı olarak çalışan memurların memnuniyet oranlarının belirli bir değerden yukarıda olması	1	1	1	1	1	1
	4. Kritik teknolojilerin hızlı tedarik edilebilmesi için yasa değişikliği / Kamu İhale Kanununda teknik satın almaları kolaylaştırıcı, kaliteli ürün alınmasını sağlayıcı düzenlemelerin yapılmış olması	2	2	2	2	0	2
	5. Devlette güvenlik uzmanı olarak çalışan memurların ürünlerden memnuniyet oranı	0	0	0	2	0	0
5	1. Ulusal seviyede kapasite geliştirme çalışmalarının varlığı / Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planının olması	2	3	3	3	1	1

Root cause #	The set of principles	W1	W2	W3	W4	W5	W6
	2. Siber güvenlik alanında insan kaynağı geliştirilmesini koordine etmekle görevli/sorumlu kurum ya da kurul gibi bir yapının varlığı	0	0	1	0	0	2
	3. Sadece siber güvenlik üzerine çalışan kişi sayısının oranının belirli bir değerden fazla olması	2	2	1	2	0	1
	4. Sertifikalı devlet çalışanlarının oranı / Uluslararası geçerliliği olan sertifikaların kamu kurumları tarafından işe alımda tercih edilmesi	2	2	1	2	2	2
	5. Siber güvenlik tatbikatlarındaki takımların başarı durumu	2	0	0	0	1	0
	6. Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi / Özellikle sektöre yönelik eğitim veren kurumların varlığı ve fazlalığı	3	2	0	2	2	1
	7. Eğitim veren yerler için devlet tarafından teşvik verilmesi	3	1	1	0	0	1
	8. Tüm eğitim seviyelerinde (ilkokuldan doktoraya) BT ve siber güvenlik konularında müfredatın olması / Siber güvenlik eğitimi veren akademik kurumlar yeterli sayıda olması	3	2	2	0	3	1
	9. Personel sayısının yetersiz kaldığı durumlarda, yabancı memur ve işçi alımının önünü açacak yasal düzenlemeler yürürlüktedir. Bunun için klerans çıkarılması gibi güvenlik soruşturmaları devreye alınmıştır	2	0	1	0	0	0
	10. Kritik altyapı operatörlerinde sadece siber güvenliğe ilişkin kadroların varlığı	3	2	0	2	0	1
6	1. Özel sektörden kabul edilebilir hizmet alma standartlarının belirlenmesi / Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları	0	3	3	3	2	2
	2. Kritik altyapı işletmecilerinin dışardan IT hizmeti aldıkları kuruluşlarla ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı / ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır	3	3	2	0	3	2
	3. Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı	2	2	1	3	3	1
	4. Kritik altyapı işletmecilerinin ürün/hizmet sağlayıcıları ile bir araya gelebildikleri sivil toplum örgütleri vardır	0	1	0	2	0	0
	5. İşletmecilerle ürün sağlayıcılar arasında güvenlikle ilgili sorunların iletildiği kanalların oluşturulup oluşturulmadığı	0	0	0	3	1	0

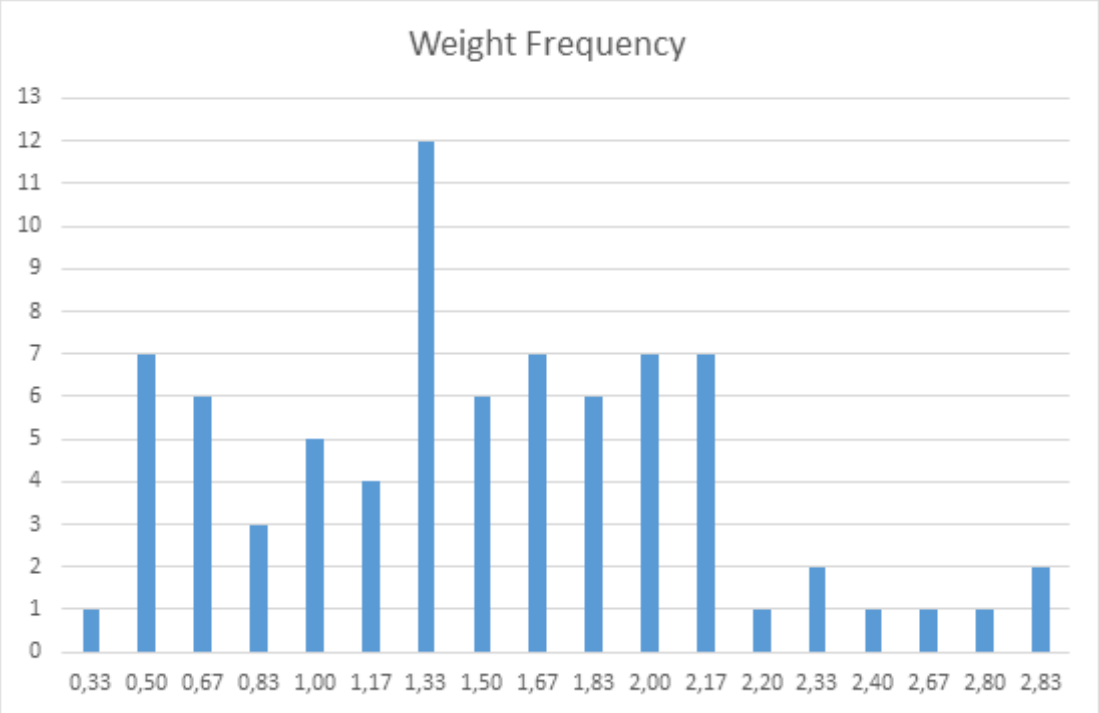
Root cause #	The set of principles	W1	W2	W3	W4	W5	W6
	6. Ürün güvenliği ile ilgili standartların belirli olması	3	2	1	0	1	1
	7. Ürün/hizmet sağlayıcılarını bilgilendirici ve katılım zorunluluğu olan eğitim/konferans/seminer vb. faaliyetler yapılmaktadır. / İşletmeciler ve ürün/hizmet sağlayıcıların katılacağı sektör spesifik tatbikatlar ve konferansların varlığı	2	0	0	1	0	1
7	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı / Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir.	3	3	2	3	2	3
	2. Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar / Her sektörün üst kurulunun mevzuat ile denetim yapması	3	3	3	3	3	2
	3. İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı	2	2	0	2	2	1
	4. IT denetim Planlarının varlığı	0	1	1	3	2	1
	5. Genel sektörel durumun ölçümlendiği bir bilgi toplama mekanizmasının varlığı ve işlerliği	0	0	0	3	0	0
	6. Denetimlerin yapılması ve çıktılarının merkezi bir ortamda toplanıp düzenli olarak değerlendirilmesine imkan sağlayan teknik çözümler devreye alınmıştır.	1	0	0	2	0	0
	7. Denetim sonuçlarının ciddi yaptırımlarının olması (örneğin lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir)	3	1	1	3	2	0
8	1. Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı	3	3	3	2	2	3
	2. Kurumsal bilgi güvenliği politikasının varlığı	1	0	1	3	3	1
	3. Kurumsal yönetimsel toplantı tutanaklarında siber güvenlik ile ilgili kararların bulunması	2	1	0	2	3	1
	4. Kurumsal siber güvenlik metriklerinin belirlenmiş olması, metriklerin hesaplanması ve raporlanması	2	0	0	2	2	1
	5. Bu yöneticilerin görev tanımlarında siber güvenlik sorumluluğu net olarak tanımlanmıştır.	0	2	2	3	2	3
	6. Konunun önemine dikkat çekmek için yöneticilere odaklı bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) / Kritik altyapı işletmecilerinin tepe yöneticilerine bilgilendirme eğitimleri düzenli olarak verilmektedir.	3	0	1	3	1	0
	7. Siber güvenlikle ilgili kurumsal sorumlu kişilerin belirlenmesi	2	0	0	3	2	0
	8. Yöneticilerin bir denetim mekanizması oluşturması	1	0	1	3	2	1

Root cause #	The set of principles	W1	W2	W3	W4	W5	W6
9	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı / Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır. / Kritik altyapı işletmecilerine yönelik risk yönetimi ve BGYS konularında yaptırım getiren kanuni düzenleme ve düzenleyici kurulun buna göre denetimi	3	3	3	3	3	2
	2. Kritik altyapı işletmecileri için ISO 27001 gibi bir güvenlik standardı zorunluluğu olması	1	3	2	2	3	2
	3. Kurumlarda siber güvenliği de kapsayan tanımlı bir risk yönetim sürecinin var olması	2	0	0	3	3	2
	4. Risk yönetim süreci işletimiyle ilgili kayıtların varlığı	1	0	0	2	0	1
	5. Konunun önemine dikkat çekmek için bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.)	2	0	1	0	1	0
10	1. Mevzuat ile zorunlu tutulan sektörel / ulusal minimum güvenlik önlemlerinin varlığı / Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır	3	3	2	3	2	1
	2. Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmesi / Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır.	3	2	3	3	2	2
	3. Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar	2	1	1	2	2	1
	4. Sektör bazlı güvenlik standartlarının oluşturulmuş ve yayınlanmış olması	2	3	1	2	2	1
	5. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	1	0	0	1	1	0
	6. Operatörlerin iş geliştirme ve tasarım süreçlerinde güvenlik farkındalığı düzenli olarak ölçülmektedir.	1	0	1	0	2	0
	7. Geliştirme yapacak personelin teknik olgunluğu ölçülmekte ve gerekli görüldüğünde zorunlu eğitime gönderilmektedir.	2	0	0	1	2	1

Round -3: Controlled opinion feedback

We are in the third round of Delphi. You will see the others' grades (weights of the principles) for the criteria, along with your own. Your grades are in the Points-x column. You can change your grades if you like, after you look at the grades by the other experts.

In the last right column, there are the arithmetic averages of the grades as to assist you in your decisions. And the frequency of each arithmetic average is shown in another chart.



