TECHNOLOGY FORESIGHT AND MODELING: TURKISH CYBERSECURITY FORESIGHT 2040

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

HASAN ÇİFCİ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
SCIENCE AND TECHNOLOGY POLICY STUDIES

MAY 2019

Approval of the Graduate School of Social Sciences

_____

Prof. Dr. Tülin Gençöz
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

_____

Prof. Dr. Teoman Pamukçu
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

_____

Assoc. Prof. Dr. Serhat Çakır
Supervisor

Examining Committee Members

Prof. Dr. Çiğdem Erçelebi	(METU, PHYS)	_____
Assoc. Prof. Dr. Serhat Çakır	(METU, PHYS)	_____
Assoc. Prof. Dr. Ertan Onur	(METU, CENG)	_____
Assist. Prof. Dr. Altan Özkil	(Atılım Uni., AVM)	_____
Assist. Prof. Dr. Pelin Angın	(METU, CENG)	_____

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 : Hasan Çifci

Signature :

ABSTRACT

TECHNOLOGY FORESIGHT AND MODELING: TURKISH CYBERSECURITY FORESIGHT 2040

Çifci, Hasan
Ph.D., Science and Technology Policy Studies
Supervisor: Assoc. Prof. Dr. Serhat Çakır

May 2019, 323 pages

Foresight is a systematic and multidisciplinary process with proper methodology combinations for identifying technological, economic and social areas to prioritize investments and research to realize medium or long-term future strategies by using various resources from organizational to international level. Cybersecurity is the protection of cyber systems from cyber-attacks and providing integrity, confidentiality, and availability of those systems. In this thesis, information about technology foresight and cybersecurity is given through a detailed literature review and with the examples from all over the world. Two round Delphi survey, focus group, and scenario methods were mainly performed in order to develop Turkey's national cybersecurity technology foresight. In the study, a new technology foresight model and framework created by the researcher and thesis supervisor were followed to keep up with an optimum approach. The thesis is concluded by the concrete policy suggestions based on the foresight outputs.

Keywords: Technology Foresight, Cybersecurity, Foresight Periscope Model, Cybersecurity Technology Taxonomy, Cybersecurity in Turkey

ÖZ

TEKNOLOJİ ÖNGÖRÜSÜ VE MODELLEMESİ: TÜRKİYE'NİN SİBER GÜVENLİK ÖNGÖRÜSÜ 2040

Çifci, Hasan
Doktora, Bilim ve Teknoloji Politikaları Çalışmaları Bölümü
Tez Yöneticisi: Doç. Dr. Serhat Çakır

Mayıs 2019, 323 sayfa

Öngörü, organizasyondan uluslararası seviyeye kadar çeşitli kaynakları kullanmak suretiyle orta veya uzun vadeli gelecek stratejilerini gerçekleştirmek amacıyla teknolojik, ekonomik ve sosyal alanları tanımlayarak yatırım ve araştırmaları önceliklendirmek için doğru metodoloji kombinasyonlarıyla yürütülen sistematik ve çok disiplinli bir süreçtir. Siber güvenlik, siber saldırılara karşı siber sistemlerin korunmasını ve bu sistemlerin bütünlüğünü, gizliliğini ve erişilebilirliğini sağlamaktır. Bu tezde, teknoloji öngörüsü ve siber güvenlik hakkında ayrıntılı bir literatür taraması, tüm dünyadan örneklerle birlikte verilmektedir. Türkiye'nin ulusal siber güvenlik teknoloji öngörüsünü ortaya koymak için iki aşamalı Delfi, odak grup ve senaryo yöntemleri uygulanmıştır. Çalışmada optimum bir yaklaşımı yakalamak için, araştırmacı ve tez yöneticisi tarafından geliştirilen yeni bir teknoloji öngörüsü modeli ve çerçevesi takip edilmiştir. Tez, öngörü çıktılarına dayalı somut politika önerileri ile tamamlanmıştır.

Anahtar Sözcükler: Teknoloji Öngörüsü, Siber Güvenlik, Öngörü Periskobu Modeli, Siber Güvenlik Teknoloji Taksonomisi, Türkiye'de Siber Güvenlik

To my dear wife Bahar and lovely daughters Elifnur and Pınar…

ACKNOWLEDGMENTS

First, I would like to express grateful acknowledgment for the valuable suggestions and help given by my thesis supervisor Assoc. Prof. Dr. Serhat Çakır.

I would also like to express my gratitude to Prof. Dr. Çiğdem Erçelebi and Prof. Dr. Türksel Kaya Bensghir for their guidance and support during thesis monitoring process.

Finally, I would like to thank to Assoc. Prof. Dr. Ertan Onur, Assist. Prof. Dr. Altan Özkil, Assist. Prof. Dr. Pelin Angın and Assist. Prof. Dr. Emin Kuğu for their precious support and Nurdan Yüksel, although no longer with us, for her contribution to my studies.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
BMBF	German Federal Ministry of Education and Research
COTS	Commercial Off The Shelf
CPS	Cyber-Physical Systems
DCDC	Development, Concepts and Doctrine Centre
DSTL	UK Defense Science and Technology Laboratory
EDA	European Defense Agency
ENISA	European Union Agency for Network and Information Security
EU	European Union
FPM	Foresight Periscope Model
FTA	Future-oriented Technology Analysis
GCI	Global Cybersecurity Index
GDP	Gross Domestic Products
GERD	Gross Domestic Expenditure on R&D
GII	Global Innovation Index
ICT	Information and Communications Technologies
IDI	Information and Communication Technologies Development Index
INSEAD	European Institute of Business Administration (Institut Européen d'Administration des Affaires)
IoT	Internet of Things
IT	Information Technologies
ITU	International Telecommunication Union
KISTEP	Korean Institute for Science and Technology Evaluation and Planning
METU	Middle East Technical University (Orta Doğu Teknik Üniversitesi)
MGK	Turkish National Defense Council

	(Millî Güvenlik Kurulu)
MS	Master of Science
MSB	Turkish Ministry of National Defense (Millî Savunma Bakanlığı)
NIST	National Institute of Standards and Technologies
NISTEP	National Institute of Science and Technology Policy
OECD	Economic Cooperation and Development
PhD	Doctor of Philosophy
R&D	Research and Development
RF	Russian Federation
S&T	Science and Technology
SCADA	Supervisory Control and Data Acquisition
SCST	Turkish Supreme Council of Science and Technology
SFM	Systemic Foresight Model
SIEM	Security Information and Event Management
SMIC	Cross Impact Systems and Matrices
SSB	Turkish Presidency of Defense Industries (Savunma Sanayii Başkanlığı)
SSM	Turkish Undersecretaries for Defense Industries (Savunma Sanayii Müsteşarlığı)
STA	Science and Technology Agency
STEEPLE	Social, Technological, Economic, Environmental, Political, Legal, Ethical
STEEPV	Social, Technological, Economic, Environmental, Political, and Value
STI	Science, Technology and Innovation
SWOT	Strengths, Weaknesses, Opportunities, Threats
TAA	Technology Activity Areas
TCC	Turkish Cybersecurity Cluster
TF	Technology Foresight
TFA	Technology Futures Analysis

TFAMWG	Technology Futures Analysis Methods Working Group
TIF	Technologies and Innovation Futures
TSA	Time Series Analysis
TÜBİTAK	Scientific and Technological Research Council of Turkey (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu)
UK	United Kingdom
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNIDO	United Nations Industrial Development Organization
US	United States
USA	United States of America

CHAPTER 1

INTRODUCTION

Today, technology has commenced to penetrate virtually every aspect of our lives. The widespread utilization of information and communications technologies (ICTs) and the internet, and the connection of various devices, from computers and mobile phones to smart vehicles and smart household appliances, led to the emergence of the incipient environment called “cyberspace”. Cyberspace is the environment which comprises interconnected or stand-alone information systems that are composed of all kinds of software, hardware and communication infrastructure (Çifci, 2017). Cyberspace is formed by many different and generally overlapping networks, nodes (device or logical location) and data (US Joint Chief of Staff, 2013).

With technology entering into every side of daily life, dependence on technology is increasing and this dependence brings new vulnerabilities and threats to personal, national and global security while technology is facilitating daily life and raising living standards. As the cyberspace becomes widespread, it is not a surprise that the security aspects become crucial. Cybersecurity is one of the expeditious growing and largest technology sectors.

Cybersecurity refers to the precautions and actions that can be used to protect the cyberspace from the threats and striving to safeguard the availability, integrity, and confidentiality of the information systems and data contained therein (European Commission, 2013). It is the process of protecting information by means of preventing, detecting and responding to cyber attacks (NIST, 2014).

According to the predictions on cybersecurity economy over the next five years from 2017 to 2021 (Morgan, 2017), global spending on cybersecurity products and

services to deal with cybercrime will exceed $1 trillion cumulatively over the next five years, cybercrime damages will cost the world $6 trillion annually by 2021 which is twofold from 2015 and the demand for cybersecurity professionals will increase to approximately 6 million globally by 2019 while cybersecurity unemployment rate will remain zero until 2021.

Number and severity of cyber attacks are increasing day by day. In 2015, 431 million new malware was released (Symantec, 2016) and the number of malware used for ransom exceeded 1 million (McAfee, 2015) by 35 percent increase compared to the previous year (Symantec, 2016).

Cybersecurity strategy is required in order to manage risks, to cope with cyber attacks, to protect people's, organization's and country's privacy and security in the cyberspace, to continue business operations, to promote cooperation between institutions, to connect with the world and to survive in digital domain (ENISA, 2012).

Technology Foresight (TF) is a systematic process of looking into long term future of science, technology, economy, and society to identify strategic research areas and emerging generic technologies that may bring substantial economic and social gains (Martin, 1995). According to Yüksel and Çifci (2017), foresight is multidisciplinary process with suitable method combinations to prioritize research areas or to identify medium or long term future strategies by using all level of resources. TF is used widespread especially after the 1990s because it provides approaches to identify priority science and technology areas, it suggests mechanisms to integrate research and development activities with economic and social needs and it helps interaction, partnership and common understanding among TF stakeholders (Martin & Johnston, 1999).

In the literature and practice, there are different TF approaches, frameworks, and models to be followed in foresight studies. Foresight Periscope Model (FPM), which is developed by Yüksel and Çifci (2017), is a new technology foresight approach which has three interdependent modules; Resources, Methodology and Futures Strategies. The model makes use of periscope resemblance, that is,

resources and methodology are underlying parts that enable an organization to see alternative futures and provide futures strategies to follow in order to survive and compete in the environment. A generic foresight functional framework with nine consecutive phases (Framing, Obtaining, Reviewing, Establishing, Synthesizing, Illustrating, Guiding, Handling, Tracking) named 'FORESIGHT' is also developed by Yüksel and Çifci (2017) to be used in integration with FPM. Functions in the FORESIGHT framework are matched with the phases of prominent foresight frameworks in the literature based on their actions and artifacts within specific phases.

1.1 Statement of the Problem

Cyberspace is a borderless environment that connects all actors including individuals, organizations, and states. Security of the cyberspace becomes a priority issue because of growing and accelerating reliance on cyberspace. In order to tackle the risks and threats in cyberspace and to preserve the ability to leverage cyberspace, it is vital to develop policies, strategies, and plans to address cybersecurity.

Based on the literature survey and analysis of publicly available cybersecurity strategies, nations are rarely applying foresight methodologies for the cybersecurity field. Besides, cybersecurity was not treated as a main field or theme in Delphi based foresights but just some of the cybersecurity topics were handled under ICT field, like Japan's 10^{th} Foresight Study (Ogasawara, 2015). In some cases, only limited cybersecurity issues were handled in cybersecurity foresight exercises, such as European Foresight Cybersecurity in which only Internet of Things and harmonization of duties of care within the European Union were addressed (Cybersecurity Council, 2016).

In Turkey, cybersecurity issues were given importance more than 15 years in the government level and it can be put forward that official applications and actions were started by e-Transformation Turkey Project back to 2003 (Çifci, 2017). Later on, several studies were performed until today. The most prominent and important

pace related to cybersecurity is Turkey's National Cybersecurity Strategy and Action Plan 2013-2014 (Ministry of Transport and Infrastructure, 2012) and National Cybersecurity Strategy and Action Plan 2016-2019 (Ministry of Transport and Infrastructure, 2016). The methodology of the mentioned strategies and action plans was conducting meetings, workshops, seminars, and conferences with specialists from institutions and organizations representing public institutions, critical infrastructure operators, the ICT sector, universities and non-governmental organizations (Şentürk, Çil, & Sağıroğlu, 2012), which lacks foresight methodologies.

To develop a proper strategy and action plan it is an obligation to achieve cooperation and agreement from a wide range of stakeholders and the process of developing the strategy and action plan is probably as important as the final document (ENISA, 2012).

1.2 Purpose of the Study

The main purpose of this study is to perform cybersecurity technology foresight for Turkey in the next 20 years until the year 2040 and to determine concrete policy proposals according to the preliminary results of cybersecurity foresight for Turkey by applying generic foresight model FPM and FORESIGHT framework created by Yüksel and Çifci (2017).

In the study, trend analysis, Delphi, focus group and scenario techniques are used as primary foresight methods.

1.3 Research Questions

Answers to the following questions are given in the study:

(1) Which cybersecurity-related foresight activities were carried out in the nations?

(2) What kind of technology foresight methods, generations and frameworks exist in the literature in order to prioritize the resources to invest to reach foreseen or desired future technology capabilities?

(3) What are the strengths and weaknesses of Turkey in terms of cybersecurity, and which opportunities and threats are available in the cybersecurity field?

(4) What is the current cybersecurity situation and posture of Turkey in terms of products and services?

(5) What kind of cybersecurity capabilities, services, products, and technologies should be created or worked in Turkey for the next 20 years until 2040 and what should be done in order to reach the cybersecurity vision and goals?

1.4 Researcher's Motivation and Significance of the Study

In today's digital world, economy, scientific activities, trade, communications, and social life are linked through a networked infrastructure called "cyberspace" that is targeted by malicious actors (The White House, 2015). The danger of disruptive and even destructive cyber attacks is growing in the interconnected world. Cybersecurity is one of the main security concerns in nation states' broader national security strategies. It is recognized that there is a need for long term, strategic approaches related to cybersecurity of new technological developments (Cybersecurity Council, 2016).

Organizations hide data breach incidents in order not to be embarrassed by companies, partners, customers, and competitors, not to lose their reputation and not to be sued. Nonetheless, it is said from different sources that cyber attacks are causing hundreds of billions of dollars of damage worldwide. According to the "2018 Cost of Data Breach Study" (IBM, 2018) from IBM Security and Ponemon Institute, the average cost of a data breach in the world is $3.86 million, which

pose 6.4% increase from 2017. It is alleged that the total cost of a data breach is about $400 billion a year throughout the world (Fortune, 2016).

With the use of ICT in every field from daily life to the most critical military systems, protection of the cyberspace has become one of the important elements of national security of nation-states (Çifci, 2017). Nowadays, as well as land, sea, air, and space, cyberspace has emerged as a new operational domain or battlefield. While technological developments are advancing with the speed of light, it is of great importance to take and implement measures against threats, weaknesses, and risks caused by these developments. For this purpose, the security of the cyberspace is a strategic goal that must be achieved, to gain defense and attack capabilities by providing the necessary infrastructure.

At the beginning of this study, after analyzing of the foresight literature, a generic foresight model (Foresight Periscope Model -FPM) and foresight framework (FORESIGHT) were developed and brought in the literature by Yüksel and Çifci (2017) in order to cover and standardize not only the process but also the resources that are required to carry out a foresight project.

FPM gives the main pillars of foresight by emulating it to a periscope. In the model, based on the tangible and intangible resources, methodologies are selected and applied for the alternative futures states. Methodologies to look forward, back and present are determined together with the scope and objective of foresight. Resources and methods have been formed onto past and present experience, accumulated knowledge and capabilities like the parts of periscope under the sea. With the search of frameworks in the literature, a generic foresight functional framework with nine consecutive phases named FORESIGHT covers the phases of a generic foresight process regarding its activities done.

In the academic literature and professional publications, there is no specific model or set of standard techniques special for or dedicated to cybersecurity foresight. In this study, FPM model and FORESIGHT framework have been followed and their specific application has been created for cybersecurity technology foresight.

With the extensive literature survey, technology foresight methods, generations and frameworks were analyzed and briefed into a chapter. Besides, foresight projects of countries were examined to find out cybersecurity capabilities that are listed to implement within those projects.

In the course of time, a new foresight generation (Foresight 6.0), which is founded on Industry 4.0 and Society 5.0, with its unique characteristics was created and published by Yüksel, Çifci and Çakir (2017).

Together with cybersecurity experts, very extensive cybersecurity technology taxonomy with underpinning technologies, system related technologies, and systems/products were created under this study. Furthermore, technologies were prioritized and listed against their contribution to security and economy through expert judgments.

Finally, the strengths and weaknesses of Turkey in terms of cybersecurity, opportunities, and threats in the cybersecurity field were determined. Universities and cybersecurity sector were analyzed, and actions and roadmaps were created for Turkey's cybersecurity long-term future until 2040. Table 1 summarizes some of the significant contributions of the study.

Table 1: Significant Contributions of the Study

No	Contribution
1	A new foresight model, Foresight Periscope Model (FPM)
2	A new generic foresight framework, FORESIGHT
3	Implementation of FPM and FORESIGHT for cybersecurity field
4	A new foresight generation with unique traits, Foresight 6.0
5	Very extensive Cybersecurity Technology Taxonomy
6	SWOT and STEEPLE analysis for Turkey in terms of cybersecurity
7	Detailed analysis of cybersecurity courses and departments in Turkish universities, which is the first study in these details in the literature regarding Turkish universities' circumstance.

Table 1 (Cont'd)

No	Contribution
8	Detailed analysis of Turkish cybersecurity sector in terms of companies, products, services, and technologies, which is the first study in these aspects and details in the literature regarding Turkish cybersecurity sector.
9	Cybersecurity actions and roadmaps for Turkey covering 20 years-timeframe

At the beginning of the study, "Turkey's Cybersecurity Roadmap" working group was constituted officially under the technology panels of the Turkish Undersecretaries for Defense Industries (Savunma Sanayii Müsteşarlığı -SSM) to conduct all activities under the auspices of SSM Research and Development Division. Experts were selected and the researcher was appointed as the group's chairperson. After the second focus group meeting, in July 2018, following the reorganization of SSM as the Presidency of Defense Industries (Savunma Sanayii Başkanlığı -SSB), the working group was terminated unofficially and the participant support provided by SSB was withdrawn.