Root cause #	Principles	Average weight
1	1. Siber tehditleri dikkate alan bir kritik altyapıların korunması programının (CIPP) varlığı	2,33
	2. Ulusal güvenlikten sorumlusu kurum ve kuruluşların aynı zamanda kritik altyapıları siber tehditlere karşı koruma sorumlulukları olması (ABD'de DHS örneği) / Kritik altyapıların siber güvenliğinden kanunen sorumlu kurum ile ulusal güvenlikten sorumlu kurum ve kuruluşlar arasında eşgüdüm mekanizmalarının oluşturulmuş olması / Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) / Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması	2,17
	3. Üst düzey karar alıcıların (başbakan, bakan vb.) siber güvenlik danışmanı olması	1,17
	4. Kamuda üst düzey yöneticilerin siber güvenlik farkındalık eğitimi almış olması	0,83
	5. Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı	2,00

Root cause #	Principles	Average weight
	6. Her bir kritik altyapı sektörü için oluşturulmuş siber güvenliği de sorumluluk alanı olarak tanımlamış denetleyici / düzenleyici kurum yapılanmasının varlığı	1,67
	7. Ülkedeki her bir kritik altyapı sektörü için BDDK'nın yaptığına benzer, sektör spesifik kanuni siber güvenlik düzenlemelerinin varlığı	1,67
	8. Kritik altyapıların ihtiyaçları dikkate alınarak kurulmuş bir CERT yapılanmasının varlığı (ABD'deki ICS-CERT örneği)	1,83
	9. Kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendiren bir ulusal Siber Güvenlik Stratejisinin varlığı	2,00
	10. Sektör spesifik (sektörel) veya tüm kritik altyapıları içine alan risk yönetimi sürecinin veya teknik kılavuz, dokümantasyonun varlığı	2,00
2	1. Devlet tarafından geliştirilip desteklenen public-private partnership programının varlığı	2,17
	2. Bilgileri gizliliğine göre sınıflandırmakta kullanılan, bu sınıflandırmaya göre de bilginin paylaşımı ile ilgili kuralların belirlenmesinde rol oynayan bir veri koruma kanununun varlığı	1,00
	3. Sektör içi ve sektörler arası belirlenmiş bilgi paylaşımı kurallarının varlığı / Bilgi paylaşımı ve işbirliği için mevzuat altyapısının varlığı / İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması	2,00
	4. Bilgi paylaşım yükümlülükleri kanun ve yönetmeliklerle tespit edilmiş kurumsal, sektörel CERT'lerin varlığı	1,50
	5. Kurulmuş bir Ulusal CERT'in varlığı ve bunun uluslararası CERT'lerle işbirliği sağlıyor olması.	2,00
	6. Bilgi paylaşımı ve işbirliği için teknik altyapının varlığı / Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır. / Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi / Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması	1,67
	7. İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımını koordine etmek üzere bir kurumun görevlendirilmiş olması / Amerika'da her sektör için bir bilgi paylaşım merkezi (ISAC-Information Sharing Center) tesis edilmiştir. Bu merkezler aracılığı ile sektör oyuncuları bilgi paylaşımında bulunabilmektedir. Bu gibi merkezlerin varlığı,	1,33
	8. Sektör içi ve sektörler arası organizasyonların (konferans, workshop vb) varlığı	0,83
	9. Ulusal CSIRT (USOM) üzerinden yapılan bilgi paylaşımının varlığı	1,33
	10. Ulusal CSIRT'in kritik altyapılara yönelik yapılan ihbarları koordine etmesi, ilgili operatörlere eşgüdüm içerisinde çalışması	1,50
	11. Özel sektörün siber saldırılara ilişkin gerçek verileri paylaşmaktan imtina etmesini engelleyecek yasal düzenlemelerin varlığı	1,33
3	1. Özel sektörü siber güvenlik alanında önemli bir oyuncu yapacak politika ve stratejilerin varlığı	2,17
	2. Kritik altyapı programında özel sektöre verilmiş somut görevlerin varlığı	1,33

Root cause #	Principles	Average weight
	3. Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması	1,83
	4. Özel sektörün siber güvenlik kurulu gibi yapılanmaların daimi üyesi olması	1,33
	5. Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması / Devlet tarafından öncelikli alanların belirlenmiş olması özel sektörün bu alanlara sevk edilmesi	1,83
	6. Özel sektörü teşvik edici maddi çözümler (vergi muafiyeti, kamunun teknik imkânlarından ücretsiz faydalanma, ulusal siber güvenlik kurumlarından ücretsiz danışmanlık alınması vb.) yürürlüktedir. / Özel sektörün çalışmalara katılması için devlet ve sektör işletmecileri tarafından maddi kaynak ayrılması	1,00
	7. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	0,67
	8. Özel sektörü temsil eden sivil inisiyatif gruplarının var olması ve aktif faaliyetler yapması	0,67
	9. Ulusal siber güvenlik tatbikatlarına özel sektörün kapsamlı bir şekilde katılıyor olması	1,33
	10. Özel sektörün siber güvenlik önlemlerini ilave masraf olarak görerek uygulamamasının önüne geçerek Yasal düzenlemelerin varlığı	0,83
4	1. Hâlihazırdaki önemli yasaların kritik gözden geçirmesinin yapılmış olması (critical review of the current laws)	1,17
	2. Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması / Sözleşmeli personel çalıştırma, outsource hizmet alımı ve personel kiralama için yapılmış düzenlemeler / Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmış olması (Yüksek maaş ve geniş imkanlar vb.)/ Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için yapılmış düzenlemeler	2,17
	3. Devlette güvenlik uzmanı olarak çalışan memurların memnuniyet oranlarının belirli bir değerden yukarıda olması	1,00
	4. Kritik teknolojilerin hızlı tedarik edilebilmesi için yasa değişikliği / Kamu İhale Kanununda teknik satın almaları kolaylaştırıcı, kaliteli ürün alınmasını sağlayıcı düzenlemelerin yapılmış olması	1,67
	5. Devlette güvenlik uzmanı olarak çalışan memurların ürünlerden memnuniyet oranı	0,33
5	1. Ulusal seviyede kapasite geliştirme çalışmalarının varlığı / Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planının olması	2,17
	2. Siber güvenlik alanında insan kaynağı geliştirilmesini koordine etmekle görevli/sorumlu kurum ya da kurul gibi bir yapının varlığı	0,50
	3. Sadece siber güvenlik üzerine çalışan kişi sayısının oranının belirli bir değerden fazla olması	1,33

Root cause #	Principles	Average weight
	4. Sertifikalı devlet çalışanlarının oranı / Uluslararası geçerliliği olan sertifikaların kamu kurumları tarafından işe alımda tercih edilmesi	1,83
	5. Siber güvenlik tatbikatlarındaki takımların başarı durumu	0,50
	6. Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi / Özellikle sektöre yönelik eğitim veren kurumların varlığı ve fazlalığı	1,67
	7. Eğitim veren yerler için devlet tarafından teşvik verilmesi	1,00
	8. Tüm eğitim seviyelerinde (ilkokuldan doktoraya) BT ve siber güvenlik konularında müfredatın olması / Siber güvenlik eğitimi veren akademik kurumlar yeterli sayıda olması	1,83
	9. Personel sayısının yetersiz kaldığı durumlarda, yabancı memur ve işçi alımının önünü açacak yasal düzenlemeler yürürlüktedir. Bunun için klerans çıkarılması gibi güvenlik soruşturmaları devreye alınmıştır	0,50
	10. Kritik altyapı operatörlerinde sadece siber güvenliğe ilişkin kadroların varlığı	1,33
6	1. Özel sektörden kabul edilebilir hizmet alma standartlarının belirlenmesi / Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları	2,17
	2. Kritik altyapı işletmecilerinin dışardan IT hizmeti aldıkları kuruluşlarla ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı / ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır	2,17
	3. Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı	2,00
	4. Kritik altyapı işletmecilerinin ürün/hizmet sağlayıcıları ile bir araya gelebildikleri sivil toplum örgütleri vardır	0,50
	5. İşletmecilerle ürün sağlayıcılar arasında güvenlikle ilgili sorunların iletildiği kanalların oluşturulup oluşturulmadığı	0,67
	6. Ürün güvenliği ile ilgili standartların belirli olması	1,33
	7. Ürün/hizmet sağlayıcılarını bilgilendirici ve katılım zorunluluğu olan eğitim/konferans/seminer vb. faaliyetler yapılmaktadır. / İşletmeciler ve ürün/hizmet sağlayıcıların katılacağı sektör spesifik tatbikatlar ve konferansların varlığı	0,60
7	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı / Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir.	2,67
	2. Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar / Her sektörün üst kurulunun mevzuat ile denetim yapması	2,83
	3. İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı	1,50
	4. IT denetim Planlarının varlığı	1,33
	5. Genel sektörel durumun ölçümlendiği bir bilgi toplama mekanizmasının varlığı ve işlerliği	0,50

Root cause #	Principles	Average weight
	6. Denetimlerin yapılması ve çıktılarının merkezi bir ortamda toplanıp düzenli olarak değerlendirilmesine imkan sağlayan teknik çözümler devreye alınmıştır.	0,50
	7. Denetim sonuçlarının ciddi yaptırımlarının olması (örneğin lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir)	1,67
8	1. Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı	2,80
	2. Kurumsal bilgi güvenliği politikasının varlığı	1,50
	3. Kurumsal yönetimsel toplantı tutanaklarında siber güvenlik ile ilgili kararların bulunması	1,50
	4. Kurumsal siber güvenlik metriklerinin belirlenmiş olması, metriklerin hesaplanması ve raporlanması	1,17
	5. Bu yöneticilerin görev tanımlarında siber güvenlik sorumluluğu net olarak tanımlanmıştır.	2,00
	6. Konunun önemine dikkat çekmek için yöneticilere odaklı bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) / Kritik altyapı işletmecilerinin tepe yöneticilerine bilgilendirme eğitimleri düzenli olarak verilmektedir.	1,33
	7. Siber güvenlikle ilgili kurumsal sorumlu kişilerin belirlenmesi	1,17
	8. Yöneticilerin bir denetim mekanizması oluşturması	1,33
9	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı / Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır. / Kritik altyapı işletmecilerine yönelik risk yönetimi ve BGYS konularında yaptırım getiren kanuni düzenleme ve düzenleyici kurulun buna göre denetimi	2,83
	2. Kritik altyapı işletmecileri için ISO 27001 gibi bir güvenlik standardı zorunluluğu olması	2,20
	3. Kurumlarda siber güvenliği de kapsayan tanımlı bir risk yönetim sürecinin var olması	1,67
	4. Risk yönetim süreci işletimiyle ilgili kayıtların varlığı	0,67
	5. Konunun önemine dikkat çekmek için bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.)	0,67
10	1. Mevzuat ile zorunlu tutulan sektörel / ulusal minimum güvenlik önlemlerinin varlığı / Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır	2,33
	2. Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmesi / Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır.	2,40
	3. Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar	1,50
	4. Sektör bazlı güvenlik standartlarının oluşturulmuş ve yayınlanmış olması	1,83

Root cause #	Principles	Average weight
	5. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	0,50
	6. Operatörlerin iş geliştirme ve tasarım süreçlerinde güvenlik farkındalığı düzenli olarak ölçülmektedir.	0,67
	7. Geliştirme yapacak personelin teknik olgunluğu ölçülmekte ve gerekli görüldüğünde zorunlu eğitime gönderilmektedir.	1,00

Round-3: Output

Each expert reviewed their weights separately by looking at the weights of the others experts and arithmetic averages. Please see the input of the Round-4 (below) for the individual weight values.

Round-4: Input

Principles	W1	W2	W3	W4	W5	W6	Average
Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar / Her sektörün üst kurulunun mevzuat ile denetim yapması	3	3	3	3	3	3	3,00
Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı / Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır. / Kritik altyapı işletmecilerine yönelik risk yönetimi ve BGYS konularında yaptırım getiren kanuni düzenleme ve düzenleyici kurulun buna göre denetimi	3	3	3	3	3	3	3,00
Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı	3	3	3	3	2	3	2,83
Kritik altyapı işletmecilerinin dışardan IT hizmeti aldıkları kuruluşlarla ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı / ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır	3	3	2	2	3	3	2,67
Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı / Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir.	3	3	2	3	2	3	2,67
Siber tehditleri dikkate alan bir kritik altyapıların korunması programının (CIPP) varlığı	2	3	3	2	3	2	2,50
Ulusal güvenlikten sorumlusu kurum ve kuruluşların aynı zamanda kritik altyapıları siber tehditlere karşı koruma sorumlulukları olması (ABD'de DHS örneği) / Kritik altyapıların siber güvenliğinden kanunen sorumlu kurum ile ulusal güvenlikten sorumlu kurum ve kuruluşlar arasında eşgüdüm mekanizmalarının oluşturulmuş olması / Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) / Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması	2	3	2	3	3	2	2,50

Principles	W1	W2	W3	W4	W5	W6	Average
Özel sektörü siber güvenlik alanında önemli bir oyuncu yapacak politika ve stratejilerin varlığı	2	3	3	3	2	2	2,50
Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması / Sözleşmeli personel çalıştırma, outsource hizmet alımı ve personel kiralama için yapılmış düzenlemeler / Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmış olması (Yüksek maaş ve geniş imkanlar vb.)/ Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için yapılmış düzenlemeler	3	2	3	2	2	3	2,50
Özel sektörden kabul edilebilir hizmet alma standartlarının belirlenmesi / Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları	1	3	3	3	2	3	2,50
Sektör spesifik (sektörel) veya tüm kritik altyapıları içine alan risk yönetimi sürecinin veya teknik kılavuz, dokümantasyonun varlığı	3	3	2	3	2	2	2,50
Mevzuat ile zorunlu tutulan sektörel / ulusal minimum güvenlik önlemlerinin varlığı / Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır	3	3	2	3	2	2	2,50
Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı	3	3	2	2	3	1	2,33
Devlet tarafından geliştirilip desteklenen public-private partnership programının varlığı	1	3	3	3	2	2	2,33
Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması / Devlet tarafından öncelikli alanların belirlenmiş olması özel sektörün bu alanlara sevk edilmesi	3	3	2	2	2	2	2,33
Ulusal seviyede kapasite geliştirme çalışmalarının varlığı / Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planının olması	2	3	3	3	1	2	2,33
Tüm eğitim seviyelerinde (ilkokuldan doktoraya) BT ve siber güvenlik konularında müfredatın olması / Siber güvenlik eğitimi veren akademik kurumlar yeterli sayıda olması	3	2	2	2	3	2	2,33

Principles	W1	W2	W3	W4	W5	W6	Average
Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmesi / Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır.	3	2	3	2	2	2	2,33
Kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendiren bir ulusal Siber Güvenlik Stratejisinin varlığı	3	1	2	3	3	1	2,17
Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı	2	2	1	3	3	2	2,17
Kritik altyapı işletmecileri için ISO 27001 gibi bir güvenlik standardı zorunluluğu olması	1	3	2	2	3	2	2,17
Sektör içi ve sektörler arası belirlenmiş bilgi paylaşımı kurallarının varlığı / Bilgi paylaşımı ve işbirliği için mevzuat altyapısının varlığı / İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması	1	3	2	2	2	2	2,00
Kurulmuş bir Ulusal CERT'in varlığı ve bunun uluslararası CERT'lerle işbirliği sağlıyor olması.	2	2	1	3	3	1	2,00
Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması	3	2	1	3	2	1	2,00
Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi / Özellikle sektöre yönelik eğitim veren kurumların varlığı ve fazlalığı	3	2	1	2	2	2	2,00
Bu yöneticilerin görev tanımlarında siber güvenlik sorumluluğu net olarak tanımlanmıştır.	1	2	2	3	2	2	2,00
Kurumlarda siber güvenliği de kapsayan tanımlı bir risk yönetim sürecinin var olması	2	1	1	3	3	2	2,00
Ulusal CSIRT'in kritik altyapılara yönelik yapılan ihbarları koordine etmesi, ilgili operatörlere eşgüdüm içerisinde çalışması	2	1	1	3	2	2	1,83
Sertifikalı devlet çalışanlarının oranı / Uluslararası geçerliliği olan sertifikaların kamu kurumları tarafından işe alımda tercih edilmesi	2	2	1	2	2	2	1,83
Sektör bazlı güvenlik standartlarının oluşturulmuş ve yayınlanmış olması	2	3	1	2	2	1	1,83
Ülkedeki her bir kritik altyapı sektörü için BDDK'nın yaptığına benzer, sektör spesifik kanuni siber güvenlik düzenlemelerinin varlığı	2	1	1	2	2	2	1,67
Kritik altyapıların ihtiyaçları dikkate alınarak kurulmuş bir CERT yapılanmasının varlığı (ABD'deki ICS-CERT örneği)	3	0	2	2	2	1	1,67

Principles	W1	W2	W3	W4	W5	W6	Average
Bilgi paylaşımı ve işbirliği için teknik altyapının varlığı / Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır. / Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi / Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması	3	1	1	3	1	1	1,67
İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımını koordine etmek üzere bir kurumun görevlendirilmiş olması / Amerika'da her sektör için bir bilgi paylaşım merkezi (ISAC- Information Sharing Center) tesis edilmiştir. Bu merkezler aracılığı ile sektör oyuncuları bilgi paylaşımında bulunabilmektedir. Bu gibi merkezlerin varlığı,	3	1	2	2	0	2	1,67
Kritik altyapı programında özel sektöre verilmiş somut görevlerin varlığı	0	2	2	2	2	2	1,67
Kritik teknolojilerin hızlı tedarik edilebilmesi için yasa değişikliği / Kamu İhale Kanununda teknik satın almaları kolaylaştırıcı, kaliteli ürün alınmasını sağlayıcı düzenlemelerin yapılmış olması	2	2	2	2	0	2	1,67
Ürün güvenliği ile ilgili standartların belirli olması	3	2	1	2	1	1	1,67
İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı	2	2	1	2	2	1	1,67
Denetim sonuçlarının ciddi yaptırımlarının olması (örneğin lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir)	3	1	1	3	2	0	1,67
Kurumsal bilgi güvenliği politikasının varlığı	1	1	1	3	3	1	1,67
Kurumsal yönetimsel toplantı tutanaklarında siber güvenlik ile ilgili kararların bulunması	2	1	1	2	3	1	1,67
Her bir kritik altyapı sektörü için oluşturulmuş siber güvenliği de sorumluluk alanı olarak tanımlamış denetleyici / düzenleyici kurum yapılanmasının varlığı	0	2	2	3	1	1	1,50
Bilgi paylaşım yükümlülükleri kanun ve yönetmeliklerle tespit edilmiş kurumsal, sektörel CERT'lerin varlığı	2	1	1	1	2	2	1,50
Ulusal siber güvenlik tatbikatlarına özel sektörün kapsamlı bir şekilde katılıyor olması	1	1	1	3	2	1	1,50
Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar	2	1	1	2	2	1	1,50
Sadece siber güvenlik üzerine çalışan kişi sayısının oranının belirli bir değerden fazla olması	2	2	1	2	0	1	1,33

Principles	W1	W2	W3	W4	W5	W6	Average
Kritik altyapı operatörlerinde sadece siber güvenliğe ilişkin kadroların varlığı	2	2	0	2	0	2	1,33
IT denetim Planlarının varlığı	0	1	1	3	2	1	1,33
Konunun önemine dikkat çekmek için yöneticilere odaklı bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) / Kritik altyapı işletmecilerinin tepe yöneticilerine bilgilendirme eğitimleri düzenli olarak verilmektedir.	2	0	1	3	1	1	1,33
Ulusal CSIRT (USOM) üzerinden yapılan bilgi paylaşımının varlığı	2	1	1	0	2	1	1,17
Özel sektörün siber güvenlik kurulu gibi yapılanmaların daimi üyesi olması	1	2	1	0	1	2	1,17
Hâlihazırdaki önemli yasaların kritik gözden geçirmesinin yapılmış olması (critical review of the current laws)	2	3	1	0	1	0	1,17
Kurumsal siber güvenlik metriklerinin belirlenmiş olması, metriklerin hesaplanması ve raporlanması	2	0	0	2	2	1	1,17
Siber güvenlikle ilgili kurumsal sorumlu kişilerin belirlenmesi	2	0	0	3	1	1	1,17
Yöneticilerin bir denetim mekanizması oluşturması	1	0	1	3	1	1	1,17
Üst düzey karar alıcıların (başbakan, bakan vb.) siber güvenlik danışmanı olması	**3**	0	0	2	1	0	1,00
Özel sektörü teşvik edici maddi çözümler (vergi muafiyeti, kamunun teknik imkânlarından ücretsiz faydalanma, ulusal siber güvenlik kurumlarından ücretsiz danışmanlık alınması vb.) yürürlüktedir. / Özel sektörün çalışmalara katılması için devlet ve sektör işletmecileri tarafından maddi kaynak ayrılması	3	0	1	0	1	1	1,00
Devlette güvenlik uzmanı olarak çalışan memurların memnuniyet oranlarının belirli bir değerden yukarıda olması	1	1	1	1	1	1	1,00
Eğitim veren yerler için devlet tarafından teşvik verilmesi	3	1	1	0	0	1	1,00
Özel sektörün siber saldırılara ilişkin gerçek verileri paylaşmaktan imtina etmesini engelleyecek yasal düzenlemelerin varlığı	0	0	1	0	2	2	0,83
Özel sektörün siber güvenlik önlemlerini ilave masraf olarak görerek uygulamamasının önüne geçerek Yasal düzenlemelerin varlığı	0	0	2	0	2	1	0,83
Geliştirme yapacak personelin teknik olgunluğu ölçülmekte ve gerekli görüldüğünde zorunlu eğitime gönderilmektedir.	2	0	0	1	1	1	0,83