The study has been completed with the experts from Turkish Armed Forces, TÜBİTAK, some government institutions, Turkish universities, and the cybersecurity sector. It should be noted that all of the experts represented only themselves but not the organizations' ideas or perspectives. Therefore, this study is an academic artifact rather than an official document.

CHAPTER 2

LITERATURE REVIEW

2.1 Technology Foresight Basics

2.1.1 Definitions of Technology Foresight

People have always been curious about the future and they have been using various concepts, methods, and means to learn what the future will bring and what the future incidents are. Considering the future is a wide concept, there are myriad of terminology about it such as futures research, futures studies, futures analysis, futurism and futurology (Voros, 2001). Futures are considered as broad professional and academic domain developing with its methods and tools (Conway, 2015). Futures studies are both multi-disciplinary and trans-disciplinary activities regarding the future.

There are various definitions of “technology” in the literature. Analyzing these definitions discovers a number of factors that identify technology. The main characteristic of technology is that it is “applied knowledge” (Phaal, Farrukh, & Probert, 2001). The technology comprises the ability to determine technical problems and the competence to create and exploit new concepts and to discover valuable solutions to these problems. It includes both skills and tacit knowledge (Molas-Gallart, 1997).

The Technology Futures Analysis Methods Working Group (TFAMWG) introduced an umbrella concept “technology futures analysis” (TFA) to integrate technology-oriented forecasting methods and practices. TFA refers to any systematic process to harvest information about technology developments in the future. Many forms of TFA coexist, for example, technology intelligence,

forecasting, roadmapping, assessment and foresight (Porter et al., 2004). The same concept is represented with another terminology namely “Future-oriented Technology Analysis” (FTA) (Haegeman, Marinelli, Scapolo, Ricci, & Sokolov, 2013).

Among the concepts in the literature, forecast and foresight are the most used terms for future studies related to technology. According to Meredith and Mantel (1995) “technology forecast” is “the process of predicting the future characteristics and timing of technology”. Martin (1995) defines “technology foresight” as "a process involved in systematically attempting to look into the longer-term future of science, technology, economy, and society with the aim of identifying the areas of strategic research and the emerging generic technologies likely to yield the greatest economic and social benefits". It is a systematic process to determine future technology developments and their relations with society and the environment in order to specify guidelines to create a more desirable future (Porter et al., 2004). According to Slaughter (1997), technology foresight is “human capacity” that must be developed and applied to use futures concepts for creating a futures discourse.

Yüksel and Çifci (2017) define foresight as:

> *A systematic and multidisciplinary process with proper methodology combinations for identifying technological, economic and social areas to prioritize investments and research in order to determine medium or long term future strategies by using all level of resources from organizational to international.*

According to Keenan (Miles & Keenan, 2003), there are five important characteristics of the foresight definitions:

(1) For foresight, future studies must be systematic so that they can be distinguished from daily internal scenario building activities.

(2) Foresight must be related to the longer time frame, typically range between five and thirty years.

(3) Market pull and technology push must be balanced by paying attention to both innovations and socio-economic factors.

(4) Emerging generic technologies have to be concerned in order to get government support in case companies are unwilling to fund the research.

(5) Attention must be focused on social issues such as crime prevention, education and skills, aging societies, etc., not just into wealth creation.

The list of the most prominent elements of foresight definitions in the literature is shown in Table 2.

Table 2: Key Elements of Various Foresight Definitions

Key Elements in Foresight Definitions	Authors
Systematic studies/process	Martin (1995), Georghiou (1996), Barre' (2001), Miles & Keenan (2002), Popper (2011), Conway (2015), Yüksel & Çifci (2017)
Looking at medium and long term future	Martin (1995), Georghiou et al. (2008), Barre' (2001), Miles (2010), Popper (2008), Yüksel & Çifci (2017)
Participatory, collective, networking process	Georghiou et al. (2008), Barre' (2001), Miles & Keenan (2002), Harper (2003), European Commission (EC) & Keenan & Popper (2007), Yüksel & Çifci (2017)
Building visions	Barre' (2001), Miles & Keenan (2002), Harper (2003), EC & Keenan & Popper (2007)
Gathering intelligence	Barre' (2001), Miles & Keenan (2002)
Learning process	EC & Keenan & Popper (2007), Popper (2008)
Joining key agents of change and knowledge sources	Barre' (2001), Popper (2008)

Foresight is a combination of approaches that taking benefit of the outputs of three interacted activity: Futures (forward thinking, forecasting, long-term, alternative futures, scenarios, visions), Planning (strategic analysis, setting priorities) and Networking (broadening participation, networking techniques, group work) (Miles, 2002). As shown in Figure 1, there are various intersections between there fundamental actions and this approach is critical for a successful foresight.

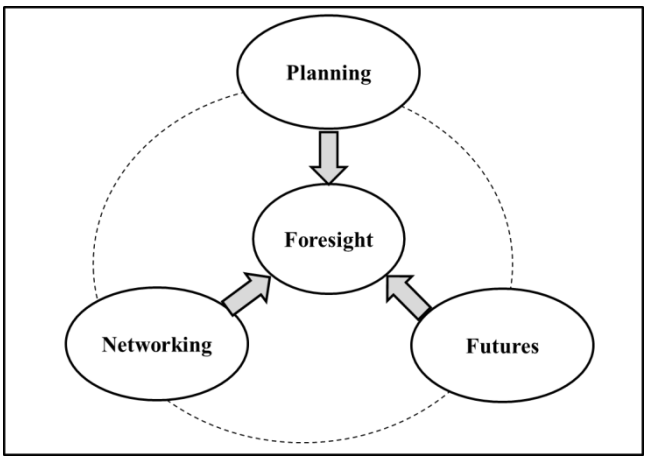


Figure 1: Fully-Fledged Foresight – Three Tenets (Miles, 2002)

There is a clear distinction between forecast and foresight. While the forecast is a probabilistic statement about the single future, accuracy is of paramount importance (Martin, 2010), foresight deals with multiple and diverse futures. Foresight is not a forecasting activity by experts (Popper, 2008a), it involves a clear perspective that today's choices can shape or create the future, therefore it is an active stance towards the future and accuracy of deterministic predictions are not as important as in forecast (Martin, 2010). Foresight activities can affect future events, and shape technologies, social and cultural interactions (Ciarli, Coad, & Rafols, 2013). The forecast provides a set of techniques to convert inputs to outputs whereas foresight, as a process, provides techniques to create common understanding and networking (Cuhls, 2003a). Foresight process has a broader aim than simply producing a forecast (Steed & Tiffin, 1986).

According to "Practical Guide to Regional Foresight in the United Kingdom" (Miles & Keenan, 2002), foresight has to have five essential elements:

(1) Disciplined anticipation and projections of long-term future (social, economic and technological).

(2) Having a broad spectrum of stakeholders (experts and non-experts) and interactive and participatory methods.

(3) Creation of new social networks.

(4) Detailed, shared and guiding strategic visions.

(5) Explicit recognition of present-day decisions and actions.

2.1.2 Technology Foresight Methods

There are numerous methods to produce judgments about the future technological developments that are used within technology foresight process. Scholars grouped these methods by characteristics, functions, spectrum, frequency, capacity, nature, purpose, technique and aspects (Yüksel & Çifci, 2017).

Glenn (1994) classified methods by their techniques (qualitative or quantitative) and their purposes (normative or exploratory). Moll (1996) used aspects of methods for classification and he broke up the methods into extrapolative, normative and pragmatic groups. Inayatullah (2001) preferred predictive, interpretive, critical and participatory groups for methods. Similar to Glenn (1994), Miles and Keenan (2003) grouped methods by their opposite characteristics as exploratory vs. normative, quantitative vs. qualitative and expert vs. assumption. Popper (2008) classified the methods by their nature as qualitative, quantitative and semi-quantitative.

Extrapolative methods essentially start with the present and try to find out alternative futures (UNIDO, 2005b) where events and trends might happen (Miles & Keenan, 2002). The process begins with a perceived future need (Porter et al., 2004). These methods focus on what might happen under various conditions (UNIDO, 2004). Extrapolative methods are “what if” approaches (Casas & Talavera, 2008) and answers to “what would be” questions are searched (Porter, 2010).

In contrast to explorative methods, normative methods: begin with a fundamental view of a possible and generally desirable set of futures (UNIDO, 2005b). The process begins with extrapolation of present technological developments and

capabilities (Porter et al., 2004). These methods examine how particular futures can be attained or averted (UNIDO, 2004) by asking what trends and events should be done to a specific future or futures (Miles & Keenan, 2002). Normative methods are goal-oriented approaches (Casas & Talavera, 2008) and "what should be" implications are in the focus (Porter, 2010). A normative step is necessary to define and achieve possible and desirable choices (Godet, 2000).

Quantitative methods consist of numerical information and a methodology applied in statistical or mathematical tools. Quantitative techniques become gradually important at present owing to the propagation of Big Data and increased computer power (Ciarli et al., 2013). These methods generally measure variables using or generating valid data and apply statistical analyses (Popper, 2008b).

Qualitative methods, on the other hand, consist of non-numerical information such as text, images, and a methodology without relying on statistical or mathematical tools (Haegeman et al., 2013). These methods are generally related to the meaning of events and perceptions. Qualitative statements such as opinions, judgments, beliefs, attitudes are based on subjectivity or creativity that is often difficult to substantiate (Popper, 2008b). Both quantitative and qualitative approaches can contribute to foresight activities.

2.1.2.1 Different Approaches to Methods Classification

In the foresight literature, there are several systematizations and classifications of foresight methods, fitted within a number of diverse attributes.

According to Popper (2008), foresight methods have two fundamental attributes: Nature and capabilities. With regards to the "nature" attribute, methods can be classified as qualitative, quantitative or semi-quantitative. The second attribute "capabilities" is the ability to collect or process information based on four key attributes:

(1) Interaction: With the help of a participatory process, interacting with other experts and non-expert stakeholders,

(2) Evidence: Reliable documentation and means of analysis,

(3) Expertise: Skills and knowledge of individuals in a specific domain,

(4) Creativity: Combination of original and imaginative thinking.

Popper (2008) created the famous Foresight Diamond (see Figure 2) of which building blocks are the four attributes of method capabilities. In the diamond, 33 foresight methods are characterized as quantitative, qualitative and semi-quantitative.

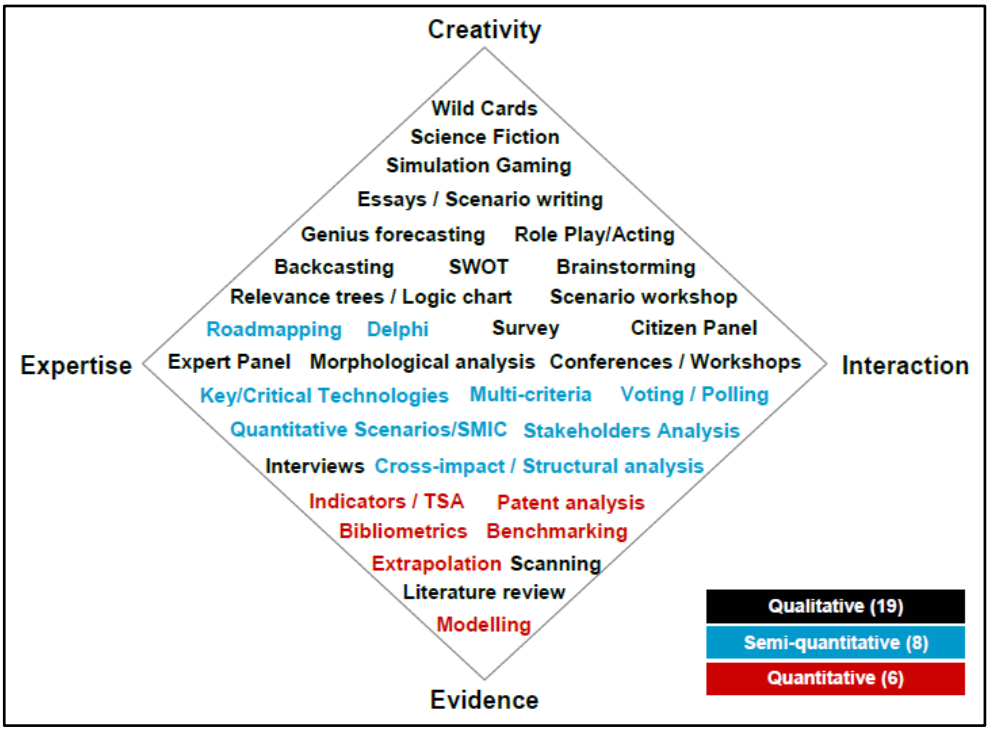


Figure 2: Rafael Popper's Foresight Diamond

In a study within Technology Futures Analysis Methods Working Group (TFAMWG), Coates et al. (2001) grouped technology foresight methods into 9 families: Expert Opinion, Trend Analysis, Monitoring & Intelligence, Modeling & Simulation, Scenarios, Statistical, Descriptive, Creativity and Valuing/Decision/Economics Methods. Porter et al. (2004) added two pairs of

attributes to method classification: “hard” (quantitative: numerical) or “soft” (qualitative: judgment based) and “normative” (starts with desired or perceived future need) or “exploratory” (starts with extrapolation of present technological capabilities). Table 3 depicts the part of 51 methods and their classifications arrayed by Porter et al., (2004).

Table 3: Classification of Foresight Methods (Porter et al., 2004)

Methods	Family*	Explorative or Normative	Hard or Soft
Backcasting	Desc	N	S
Cross-impact analysis	M&S/Stat	E	H/S
Delphi	ExOp	E/N	S
Focus groups	ExOp	E/N	S
Interviews	ExOp	E/N	S
Multi-criteria decision analyses	-	N	H
Participatory techniques	ExOp	N	S
Risk analysis	Desc/Stat	E/N	H/S
Roadmapping	Desc	E/N	H/S
Scenarios	Sc	E/N	H/S
Stakeholder analysis	Desc/V	N	S
Technology assessment	Desc/M&S	E	H/S
Trend extrapolation	Tr	E	H
Vision generation	Cr	E/N	S

***: (Family Codes**) Cr: creativity; Desc: descriptive and matrices; Stat: statistical; ExOp: expert opinion; Mon: monitoring and intelligence; M&S: modeling and simulation; Sc: scenarios; Tr: trend analyses; V: valuing/decision/economic.

In a study by Ciarli et al. (2013), family groups of Coates et al. (2001) and Porter et al. (2004) were distinguished into the following very similar 10 families: “Creative”, “Monitoring and intelligence”, “Descriptive and matrices”, “Statistical methods”, “Trends analysis”, “Economic methods”, “Modelling and simulations”, “Roadmapping”, “Scenarios” and “Valuing/Decision”. Furthermore, these method groups were described by Porter (2010) based on the following dimensions:

- Knowledge of Outcomes and Probabilities: Ignorance; Uncertainty.

- Drivers: Science (research); Technology (development); Innovation Context (problem solving).

- Locus: National; Regional; Global; Industry; Company; Sector.

- Time Horizon: Short; Mid-Range; Long.

- Purpose: Informational; Action-Oriented.

- Participants: Narrow; Intermediate; Diverse

As an example for the grouping approach by Ciarli et al. (2013), “Roadmaps” are action-oriented, mid-range or long term, science and technology-driven, have diverse participants with both ignorance and uncertainty and performed by companies, sectors or nations.

Loveridge (1996) treats the foresight methods based on whether creativity or expertise is needed to perform (see Figure 3). Interaction of expertise and creativity is a key for a foresight event and sustained information flow is vital for success.

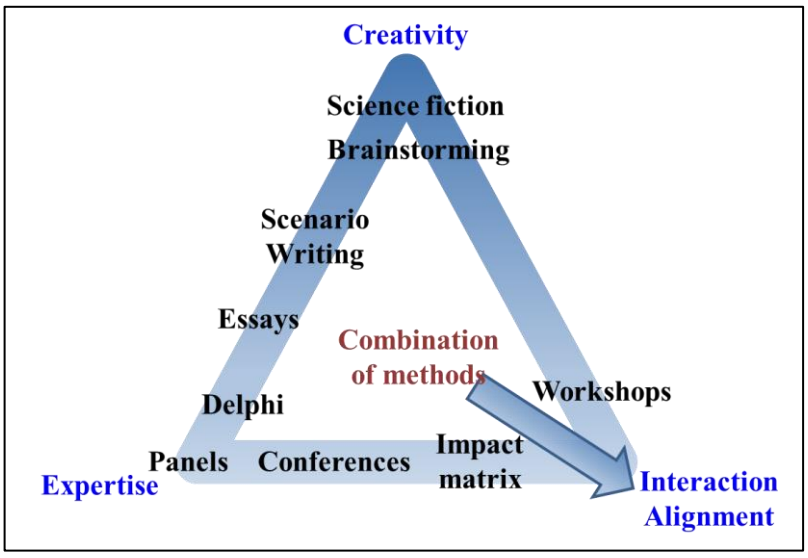


Figure 3: Foresight Methods in Relation to Activity (Loveridge, 1996)

In his paper "*Developing and Applying Strategic Foresight*" Slaughter (1997) defines strategic foresight as the ability to create high-quality future view and adapt the environment. It implies combining foresight methods with strategic management. He groups the methods into four main types (see Table 4):

Table 4: Types of Foresight Methods (Slaughter, 1997)

Type	Methods	Uses and Limitations
Input Methods	Constructing near -future context	Answers to questions about near-term future; beneficial for starting point; non-systematic.
	Delphi	Collects and converge opinions of experts and non-experts; reduces diversity; difficult to perform.
	Environmental scanning	Provides data for the future view; requires complex data processing.
Analytic Methods	Cross-impact	Determines referring impacts of factors on each other; preferable when used as part of a larger process.
	Forecasting and trend analysis	Aims to predict future alternatives; dependent on accurate data; vulnerable to unforeseen factors.
	Backcasting	Starts from the desired future towards the present; best for complicated and long-term issues.
Paradigmatic Methods	Layered causal analysis	Handles the issue to progressively deeper levels; complex because of paradigmatic nature.
	Critical futures studies	Focuses on the effects of underlying assumptions and future commitments; difficult for inexperienced participants but very productive.
	Systems thinking	Looks the issue in a holistic view; allows stakeholders to be systemic.
Iterative and Exploratory Methods	Scenarios	Provides insights about the future based on carefully constructed stories; required diligent work but very productive.
	Visioning	Sets desirable future states and then permits identifying the resource to attain goals; since susceptible to misuse it necessitates disciplined application.
	Future scanning	Combines cross-impacts and scenarios to create three diverse futures; provides strategic options; can be misused if options not performed.

(1) Input methods: These are used to gather information about the subject and finding accurate answers to the right questions to understand the case examined.

(2) Analytic methods: These methods are used to analyze the elements of the foresight subject.

(3) Paradigmatic methods: Aim of these methods is to deepen understanding about the issues in the study.

(4) Iterative and exploratory methods: These methods allow exploring multiple future options and future states.

Saritas (2006) classifies the foresight methods based on the foresight process phases which constitute his Systemic Foresight Model (SFM) as follows (Smith & Saritas, 2008):

(1) Understanding: Scanning, bibliometric, crowdsourcing, literature review, interviews, trends/driver indicators, system mapping, panels, workshops.

(2) Synthesis & Models: Gaming, scenario planning, wild card, weak signals, network analysis, agent-based modeling, dynamic variable simulations, panels, workshops,

(3) Analysis & Selection: SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis, multi-criteria analysis, scenario comparisons, prioritization, Delphi, scoring, voting/rating, benefit/cost/risk analysis, panels, workshops,

(4) Transformation: Backcasting, roadmapping, relevance trees, logic charts, technology emergence pathways, strategic planning, panels, workshops,

(5) Actions: Priority lists, critical/key technologies, research & development planning, action planning, operational planning, impact assessment, panels, workshops.

2.1.3 Foresight Frameworks

A framework is "*a system of rules, ideas, or beliefs that is used to plan or decide something*" (Cambridge Dictionary, 2018). Frameworks provide best practices and rules to perform the group of activities. Since one of the backbone attributes of foresight is being a systematic process (Martin, 1995; Georghiou, 1996; Barre', 2001; Miles & Keenan, 2002; Popper, 2011; Conway, 2015), foresight frameworks are vital for shaping the methodology followed by participants and stakeholders.

Martin (1995) takes foresight a three-phase process that was performed under UK Technology Foresight Program in 1993. The first phase is "Pre-foresight" in which preparations for the futures study take place. Participants are informed about the foresight process and the importance of foresight and methodologies. Experts are determined for the topics concerned. In the second phase, "Foresight", experts work to determine the current situation of the topics and environment, find out strengths and weaknesses of the organization or sector, identify main trends, driving factors, barriers, and challenges. In this phase, participants create scenarios and a list of priorities to start with to perform the actions for attaining the desired future (Martin, 2001). The last step is "Post-foresight" or "Implementation" in which the outputs of the previous steps such as policy decisions, research and development decisions, action items, and resource allocation are put forward for implementation. The UK followed this process in the Second Foresight Program with some differences in terms of methodologies applied (Martin, 2010).

Horton (1999) suggested a three-stage process for foresight study: "Inputs", "Foresight" and "Outputs and Actions". Foresight stage consists of two steps: in the "Translation" step, information taken in the "Input" stage is translated into a form to make it understandable for the organization, and in the "Interpretation" step, knowledge transfer occurs.

Schultz (1997) claims that foresight necessitates futures-oriented thinking which implies consistent looks at long-range alternatives considering possible futures that are demanded. The futures-oriented worldview considers the past, present and

possible futures as interrelated systems. Futures research and foresight lead the emphasis of alternative futures concept. This idea arises from the reality that the future cannot be predicted (Tilley & Fuller, 2000; Miles & Keenan, 2003) but alternative futures may be imagined, explored and assessed for validity and possibility. These alternative futures are derived out of trends and emerging issues that can be observed at present. Schultz (1997) suggests five primary activities of foresight and futures studies (see Figure 4) and names this concept as "Foresight Fan" owing to the similarity of the figure (see Figure 5) preferred to depict the process stages:

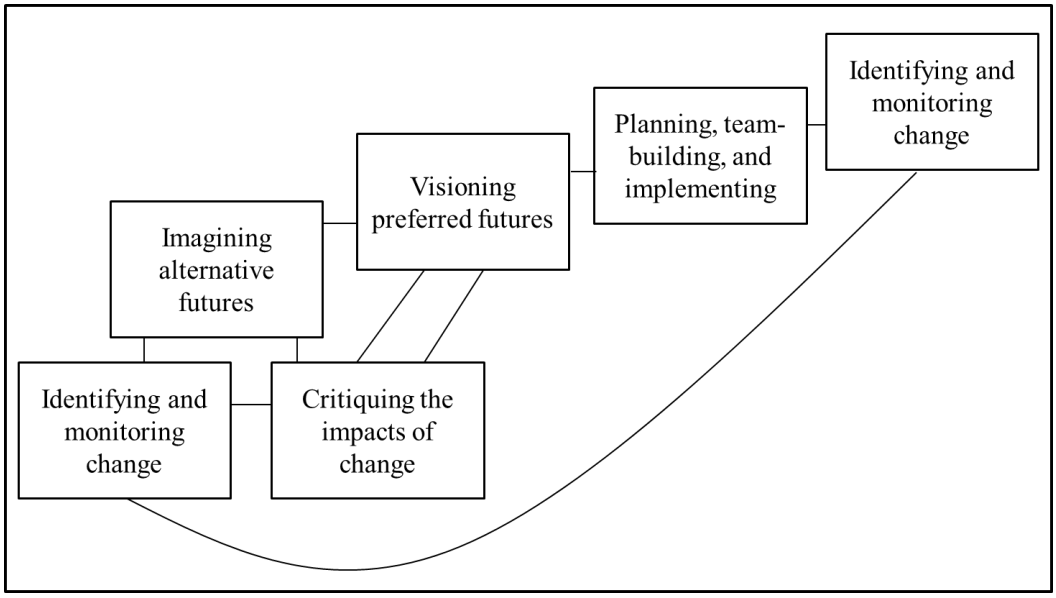


Figure 4: Foresight: Five Critical Activities (Schultz, 1997)

(1) Identifying and monitoring change: Past and present conditions are analyzed and assessed to catch the ongoing trends and emerging issues.

(2) Considering the impacts of change: Effects of the ongoing changes are assessed to find out the impacts on the macro environment and daily life.

(3) Imagining alternative possible futures: Based on the trend extrapolation and long term impacts of emerging issues of change, alternative possible futures are laid out.

(4) Visioning preferred futures: Concerning the long-term ideals, goals and values, models of the ideal future is created.

(5) Planning, team-building, and implementing the desired change: Resources are allocated to implement the change plan and organization acts to apply the desired vision and change.

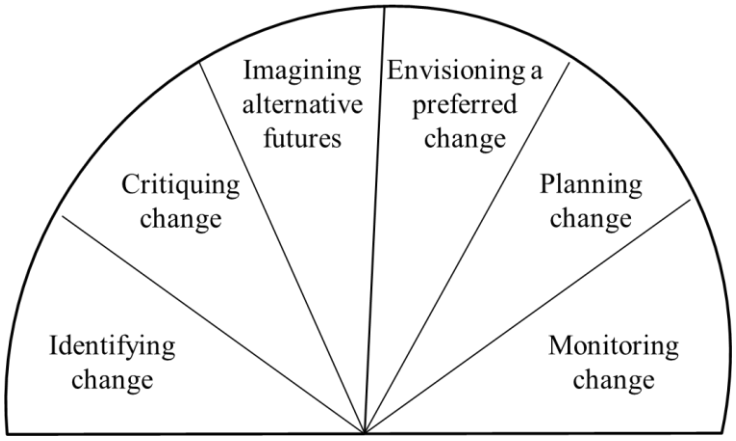


Figure 5: Foresight Fan (Schultz, 1997)

Framework Foresight is a meta-method that can incorporate other foresight methods (Hines & Bishop, 2013) developed at the University of Houston by Hines and Bishop in 2000 to perform foresight studies (Hines & Bishop, 2007). The method classifies and captures information in templates and arranges in logical flows. Baseline future and alternative futures are created with options, implications, and limitations. Framework Foresight can be viewed a version of the framework described in Thinking about the Future which is composed of six primary activities of a foresight project: Framing, scanning, forecasting, visioning, planning, and action (see Table 5). Each step feeds the following one and different set of methods can be used in the activities. Framing includes problem

identification and details of the expenses. Trends, emerging issues and details of the issues are found within the scanning activity. Baseline future and alternative futures are determined in the forecasting step by taking the input of the information from the previous step. Visioning is the step that an organization sets the goals and desired futures. All of the outputs of the study are performed in order to achieve desired aspirations within the acting step.

Table 5: Framework Foresight and Thinking about the Future Framework (Hines & Bishop, 2013)

Framework Foresight	Thinking about the Future Framework
1. Domain description	Framing
2. Current assessment	Scanning
3. Baseline future	Forecasting
4. Alternative futures	
5. Preferred future	Visioning
6. Implications analysis	
7. Futures to plans	Planning
8. Leading indicators	Acting
9. Summary	

Hines (2016) suggested Foresight Outcomes Framework for the integration of foresight outcomes for an organizational futurist to influence the decision-making process. His previous foresight framework is corroborated by three components of decision making which are learning, deciding and acting.

Learning represents data collection and discovering information to help the deciding action. Acting concludes the decision-making process and the whole process can feedback to the very first step to continue the cycle (see Figure 6).

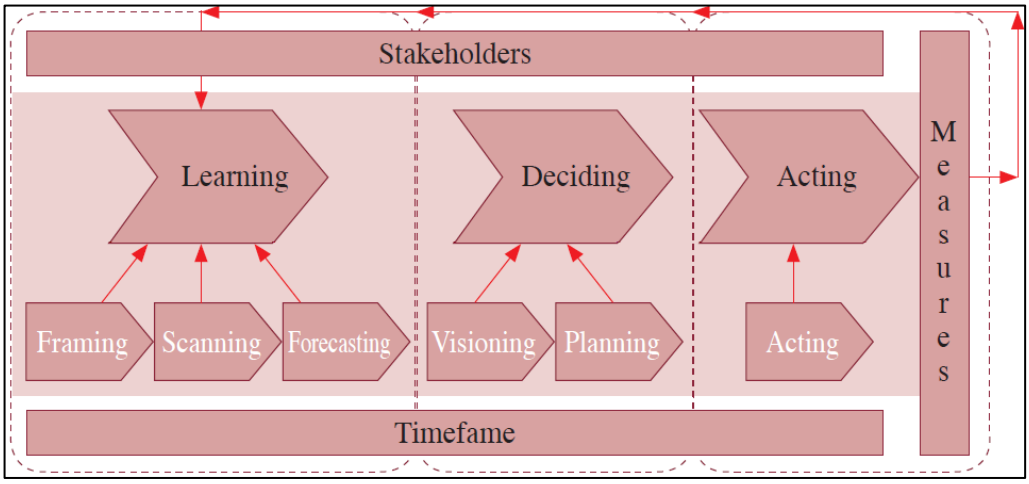


Figure 6: Foresight Outcomes Framework (Hines, 2016)

Miles (2002) outlines five complementary phases for his foresight process. These phases, Pre-Foresight, Recruitment, Generation, Action and Renewal, follow each other by taking the former steps' output as input. The process flow goes back to the first step thus making it a cycle or loop (see Figure 7).

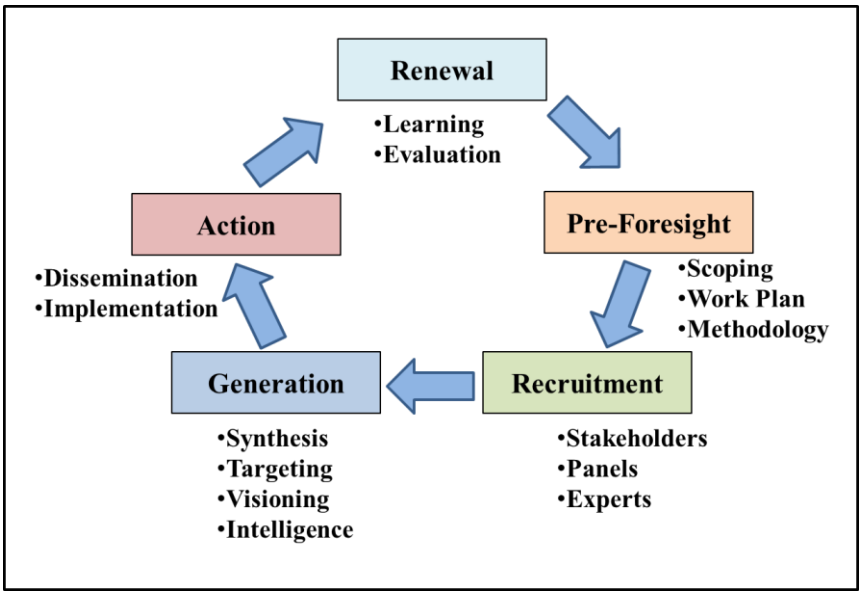


Figure 7: Miles' Foresight Process (Miles, 2002)

Voros (2003) took the base structure of Horton's foresight framework and he separated "Outputs" and "Actions into two consecutive stages. Then he added a new stage "Strategy" to his new framework. Despite being similar, Voros' framework is significantly different in the details of the stages. In Figure 8, process-flow of the framework, typical questions that are asked per steps and methods uses are depicted. In the figure, the process appears as simple linear flows but there are many feedbacks from the later steps to all of the previous ones and therefore there are loops between the steps whenever needed within the process.

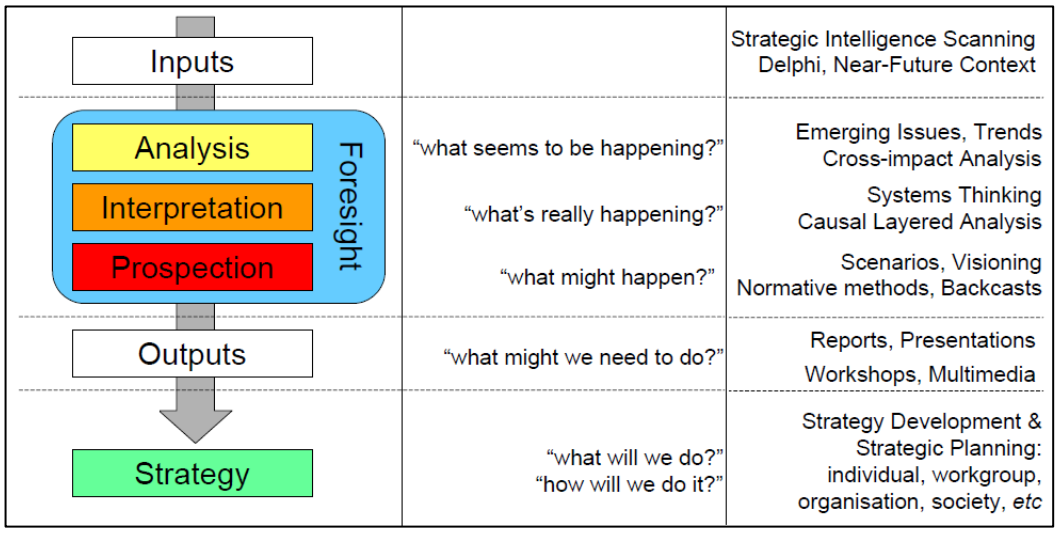


Figure 8: Voros' (2003) Foresight Framework

Four main stages of Voros' framework are described in detail as follows:

(1) Inputs: This is information collection and intelligence scanning phase. Many methods, techniques, and frameworks such as Delphi, constructing near-future context, environmental scanning can be used in this phase.

(2) Foresight: This phase has three steps that follow a logical sequence. Analysis is an essential step for a deeper understanding of the work. The sort of "what seems to be happening" questions can be asked here to collect more data about the study. Interpretation is the step seeking further details by asking "what's

really happening" questions. In the Prospection step, forward views and alternative futures are created. "What might happen" kind of questions can be asked in this step.

(3) Outputs: The outputs of a foresight study can be both tangible and intangible. Tangible outputs include the options generated by the work while intangible ones are related to the changes in thinking, perceptions, and insights. The answer to the question of "what might we need to do" has the essence of this step.

(4) Strategy: In this phase, outputs are delivered to the stakeholders and decision-makers to put forth under strategy processes and planning. In this phase "what will we do" and "how will we do it" questions are on the table.

Popper (2008b) suggests that foresight is a set of approaches composed of policy-making approaches, participative approaches and prospective approached. He revisits Miles' (2002) framework with the same fundamental steps, Pre-foresight, Recruitment, Generation, Action and Renewal, and then corroborates the process with specific actions and steps per phase (Table 6).

Saritas (2006) proposed a Systemic Foresight Methodology (SFM) based on the ideas of systems thinking. "Systems thinking" handles "events" as a whole system or parts of larger systems. His claim is that SFM is created to tackle the complexities of the human and social systems by means of more tailored methodology comprising quantitative and qualitative methods (Saritas, 2011). The social, technological, economic, environmental, political, and value (STEEPV) concepts form the external context of a foresight activity. The aim of a foresight activity is to improve or change these systems. "What is feasible?" (technology and economic dimensions), "What is possible?" (science and environmental dimensions) and "What is desirable?" (social, economic, political and values dimension) questions are asked during foresight activity).