Principles	W1	W2	W3	W4	W5	W6	Average
Kamuda üst düzey yöneticilerin siber güvenlik farkındalık eğitimi almış olması	1	0	1	1	1	0	0,67
Bilgileri gizliliğine göre sınıflandırmakta kullanılan, bu sınıflandırmaya göre de bilginin paylaşımı ile ilgili kuralların belirlenmesinde rol oynayan bir veri koruma kanununun varlığı	1	1	0	0	2	0	0,67
Sektör içi ve sektörler arası organizasyonların (konferans, workshop vb) varlığı	1	0	0	1	1	1	0,67
Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	1	0	0	1	1	1	0,67
Özel sektörü temsil eden sivil inisiyatif gruplarının var olması ve aktif faaliyetler yapması	0	0	0	3	0	1	0,67
Risk yönetim süreci işletimiyle ilgili kayıtların varlığı	1	0	0	2	0	1	0,67
Konunun önemine dikkat çekmek için bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.)	2	0	1	0	1	0	0,67
Siber güvenlik alanında insan kaynağı geliştirilmesini koordine etmekle görevli/sorumlu kurum ya da kurul gibi bir yapının varlığı	0	0	1	0	0	2	0,50
İşletmecilerle ürün sağlayıcılar arasında güvenlikle ilgili sorunların iletildiği kanalların oluşturulup oluşturulmadığı	0	0	0	3	0	0	0,50
Ürün/hizmet sağlayıcılarını bilgilendirici ve katılım zorunluluğu olan eğitim/konferans/seminer vb. faaliyetler yapılmaktadır. / İşletmeciler ve ürün/hizmet sağlayıcıların katılacağı sektör spesifik tatbikatlar ve konferansların varlığı	1	0	0	1	0	1	0,50
Genel sektörel durumun ölçümlendiği bir bilgi toplama mekanizmasının varlığı ve işlerliği	0	0	0	3	0	0	0,50
Denetimlerin yapılması ve çıktılarının merkezi bir ortamda toplanıp düzenli olarak değerlendirilmesine imkan sağlayan teknik çözümler devreye alınmıştır.	1	0	0	2	0	0	0,50
Operatörlerin iş geliştirme ve tasarım süreçlerinde güvenlik farkındalığı düzenli olarak ölçülmektedir.	1	0	1	0	1	0	0,50

Principles	W1	W2	W3	W4	W5	W6	Average
Personel sayısının yetersiz kaldığı durumlarda, yabancı memur ve işçi alımının önünü açacak yasal düzenlemeler yürürlüktedir. Bunun için klerans çıkarılması gibi güvenlik soruşturmaları devreye alınmıştır	1	0	1	0	0	0	0,33
Kritik altyapı işletmecilerinin ürün/hizmet sağlayıcıları ile bir araya gelebildikleri sivil toplum örgütleri vardır	0	0	0	2	0	0	0,33
Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	1	0	0	1	0	0	0,33
Siber güvenlik tatbikatlarındaki takımların başarı durumu	1	0	0	0	0	0	0,17
Devlette güvenlik uzmanı olarak çalışan memurların ürünlerden memnuniyet oranı	0	0	0	0	0	0	0,00

Round-4: Controlled Opinion Feedback

We are in the last round of the Delphi survey. In this round, I have organized the criteria according to their arithmetic averages, from the highest to the lowest.

As it was in the third round, I would like you to review your grades (weights of the principles) in the face of those of others. And again as in the third round, your grades are in the Points-x column.

Additionally, I would like you to evaluate your zero points for the criteria with an average of one or higher. The important matter in the Delphi survey is the consensus of the experts. Therefore, I will not include the criteria with at least one zero weight in the maturity model as the situation shows that there has been no consensus on those criteria. Please look at your zero points once more and if you still insist on a zero weight, please send me your reason not to give at least one point for them. When you are one of the few experts with zero points, you can see that the related parts are shaded gray.

Round-4: Output

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.	1. Siber tehditleri dikkate alan bir kritik altyapıların korunması programının (CIPP) varlığı	2	3	3	2	3	2	2,50
	2. Ulusal güvenlikten sorumlusu kurum ve kuruluşların aynı zamanda kritik altyapıları siber tehditlere karşı koruma sorumlulukları olması (ABD'de DHS örneği) / Kritik altyapıların siber güvenliğinden kanunen sorumlu kurum ile ulusal güvenlikten sorumlu kurum ve kuruluşlar arasında eşgüdüm mekanizmalarının oluşturulmuş olması / Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) / Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması	2	3	2	3	3	2	2,50
	3. Devletin en üst düzey yöneticilerinin siber güvenlik konusunda ciddi uzmanlığa sahip danışmanları bulunmaktadır. Bu danışmanlar teknik, hukuki ve uluslararası ilişkiler bağlamında gerekli ve yeterli bilgilendirmeleri yapmaktadır.	3	2	1	2	1	1	1,67
	4. Kamuda üst düzey yöneticilerin siber güvenlik farkındalık eğitimi almış olması	1	0	1	1	1	0	0,67
	5. Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı	3	3	2	2	3	2	2,50
	6. Her bir kritik altyapı sektörü için oluşturulmuş siber güvenliği de sorumluluk alanı olarak tanımlamış denetleyici / düzenleyici kurum yapılanmasının varlığı	2	2	2	3	1	1	1,83

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
	7. Ülkedeki her bir kritik altyapı sektörü için BDDK'nın yaptığına benzer, sektör spesifik kanuni siber güvenlik düzenlemelerinin varlığı	2	0	1	2	2	2	1,50
	8. Kritik altyapıların ihtiyaçları dikkate alınarak kurulmuş bir CERT yapılanmasının varlığı (ABD'deki ICS-CERT örneği)	3	2	2	2	2	1	2,00
	9. Kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendiren bir ulusal Siber Güvenlik Stratejisinin varlığı	3	1	2	3	3	1	2,17
	10. Sektör spesifik (sektörel) veya tüm kritik altyapıları içine alan risk yönetimi sürecinin veya teknik kılavuz, dokümantasyonun varlığı	3	3	2	3	2	2	2,50
The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.	1. Devlet tarafından geliştirilip desteklenen public-private partnership programının varlığı	1	3	3	3	2	2	2,33
	2. Bilgileri gizliliğine göre sınıflandırmakta kullanılan, bu sınıflandırmaya göre de bilginin paylaşımı ile ilgili kuralların belirlenmesinde rol oynayan bir veri koruma kanununun varlığı	1	1	0	0	1	1	0,67
	3. Sektör içi ve sektörler arası belirlenmiş bilgi paylaşımı kurallarının varlığı / Bilgi paylaşımı ve işbirliği için mevzuat altyapısının varlığı / İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması	1	3	2	2	2	2	2,00
	4. Bilgi paylaşım yükümlülükleri kanun ve yönetmeliklerle tespit edilmiş kurumsal, sektörel CERT'lerin varlığı	2	1	1	1	2	2	1,50
	5. Kurulmuş bir Ulusal CERT'in varlığı ve bunun uluslararası CERT'lerle işbirliği sağlıyor olması.	2	2	1	3	3	1	2,00

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
	6. Bilgi paylaşımı ve işbirliği için teknik altyapının varlığı / Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır. / Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi / Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması	3	1	1	3	1	1	1,67
	7. İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımını koordine etmek üzere bir kurumun görevlendirilmiş olması / Amerika'da her sektör için bir bilgi paylaşım merkezi (ISAC-Information Sharing Center) tesis edilmiştir. Bu merkezler aracılığı ile sektör oyuncuları bilgi paylaşımında bulunabilmektedir. Bu gibi merkezlerin varlığı,	3	1	2	2	0	2	1,67
	8. Sektör içi ve sektörler arası organizasyonların (konferans, workshop vb) varlığı	1	0	0	1	1	1	0,67
	9. Ulusal CSIRT (USOM) üzerinden yapılan bilgi paylaşımının varlığı	2	0	1	1	2	1	1,17
	10. Ulusal CSIRT'in kritik altyapılara yönelik yapılan ihbarları koordine etmesi, ilgili operatörlere eşgüdüm içerisinde çalışması	2	1	1	3	2	2	1,83
	11. Özel sektörün siber saldırılara ilişkin gerçek verileri paylaşmaktan imtina etmesini engelleyecek yasal düzenlemelerin varlığı	0	0	1	0	1	2	0,67
The private sector is not perceived by the government and critical infrastructure	1. Özel sektörü siber güvenlik alanında önemli bir oyuncu yapacak politika ve stratejilerin varlığı	2	3	3	3	2	2	2,50
	2. Kritik altyapı programında özel sektöre verilmiş somut görevlerin varlığı	0	2	2	2	2	2	1,67

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
operators as an important stakeholder in national cyber security efforts.	3. Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması	3	2	1	3	2	1	2,00
	4. Özel sektörün siber güvenlik kurulu gibi yapılanmaların daimi üyesi olması	1	2	1	1	1	2	1,33
	5. Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması / Devlet tarafından öncelikli alanların belirlenmiş olması özel sektörün bu alanlara sevk edilmesi	3	3	2	2	2	2	2,33
	6. Özel sektörü teşvik edici maddi çözümler (vergi muafiyeti, kamunun teknik imkânlarından ücretsiz faydalanma, ulusal siber güvenlik kurumlarından ücretsiz danışmanlık alınması vb.) yürürlüktedir. / Özel sektörün çalışmalara katılması için devlet ve sektör işletmecileri tarafından maddi kaynak ayrılması	3	0	1	1	1	1	1,17
	7. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	1	0	0	1	1	1	0,67
	8. Özel sektörü temsil eden sivil inisiyatif gruplarının var olması ve aktif faaliyetler yapması	0	0	0	1	0	1	0,33
	9. Ulusal siber güvenlik tatbikatlarına özel sektörün kapsamlı bir şekilde katılıyor olması	1	1	1	3	2	1	1,50
	10. Özel sektörün siber güvenlik önlemlerini ilave masraf olarak görerek uygulamamasının önüne geçerek Yasal düzenlemelerin varlığı	0	0	2	0	1	1	0,67
The laws of public procurements and civil	1. Hâlihazırdaki önemli yasaların kritik gözden geçirmesinin yapılmış olması (critical review of the current laws)	2	3	3	2	2	3	2,50