Table 6: Foresight Methodology Steps, Actions and Elements (Popper, 2008b)

Phase	Step	Actions or Elements
Pre-Foresight	1. Scanning and understanding considerable science and technology developments, trends and issues.	Rationales Sponsor(s) Objectives Orientation Resources Approaches Time horizon Methodology Work plan Scope
Recruitment	2. Engaging with stakeholders.	Project team Partners Sub-contractors Steering Group Experts International Panels Methodologist Facilitators Rapporteurs
Generation	3. Gaining knowledge and generating visions via exploration and analysis of possible (alternative) futures.	Existing knowledge Tacit knowledge New knowledge
Action	4. Shaping the future by means of strategic planning.	Advising Transforming
Renewal	5. Evaluating.	Learning Evaluation Dissemination

SFM has five phases which represent “mental acts” of systemic (1) Understanding, (2) Synthesis and modeling, (3) Analysis and selection, (4) Transformation and (5) Action (See Figure 9). In some works of Sarıtas, there is another phase called “Evaluation” and in some others, phases are as follows: Intelligence, Imagination, Integration, Interpretation, Intervention, and Impact.

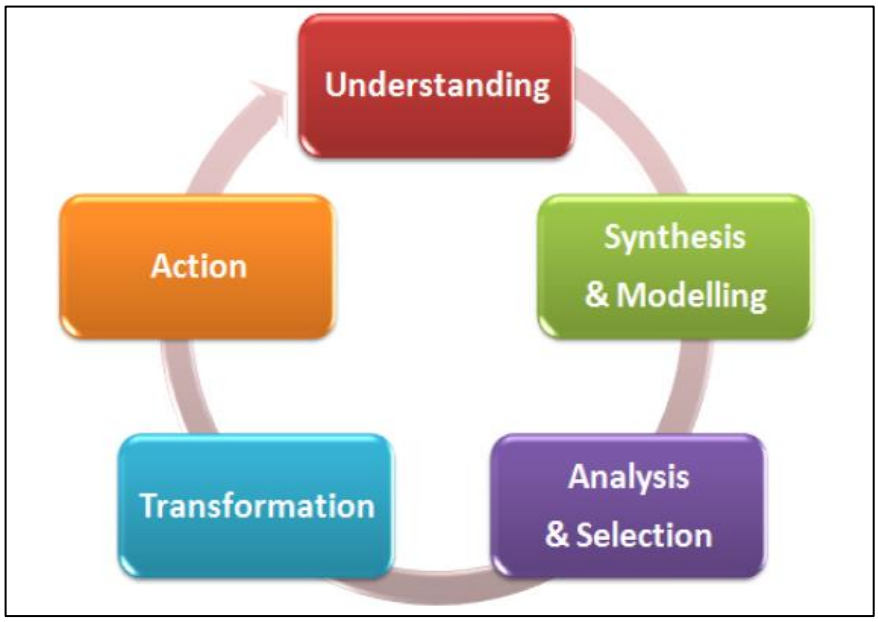


Figure 9: Phases of Systemic Foresight (Saritas, 2006)

Yüksel and Çifci (2017) created a generic foresight functional framework with sequential phases (Framing, Obtaining, Reviewing, Establishing, Synthesizing, Illustrating, Guiding, Handling, Tracking) named 'FORESIGHT'.

Functions in this framework fit the steps of famous foresight frameworks in the literature comparing the activities carried out in each step. Detailed information about the framework is given in the next chapter.

2.1.4 Foresight Generations

Throughout history, foresight studies had diverse approaches in terms of process, scope, goals, methods, and participants.

Yüksel and Çifci (2017) grouped these approaches under four different generation streams which are "based on certain society", "based on globalization phase", "based on certain era and activities" and "based on activities" (Table 7).

Table 7: Foresight Generations with Main Streams (Yüksel & Çifci, 2017)

Generation Stream	Generations
Based on Certain Society (Linstone, 2011)	1st Generation (ca. 1800) : Industrial Society 2nd Generation (ca. 1970) : Information Society 3rd Generation (ca. 2025) : Molecular Society
Based on Globalization Phase (Jemala, 2010)	1st Phase (ca. 1490s-1913) : Era of Forecast 2nd Phase (ca. 1914-1980s): Era of Forecast and 1st Generation Foresight 3rd Phase (ca. 1990s- …) 1st Generation: Science-Technology Focus 2nd Generation: Technology & Markets 3rd Generation: Technology & Markets & Social Perspective 4th Generation: Technology Management and Innovation System 5th Generation: Technology Management and Innovation System
Based on Certain Era And Activities (Reger, 2001)	1st Generation (1960s-1970s) : Technology Forecasting 2nd Generation (1970s-1990s): Technology Forecasting 3rd Generation (1990s- …) : Technology Foresight
Based on Activities (Georghiou & Keenan, 2006)	1st Generation : Technology Forecasting 2nd Generation: Technology and Markets 3rd Generation: Technology & Markets and Social Dimension 4th Generation: Distributed Role in Innovation System 5th Generation: Structural & Broad Policy Focus

Based on a certain society, foresight can be assigned into three groups (Linstone, 2011). In the first generation (industrial society), foresight activities were primarily based on technology forecasting. The second generation emerged with information society and computers were exploited for forecasting with the vast amount of data. The third generation which characterized by "molecular society" will be coming around 2025 and this era is rising on nanotechnology, biotechnology and materials science.

Jemala (2010) groups five foresight generations according to their corresponding three globalization phases. In the first globalization phase, foresight activities were based on simply prediction and forecast. Second globalization phase was influenced by world wars and forecasting was the primary approach for future studies. In the third globalization phase, it is possible to encounter all five foresight

generations which were starting from science and technology focus and peaking to manage technology and innovation system.

Reger (2001) suggests three generations based on technology foresight process and assigns certain time intervals per generation that makes another generation stream based on a certain era and activities. In the first generation, foresight was mainly based on forecasting and was a sub-task of project planning. The second generation was characterized by forecast as well; however, specialized units were responsible for future studies in organizations. In the third generation, technology foresight activities became an integral part of strategic management and decision making. Economic, social, environmental and legal trends were also considered in addition to technologic issues.

When it comes to foresight generations based on activities, Georghiou suggests five generations based on activities carried out and stakeholders involved (Georghiou & Keenan, 2006). The first generation is based on technology forecasting performed by experts. The second generation combines technology and markets while industry and academia work together to found science and business relations. Social dimension is taken into account within the third generation and more stakeholders are involved in future activities. In the fourth generation, foresight activities become integrated with science and innovation system. The fifth generation focuses on challenging issues of science, technology and innovation systems.

Yüksel, Çifci and Çakir (2017) arranged the foresight generations of Georghiou, Harper, Keenan, Miles and Popper (2008) and Harper (2013) in Table 8 with the addition of new (sixth) generation. Foresight 6.0 is the new foresight generation suggested by Çifci and Yüksel (2018) which is characterized by Industry 4.0 and beyond, Society 5.0, netocracy, cyberspace, biotechnology, more values and ethics in chaordic social dimension. This generation is explained in detail in the following chapter.

Table 8: Foresight Generations [adapted from Georghiou et.al. (2008) and Harper (2013)] with the Addition of 6th Generation

Foresight Generations	Concentration Dimensions	Participating Actors	Economic Rationales	Principle
First	Technology	Technology Experts, Professional Futurists	Economic Planning	To follow the disciplinary taxonomies of science-engineering
Second	Technology-Markets	Academics, Industrial Researchers and Managers	Market Failure	To provide a bridge between industrial/service sector and economy
Third	Technology-Markets-Social Dimension	More Social Stakeholders (NGOs, Consumer Groups	System Failure (socio-economic system)	To solve socio-economic problems
Fourth	Science-Innovation System	More Participators of National Policy Exercise	Bridging institutions in socio-economic system	To build its own structures in terms of object of analysis
Fifth	Global science-technology management-innovation systems	More experts, stakeholders and professionals with foresighting skills	Bridging institutions in socio-economic system	To build its own structures in terms of object of analysis
Sixth	Industry 4.0 and beyond, Society 5.0, netocracy, cyberspace, biotechnology, more values and ethics in chaordic social dimension	Netocrats, Netizens (crowd-sourced from a wider range of constituencies than the usual experts), Futurists, Futurizens	Blurring the roles of consumers and producers in economy	To co-create by combining the desirable visions of stakeholders with evidence from big data

2.2 Cybersecurity Foresight Studies in the Literature

2.2.1 Japanese Science and Technology Foresights

Japan started technology forecasting activities towards the end of the 1960s. Science and Technology Agency (STA) led the first future forecast of science and technology which covers the next 30 years in 1971 (Martin, 2001). They aimed to cover all science and technology areas to provide decision-makers in both public

and private sectors with the long-term trends for guidance on investments and priority settings.

National Institute of Science and Technology Policy (NISTEP) in Japan has been leading the technology foresight surveys since 1992. Japan has completed 10 technology foresight programs up to now making it an influential example for other countries in terms of foresight studies (Shengkai, Chang, Chao, & Yu, 2017).

Thousands of experts from government, universities and private sector are gathered and performed workshops about the focus areas of science and technology for possible future developments, their timeframes, importance and some other aspects through Delphi surveys. These 30-years forecasts have been repeated virtually every 5-years up to present (NISTEP, 2018). NISTEP's science and technology surveys are primarily focusing on a long time horizon, wide and diversified range of perspective and broad participation from scientists to social science experts.

Throughout the years, Japanese foresight surveys show constant progress in terms of sophistication and can be divided into three successive phases: (1) 1^{st} – 4^{th} surveys involved increasing number of experts, participants and sectors, (2) 5^{th} – 7^{th} surveys show sophistication of questionnaire design and participation, (3) 8^{th} – 10^{th} surveys include diversity of foresight methods apart from Delphi (Shengkai et al., 2017).

With the 8^{th} Technology Foresight in 2005, NISTEP has begun applying new methods such as bibliometric analysis, scenario analysis and socio-economic needs analysis in addition to the Delphi surveys (Okuwada, 2010). Through foresight studies, NISTEP provides visions of an ideal society and then tries to set forth science and technology policies to realize those visions.

In Japanese science and technology foresight series, cybersecurity issues were handled under the information and communications technologies (ICT) fields.

9^{th} S&T Foresight survey which was concluded in 2010 had 12 panels consisting of 94 areas and total of 832 topics (NISTEP, 2010). In this survey, items related to

energy, resources, and environment have been considered as having key importance for the resolution of challenges. ICT infrastructure is one of the items that received attention. Among 94 areas, there isn't any area directly addressing cybersecurity issues but just a few ones among 832 topics (Table 9).

Table 9: Cybersecurity-Related Topics in Japan's 9th S&T Foresight

Panel	Area	Topic (number and statement)
Utilization of electronics, communication, and nanotechnology in a ubiquitous society	Advanced computing systems	13. Practical quantum cryptography technology that will realize a secure global information society.
	Communications	25. Wireless sensor networks strongly supporting human activities as needed by means of many sensors placed in the living space, with guaranteed practical security.
		28. Wireless communication technology, which can be used at ease since it, secures security by automatically detecting wiretapping and/or interception and by preventing radio wave jamming of communication lines.
	Devices	57. A novel device that is capable of on-demand generation of single photons for quantum cryptography communications in order to improve the security of the network.
Information technology including media and contents	Cloud computing	4. Technology that enables information of nature highly related to public interest and social welfare to be utilized in an environment where credibility is ensured and personal information is safely managed against leakage; for example, identifying the whereabouts of missing persons by using cell phones.
	New principle for information and communication	9. Practical quantum cryptography.
	Assurance of appropriateness of information	57. A digital signature system under which citizens can use various information (such as information about noise and trouble) as evidence for disputes because the information is proved unaltered.

10th S&T Foresight study conducted between 2013 and 2015 covering up to the year 2050 had eight fields named "ICT and analytics", "health, medical care, and life sciences", "agriculture, forestry, fisheries, food, and biotechnology", "space,

ocean, earth, and science infrastructure", "environment, resources, and energy", "material, device, and technological process", "social infrastructure" and "service-oriented society" (NISTEP, 2015). The committees discussed total of 932 topics in each field. ICT topics (including cybersecurity issues) were appearing in the top topics in terms of importance, uncertainty, discontinuity and morality which were the items voted in the questionnaires (Ogasawara, 2015).

First time in Japanese foresight series, "cybersecurity" was handled as an individual item in 10th S&T Foresight survey, under ICT field which comprises 13 items (Artificial intelligence; Vision and language processing; Digital media and database; Hardware and architecture; Interaction; Network; Software; High-performance computing; Theory; Cybersecurity; Big data, Cyber-physical systems (CPS) and Internet of Things (IoT); ICT and Society) and 114 topics. Cybersecurity field exhibits high importance and following topics appears among the top topics in importance (NISTEP, 2015).

- Develop data utilization techniques with theoretically guaranteed preservation of privacy.

- Exclude software development technologies, including the technology to remotely attack security holes.

- A low cost, easy-to-use, and secure personal authentication system that can be used with confidence even when many different websites are accessed over a long period.

2.2.1.1 Society 5.0 (Super Smart Society)

Science and Technology (S&T) Policy Framework has been established in 1995 in Japan, under the name of "Science and Technology Basic Plan" encompassing five-years periods. From very first plan, primary objectives of these plans in the chronological order are; "construction of new R&D system", "promotion of R&D in prioritized areas", "promotion of R&D to address socio-economic issues". 5th Basic Plan covering 2016 to 2020 has focused on enhancing science, technology

and innovation (STI) measures with the aim of "realizing *Super Smart Society* (Society 5.0) and defining performance indicators and numerical targets (Akaike, 2016).

Information and communication technologies (ICT) is evolving, advancing and being leveraged in every aspect of daily life. Society 5.0, a buzzword put forward by the Japanese government, is a new concept that was unveiled and drafted in 5th Basic S&T Basic Plan. Society 5.0 is delineated as a society that have capability to provide needed material and services to the people whenever required and a society that can meet various social needs and overcome the differences in humanities (Hiratsuka, 2016).

Society 5.0 is an attempt for digitization of industrial and social infrastructures like Germany's "Industry 4.0", the United States' "Industrial Internet", China's "Made in China 2025" and Asia's "Smart Cities" (Harayama, 2016).

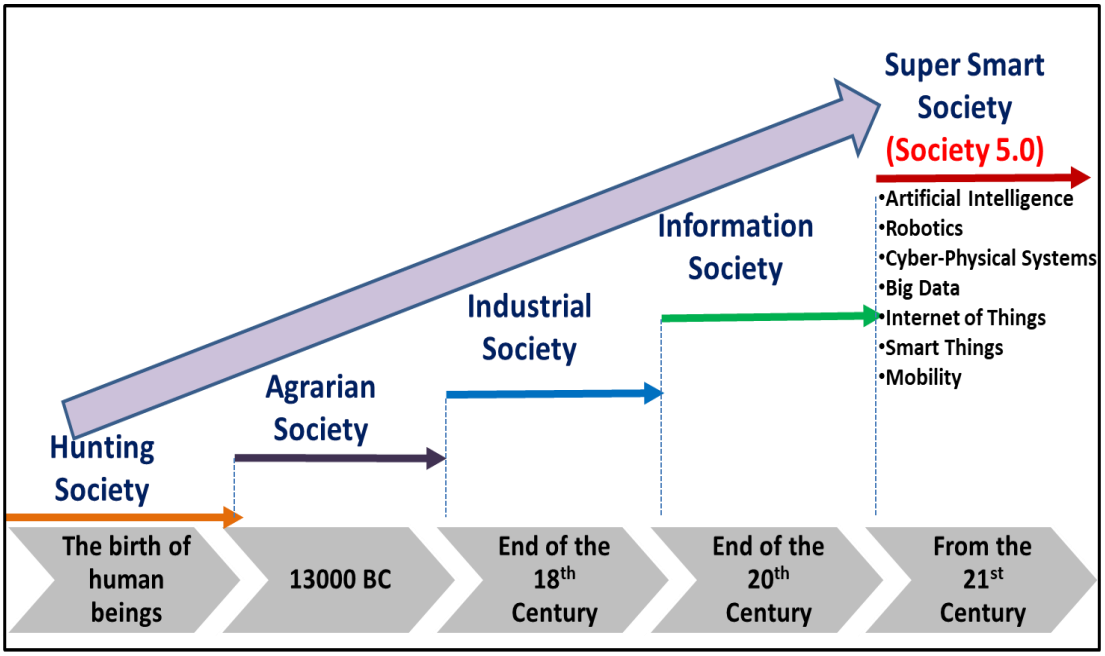


Figure 10: Human Societies and Society 5.0 "Super Smart Society"

Different eras of societies can be defined as in Figure 10, where Society 1.0 is Hunting Society in which people survive with hunting; Society 2.0 is Agrarian Society and based on agriculture; Society 3.0, Industrial Society, is characterized by industrial revolution and developments accompanying by mass production; Society 4.0 is the society in which we live and attributed to the information and computers; finally, Society 5.0 will be the next era (Keidanren, 2016) structured by artificial intelligence (AI), robotic technologies, big data, cloud computing, cyber-physical systems (CPS), Internet of Things (IoT), smart things (car, home, appliances etc.) and mobility (Hiratsuka, 2016). Society 5.0 aims integration of cyberspace with physical space (Akaike, 2016).

2.2.2 Chinese Delphi Surveys

Technology foresight in China began in the 1970s with government's first 5-years plan to determine overarching objectives and guidance for various sectors. Each industry was responsible to carry out its own foresight studies by following the major plan (H. Chen, Wakeland, & Yu, 2012). Both the Chinese Academy of Sciences and the National Research Center for Science and Technology for Development perform technology foresight for the 10 to 15-year time span within the government structure (Dreyer & Stang, 2013).

National Research Center for Science and Technology for Development carried out a foresight project between 2002 and 2004 involving investigation into science, technology, economy, and society to identify critical technologies in six fields: Information, biotechnology, new materials, energy, resources and environment, and advanced manufacturing. In the project, social and economic development issues together with technology demands in the next 15 years were addressed. Based on the two rounds Delphi surveys and suggestions from about 1000 experts from universities, research institutions and government, 483 technical topics were studied. According to the importance ratings of the topics, 26 topics in information field took place in the top100 topics. Information security technology and network security technology got the highest points, which shows the Chinese

attention to cybersecurity technologies (National Research Center for Science and Technology for Development, 2005).

Technology Foresight in China 2003-2003 project was executed by the Chinese Academy of Sciences in 2003 to identify critical technologies that China focus on. More than 1000 experts worked on eight key areas including information, communication and electronics technology with candidate 157 sub-technologies by utilizing Delphi surveys. Computer network and information security were sub-domains together with computers, communications, software, integrated circuits, video, and audio. According to the study, "large-scale anti-attack network security systems" was identified under information security as the theme to work on (H. Chen et al., 2012).

Chinese Academy of Sciences initiated the program for "Technology Foresight towards 2020 in China" in 2003. The aim of the project was to explore set of technology foresight methods suitable for Chinese development, to build scenarios for development, to conduct Delphi survey for prioritizing technology development, to construct an interactive platform for government, private sector and academia and to foster the social atmosphere and culture for technology foresight in China. Technology fields in the study were information, communication and electronics, energy, material science and technology, biotechnology and medicine, advanced manufacturing, resources and environment, chemistry and chemical and space. Thirteen information security topics were covered in the study. Widespread use of secure and cheap control technologies of large-scale electrical networks was the fourth in the top 10 important topics (Rongping & Zhongbao, 2008).

2.2.3 Nordic ICT Foresight

Nordic ICT Foresight is a technology foresight study conducted between 2005 and 2007 in order to set roadmaps for innovative ICT applications in Nordic countries (Finland, Sweden, Norway, and Denmark). ICT applications that were focused in

this study were “experience economy”, “health”, “production economy” and “security”.

The primary aims of the project were to explore proper ways to implement innovative ICT applications, estimate and examine the implications of the ICT applications, create ICT scenarios regarding possible applications for ICT with technology, application and market dimensions, discover strengths, weaknesses, opportunities and threats in terms of ICT applications in Nordic countries and create ICT applications roadmaps for ten-year period.

In the study, a combination of foresight methods was followed. These are desktop study, SWOT analyses, scenario workshop, roadmapping workshop and action workshop. In the desktop study, major development trends and attributes of Nordic countries’ ICT environments were analyzed. In SWOT analyses, strengths and weaknesses of the Nordic countries and threats and opportunities in terms of ICT technology and infrastructures were analyzed through workshops, questionnaires, and interviews. In the scenario workshop, the Shell scenario method, clustering, scenario evaluations, and brainstorming methods were applied and four scenarios were created (see Figure 11). In the roadmapping workshop, socio-technical roadmaps were produced per foresight theme. Finally, the action workshop was conducted by 21 experts through delta analysis to further elaborate on the scenarios, scenario-based matrices and action path matrices methods.

After the workshops, policy recommendations were formulated into implementation and adaptation strategies to put the policies into practice. Examples of recommendations are as follows:

(1) Create Nordic expert-based competence clusters and/or platforms in similar technological areas.

(2) Enhance remote monitoring by utilization of mobile ICT infrastructures.

(3) Create and integrate Nordic ICT application test markets.

(4) Establish a Nordic level research and policy institute to develop new concepts regarding information and general security.

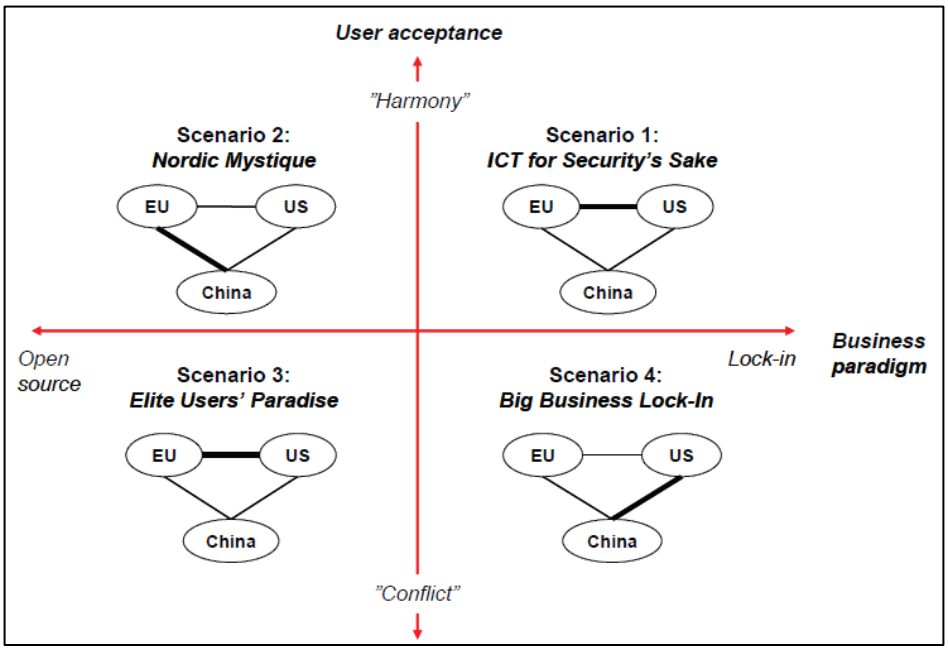


Figure 11: Nordic ICT Foresight Scenarios

Summary of the roadmaps in security is depicted in Table 10.

Table 10: Nordic ICT Foresight - Security Capabilities

Short Term (1-5 years)	Medium Term (5-10 year)	Long Term (Over 10 years)
• Simulation and scenario models for the prognoses of crises in the systems, platforms, plants and infrastructures • Simulation models for sensor systems • Development of network and infrastructure security concepts • Identity management • Long-term preservation • Distributed networks	• Biometric information in digital form (tags and bio-identifiers) • Non-reproducing technologies • Trustable and secure information systems (eavesdropping, scanning of private information, unauthorized access, backdoors etc.) • Infrastructure security applications	• Information security for ad hoc network solutions • General security and filtering solutions embedded in the communication infrastructure • Security applications in the sensor systems over the large static infrastructures, e.g. roads, electric wires and energy pipelines

2.2.4 European Foresight - Cybersecurity

Dutch Cybersecurity Council started an initiative on cybersecurity foresight during The Netherlands' presidency of the European Union (January – June 2016) and arranged first European Foresight Cybersecurity meeting on May 11th, 2016. Experts from public and private sectors and academia discussed two major issues associated with cybersecurity: Internet of Things (IoT) and harmonization of duties of care (legal obligations towards the legitimate interests of others) within the EU (Cybersecurity Council, 2016). Mainly trend analysis, brainstorming and expert panels methods were conducted during the study.

According to the results of the workshops (Cybersecurity Council, 2016), main risks of the IoT are in terms of security and privacy are manageability, lack of security incentives, impact on behaviors, surveillance and industrial espionage, and big data and privacy. IoT has dramatically changed the scope and size of accountability and responsibility of organizations in interactions with their customers. People who have suffered a loss resulting from lack of proper cybersecurity should have remedies against the organizations responsible for providing cybersecurity service. A harmonized legal framework in the EU should be established, "security by design" concept, designing the security attributes and foundations from the scratch together with the service, software and hardware design, should be taken into account.

2.2.5 German Foresight Process: "Futur"

Foresight activities in Germany were started almost parallel with Japan and Delphi studies were performed in the 1990s (Cuhls, 2003b). German Federal Ministry of Education and Research (BMBF) started a foresight process called Futur in 2001. Foresight studies to determine the priorities and agenda of German research and innovation policies cover a period of 15 years. The main objectives of the foresight studies are: To determine possible research areas, to support Germany's economic development, to improve the quality of life, developing skills in industry and academia, to contribute to the protection of resources, and to protect the climate

and the environment (BMBF, 2018). Combination of different methods such as literature survey, panels, expert reports, surveys, workshops, interviews and database bibliometric were exploited during foresight studies (Cuhls, 2010).

BMBF has adopted a two-stage process since 2007 for foresight process: Cycle I and Cycle II.

The last completed foresight Cycle I lasted between 2007 and 2009 with the emphasis on technology-oriented approach.

Cycle II was conducted between 2012 and 2014 by focusing on future social trends and challenges with a time horizon of 2030 (Zweck, Holtmannspötter, Braun, Hirt, et al., 2017). Cycle II is composed of three steps:

- Step-1: Identify social trends and challenges (60 trends)
- Step-2: Compile research and technology perspectives (101 topics)
- Step-3: Work out innovation seeds (9 fields)

In the last Cycle I ended in 2009, 14 start fields (material, ICT, nanotechnology, biotechnology, optics, production, health, water, environment, system research, energy, neurosciences, services science, mobility) and 7 future fields (Production Consumption, Human-Technology Cooperation, Transdisciplinary Models and Multi-Scale Simulation, Deciphering Ageing, Time Research, Sustainable Living Spaces, Sustainable Energy Solutions) were analyzed (Cuhls, 2016).

In Step-1 of Cycle II, 60 social trend profiles were determined (Zweck, Holtmannspötter, Braun, Hirt, et al., 2017). The trends related to cyberspace and cybersecurity are listed in Table 11.

In Step-2 of Cycle II, total of 11 fields (Table 12) were analyzed and handled in terms of research and technology perspectives (Zweck, Braun, Erdmann, Hirt, & Kimpeler, 2015).

Table 11: Cyberspace and Cybersecurity Social Trends in “Futur”

Category	Trend
Society / culture / quality of life	Digital competency pressure as a social organizational task
	Trust in the internet age
	Increasing demands for the right to use digital goods for free
	Post-privacy versus privacy protection
Business	Information technologies are replacing even currently well-paid jobs
Politics and governance	Click to protest: more activities through organization in the internet

Table 12: Technology Fields in German Foresight “Futur”

Biotechnology	Nanotechnology
Services	Photonics
Energy	Production
Health and Nutrition	Civil Security Research
Mobility	Materials Science and Engineering
Information and Communication Technology (ICT)	

Cybersecurity topics were mainly handled under the ICT field in the study. Cybersecurity topics in the study are as follows:

- Biometric methods
- Cryptography
- Security by design
- IT (Information Technologies) forensics
- Cyber-physical systems

- Cybercrime
- Intrusion of internet applications into the everyday life of broader social classes
- Homomorphic encryption
- IT security auditing
- Privacy enhancing technologies

In the last step (Step-3) of Cycle II, following innovation seeds were identified through linking the social challenges with the research and technology perspectives (Zweck, Holtmannspötter, Braun, Erdmann, et al., 2017): Do-it-yourself in Germany, citizen science in the area of health, automation and robotics, digital and virtual educational offerings, global innovation landscape, innovations support governance, infrastructures for socio-technical innovations, collaborative forms of value creation, privacy in transformation.

2.2.6 Korean Technology Foresight

In Korea, science and technology foresight activities are performed at the highest level by the Korean Institute for Science and Technology Evaluation and Planning (KISTEP) since 1993.

The main objective of technology foresight activities in Korea is to forecast the science and technology developments and use these results in creating science and technology policy and strategies (Choi & Choi, 2015).

Foresight studies are carried out by KISTEP every five years according to the national law (Framework Act of Science and Technology) and lasts between 1.5 and 2 years. Foresight results are reflected in the science and technology plan. National science and technology strategies are set forward by performing technology foresight activities (KISTEP, 2018a).

Since 1993, Korea carried out five successive technology foresight studies and reflected the results of foresight activities into S&T master plans. Foresight methods used in foresight studies and timescale are shown in Figure 12 (KISTEP, 2017).

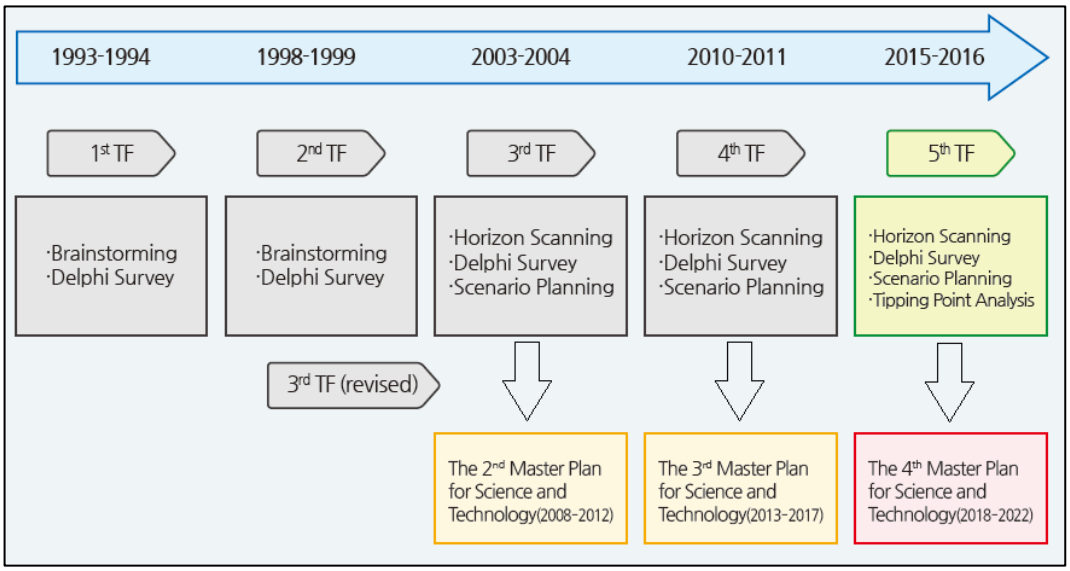


Figure 12: Outline of Korean Technology Foresight

In the 5th Technology Foresight, total of 267 technologies were identified and analyzed as future technologies for the time horizon of 2040. Distributions of the number of technologies per major issue group are in Table 13 (KISTEP, 2017).

Table 13: Number of Future Technologies by Major Issue Groups in the 5th Technology Foresight

Major Issue Group	Number of Technology
Social Infrastructure	51
Ecosystem and Environment Friendliness	59
Transportation and Robotics	43
Medical and Life	47
Manufacturing and Convergence	48
Information and Communication	39

Cybersecurity-related topics were handled under ICT issue group in the study. Cybersecurity topics in the study are as follows (KISTEP, 2017):

- Online software for terror attack crime prediction and evidence analysis,
- Quantum cryptosystem key distribution preventing inverse calculation,
- Integrated circuit falsification and information exposure prevention ,
- Information encrypted third-person computation security technology,
- Real-time self-defense technology to prevent cyber terrorism.

As a result of the foresight studies, "10 Emerging Technologies" list has been published on the KISTEP Web Site, every year since 2009 (KISTEP, 2018b). In Table 14, the last three years' technology lists are listed. Cybersecurity-related technologies are highlighted in the table.

Table 14: KISTEP Emerging Technologies*

Year	10 Emerging Technologies
2018	Responsive Housing Technology; Life-long Virtual Assistant Software Technology; Smart Tattoo Technology; Soft Robot Technology; Connected Car Technology; Modular Public Transportation System; Wireless Power Transfer Technology; **Artificial Intelligence (AI) Security Technology**; Mixed Reality
2017	IoT-based Context-aware Dimming Technology; Active Noise Control & Reduction Technology; AI Fact-checking Assistive Technology; Nuclear Power Plant Accident Response System; Non-radioactive Non-destructive Testing Technology; Particulate Matter Reduction Technology; Eco-friendly Green & Red Tide Elimination Technology; Advanced Domestic Waste Sorting and Recycling System; Real-time 3D Environmental Change Observation Technology; Ecological Restoration Technology Using Microorganisms
2016	**Big Data-based Fraud Detection and Prevention Technology**; Information of Everything (IoE) Technology; Digital Assistant based on Deep Learning; Virtual Reality Technology for Leisure; **Security Technology for Online/Mobile Financial Transaction**; Mental Health Diagnostic and Treatment Technology; Social Robots; **IoT Security**; Big Data-based Infectious Disease Prediction and Alert System; System-based Technology for Particulate Matter Control

*: Cybersecurity related technologies are **bold**.

2.2.7 Russian Science and Technology Foresight 2030

In Russia, a significant number of foresight studies have been carried out in the last decade, the initiative especially came from the federal government agencies. The first national-level technology foresight was the Science and Technology (S&T) Foresight 2025 started in 2007 by the Russian Ministry of Education and Science including three areas: Macroeconomic forecast for the Russian economy, prioritized are of technology, foresight for economy sectors (Sokolov, 2018).

Russian Foresight 2030 was conducted between 2011 and 2013 involving a dozen of institutions with more than 3000 experts in various fields for the identification of the most promising science and technology development areas in Russia towards 2030 to maintain competitive advantages (Sokolov & Chulok, 2014).

In the study, a set of quantitative and qualitative methods including Delphi were applied for seven areas (energy, nanotechnology, ICT, biotechnology & medicine, ecology, and transport). Outputs of the study are as follows:

- Global trends
- Grand challenges
- Windows of opportunities for each area
- New markets and niches per area
- Innovative products and services for each market
- Assessment of Russia versus world leaders
- Policy recommendations for science, technology and innovation

ICT is considered among the key drivers for a knowledge-based economy. Based on the conclusions, seven research areas were identified in ICT: Telecommunication, data processing and analysis, hardware components, electronic devices and robotics, predictive modeling and simulation, software,

computer architecture, and information security. Cybersecurity-related technologies were identified and treated under the “information security” research area (Sokolov & Chulok, 2014).

2.2.8 French Key Technologies 2020

France has been conducting foresight studies in Europe since the 1960s. These studies are carried out in almost every department directly under the auspices of the Prime Minister through the Strategic Analysis Center (Dreyer & Stang, 2013). France uses technology foresight in support of policymaking at both national and regional level. “Key Technologies” named series of technology-oriented foresight exercises exploiting Delphi method was started in 1994 by the Ministry of Industry (The European Foresight Platform, 2010).

Key Technologies foresight studies are conducted every five years by The Ministry of Economy and Industry to identify strategic technologies for the competitiveness of French companies. Key Technologies 2020, which is the 5th edition and conducted between 2014 and 2016, has become a reference for French companies. The study identifies 47 key technologies in 9 application areas: food, environment, housing, security, health and well-being, mobility, energy, digital, leisure, and culture (French Government, 2018).

Advanced and active materials, sensors, valorization and intelligence of big data, modeling, simulation and numerical engineering, IoT, 5th generation infrastructures, secure distributed embedded systems, human augmentation, artificial intelligence, autonomous robotics, secure communications, behavioral analysis, new hardware-software integrations, supercomputers and strong authentication are the 15 of technologies out of 47 listed under the security area. Among those, secure distributed embedded systems, secure communications and strong authentication are directly related to cybersecurity (Ministère De L’Économie, 2017).