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
servants have adverse effects on the cyber security of governmental critical infrastructure owners.	2. Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması / Sözleşmeli personel çalıştırma, outsource hizmet alımı ve personel kiralama için yapılmış düzenlemeler / Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmış olması (Yüksek maaş ve geniş imkanlar vb.)/ Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için yapılmış düzenlemeler	3	2	3	2	2	3	2,50
	3. Devlette güvenlik uzmanı olarak çalışan memurların memnuniyet oranlarının belirli bir değerden yukarıda olması	1	0	1	1	1	1	0,83
	4. Kritik teknolojilerin hızlı tedarik edilebilmesi için yasa değişikliği / Kamu İhale Kanununda teknik satın almaları kolaylaştırıcı, kaliteli ürün alınmasını sağlayıcı düzenlemelerin yapılmış olması	2	2	2	2	0	2	1,67
	5. Devlette güvenlik uzmanı olarak çalışan memurların ürünlerden memnuniyet oranı	0	0	0	0	0	0	0,00
The number of qualified cyber security experts is limited.	1. Ulusal seviyede kapasite geliştirme çalışmalarının varlığı / Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planının olması	2	3	3	3	2	2	2,50
	2. Siber güvenlik alanında insan kaynağı geliştirilmesini koordine etmekle görevli/sorumlu kurum ya da kurul gibi bir yapının varlığı	0	0	1	0	0	2	0,50
	3. Sadece siber güvenlik üzerine çalışan kişi sayısının oranının belirli bir değerden fazla olması	2	2	1	2	0	1	1,33
	4. Sertifikalı devlet çalışanlarının oranı / Uluslararası geçerliliği olan sertifikaların kamu kurumları tarafından işe alımda tercih edilmesi	2	1	1	2	2	2	1,67

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
	5. Siber güvenlik tatbikatlarındaki takımların başarı durumu	1	0	0	0	0	0	0,17
	6. Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi / Özellikle sektöre yönelik eğitim veren kurumların varlığı ve fazlalığı	3	1	1	2	2	2	1,83
	7. Eğitim veren yerler için devlet tarafından teşvik verilmesi	3	1	1	1	0	1	1,17
	8. Tüm eğitim seviyelerinde (ilkokuldan doktoraya) BT ve siber güvenlik konularında müfredatın olması / Siber güvenlik eğitimi veren akademik kurumlar yeterli sayıda olması	3	2	2	2	3	2	2,33
	9. Personel sayısının yetersiz kaldığı durumlarda, yabancı memur ve işçi alımının önünü açacak yasal düzenlemeler yürürlüktedir. Bunun için klerans çıkarılması gibi güvenlik soruşturmaları devreye alınmıştır	1	0	1	0	0	0	0,33
	10. Kritik altyapı operatörlerinde sadece siber güvenliğe ilişkin kadroların varlığı	2	3	1	2	1	1	1,67
The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.	1. Özel sektörden kabul edilebilir hizmet alma standartlarının belirlenmesi / Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları	2	3	3	3	2	3	2,67
	2. Kritik altyapı işletmecilerinin dışardan IT hizmeti aldıkları kuruluşlarla ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı / ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır	3	3	2	2	3	3	2,67
	3. Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı	2	2	1	3	3	2	2,17

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
	4. Kritik altyapı işletmecilerinin ürün/hizmet sağlayıcıları ile bir araya gelebildikleri sivil toplum örgütleri vardır	0	0	0	1	0	0	0,17
	5. İşletmecilerle ürün sağlayıcılar arasında güvenlikle ilgili sorunların iletildiği kanalların oluşturulup oluşturulmadığı	0	0	0	2	0	0	0,33
	6. Ürün güvenliği ile ilgili standartların belirli olması	3	2	1	2	2	1	1,83
	7. Ürün/hizmet sağlayıcılarını bilgilendirici ve katılım zorunluluğu olan eğitim/konferans/seminer vb. faaliyetler yapılmaktadır. / İşletmeciler ve ürün/hizmet sağlayıcıların katılacağı sektör spesifik tatbikatlar ve konferansların varlığı	1	0	0	1	0	1	0,50
The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı / Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir.	3	3	2	3	2	3	2,67
	2. Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar / Her sektörün üst kurulunun mevzuat ile denetim yapması	3	3	3	3	3	3	3,00
	3. İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı	2	2	1	2	2	1	1,67
	4. IT denetim Planlarının varlığı	1	0	1	2	2	1	1,17
	5. Genel sektörel durumun ölçümlendiği bir bilgi toplama mekanizmasının varlığı ve işlerliği	0	0	0	2	0	0	0,33
	6. Denetimlerin yapılması ve çıktılarının merkezi bir ortamda toplanıp düzenli olarak değerlendirilmesine imkan sağlayan teknik çözümler devreye alınmıştır.	1	0	0	1	0	0	0,33

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
	7. Denetim sonuçlarının ciddi yaptırımlarının olması (örneğin lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir)	3	1	1	2	2	2	1,83
The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.	1. Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı	3	3	3	3	2	3	2,83
	2. Kurumsal bilgi güvenliği politikasının varlığı	1	0	1	3	3	1	1,50
	3. Kurumsal yönetimsel toplantı tutanaklarında siber güvenlik ile ilgili kararların bulunması	2	0	1	2	2	1	1,33
	4. Kurumsal siber güvenlik metriklerinin belirlenmiş olması, metriklerin hesaplanması ve raporlanması	2	0	0	2	2	1	1,17
	5. Bu yöneticilerin görev tanımlarında siber güvenlik sorumluluğu net olarak tanımlanmıştır.	1	0	2	3	2	2	1,67
	6. Konunun önemine dikkat çekmek için yöneticilere odaklı bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.) / Kritik altyapı işletmecilerinin tepe yöneticilerine bilgilendirme eğitimleri düzenli olarak verilmektedir.	2	0	1	2	1	1	1,17
	7. Siber güvenlikle ilgili kurumsal sorumlu kişilerin belirlenmesi	2	0	0	3	1	0	1,00
	8. Yöneticilerin bir denetim mekanizması oluşturması	1	0	1	3	1	1	1,17
The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.	1. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı / Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır. / Kritik altyapı işletmecilerine yönelik risk yönetimi ve BGYS konularında yaptırım getiren kanuni düzenleme ve düzenleyici kurulun buna göre denetimi	3	3	3	3	3	3	3,00

Root Causes	Principles	W1	W2	W3	W4	W5	W6	Average
	2. Kritik altyapı işletmecileri için ISO 27001 gibi bir güvenlik standardı zorunluluğu olması	1	3	2	2	3	2	2,17
	3. Kurumlarda siber güvenliği de kapsayan tanımlı bir risk yönetim sürecinin var olması	2	0	1	3	3	2	1,83
	4. Risk yönetim süreci işletimiyle ilgili kayıtların varlığı	1	0	0	2	0	1	0,67
	5. Konunun önemine dikkat çekmek için bilgilendirme faaliyetleri (konferans, hacking yarışması, seminer, eğitim v.s.)	2	0	1	0	1	0	0,67
Security is considered by governmental critical infrastructure owners as an add-on and not as a design construct.	1. Mevzuat ile zorunlu tutulan sektörel / ulusal minimum güvenlik önlemlerinin varlığı / Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır	3	3	2	3	2	2	2,50
	2. Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmesi / Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır.	3	2	3	2	2	2	2,33
	3. Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar	2	1	1	2	2	1	1,50
	4. Sektör bazlı güvenlik standartlarının oluşturulmuş ve yayınlanmış olması	2	3	1	2	2	1	1,83
	5. Kritik altyapılarda Siber Güvenlik konulu, özel sektör (hem vendor hem de işletmeci) ve kamunun (hem işletmeci hem de regülatör) bir araya geldiği etkinliklerin düzenli olarak yapılıyor olması	1	0	0	1	0	0	0,33
	6. Operatörlerin iş geliştirme ve tasarım süreçlerinde güvenlik farkındalığı düzenli olarak ölçülmektedir.	1	0	1	0	0	0	0,33
	7. Geliştirme yapacak personelin teknik olgunluğu ölçülmekte ve gerekli görüldüğünde zorunlu eğitime gönderilmektedir.	2	0	0	1	1	1	0,83

Round-5: Input

No	Türkçe	English
1	A. Siber tehditleri dikkate alan bir kritik altyapıların korunması programı (CIPP) var mıdır?	1) A Critical Infrastructure Protection Program (CIPP) that considers cyber threats
2	B. Ulusal güvenlikten sorumlusu kurum ve kuruluşların aynı zamanda kritik altyapıları siber tehditlere karşı koruma sorumlulukları olması (ABD'de DHS örneği) / Kritik altyapıların siber güvenliğinden kanunen sorumlu kurum ile ulusal güvenlikten sorumlu kurum ve kuruluşlar arasında eşgüdüm mekanizmalarının oluşturulmuş olması / Önemli karar alma mekanizmalarında (Başkanlık, başbakanlık, MGK gibi) siber güvenlikle ilgili bir birimin olması (bilgi işlem içindeki kuruma iç hizmet veren birimi kastetmiyorum) / Siber Güvenlik Kurulu Başkanının MGK toplantısına (benzeri) zaman zaman katılması	2) The management of the CIPP by a governmental organization which has responsibilities on national security as well OR the communication between CIPP body and national security body
3	C. Devletin en üst düzey yöneticilerinin siber güvenlik konusunda ciddi uzmanlığa sahip danışmanları bulunmaktadır. Bu danışmanlar teknik, hukuki ve uluslararası ilişkiler bağlamında gerekli ve yeterli bilgilendirmeleri yapmaktadır.	3) The existence of the staff who provides technical, regulatory and diplomatic cyber security consultancy to the head of the state
4	D. Kritik altyapıların siber tehditlerden korunması çalışmalarına özel olarak belirlenmiş yıllık bütçenin varlığı	4) The dedicated budget to critical infrastructure protection efforts
5	E. Her bir kritik altyapı sektörü için oluşturulmuş siber güvenliği de sorumluluk alanı olarak tanımlamış denetleyici / düzenleyici kurum yapılanmasının varlığı	5) The regulatory and supervision agencies for each critical sector that control and direct the critical infrastructure owners on cyber security
6	F. Kritik altyapıların ihtiyaçları dikkate alınarak kurulmuş bir CERT yapılanmasının varlığı (ABD'deki ICS-CERT örneği)	6) CSIRT organization dedicated to the protection of the critical infrastructures
7	G. Kritik altyapıları ulusal güvenliğinin bir parçası olarak değerlendiren bir ulusal Siber Güvenlik Stratejisinin varlığı	7) Up-to-date National cyber security strategy that considers cyber security of critical infrastructures as part of national security
8	H. Sektör spesifik (sektörel) veya tüm kritik altyapıları içine alan risk yönetimi sürecinin veya teknik kılavuz, dokümantasyonun varlığı	8) Nation-wide or sector-wide risk analysis and risk management activities
9	I. Devlet tarafından geliştirilip desteklenen public-private partnership programının varlığı	9) Public-private partnership program which is developed and supported by the government