2.2.9 UK's Cyber-Related Foresights

The UK has been conducting foresight studies since the early 1990s, with the UK Foresight Program in 1994 for the aim of supporting policy and planning (Schmidt, 2015).

Government foresight exercises in the UK is led by the UK Foresight Office which is a central government organization directly reporting to the Cabinet. The efforts used to be dedicated mainly to technology but now new thematic topics are pursued to look at the challenges for the future. Separately, the Ministry of Defense carries out foresight activities under Development, Concepts and Doctrine Centre (DCDC) and the UK Defense Science and Technology Laboratory (DSTL) (Dreyer & Stang, 2013).

Cyber Trust and Crime Prevention Project was carried out in 2004 within Home Office Ministry for Crime Reduction, Policing, Community Safety and Counter-Terrorism with the participation of over 45 scientists and 260 experts overall from various sectors. The aim of the project was to provide a look for future technologies and to establish the actions to establish cyber trust and prevent cyber crimes. Outputs of the projects were (Office of Science and Technology, 2004):

- The current state of the technology in the relevant areas including identification, authentication, trust and issues regarding reliance on behavioral analysis software,
- Possible developments in hardware and software,
- Scenarios of how risks and opportunities are developed in the future and how to respond to that development.

Technologies and Innovation Futures (TIF) series of foresight exercises are conducted periodically by the Government Office for Science in order to look for potential enablers of long-term economic growth in the UK.

The first TIF was carried out in 2010 and second in 2012 and the last in 2017. A number of significant technologies were classified as “Eight Great Technologies” (Advanced materials, Satellites, Energy storage, Robotics and autonomous systems, Agri-science, Regenerative medicine, big data, Synthetic biology). Quantum technologies and IoT were added to the promising technologies for investment.

“Eight Great Technologies” have received over £900 million since the program started. Over 1000 experts from academic and industrial technologies participated in the analysis of over 50 technologies, around 100 articles were published since 2012, almost 20,000 patents received.

Quantum security for internet, machine learning and algorithms for security are the main technology topics for cybersecurity in the TIF foresight series (Government Office for Science, 2017).

2.2.10 Turkey’s Vision 2023 Foresight Project

In 2000, Turkish Supreme Council of Science and Technology (SCST) appointed Scientific and Technological Research Council of Turkey (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu -TÜBİTAK) to determine the new science and technology policies for a period of 20 years to 2023, 100th anniversary of Turkish Republic, based on the fact that the last science and technology policy work was carried out in 1993. Therefore, the project was entitled “Vision 2023” (TÜBİTAK, 2004b).

The project mainly aimed to determine strategic technologies and priority areas of research and development and lasted almost two years by applying expert panels and Delphi method as the main foresight methods.

Ten panels and two crosscutting thematic areas were set up under Vision 2023 as shown in Table 15.

Table 15: Vision 2023 Panels and Thematic Areas

Technology Panels	1	Information and Communication
	2	Energy and Natural Resources
	3	Health and Pharmaceuticals
	4	Defense, Aeronautics and Space Industries
	5	Agriculture and Food
	6	Machinery and Materials
	7	Transportation and Tourism
	8	Textiles
	8	Chemicals
	10	Construction and Infrastructure
Thematic Areas	1	Education and Human Resources
	2	Environment and Sustainable Development

Panels created 413 Delphi statements, which were sent to nearly 7,000 experts via mail and e-mail. 2,400 experts (34%) responded to the survey. After the second round of Delphi survey, importance and feasibility indices were calculated per statement. Technology Panels suggested 94 Technology Activity Areas (TAA) that represent a cluster of technological developments mostly based on Delphi statements and new product or service. A roadmap was created for each of the TAA. Then, a workshop was conducted to identify strategic technology fields. Identified strategic technologies were congregated under 8 technology topics: (1) Information and communication technologies, (2) Biotechnology and gene technologies, (3) Nanotechnology, (4) Mechatronics, (5) Production process and technologies, (6) Material technologies, (7) Energy and environmental technologies and (8) Design technologies. Expert groups carried out studies to create 20-years roadmaps for each strategic technology fields (TÜBİTAK, 2004b).

Cybersecurity capability statements were held under two panels, Information and Communication Panel and Defense, Aeronautics and Space Industries Panel. Information security was one of the 10 TAA with 4 Delphi statements and cryptology was one of the 32 technology fields under the Information and Communication Panel (TÜBİTAK, 2004a). Additionally, cyberwarfare, cryptology, web security and information security were deemed as critical technology topics (TÜBİTAK, 2003).

CHAPTER 3

"FORESIGHT" FRAMEWORK, FORESIGHT PERISCOPE MODEL AND NEW GENERATION OF FORESIGHT

3.1 "FORESIGHT" Framework

A generic foresight framework named "FORESIGHT" was created by Yüksel and Çifci (2017), which has consecutive functional steps in the order of letters in "foresight" word:

- **Framing**: Fulfilling the tasks of determining foresight purpose, scope, content and time horizon.

- **Obtaining**: Collecting data and information, gathering participants also by using co-nomination in an iterative way which are consistent with its frame stated in the previous function.

- **Reviewing**: Sharing ideas and opinions on the accessed data and information related to past and present, summarizing, analyzing them to be processed.

- **Establishing**: Thinking about the future with the knowledge created, picturing possibilities in the minds and imagining the alternatives to create futures.

- **Synthesizing**: Combining all alternative future thoughts with the present state conditions and resources in an interpretive way. Discussion, negotiation, facilitation and conflict resolution takes place in this function.

- **Illustrating**: Pointing out the possible futures, visioning and generating reports, broadcasting with multimedia, sharing in social media.

- **Guiding**: Defining actions and changes that will be performed, determining the sequencing of them to reach different futures, strategy development and planning.

- **Handling**: Taking actions, making changes and solving application problems.

- **Tracking**: Evaluating outcomes and results of handling, performing impact analysis to take lessons for a learning process.

In Table 16, functions in the FORESIGHT have been matched with the phases of mentioned foresight frameworks based on their actions and artifacts within specific phases.

Table 16: Foresight Frameworks in the Literature

<table>
<tr><th></th><th>Yüksel&Çifci (2017)</th><th>Martin (1995)</th><th>Miles (2002)</th><th>Voros (2003)</th><th>Bishop&Hines (2006)</th><th>Schultz (2006)</th><th>Sarıtaş (2011)</th></tr>
<tr><th></th><th>Foresight Functions</th><th>Foresight Process</th><th>The Foresight Cycle</th><th>A Generic Foresight</th><th>Framework Foresight</th><th>Key Activities of Integrated Foresight</th><th>Systemic Foresight</th></tr>
<tr><td>F</td><td>Framing</td><td rowspan="2">Pre-Foresight (Decision, Preparation)</td><td>Pre-Foresight</td><td rowspan="2">Inputs</td><td>Framing</td><td></td><td></td></tr>
<tr><td>O</td><td>Obtaining</td><td>Recruitment</td><td rowspan="2">Scanning</td><td>Identify and monitor change</td><td>Intelligence</td></tr>
<tr><td>R</td><td>Reviewing</td><td rowspan="5">Foresight (Process Design, Strategic Analysis, Agreeing, Disseminating)</td><td rowspan="5">Generation</td><td>Analysis Interpretation</td><td>Asses and Critique Impacts</td><td>Imagination</td></tr>
<tr><td>E</td><td>Establishing</td><td rowspan="2">Prospection</td><td rowspan="2">Forecasting</td><td rowspan="2">Envision Preferred Futures</td><td rowspan="2">Integration Interpretation</td></tr>
<tr><td>S</td><td>Sythesizing</td></tr>
<tr><td>I</td><td>Illustrating</td><td>Outputs</td><td rowspan="2">Visioning Planning</td><td></td><td></td></tr>
<tr><td>G</td><td>Guiding</td><td rowspan="2">Strategy</td><td rowspan="2">Plan and Implement Change</td><td rowspan="2">Intervention</td></tr>
<tr><td>H</td><td>Handling</td><td>Post-Foresight (Implemantation, Allocation)</td><td>Action</td><td>Action</td></tr>
<tr><td>T</td><td>Tracking</td><td></td><td>Renewal</td><td></td><td></td><td></td><td>Impact</td></tr>
</table>

FORESIGHT framework does not enforce specific methods for the functions. On the other hand, there are suitable methods for each step that fulfill the activities needed in the steps.

Table 17 depicts some of the well-known methods that can be used in the steps of the framework.

Table 17: FORESIGHT Framework's Functions and Suitable Methods

Functions	Suitable Methods
Framing	Visioning, Horizon Scanning, Literature Review
Obtaining	Data Mining, Bibliometric Analysis, Literature and Statistics Review, Patent Analysis, Conferences/Workshops, Citizen Panels, Voting/Polling, Brainstorming, Interviews, Surveys, Benchmarking, Focus Group
Reviewing	Trend Analysis, Agent-based Modeling, System Dynamics, SWOT Analysis, Horizon Scanning, Stakeholder Analysis, Cross-impact/Structural Analysis, Indicators/Time Series Analysis (TSA), Extrapolation, STEEPLE Analysis, Focus Group
Establishing	Delphi, Simulation/Gaming, Expert Panel, Wild Cards, Science Fictioning, Backcasting, Genius Forecast, Multi-criteria
Synthesizing	Scenario Building, Visioning, Key/Critical Technologies, Quantitative Scenarios/ Cross Impact Systems and Matrices (SMIC)
Illustrating	Roadmapping, Essays/Scenarios
Guiding	Strategy Planning, Policy Recommendations, Critical/Key Technologies
Handling	Strategies, Policies
Tracking	Assessment, Survey, Bibliometric Analysis, Impact Indicator Development, Post Mortem Project, Policy Impact

3.2 Foresight Periscope Model (FPM)

Foresight Periscope Model (FPM), created by Yüksel and Çifci (2017), is a foresight model that facilitates foresight activities from the beginning to the end. Similar to the periscope tool used in maritime operations, the model aims to determine future strategies as clearly as possible by depending on the resources and methodologies therein (See Figure 13).

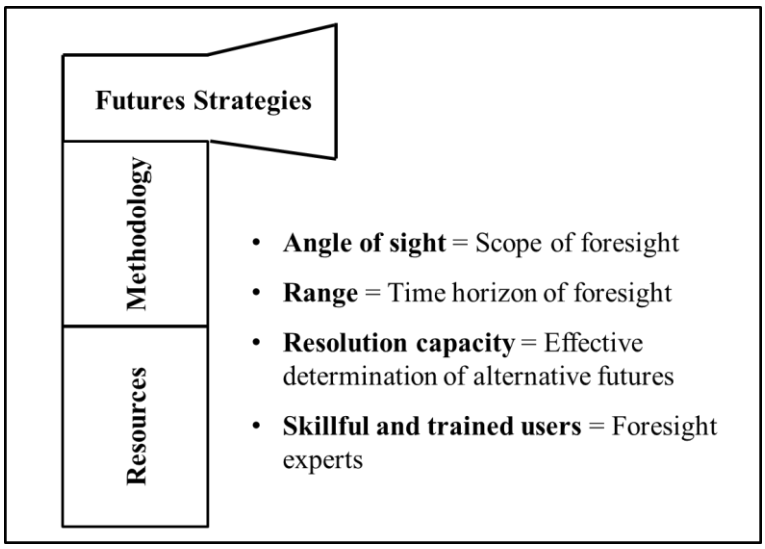


Figure 13: Foresight Periscope Model in the Periscope Tool

Resources form the base of the model, the methodology is selected according to the resources, aim and scope of the foresight study and future strategies are identified through the results of the activities that follow the chosen methodology.

In the FPM, tangible and intangible resources and their footprints in organizational, sectoral, national and international levels are the determiners of the methods. Selection of proper method combinations is highly dependent on the resources and the nature of the foresight study. Future strategies are the alternative futures among which the desired or the possible future exists.

3.2.1 Foresight Resources

A company's resources include all capabilities, assets, information, knowledge, and processes that enable the company to carry out its missions (Barney, 1991). Resources required for a foresight study are generally reduced to the finance while the foresight scope relies on other factors such as personnel, time, organizational infrastructure, political support and the organizational culture (United Nations Industrial Development Organization [UNIDO] 2005a). Popper (2010) claims that resources constitute time, money, team, infrastructure, culture, and political

support. In FPM, resources are split into tangible and intangible resources with different levels: organizational, sectoral, national and international (Figure 14).

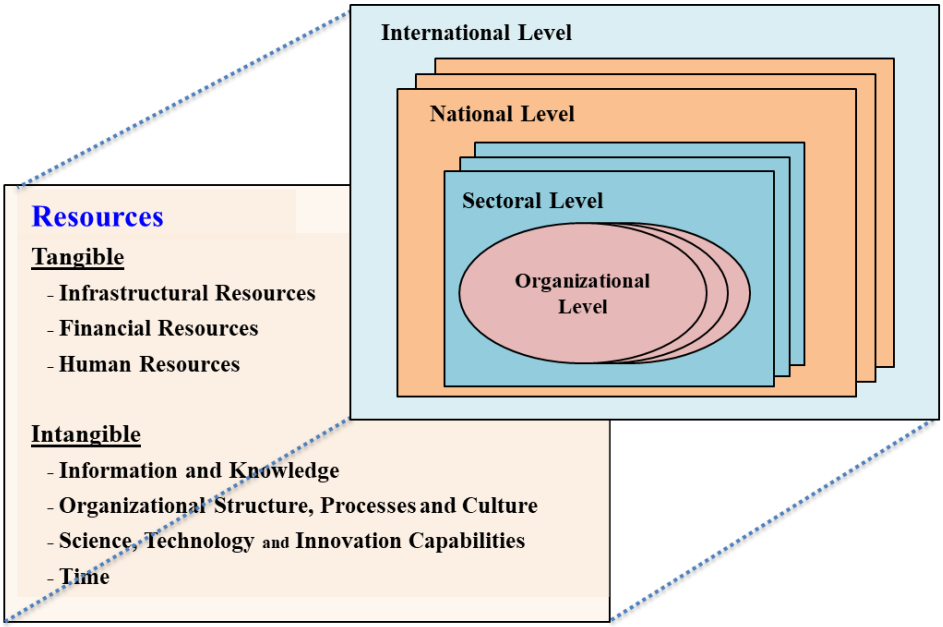


Figure 14: Resource Levels and Resources Used for Foresight Activities

3.2.1.1 Tangible Resources:

(1) Infrastructural Resources: These are physical structures required for an organization to survive. Additionally, institutions that the organization can interact with are among the infrastructure resources. Superb infrastructure resources ease foresight studies by providing beneficial inputs (Miles & Keenan, 2003). Research infrastructure elements should be integrated into science, technology and innovation policies (Popper, Georghiou, Keenan, & Miles, 2010).

(2) Financial Resources: Foresight activities require finance in order to access and utilize other resources to conduct the foresight. Financial costs chiefly stem from foresight project team, events and meetings, travel, and consultation expenses (UNIDO, 2005b).

(3) Human Resources: This is the workforce of an organization. Peter F. Drucker defined the “human resource” that human has the ability to coordinate, integrate, judge and imagine that other resources do not have (Marciano, 1995). Foresight requires expertise for the topics under consideration use of foresight methods (UNIDO, 2005b). One of the most critical success factors in foresight is finding proper experts and stakeholders throughout the study (Popper, Keenan, Miles, Butter, & Sainz, 2007).

3.2.1.2 Intangible Resources:

(1) Information and Knowledge: Davenport and Prusak (1998) define “data” as a set of objective facts about events and “information” as data with purpose and relevance. Nonaka and Takeuchi (1995) define “knowledge” as “*a dynamic human process of justifying personal belief toward the truth*”. It is taken for as the most important organizational asset (Nah, Siau, Tian, & Ling, 2002) and renewable and reusable resource of organizations (Aktharsha, 2010). Effective organizational performance requires possessing necessary information and knowledge resources (Ray, 2003) which is the source of sustaining success and competitive advantage (Rodriguez & Ordóñez de Pablos, 2003).

(2) Organizational Structure, Processes and Culture: Organizational structure refers to static posture while organizational processes mean how an organization performs its missions (Rant, 2004). Hao, Kasper and Muehlbacher (2012) suggest that the structure of an organization have an impact on organizational performance and organizational innovation (Chen and Chang, 2012). Schein (1992) defines “organizational culture” as a pattern of fundamental assumptions gained through the problem solving and norms that shape how the members perceive, think and feel when countering those problems. Culture has an influence on the conduct of technology foresight. Cultural resources include tendency for taking risks, degree of collaboration with other organizations and competitors (Miles & Keenan, 2003).

(3) Science, Technology and Innovation Capabilities: Science is a mechanism used to explain the natural universe and collection of data (Shrake, Elfner, Hummon, Janson, & Free, 2006). According to Misa (2009), Jacob Bigelow coined the "technology" term with the meaning of the processes, terminology and principles of an area of arts integrated into the application of science. Science and technology are vital for organizational and national resource (Xu, 2012). Rogers (1995) defines innovation as "*an idea, practice, or object that is perceived as new by an individual or another unit of adoption*". Changing business environment and customer needs, technological developments and intense competition enforce innovations (Goffin & Mitchell, 2010). For success in the future, organizations have to enhance innovation capability and creativity (Saunila & Ukko, 2012).

(4) Time: Time is another important resource for foresight studies. Proper timing is crucial for both appropriate exploitation of other resources and decision-making. Typically, national foresights last one or two years depending on the aims and scope while private sectors' are relatively shorter (UNIDO, 2005a).

3.2.1.3 Importance of Resources

Srivastava and Misra (2014) suggest that there are 16 critical success factors for technology forecasting which can be deemed a subset of technology foresight.

In Table 18, these factors and corresponding resource elements are listed. Some factors match with merely one resource while some match multiple (Yüksel & Çifci, 2017). From the table, it can be seen that FPM's resources cover all of the critical success factors of technology forecasting. In a foresight exercise, any level of resources can be used depending on the scope of the activity and available resources directly influence the quality and scope of the foresight (Miles & Keenan, 2003).