No	Türkçe	English
10	J. Sektör içi ve sektörler arası belirlenmiş bilgi paylaşımı kurallarının varlığı / Bilgi paylaşımı ve işbirliği için mevzuat altyapısının varlığı / İlgili kuruluşlar arasında siber güvenlikle ilgili bilgi paylaşımı esaslarının belirlenip yayınlanmış olması	10) Regulation that specifies the inter/intra sector information sharing and cooperation principals
11	K. Bilgi paylaşım yükümlülükleri kanun ve yönetmeliklerle tespit edilmiş kurumsal, sektörel CERT'lerin varlığı	11) Sector based CSIRTs that have information sharing responsibilities determined by the regulations
12	L. Kurulmuş bir Ulusal CERT'in varlığı ve bunun uluslararası CERT'lerle işbirliği sağlıyor olması.	12) National CSIRT and the international cooperation of the National CSIRT with other CSIRTs
13	M. Bilgi paylaşımı ve işbirliği için teknik altyapının varlığı / Bilgi paylaşımı ve işbirliğini kolaylaştıracak teknik çözümler hazırlanmıştır. / Kritik sektörlerde yaşanan güvenlik olaylarının bir merkezde toplanması ve istatistik oluşturulabilmesi / Sektör içi ve sektörler arası online bilgi paylaşım platformlarının oluşturulmuş olması	13) The technical setup to fulfill the inter/intra sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers)
14	N. Ulusal CSIRT'in kritik altyapılara yönelik yapılan ihbarları koordine etmesi, ilgili operatörlere eşgüdüm içerisinde çalışması	14) National CSIRT that coordinates the cyber incidents related to critical infrastructures by including the relevant sectorial CSIRTs and critical infrastructure owners as needed
15	O. Özel sektörü siber güvenlik alanında önemli bir oyuncu yapacak politika ve stratejilerin varlığı	15) The government policies that position private sector as a key player in national cyber security efforts
16	P. Ulusal siber güvenlik stratejisi ya da sektörel strateji hazırlık aşamalarında özel sektörün de katkısının alınması	16) The participation of the private sector in preparation of the national or sectorial cyber security strategies **(Should the principle-16 be chosen as a unique principle or considered as a part of the principle-15?)** **PRINCIPLE-1**

No	Türkçe	English
17	Q. Özel sektörün siber güvenlik kurulu gibi yapılanmaların daimi üyesi olması	17) The permanent seat of private sector at the national boards like cyber security council **(Should the principle-17 be chosen as a unique principle or considered as a part of the principle-15?)** **PRINCIPLE-2**
18	R. Girişimcilik, araştırma ve geliştirme faaliyetleri için devletin liderlik yapması / Devlet tarafından öncelikli alanların belirlenmiş olması özel sektörün bu alanlara sevk edilmesi	18) The government leadership for the identification of the priority areas in cyber security, innovation, and research & development
19	S. Ulusal siber güvenlik tatbikatlarına özel sektörün kapsamlı bir şekilde katılıyor olması	19) The participation of the private sector in the national cyber security exercises extensively **(Should the principle-19 be chosen as a unique principle or considered as a part of the principle-15?)** **PRINCIPLE-3**
20	T. Hâlihazırdaki önemli yasaların kritik gözden geçirmesinin yapılmış olması (critical review of the current laws)	20) Critical review and update of the existing legislation especially for governmental critical infrastructure operators
21	U. Yetkin personeli yüksek maaşla çalıştırmak için imkanların (sözleşmeli personel, özel firmadan personel kiralama) tesis edilmiş olması / Sözleşmeli personel çalıştırma, outsource hizmet alımı ve personel kiralama için yapılmış düzenlemeler / Kaliteli personel alınmasını kolaylaştırıcı mevzuat hazırlanmış olması (Yüksek maaş ve geniş imkanlar vb.)/ Kritik altyapı işletmecilerinde çalışacak bilgi işlem ve siber güvenlik personeline daha cazip ücretlerin verilmesi için yapılmış düzenlemeler	21) Making amendments to regulations so that outsourced personnel / qualified government officials with higher salaries / contracted personnel can be hired in governmental critical infrastructures **(Should the principle-21 be chosen as a unique principle or considered as a part of the principle-20?)** **PRINCIPLE-4**
22	V. Ulusal seviyede kapasite geliştirme çalışmalarının varlığı / Devletin genel olarak ya da spesifik sektörlerin siber işgücü geliştirme stratejisi/planının olması	22) National capacity building efforts such as the existence of national / sectorial plans and strategies on cyber security capacity building

No	Türkçe	English
23	W. Sertifikalı devlet çalışanlarının oranı / Uluslararası geçerliliği olan sertifikaların kamu kurumları tarafından işe alımda tercih edilmesi	23) The requirement of the internationally accepted certificates in the recruitments at the critical infrastructure owners
24	X. Siber güvenlik eğitimleri veren özel, kamu ve akademik kurumların sayısı ve kalitesi / Özellikle sektöre yönelik eğitim veren kurumların varlığı ve fazlalığı	24) Qualified cyber security training institutions (private, academic or governmental) dedicated to the critical infrastructure operators
25	Y. Tüm eğitim seviyelerinde (ilkokuldan doktoraya) BT ve siber güvenlik konularında müfredatın olması / Siber güvenlik eğitimi veren akademik kurumlar yeterli sayıda olması	25) Cyber security and IT curriculum for all levels of the education from elementary schools to universities
26	Z. Kritik altyapı operatörlerinde sadece siber güvenliğe ilişkin kadroların varlığı	26) The dedicated cyber security personnel at critical infrastructure operators
27	AA. Özel sektörden kabul edilebilir hizmet alma standartlarının belirlenmesi / Kritik altyapı operatörlerinin uyacağı sektörel veya ulusal seviye dış hizmet / ürün alım kuralları	27) National / sectorial product and service procurement standards or rules for critical infrastructure operators
28	BB. Kritik altyapı işletmecilerinin dışardan IT hizmeti aldıkları kuruluşlarla ilişkilerini hangi esaslara göre yöneteceklerini belirleyen bir mevzuat olmalı / ABD'de sağlık sektöründe çok sıkı takip edilen FDA yükümlülükleri benzeri, kamuya alınacak her türlü ürün ve hizmetin çok sıkı regüle edilmesine yönelik düzenlemeler yapılmıştır	28) Regulation that specifies the fundamentals of the relations with third parties **(Is the principle-28 same as the principle-27 or are they different?)** **PRINCIPLE-5**
29	CC. Kritik altyapı işletmecilerinin IT hizmeti alacakları kuruluşları akredite eden bir sistem kurulmuş olmalı	29) The certification of IT companies that are eligible for IT service procurements by critical infrastructure operators
30	DD. Ürün güvenliği ile ilgili standartların belirli olması	30) The security standards for the IT products to be used by critical infrastructure operators
31	EE. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal iç/dış tetkik kurallarının varlığı / Kritik altyapı işletmecilerinin BT denetim mekanizmalarına uyumluluğu yasal zorunluluk ile düzenlenmiştir.	31) The national or sectorial regulations that enforce the internal / external audit for critical infrastructure operators

No	Türkçe	English
32	FF. Her bir kritik altyapı sektörünün regülatör kuruluşu sektördeki işletmecilere düzenli olarak BT denetimi (siber güvenliği de kapsayacak şekilde) yapar / Her sektörün üst kurulunun mevzuat ile denetim yapması	32) The regular cyber security audits for critical infrastructure operators performed by the regulatory agencies of the sectors
33	GG. İç denetim birimlerinde IT denetim bilgi birikimine sahip personel sayısı	33) The experienced IT auditors who are employed within the internal audit units of the critical infrastructure operators
34	HH. Denetim sonuçlarının ciddi yaptırımlarının olması (örneğin lisans iptali veya iş alanının kısıtlanmasına kadar gidebilmelidir)	34) The sanctions imposed by the regulatory agencies to the critical infrastructure operators for the nonconformities
35	II. Kritik altyapı operatörlerinin siber güvenliğinden doğrudan kurum yöneticilerini sorumlu tutan düzenlemelerin varlığı	35) The regulation that makes top level management of the critical infrastructure operators responsible for the cyber security by imposing information security governance
36	JJ. Kritik altyapı işletmecilerinin uyacağı sektörel veya ulusal risk yönetimi kurallarının varlığı / Kritik altyapı işletmelerinde yazılı bir risk yönetim süreci, tabi oldukları mevzuat düzenlenerek zorunlu kılınmıştır. / Kritik altyapı işletmecilerine yönelik risk yönetimi ve BGYS konularında yaptırım getiren kanuni düzenleme ve düzenleyici kurulun buna göre denetimi	36) The regulation that enforces the cyber security risk management process to be conducted by critical infrastructure owners
37	KK. Kritik altyapı işletmecileri için ISO 27001 gibi bir güvenlik standardı zorunluluğu olması	37) The obligation of a comprehensive security standard such as ISO 27001 for the critical infrastructure owners **(Should the principle-37 be chosen as a unique principle or considered as a part of the principle-40?)** **PRINCIPLE-6**
38	LL. Mevzuat ile zorunlu tutulan sektörel / ulusal minimum güvenlik önlemlerinin varlığı / Kritik altyapı işletmelerinin uyması gereken minimum güvenlik önemleri önlemleri dokümanı yayımlanmıştır	38) Minimum security countermeasures for the critical infrastructure owners that are obliged by regulations

No	Türkçe	English
39	MM. Kritik altyapı operatörlerinde kurulacak bilgi sistemleri için mevzuatta düzenleme getirilmesi / Güvenlik tedbirlerinin alınması yasal olarak zorlanmaktadır.	39) The regulations for information system and security countermeasures to be installed at critical infrastructure operators **(Should the principle-39 chosen as a unique principle or considered as a part of the principle-38?)** **PRINCIPLE-7**
40	NN. Sektör spesifik bilgi sistemleri tasarımı ve kurulumu için teknik kılavuzlar	40) Sector-specific technical guidance documents for the secure design, set-up and operation of the networks of critical infrastructure operators
41	OO. Sektör bazlı güvenlik standartlarının oluşturulmuş ve yayınlanmış olması	41) The sectorial or national security standard for critical infrastructure operators that sets outs the security best practices for the sectors

Round -5: Controlled opinion feedback
Do you have comments on the English translations of the principles?
What is your answer for the questions in the second column of the rows of 16, 17, 19, 21, 28, 37, and 39?

Round -5: Output

Principle under consideration*	Expert-1	Expert-2	Expert-3	Expert-4	Expert-5	Expert-6
PRINCIPLE-1	Keep	Keep	Keep	Keep	Keep	Keep
PRINCIPLE-2	Hesitant	Discard	Keep	Keep	Keep	Keep
PRINCIPLE-3	Keep	Discard	Keep	Keep	Discard	Keep
PRINCIPLE-4	Keep	Discard	Keep	Keep	Keep	Keep
PRINCIPLE-5	Discard	Discard	Discard	Discard	Discard	Discard
PRINCIPLE-6	Keep	Keep	Keep	Keep	Keep	Hesitant
PRINCIPLE-7	Discard	Keep	Discard	Keep	Discard	Discard

* The descriptions of the principles are at the second column of the table under the section "Round-5: Input".
Selected principles: Principle-1, Principle-2, Principle-3, Principle-4, Principle-6, Principle-7
Discarded principle: Principle-5

English Translation (Input of the Round-5)	English Translation – Comments of the Experts Reflected (Output of the Round-5)
1. A Critical Infrastructure Protection Program (CIPP) that considers cyber threats	1) A Critical Infrastructure Protection Program (CIPP) that considers cyber threats
2. The management of the CIPP by a governmental organization which has responsibilities on national security as well OR the communication between CIPP body and national security body	2) The management of the CIPP by a governmental organization which has responsibilities for the national security as well / the communication between CIPP and national security bodies
3. The existence of the staff who provides technical, regulatory and diplomatic cyber security consultancy to the head of the state	3) The existence of a consultant who provides technical, regulatory and diplomatic cyber security consultancy for the head of the state
4. The dedicated budget to critical infrastructure protection efforts	4) Budget allocated to critical infrastructure protection efforts
5. The regulatory and supervision agencies for each critical sector that control and direct the critical infrastructure owners on cyber security	5) Regulatory agencies that set cyber security regulations and check their applications for each critical sector
6. CSIRT organization dedicated to the protection of the critical infrastructures	6) A CSIRT organization dedicated to the protection of critical infrastructures
7. Up-to-date National cyber security strategy that considers cyber security of critical infrastructures as part of national security	7) A national cyber security strategy that considers the cyber security of critical infrastructures as part of national security
8. Nation-wide or sector-wide risk analysis and risk management activities	8) Nation-wide risk analysis and risk management activities which cover all critical sectors / sector-wide wide risk analysis and risk management activities
9. Public-private partnership program which is developed and supported by the government	9) A public-private partnership program which is developed and supported by the government
10. Regulation that specifies the inter/intra sector information sharing and cooperation principals	10) Regulations that specify the inner - inter sector information sharing and cooperation principles
11. Sector based CSIRTs that have information sharing responsibilities determined by the regulations	11) Sector based CSIRTs that have information sharing responsibilities determined by the regulations

English Translation (Input of the Round-5)	English Translation – Comments of the Experts Reflected (Output of the Round-5)
12. National CSIRT and the international cooperation of the National CSIRT with other CSIRTs	12) The existence of an internationally recognized National CSIRT that performs international cooperation with other CSIRTs
13. The technical setup to fulfill the inter/intra sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers)	13) A technical infrastructure to fulfill the inner - inter sector information sharing needs (online information sharing portals, statistics dashboards, data collections centers)
14. National CSIRT that coordinates the cyber incidents related to critical infrastructures by including the relevant sectorial CSIRTs and critical infrastructure owners as needed	14) A National CSIRT that handles the warnings of cyber incidents related to critical infrastructures by coordinating with the relevant sectorial CSIRTs and critical infrastructure owners when needed
15. The government policies that position private sector as a key player in national cyber security efforts	15) Government policies and strategies that position private sector as a key player in national cyber security efforts
16. The participation of the private sector in preparation of the national or sectorial cyber security strategies	16) The participation of the private sector in the preparation of the national or sectorial cyber security strategies
17. The permanent seat of private sector at the national boards like cyber security council	17) Permanent seat for the private sector in the national boards like the cyber security council
18. The government leadership for the identification of the priority areas in cyber security, innovation, and research & development	18) Government leadership for innovation, research & development activities, and the identification of the priority areas in cyber security by the government
19. The participation of the private sector in the national cyber security exercises extensively	19) The extensive participation of the private sector in the national cyber security exercises
20. Critical review and update of the existing legislation especially for governmental critical infrastructure operators	20) Critical review and update of the existing legislation that may affect critical infrastructures (especially for the needs of the governmental critical infrastructure operators)

English Translation (Input of the Round-5)	English Translation – Comments of the Experts Reflected (Output of the Round-5)
21. Making amendments to regulations so that outsourced personnel / qualified government officials with higher salaries / contracted personnel can be hired in governmental critical infrastructures	21) Making amendments to the regulations to hire outsourced personnel / qualified government officials with higher salaries / contracted personnel in governmental critical infrastructures
22. National capacity building efforts such as the existence of national / sectorial plans and strategies on cyber security capacity building	22) National capacity building plans and strategies
23. The requirement of the internationally accepted certificates in the recruitments at the critical infrastructure owners	23) Preference of the internationally accepted certificate owners in the recruitments by critical infrastructure owners
24. Qualified cyber security training institutions (private, academic or governmental) dedicated to the critical infrastructure operators	24) Qualified and sufficient number of cyber security training institutions (private, academic or governmental) that support/train the personnel of critical infrastructure operators
25. Cyber security and IT curriculum for all levels of the education from elementary schools to universities	25) Cyber security and IT curriculum for all levels of the education, from elementary schools to universities
26. The dedicated cyber security personnel at critical infrastructure operators	26) Special positions for cyber security experts in critical infrastructure operators
27. National / sectorial product and service procurement standards or rules for critical infrastructure operators	27) National / sectorial products and service procurement standards or rules for critical infrastructure operators
28. Regulation that specifies the fundamentals of the relations with third parties	Discarded
29. The certification of IT companies that are eligible for IT service procurements by critical infrastructure operators	28) The establishment of a system for the eligibility certifications of the IT companies to provide IT services for critical infrastructure operators
30. The security standards for the IT products to be used by critical infrastructure operators	29) Security standards for the IT products to be used by critical infrastructure operators
31. The national or sectorial regulations that enforce the internal / external audit for critical infrastructure operators	30) National or sectorial regulations that enforce the internal / external audit for critical infrastructure operators

English Translation (Input of the Round-5)	English Translation – Comments of the Experts Reflected (Output of the Round-5)
32. The regular cyber security audits for critical infrastructure operators performed by the regulatory agencies of the sectors	31) Regular cyber security audits performed by the regulatory authorities of the sectors for critical infrastructure operators
33. The experienced IT auditors who are employed within the internal audit units of the critical infrastructure operators	32) Experienced IT auditors who are employed within the internal audit units of critical infrastructure operators
34. The sanctions imposed by the regulatory agencies to the critical infrastructure operators for the nonconformities	33) Sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities
35. The regulation that makes top level management of the critical infrastructure operators responsible for the cyber security by imposing information security governance	34) Regulations that render top level management of critical infrastructure operators responsible for cyber security
36. The regulation that enforces the cyber security risk management process to be conducted by critical infrastructure owners	35) Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process
37. The obligation of a comprehensive security standard such as ISO 27001 for the critical infrastructure owners	36) Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners
38. Minimum security countermeasures for the critical infrastructure owners that are obliged by regulations	37) Minimum security countermeasures that are obliged by regulations for critical infrastructure owners
39. The regulations for information system and security countermeasures to be installed at critical infrastructure operators	38) Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators
40. Sector-specific technical guidance documents for the secure design, set-up and operation of the networks of critical infrastructure operators	39) Sector-specific technical guidance documents for the secure design, set-up and operation of the networks of critical infrastructure operators
41. The sectorial or national security standard for critical infrastructure operators that sets outs the security best practices for the sectors	40) Sectorial or national security standards that set out the best security practices for each critical sector

Appendix B: Maturity Survey

Questionnaire Form

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
1.	Is there a Critical Infrastructure Protection Program (CIPP) that considers cyber threats?	No CIPP	CIPP does not consider cyber threats or consider insufficiently.	CIPP considers cyber threats and physical threats equally.
2.	Is the management of the CIPP performed by a governmental organization which has responsibilities for the national security as well? / Is there the communication between CIPP body and national security body? (Please answer the most applicable one)	There is no assigned responsibility. There is no communication.	Critical infrastructure protection program is managed by a governmental organization that has no responsibility on national security. There is a weak communication path between two bodies.	Yes, CIP program is managed by a governmental organization that has the responsibilities on national security. OR There is a strong communication path between two bodies.
3.	Is there a consultant who provides technical, regulatory and diplomatic cyber security consultancy for the head of the state?	No	There is no official appointment.	There is a nationally recognized staff.
4.	Is there an allocated budget for critical infrastructure protection efforts?	No or very limited dedicated budget	There is no dedicated budget; however government gives some funding to the projects.	Dedicated and sufficient amount of budget is assigned for critical infrastructure protection program.
5.	Are there regulatory agencies that set cyber security regulations and check the application of them for each critical sector?	No regulatory authority or no cyber security regulation.	There is limited direction on cyber security.	There is comprehensive direction on cyber security.

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
6.	Is there a CSIRT organization dedicated to the protection of critical infrastructures?	No	Existing –national- CSIRT performs some limited efforts for critical infrastructures.	There is dedicated CSIRT for critical infrastructures.
7.	Is there a national cyber security strategy that considers the cyber security of critical infrastructures as part of national security?	No	There is a national cyber security strategy, however limited consideration for the cyber security of critical infrastructures.	Yes
8.	Is there nation-wide risk analysis and risk management activities which cover all critical sectors? / is there sector-wide risk analysis and risk management activities? (Please answer the most applicable one)	No	There are limited action in some sectors.	There is periodic and formal nation-wide/sector wide risk management process.
9.	Is there a public-private partnership program which is developed and supported by the government?	There is no public-program partnership program or any apparent public-private partnership practices.	There are some practices; however these are not the result of a program.	Yes, there is an active public-private partnership program managed by government.
10.	Are there regulations that specify inner – inter sector information sharing and cooperation principles?	There is no rule on information sharing.	There are no / immature rules. There are some practices on information sharing. However these are sector or operator specific.	Yes, there is written set of rules on information sharing. Every critical infrastructure operator performs information sharing according to these rules.
11.	Are there sector-based CSIRTs that have information sharing responsibilities determined by the regulations?	No	In some sectors	Yes. There are CSIRTs for all critical sectors.