Table 18: Technology Forecasting Critical Success Factors and FPM Resource Elements

No.	Critical Success Factor	Resource Elements
1	Accuracy in forecast	Infrastructural Resources Human Resources Information and Knowledge
2	Understanding the nature and evolution of technological change	
3	Understanding the technology ecosystem	
4	Developing a forecasting method	
5	Degree of reliability and validity of the forecast	
6	Technical sophistication	
7	Identifying present key technologies	
8	Clear strategy	
9	Time horizons (forecasted period)	
10	Availability of accurate historical data	Information and Knowledge
11	Extent of data availability	
12	Degree of data validity	
13	Related cost	Financial Resources
14	Satisfy the objective of technological competitiveness	Organizational Structure, Processes and Culture
15	Timing of forecast	Time
16	Number of variables affecting the development of technology	Science, Technology and Innovation Capabilities

3.2.2 Future Strategies

The last module of the FPM is “Future Strategies” which is on the resources and methodology and provides a view for alternative futures and vision for strategies. The main aim is to attain the desired future.

There are six different types of alternative futures defined in “Futures Cone” (see Figure 15) which was created by Hancock and Bezold and reorganized by Voros (2005). “Potential” includes even the imagination cannot reach yet. “Possible” is the one that we think “might” happen in someday in the future. “Plausible” is the

one that we think "could" happen based on our current comprehension. "Probable" is the one that "likely to" happen usually based on current trends. "Preferable" is the one that we prefer to happen and "Projected" is the singular default future, which is the most probable of the probable ones.

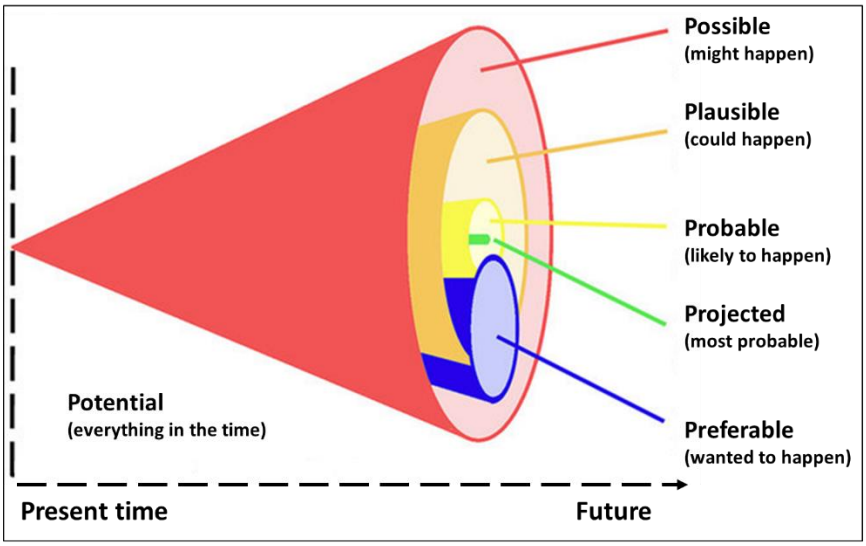


Figure 15: Futures Cone (Voros, 2005)

It is always a challenge to reach the preferred future, which is the main goal of strategic vision, because of the uncertainties happening in the time. Visions should be disciplined to attain the goals (Haig, Alexander M., 1984), therefore, some systematic approaches and specific methods should be adopted for shaping the future. In this context, foresight disciplines are aware of the presence of many potential futures but only one them will happen (Grupp & Linstone, 1999).

Dator's first law of futures states that "*The future cannot be 'predicted' but alternative futures can be 'forecasted' and preferred futures can be 'envisioned' and 'invented'*" (Sardar, 2010). Slaughter (1995) highlights the misconception in the perception of foresight as "predicting the future" and he states that foresight is a human attribute allowing them to choose the proper course of actions to invest possible futures. Since there are various futures in hand, there may be multiple

paths for them and scenarios are the tool combinations for alternative futures (Godet & Roubelat, 1996). Scenarios show the projections of change about the futures (Ringland, 2010).

Scenarios are one of the factors that can be considered in strategy development process. Scenarios can even shape strategies. Strategies embody the risks since the future is uncertain to some degree. Risk assessment and foresight share many similarities except for risk assessment focus on negative events (Durance & Godet, 2010).

Strategic foresight enhances the perception of future possibilities (Slaughter, 1995) and focuses on the forces which may promote the desired outcome (Hammett, 2005). Within the context, foresight can be qualified as strategic thinking, which is finding reasonable alternatives, and incorporated into strategy development and planning process in organizations (Voros, 2005). The goal of strategies is to improve the awareness of possible futures and the driven factors to lessen ambiguity in addition to saving time in strategic process (Luhmann, 2006). Being aware of alternative futures and potential paths to success is a substantial success factor in a foresight process (Schatzmann, Schäfer, & Eichelbaum, 2013).

FPM does not impose or enforce a specific approach to handle and manage the futures strategies. Suitable methods in the FORESIGHT framework can be exploited to identify, create, implement and track future strategies.

3.3 Foresight 6.0

Foresight generations are shaped by organizations' needs and technological developments. In the literature, foresight was divided into five generations based on objective, scope, methods, actors, and context. Any foresight exercise can have one or more generations' features. Çifci and Yüksel (2018) suggest new (sixth) foresight generation, which is named Foresight 6.0, concentrates on Industry 4.0 and beyond, Society 5.0, netocracy, cyberspace, biotechnology and more values and ethics in chaordic social dimension.

Prevalence of cyberspace through networks and increasing power of communication through the internet makes the netocracy be rising management concept in networked societies. Performers and stakeholders of the sixth foresight generation will be the netocrats, netizens, futurists, and futurizens as seen in Figure 16. This generation provides more effective implementation of foresight exercises through facilitating the participation of diverse stakeholders on global scope through the network. Foresight data can be obtained online; big data can be utilized by netocrats and futurists. This new foresight generation also utilizes artificial intelligence, machine learning of cyborgs, biotechnological and cybernetics advancements within the foresight process. Because some actors of the foresight (futurizens and netizens) are comprised not only people but also robots and cyborgs, this new foresight generation encompasses new economic models, new legislation and ethical norms.

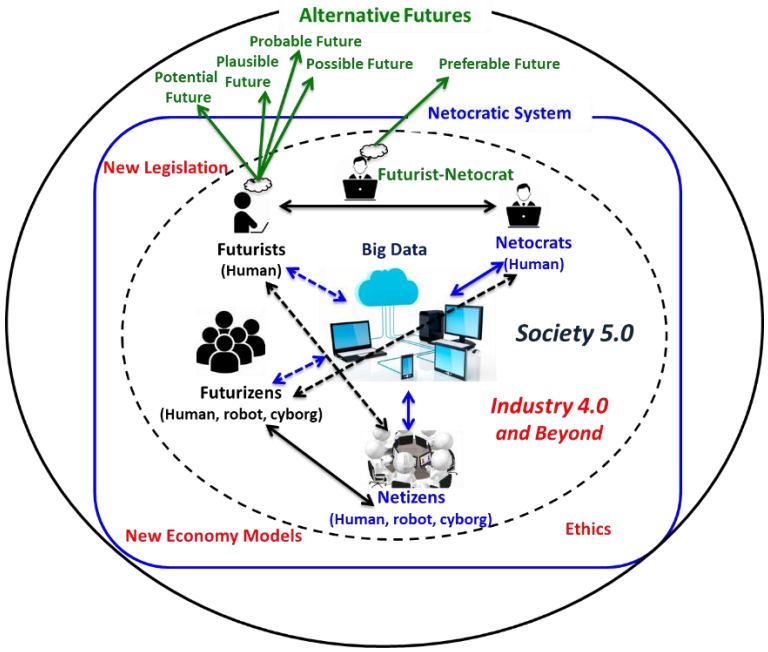


Figure 16: Foresight 6.0 Scheme (Çifci & Yüksel, 2018)

In Figure 16, solid bidirectional black arrows between netocrats and futurists, likewise between futurizens and netizens show direct interaction. Discrete

bidirectional black arrows show a lower probability of interaction between futurists and netizens and between futurizens and netocrats. Netocrats might turn into futurist and netizens might become futurizens. Netocrats, which are network managers, and netizens, which are network users, have strong participation in the network; these relations are shown by solid bidirectional blue arrows. Weaker relation with the network is shown by discrete bidirectional blue arrows.

CHAPTER 4

RESEARCH METHODOLOGY AND DESIGN

4.1 Introduction

Foresight Periscope Model (FPM) by Yüksel and Çifci (2017) was followed in this study. The study was conducted at the national level within Turkey and the application of the FPM metadata is shown in Table 19.

Table 19: FPM's Application for this Study

Future Strategies	Scenarios, strategy planning, and policy recommendations were conducted by expert panels and workshops.	
Methodologies	Primary methods of the study are Delphi survey and focus groups. Other methods are visioning, literature review, brainstorming, trend analysis, survey, expert panel, SWOT, STEEPLE, critical technologies, strategy planning, policy recommendation, and roadmapping.	
Resources	Infrastructural Resources	Internet is the main infrastructure to access papers, data, and participants. ProQuest Database containing 10 digital databases was used as a primary source for white papers.
	Financial Resources	All activities under this study were based on voluntariness. Meetings venues were government-owned facilities.
	Human Resources	Experts from Turkish universities, Turkish Armed Forces, governmental agencies and defense industry companies. Among them, nearly 30 experts conducted panels and workshops while 150 experts from almost all universities in Turkey participated in the surveys.
	Time	16 months.

4.2 Selection of Foresight Methods

Different foresight types require different methods (Loveridge, 1996) and foresight types and methods are too complicated to prepare a concrete prescription which comprises a set of methods for a specific foresight activity.

Porter (2010) suggests considering alternative methods and weighing the advantages and disadvantages of different approaches for a specific foresight case. He argues that it is needed to avoid thinking of foresight as a simple activity that "one size fits all" concept works and claims that, motivation, drivers, scope, locus, title, time horizon, purpose, target users, participation and study duration should be considered to select right methods for a foresight activity. In a particular case, suitable methods must be picked up based on data availability. It is advised to use multiple methods that eliminate each other's disadvantages or weaknesses. Since foresight study outputs must be available on time, resources for a foresight study and the time available also need to be considered for method selection (Porter, 2010).

According to Slaughter (1997), there is no easy answer for selecting foresight methodologies, it depends on the organization's needs and the priorities of the stakeholders and decision makers. He claims that it is a common mistake to assume that a successful foresight is just matter of finding and performing the right methodologies but is actually the most successful when stakeholders have high-quality international resources and are actively immersed in a high-quality futures discourse. Immersion is favorably important that it prevents undermining personal, cultural or organizational factors contributing to the success of the work. He also makes the distinction between "tools" and "methodologies" in that while tools are just simple and modest ways of carrying small scale tasks, methodologies are substantive and encompassing ways to produce significant results.

In this study, various methods in the literature were utilized together with experts from different backgrounds. These methods can be seen in Table 20.

Table 20: Methods Used in this Study

Functions	Methods
Framing	Visioning, Literature Review
Obtaining	Literature and Statistics Review, Workshops, Brainstorming, Focus Group
Reviewing	Trend Analysis, SWOT Analysis, STEEPLE Analysis, Focus Group
Establishing	Delphi, Expert Panel
Synthesizing	Scenario Building, Visioning, Key/Critical Technologies
Illustrating	Roadmapping, Scenarios
Guiding	Strategy Planning, Policy Recommendations, Critical/Key Technologies
Handling	Strategies, Policies
Tracking	*(Tracking step is out of the scope of this study)*

4.3 Main Flow of Activities in the Study

Main activities in this study are as follows:

- Focus group meeting (12 January 2018): Vision study, SWOT analysis, STEEPLE analysis, determining the criteria for weighting cybersecurity technologies.
- Determining cybersecurity technologies by the researcher.
- Prioritization of cybersecurity technologies by experts.
- Creating Delphi questions and statements by the researcher.
- Focus group meeting (4 May 2018): Cybersecurity technology review, finalizing the Delphi questions and statements.
- Prioritization of Delphi statements study with experts.
- Delphi survey (two rounds).

- Turkey's cybersecurity review (departments and courses in the Turkish universities, products and services of Turkish companies) by the researcher.

- Focus group meeting (17 December 2018): Scenario, actions and roadmap workshop.

4.4 First Focus Group Meeting

The first focus group meeting was held in the SSB's facilities with the participation of 17 experts from Turkish Armed Forces, government, academia, and cybersecurity companies. All of the participants of the studies conducted in this thesis are listed in Appendix A. Meeting agenda and flow was as follows:

- Vision study.

- SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis.

- STEEPLE (Social, Technological, Economic, Environmental, Political, Legal, Ethical) analysis.

- Cybersecurity trends survey.

- Determining the weight of criteria for prioritizing cybersecurity technologies to be developed.

4.4.1 Vision Study

In this study, cybersecurity vision of Turkey was created in the following manner:

The participants were divided into 3 groups. Everybody wrote a vision phrase on a post-it and affixed it to the A3 paper in front of them. Then A3 paper was passed to the next person in the group and everyone attached post-it containing vision phrase to the paper. Until all of the ideas were written, the paper with the post-its was shuffled in the group.

Then, spokespersons of each group collected post-its, read them loudly and pasted the similar phrases in the same column on the white-board.

Then, groups gathered next to the white-boards of their own group and put the small sticky voting papers next to the phrases that they liked. Each group formed its own vision statement based on the 5 high-score phrases. These 3 vision statements were combined by the researcher after the study and a single vision statement was formed.

4.4.2 SWOT Analysis

In SWOT analysis, strengths and weaknesses are internal qualities of Turkey where opportunities and threats are external factors that affect the cybersecurity ecosystem. In this study, all items in SWOT were matched with STEEPLE (Social, Technological, Economic, Environmental, Political, Legal, and Ethical) viewpoints. Factors of STEEPLE can be shown in Table 21.

Table 21: Factors of STEEPLE

Social	Population structure; Changes in values and attitudes; Changes in lifestyle; Attitudes and trends in business and leisure; Training conditions; Working environment and conditions; Health situation; Other social factors.
Technological	Diffusion of new technologies; The existence of supported R&D projects; New products and patents; Innovation. Other technological factors.
Economic	GDP; Inflation rate; People's income; Public finance; Unemployment status; Economic situation and stability; Access to credits; Other economic factors.
Environmental	Environment; Green energy; Energy consumption; Handling of waste; Other environmental factors.
Political	Global and national political developments (government, parties, elections, etc.); Tax policies; Labor policies; Trade and industrial policies; Political stability; Other political factors.
Legal	Laws, rules and other regulations; Other legal factors.
Ethical	Sense of responsibility; Respect for values; Other ethical factors.

Items for strengths, weaknesses, opportunities and threats were prepared by the researcher and handed on the participants during the workshop (from Table 22 to Table 25) Participants were requested to write down additional statements and prioritize them all.

Table 22: Strengths of Turkey (Pre-written statements by the researcher)

STEEPLE	Strengths		Priority
Social	Young and entrepreneurial manpower		
	A science and technology community integrated into the international community		
Technological	An industry that is open to the international arena		
Economic	Our country to be among the 20 largest economies in the world		
Environmental	-		
Political	Government's support for cybersecurity		
	The existence of the institutions to realize the strategies (SSB, TÜBITAK, ministries, etc.)		
Legal	Presence of legal infrastructure that protects personal data, ideas and works (Law of Intellectual and Artistic Works and Protection of Personal Data, etc.)		
Ethical	-		
Additional Strengths (Your statements)		STEEPLE?	Priority

Table 23: Weaknesses of Turkey (Pre-written statements by the researcher)

STEEPLE	Weaknesses	Priority
Social	Lack of skilled human resources	
	Lack of cooperation culture	
	Keeping cybersecurity as a secondary issue on the personal and institutional basis	
	Poor cooperation between public, industrial and academic community	
	Institutions' not being aware of the real needs in terms of cybersecurity	

Table 23 (Cont'd)

STEEPLE	Weaknesses	Priority
Technological	Dependency on foreign countries in terms of information technologies (especially in terms of hardware) on which cybersecurity is built	
	The low number of domestic cybersecurity products and functional diversity	
	Many firms focusing on a limited number of specific cybersecurity products and services	
	Lack of research data	
	Failure to implement certification and testing mechanisms	
	Lack of national products and technologies for information systems and cybersecurity	
	Inadequate institutional competencies (organization, infrastructure, personnel, resources) in cybersecurity	
Economic	Lack of scale economy	
Environmental	-	
Political	Failure to be successful in the implementation of cybersecurity strategy and action plans	
	Problems and challenges in education and training	
	Insufficiency of cooperation mechanisms	
Legal	Inadequate legislation to counter international cyber threats and cyber incidents	
Ethical	Personal deficiencies in compliance with the principles for the protection of intellectual and artistic works.	
Additional Weaknesses (Your statements)	STEEPLE?	Priority

Table 24: Opportunities for Turkey (Pre-written statements by the researcher)

STEEPLE	Opportunities	Priority
Social	Cybersecurity needs caused by social, technological, economic, environmental and political factors	
	Increased need for cybersecurity because of increased cyber threats and their complexity	
	Training needs for cybersecurity	
Technological	Due to the nature of cybersecurity, the need for domestic products	
	Lack of institutional establishment of cybersecurity systems	

Table 24 (Cont'd)

STEEPLE	Opportunities	Priority
Economic	The width of internal and external market	
	The willingness of the public and private sector to invest in cybersecurity	
Environmental	-	
Political	Adoption of cybersecurity among elements of national security in many countries around the world, including our country	
Legal	-	
Ethical	-	
Additional Opportunities (Your statements)	STEEPLE?	Priority

Table 25: Threats for Turkey (Pre-written statements by the researcher)

STEEPLE	Threats	Priority
Social	Lack of confidence in domestic products	
	A culture spreading in the society that is eager to make easy money	
Technological	Rapid evolvement of cyber threats	
	Increased number and competence of cyber threat sources	
	Vulnerabilities in software and hardware	
	The spread of technologies based on cloud computing and the dominance of foreign firms in this field	
	Failure to give sufficient importance to the national development of systems due to urgent supply demands	
Economic	Foreign products' domination in most of the market	
	Investments and partnerships of foreign companies in our country	
	International competition	
Environmental	-	
Political	Lack of investment in R&D than required	
	The potential of the geopolitical environment in which our country is located and the instability in the surrounding countries to influence foreign investor	
Additional Threats (Your statements)	STEEPLE?	Priority

4.4.3 STEEPLE Analysis

Social, technological, economic, environmental, political, legal and ethical factors were prepared by the researcher and participants were requested to add new ones and prioritize all during the workshop (from Table 26 to Table 32).