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
12.	Is there an internationally recognized national CSIRT that performs international cooperation with other CSIRTs?	No	Yes; however it does not have international actions.	Yes.
13.	Is there a technical infrastructure to fulfill the inner - inter sector information sharing needs? (online information sharing portals, statistics dashboards, data collections centers)	No	There are some limited utilities.	There are necessary technical infrastructures and utilities.
14.	Does the National CSIRT handle the warnings of cyber incidents related to critical infrastructures by coordinating with the relevant sectorial CSIRTs and critical infrastructure owners when needed?	No	There are some limited actions. It coordinates some events.	Yes
15.	Are there government policies and strategies that position private sector as a key player in national cyber security efforts?	No	There are some isolated efforts.	There is a comprehensive policy, strategy and associated action items.
16.	Does the private sector participate in the preparation of the national or sectorial cyber security strategies?	No, there are some minor engagements	In some sectors / for some operators, private sector is an important role player. However this is not the result of high level policy.	Private sector is positioned as an essential partner in the preparation of the strategies. It sometimes directs the efforts, produces solutions.
17.	Does the private sector have permanent seat in the national boards like the cyber security council?	No	Private sector is invited sometimes.	Yes

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
18.	Does the government show leadership for innovation, research & development activities, and the identification of the priority areas in cyber security?	No	Limited efforts	Government direct the private sector in producing cyber security products.
19.	Does the private sector participate in the national cyber security exercises extensively?	No	Limited	Yes
20.	Is the existing legislation that may affect critical infrastructures reviewed and updated especially for the needs of the governmental critical infrastructure operators?	No	Some sector specific efforts may appear. However there is no exclusive practices.	Yes. The required amendments are determined and applied for all sectors.
21.	Is the necessary amendments to the regulations performed to hire outsourced personnel / qualified government officials with higher salaries / contracted personnel in governmental critical infrastructures?	No	There are some limited efforts for some sectors.	Yes
22.	Are there national capacity building plans and strategies?	No	There are some practices. However, these are not sufficient for capacity building.	There are national efforts that covers formal education, universities. There are personnel certification schemes.
23.	Are internationally accepted certificate owners preferred in the recruitments by critical infrastructure owners?	No or Few practices	Some organizations or sectors urges the certifications. However it is not prevalent.	There are common practices for all critical sectors.

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
24.	Are there qualified and sufficient number of cyber security training institutions (private, academic or governmental) that support/train the personnel of critical infrastructure operators?	Very limited	There are some institutions; however they are not enough in number or there are specific to some of the critical sectors.	There are adept and plenty of institutions for all of the critical sectors.
25.	Is there cyber security and IT curriculum for all levels of the education from elementary schools to universities?	Very limited	There are some efforts in some universities. However the percentage of these universities are quiet low.	There are sufficient curriculum in considerable amount of universities.
26.	Are there special positions for cyber security experts in critical infrastructure operators?	No	There are limited qualified staff or there are enough number of qualified staff in some of the infrastructures.	There are enough number of qualified staff in all of the critical infrastructure operators.
27.	Are there national / sectorial products and service procurement standards or rules for critical infrastructure operators?	No	There are some limited rules. However these are not widespread or mature.	Yes, the critical infrastructure operators procure products / services according to these rules.
28.	Is a system established for the eligibility certifications of the IT companies to provide IT services for critical infrastructure operators?	No	There are some informal lists for credible firms.	Yes. There is a government-controlled accreditation scheme.
29.	Are there security standards for the IT products to be used by critical infrastructure operators?	No	There are some standards; however they are not detailed enough or they are specific to some of the sectors.	There are detailed security standards for all of the sectors.

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
30.	Are there national or sectorial regulations that enforce the internal / external audit for critical infrastructure operators?	No. critical infrastructure operators are not audited regularly. Also internal audit process does not exist.	There are some audit practices. However these are not enough to improve the national security posture.	Audit is an essential process for critical infrastructure operators.
31.	Are there regular cyber security audits performed by the regulatory authorities of the sectors for critical infrastructure operators?	No	There are limited efforts. However they are specific to only some sectors or they are not detailed enough.	There are regular and qualified audits for all sectors.
32.	Are there experienced IT auditors who are employed within the internal audit units of critical infrastructure operators?	No or very limited	There are some security auditor in some sectors. However they are not experienced enough.	Most / all of the organizations in all sectors employ experienced auditors.
33.	Are there sanctions imposed by the regulatory authorities on critical infrastructure operators for the nonconformities?	No or very limited practices	There are some practices in only small portion of the sectors.	There are written rules for sanction for all sectors. They are imposed as needed.
34.	Are there regulations that renders top level management of critical infrastructure operators responsible for cyber security?	No	There are some sector specific enforcement; however these are not enough in terms of national security.	There are particular set of rules that makes manager of the critical infrastructures responsible for cyber security.
35.	Are there regulations that enforce critical infrastructure owners to conduct the cyber security risk management process?	No	There are some sector specific enforcement; however these are not enough in terms of national security.	Yes, regular risk management proves is a must-do process for every operators in every sector.

No	Question	No action or very limited action (0)	Partial Action (1)	Comprehensive Action (2)
36.	Is there an obligation of a comprehensive security standard such as ISO 27001 for critical infrastructure owners?	No	There is obligations for some sectors.	Yes
37.	Are minimum security countermeasures obliged by regulations for critical infrastructure owners?	No.	There are some limited works for some sectors.	Yes.
38.	Are there regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators?	No	There are some regulations for some sectors.	Yes
39.	Are there sector-specific technical guidance documents for the secure design, set-up and operation of the networks of critical infrastructure operators?	No	There are some limited guidance documents for some sectors.	There are comprehensive documents for all sectors.
40.	Are there sectorial or national security standards that set out the best security practices for each critical sector?	No	There are standards for some sectors. However there are not detailed enough or the covered sectors are very limited.	There are comprehensive national or sectorial standards for all critical sectors.

Answers of the Participants of the Pilot Survey

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Question-1	1	0	0	1	0	0	1	1	1	0
Question-2	0	0	0	1	1	0	0	1	2	0
Question-3	0	0	0	0	0	0	0	0	1	0
Question-4	0	0	1	0	0	0	0	0	0	0
Question-5	1	1	0	0	1	1	0	0	1	1
Question-6	0	0	1	1	1	0	0	1	0	0
Question-7	0	0	0	2	1	1	1	2	1	2
Question-8	0	0	0	0	0	1	0	0	0	0

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Question-9	0	1	0	0	0	0	0	0	0	0
Question-10	0	1	0	0	1	0	1	0	0	0
Question-11	0	1	0	1	0	1	1	0	0	0
Question-12	0	1	0	1	1	1	1	0	1	1
Question-13	0	0	1	0	0	0	0	1	0	0
Question-14	0	0	0	1	1	1	1	0	1	0
Question-15	0	0	0	0	0	0	1	0	0	0
Question-16	0	1	0	1	1	0	0	1	2	1
Question-17	0	0	1	1	0	0	0	1	0	0
Question-18	0	0	1	1	0	0	2	0	1	0
Question-19	0	1	1	0	1	1	0	0	1	1
Question-20	0	0	1	0	0	0	0	0	1	1
Question-21	1	1	0	1	0	0	1	1	1	0
Question-22	0	1	1	1	1	0	2	0	0	0
Question-23	0	0	0	1	0	1	0	0	1	0
Question-24	0	1	0	0	1	0	0	0	0	0
Question-25	0	1	0	0	0	0	0	0	0	0
Question-26	1	1	1	1	1	1	0	1	1	1
Question-27	1	1	1	0	1	1	0	1	1	0
Question-28	0	0	0	1	1	1	0	1	1	0
Question-29	0	2	0	1	1	1	0	0	1	1
Question-30	0	1	0	0	0	1	0	1	0	0
Question-31	1	1	1	1	0	1	0	0	1	0
Question-32	0	1	1	1	0	1	0	0	1	0
Question-33	1	0	0	0	1	0	0	0	0	0
Question-34	0	0	1	2	0	0	0	1	0	0
Question-35	0	0	1	1	0	0	0	1	0	0
Question-36	0	0	0	0	0	0	0	0	0	0
Question-37	1	0	1	0	1	0	1	1	1	1
Question-38	0	1	1	0	0	0	1	1	0	1
Question-39	0	0	0	0	0	0	0	0	0	0
Question-40	0	0	0	0	1	0	1	0	0	1

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Karabacak, Bilge
Nationality: Turkish
E-mail: bilgek@gmail.com
Scholar: https://scholar.google.com.tr/citations?user=yW4nh4EAAAAJ
Academia: http://metu.academia.edu/BilgeKarabacak

EDUCATION

Degree	Institution	Department	Year of Graduation
PhD	METU Informatics Institute	Information Systems	2015
MS	Gebze Institute of Technology	Computer Engineering	2003
BS	Bilkent University	Electrical and Electronics Engineering	1999

WORK EXPERIENCE

Place	Enrollment	Year
TOBB ETU	Adjunct Faculty	2015 Spring Semester
TUBITAK	Researcher	2000-2014
MIKES	System Engineer	1999

PUBLICATIONS

1) B. Karabacak, S. Ozkan and N. Baykal, “The Regulatory Options for the Cyber Security of Critical Infrastructures: The Case of Turkey”. (Manuscript submitted for publication, in editorial review)
2) B. Karabacak, S. Ozkan and N. Baykal, “A Vulnerability-Driven Cyber Security Maturity Model to Measure the National Critical Infrastructure Protection Preparedness”, International Journal of Critical Infrastructure Protection. (Manuscript submitted for publication, in editorial review)
3) B. Karabacak, U. Tatar, (in press). “From the National Cyber Maturity to the Cyber Resilience: An Assessment of the Strategic Efforts of Turkey”, Terrorism and Cyberspace: Comprehensive Analysis and Strategic Response. Amsterdam: IOS Press.
4) B. Karabacak, U. Tatar, “Strategies to Counter Cyberattacks: Cyber threats and Critical Infrastructure Protection”, NATO Science for Peace and Security Series: Human and Societal Dynamics – Vol. 116, Critical Infrastructure Protection, January 2014.
5) S. Ozkan and B. Karabacak, “Collaborative risk method for information security management practices: A case context within Turkey”, International Journal of Information Management, vol. 30, pp. 567–572, 2010.
6) B. Karabacak and I. Sogukpinar, “A quantitative method for ISO 17799 gap analysis”, Computers & Security, vol. 25, pp. 413–419, 2006.
7) M. Uneri, B. Karabacak, “Securing networks in the information age”, Cyberwar-Netwar, Security in the Information Age, Vol. 4 NATO Security through Science Series: Information and Communication Security, May 2006.
8) B. Karabacak and I. Sogukpinar, “ISRAM: information security risk analysis method”, Computers & Security, vol. 24, pp. 147–159, 2005