Table 26: Social Factors (Pre-written statements by the researcher)

No	Social Factors	Priority
1	Increase in online education and training activities	
2	Widespread use of social media	
3	Widespread use of the Internet	
4	Widespread use of mobile phones	
5	Widespread use of smart things (home, car, household goods, etc.)	
6	Public services through the digital environment (internet)	
7	The penetration of internet and digital services into every aspect of life (health, shopping, information sharing, etc.)	
8	The penetration of robotic and autonomous systems into social life	
9	Increased emphasis on privacy and security	
10	Increased use and penetration of technology in every area of life	
11	Increase in cybercrime	
No	Your Factors (Please add below)	Priority

Table 27: Technological Factors (Pre-written statements by the researcher)

No	Technological Factors	Priority
1	Diffusion of online services	
2	Expansion of industrial control systems	
3	Expansion of Industry 4.0 concept (cyber-physical systems, big data, artificial intelligence, internet of things, etc.)	
4	Widespread use of global internet access	
5	More complex systems in terms of hardware and software	
6	The spread of robotics and autonomous systems	
7	The proliferation of artificial intelligence, machine learning and methods of deep learning	
8	Widespread transition to cloud computing	
9	Widespread use of multi-factor authentication mechanisms	
10	Increase in importance of technologies to protect data security	

Table 27 (Cont'd)

No	Technological Factors	Priority
11	More widespread behavior-based security mechanisms than signature-based security mechanisms	
12	Widespread use of smart things (home, car, household goods, etc.)	
13	Widespread use of crypto coins	
14	Widespread use of mobile and wireless systems	
15	Widespread use of human-machine interfaces	
16	Widespread use of wearable smart objects	
17	Faster technological developments and transformations	
18	The impact of the private sector on technological developments in comparison with the state	
19	Increased technological interdependence and interaction between countries	
No	Your Factors (Please add below)	Priority

Table 28: Economic Factors (Pre-written statements by the researcher)

No	Economic Factors	Priority
1	Increased purchasing power in our country and in the world	
2	The decrease in prices of electronic and online systems	
3	Facilitation of access to international markets due to global economic policies	
4	Increased demand for online systems	
5	Globalization of financial resources	
6	Inquire about the defense expenditures in the Western world	
No	Your Factors (Please add below)	Priority

Table 29: Environmental Factors (Pre-written statements by the researcher)

No	Environmental Factors	Priority
1	Widespread use of renewable energy	
2	Increase in environmental awareness and the importance of the environment	
No	Your Factors (Please add below)	Priority

Table 30: Political Factors (Pre-written statements by the researcher)

No	Political Factors	Priority
1	The transition of countries to e-government and digitization	
2	Increased state support for electronic and online technologies	
3	Increased state support for information technologies and cybersecurity	
4	Increasing the state's efforts and incentives to protect data (technological, personal, etc.)	
5	Use of cyber attacks as an element of power among states	
6	More complex cyber espionage actions of states	
7	Adoption of cybersecurity as part of national security by states	
8	Introducing restrictions on the sale of advanced cybersecurity products and technologies	
Priority	Your Factors (Please add below)	Priority

Table 31: Legal Factors (Pre-written statements by the researcher)

No	Legal Factors	Priority
1	Taking steps to protect intellectual property rights	
2	Establishment and dissemination of national and international legislation on cybercrime	
3	New arrangements in nations (e.g. USA) and international communities (e.g. European Union) for the compliance of systems with personal data to the security criteria	
No	Your Factors (Please add below)	Priority

Table 32: Ethical Factors (Pre-written statements by the researcher)

No	Ethical Factors	Priority
1	….	
No	Your Factors (Please add below)	Priority

4.4.4 Cybersecurity Trends Survey

A cybersecurity survey was conducted with the experts in the workshop. The survey contained the six questions related to cybersecurity, cyber attack sources, cyber attack targets, types of cyber attacks, target sectors and supplementary technologies connected with cybersecurity. The survey is provided in Appendix F.

4.4.5 Technology Selection Criteria

For the selection of critical cybersecurity technology groups and technologies, three criteria were used in the study.

The first criterion is “Meeting National Security Needs”. Its objective is to select the important technologies that are mandatory and critical and which include internationally transfer-controlled technologies, within the scope of the defense technologies, and which meet our national security needs. Scope of the criterion:

- The technology that should be national (even if it is supplied from abroad, the technologies that are inconvenient because of security risks and must be developed domestically).

- Critical technology (technologies that are not available from abroad or that may endanger the operation by providing them from abroad for a variety of reasons and therefore are required to be developed domestically).

- Technology that directly contributes to our national security (technologies to be used in security tools, tools, and systems).

- Technology that indirectly contributes to our national security (technologies to be used in systems to be used for security reasons).

The second criterion is “World-Class Competitiveness, Collaboration or Mutual Dependence”. Its objective is to select the technologies that determine the tendency of technological development or the technologies that are at the beginning of the life cycle. Scope:

- Dual usable technology (technology areas in which capabilities gained in the defense industry can be transferred in a similar way to civilian areas).

- Developing or emerging technology.

- Technology that contributes significantly to the economy of the country.

The last criterion is “Supporting the Development of the National Science, Technology and Innovation (STI) Infrastructure”. The aim is to highlight the technologies that can support the STI infrastructure of the country. Scope:

- Technology contributing to the development of human resources.

- Technology contributing to the creation of infrastructure (research centers, networks, laboratories, etc.) for science, technology, and innovation.

- Technology that can be used in other technological areas.

Comparison and weighing technology selection criteria table (Table 33) was filled out by 22 cybersecurity experts.

Table 33: Technology Selection Criteria Weighting Table

Compare the criteria according to the explanations below (Whichever is more important put "X" to the side where it is. If they are equal, put "X" under "Equal.") Pay attention not to contradict with yourself										
	Extremely important	Too much important	Very important	A bit more important	Equal	A bit more important	Very important	Too much important	Extremely important	
Meeting National Security Needs										World-Class Competitiveness, Collaboration or Mutual Dependence
Meeting National Security Needs										Supporting the Development of the National Science, Technology and Innovation Infrastructure
World-Class Competitiveness, Collaboration or Mutual Dependence										Supporting the Development of the National Science, Technology and Innovation Infrastructure

The weights of the three criteria were calculated by using the Analytical Hierarchical Process (AHP) by considering the consistency of the inputs. AHP is a method developed by Saaty (1980) to evaluate multiple criteria and alternatives.

4.5 Key/Critical Technologies Study

In this study, cybersecurity technology list and technology taxonomy were created using mainly technology taxonomy of Turkish Presidency of Defense Industries (Savunma Sanayii Başkanlığı -SSB), cybersecurity technology and product taxonomy of the Scientific and Technological Research Council of Turkey (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu -TÜBİTAK) and cybersecurity product list of international companies.

TÜBİTAK's taxonomy groups the 106 cybersecurity technologies under six main categories (TÜBİTAK, 2017) first two of which were benefited in the study to prepare an extensive list:

(1) According to the Areas of Use: Network Security, Endpoint Detection and Protection, Identity and Access Management, Messaging and Communication Security, Data Security, Cloud Computing Security, Security Analytics and Cyber Intelligence, Cybersecurity Operations, Event Management and Forensics, Cybersecurity Risk and Compliance Management, Application and Internet Security, Mobile Devices Security, Industrial Control (SCADA) Systems and IoT Security.

(2) According to Technologies Integrated Into: Cloud Computing Security, IoT Security, Big Data Security, Operating Systems and Container Security, Virtualization Security, Mobile Devices Security, Wearable Technology Security, Database Security, Hardware and Firmware Security, Cryptology.

(3) Based on the Organization Types: Personal, Enterprise Infrastructures, Industrial Systems, Small and Medium-Sized Organizations.

(4) According to Maturity Levels: In Laboratory, Emerging, Semi-Mature, Obsolete, Mature.

(5) According to Threats: Phishing, Ransomware, Denial of Service, Advanced Persistent Threats, Trojan Horse, Man in the Middle, Rootkits, Malware, Keylogger, Misconfiguration.

(6) Based on Installation Methods: Server/Client, Hardware/Software Commercial off the Shelf, Virtual Server, Cloud.

SSB's technology taxonomy is based on the European Defense Agency's (EDA) and covers not only cybersecurity but also all defense industry related technologies (SSB, 2017). The taxonomy divides the technologies into three main groups:

(1) Group A (Underpinning Technologies): There are total 13 technology sub-groups under this main group and "A13" is the "Cybersecurity Operations" contains four sub-groups: Event Management and Intervention, Laboratory Services, Energy Systems Security and Attack.

(2) Group B (Systems-related Technologies): This group has 14 technology sub-groups and "B14" is the "Cybersecurity Solutions" which has following 23 technologies therein: Next Generation Firewall, Web Application Firewall, Security Information and Event Management (SIEM), Cloud Computing Systems, Web Page Monitoring Systems, Data Leakage Prevention Software, Honeypots, Cyber Drill Systems, Secure Communications Software Real Time Event Monitoring, Cyber Threat Intelligence, Malware Analysis, Penetration Tests, Web Application Vulnerability Assessment, Web Application Code Analysis, Operating Systems Vulnerability Assessment, SCADA Systems Vulnerability Assessment, Network Vulnerability Analysis, Database Vulnerability Analysis, Configuration Control, Cybersecurity Operation Center, Consultancy and Red Team Services.

(3) Group C (Systems/Products): There are 8 sub-groups under this group but cybersecurity related group does not exist.

In this study, a new cybersecurity technology taxonomy was created with the aim of having the most extensive and inclusive list under proper categories that can address the academic and industrial cybersecurity technology and product lists. This taxonomy matches with the SSB's (so the EDA's) grouping logic and covers the TÜBİTAK's technology list with additional 75 technologies.

In Table 34, a snapshot of the taxonomy is depicted and the full list of 169 technologies is in Appendix B. As seen in the table, every technology is put under one or more technology groups under 15 "Group B" (system-related technologies) and 6 "Group C" (systems/products) technologies.

Table 34: A Snapshot of Cybersecurity Technology Taxonomy of the Study

	Group A	Group B															Group C					
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
No		Network Security	Endpoint Detection and Protection	Identity and Access Management (IAM)	Messaging and Communication Security	Data Security	Cloud Computing Security	Application Security	Internet Security	Mobile Devices Security	Industrial Control (SCADA) Systems Security	Internet of Things (IoT) Security	Operating Systems and Container Security	Cybersecurity for Autonomous and Smart Platforms	Hardware Security	Firmware Security	Cybersecurity Analytics	Cyber Intelligence	Cybersecurity Operations	Cybersecurity Event Management	Cyber Forensics	Cybersecurity Risk and Compliance Management
1	Network Security Management	X																				
2	Network Access Control	X																				
3	Software-Defined Security	X																				
169	Risk Management																					X

List of technology groups and technologies were sent to experts by e-mail after the first focus group meeting to the participants and to other experts who were not members of the working group (total 22 experts). Participants requested to weight the cyber technology groups and technologies according to Table 35.

Table 35: Technology Weighting Scores

Score	Denotation	Score	Denotation
0-10	Unnecessary	51-70	Important
11-30	Not important	71-90	Very important
31-50	A bit important	91-100	Extremely important

21 cybersecurity technology groups and 169 technologies were weighted against the three criteria *(Meeting national security needs; supporting the development of the national science, technology and innovation infrastructure; world-class competitiveness, collaboration or mutual dependence).*

Experts were also requested to add further cybersecurity technologies that are not covered in the current list. Table 36 shows the snapshot of the list what were sent to experts.

Table 36: A Snapshot of Cybersecurity Technology Weighting List

No	Technology Group / Technology	Your expert level in this topic (3: Good; 2: Medium; 1: Poor)	Meeting National Security Needs	World-Class Competitiveness, Collaboration or Mutual Dependence	Supporting the Development of the National STI Infrastructure
Cyber Security Technology Groups					
1	Network Security				
21	Cybersecurity Risks and Compliance Management				
Cyber Security Technologies					
1	Network Security Management				
169	Risk Management				
Additional Technologies (Please add below)					
1					
2					
3					
4					
5					

4.5.1 Technology Prioritization

In the study, the level of expertise was given weight in order to increase the effect of experts' scores in technologies in which they have sufficient knowledge. Weights of expertise levels for cyber technologies were determined by researcher together with three experts (Table 37).

Table 37: Weights of Expertise Levels

Expertise Level	Weight
Level=1 (Poor)	0,075460
Level=2 (Medium)	0,333821
Level=3 (Good)	0,590719

Expertise level 1 and 2 were deemed as “non-expert”, their scores were combined under the “non-expert” category, and technology scores were calculated by using expertise level weights.

In Table 38, number of experts, number of non-experts, orders and scores according to experts and non-experts, and finally orders and scores of the composite results are shown in a snapshot with only top and bottom five technologies have shown here while the full list is in Appendix C.

Table 38: Snapshot of Technology Ranks and Scores

Rank	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Experts' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
1	Quantum Cryptography	3	19	89,44	5	86,60	3	2	87,12
2	Quantum-Safe Cryptographic Algorithms	4	18	92,79	2	85,02	4	2	86,91
3	Cybersecurity Training and Exercise Systems	15	6	84,54	26	82,10	7	19	84,01
4	Cyber Offense	12	9	87,64	11	75,37	42	31	83,45
5	Cyber-Physical Systems (CPS) Security	6	15	90,93	3	78,92	22	19	83,32
…	……	..	..	..	..	..	..	..	..
165	System for Cross-domain Identity Management (SCIM)	3	18	77,48	86	52,64	167	81	57,46
166	Mobile Single Sign-On	9	12	52,55	168	59,23	160	8	55,76
167	Mobile-Apt User Authentication Methods	2	19	61,00	163	53,43	166	3	54,43
168	Phone-as-a-Token Authentication Methods	4	17	62,10	161	51,78	168	7	54,39
169	Externalized Authorization Management	1	20	57,04	165	50,69	169	4	51,12

4.6 Creating Delphi Statements

Delphi statements were created by the researcher based on the technology scores given by the participants. The scoring of both experts and non-experts was taken into consideration and technologies that met the following criteria were selected:

- Top 50 technologies in experts' **or** non-experts' scores.
- Top 100 technologies for both experts' **and** non-experts' scores.

Delphi statements were written by the researcher in a way to cover selected top-scored technologies. Similar technologies were grouped to address as many technologies as possible. In the second focus group, participants were urged to cover all of the 169 technologies that they think a capability shall be attained based on those technologies.

Technology and Delphi matching is shown in Table 39. Total 37 Delphi statements created by the researcher are in Appendix D.

Table 39: Researcher's Delphi Statements and Matching Technologies

Technology	Order (Expert)	Order (Non-Expert)	Delphi No
Microelectronics Security Tests	1	33	1
Embedded Software and Systems Security	63	19	
Quantum-Safe Cryptographic Algorithms	2	4	2
Quantum Cryptography	5	3	
Encryption Algorithms	7	53	
Encryption Technologies	8	74	
Fully Homomorphic Encryption	21	84	
Cryptographic Chips and Modules	19	21	
Secure Texting	142	25	
Cyber-Physical Systems (CPS) Security	3	22	3
Operational Technology Security	25	71	
Lightweight Cryptography	4	76	4
Secure Aviation Protocols and Architecture	6	29	5
Wearable Technologies Security	9	121	6
Application Shielding	10	102	7
Runtime Application Self-Protection (RASP)	22	83	

Table 39 (Cont'd)

Technology	Order (Expert)	Order (Non-Expert)	Delphi No
Cyber Offense	11	42	8
New Generation (4G, 5G, etc.) Wireless Security	12	36	9
Mobile Voice Protection	104	47	
Wireless Devices Security	17	122	
Mobile Virtual Private Networks	43	124	
Virtual Trusted Platform Module (vTPM)	13	89	10
Hardware Trusted Platform Module (TPM)	18	49	
Hardware Roots of Trust	55	90	
Privacy in IoT	14	140	11
Secure IoT Routing Protocols	20	50	
IoT Authentication	29	155	
Privacy Management Technologies and Tools	16	67	
Fraud Detection and Transaction Security	65	86	
Blockchain for Identity & Access Management	15	20	12
New Generation User and Object Identification and Access Control Technologies	38	158	
Blockchain Security	23	48	
Blockchain for Data Security	24	30	
Cybersecurity Training and Exercise Systems	26	7	13
Cybersecurity Testbed	44	31	
Hypervisor Security	27	52	14
Virtualization Security	34	108	
Data Farming based Threat Analytics	28	58	15
Threat Intelligence Platforms	49	114	
Crowdsourced Threat Intelligence and Protection	76	32	
Threat Analytics	82	23	
Cyber Analytics and Decision Support Systems	73	10	
Big Data Security	30	38	16
Format Preserving Encryption	37	69	
Database Security (Audit, Protection, Encryption)	84	41	
Pervasive Trust Services (Distributed Trust, Blockchain-like Architectures, etc.)	31	77	17
Distributed Trust Mechanisms	42	60	
Privacy-Preserving Machine Learning	32	59	18
Interoperable Storage Encryption	33	110	19
Trusted Portable Storage Security	47	118	
Configuration Auditing	35	87	20
Mobile Vulnerability Management Tools	39	144	21
Vulnerability Management	85	44	
Cybersecurity Assessment and Evaluation	40	51	
Penetration Testing	41	75	22
Network Penetration Testing Tools	99	63	

Table 39 (Cont'd)

Technology	Order (Expert)	Order (Non-Expert)	Delphi No
Software-Defined Security	45	88	23
Cyber Forensics (stand-alone, mobile, disk, memory)	48	16	24
Dynamic Network/Computer Forensics	78	26	
Network-based Cyber Forensics	110	13	
Security Information and Event Management (SIEM)	118	6	25
Incident Response and Management	50	40	
Cyber Automated Response	56	12	
Model-Driven Cyber Defense	62	35	
Cybersecurity Sense-Making	136	14	
Advanced Persistent Threat (APT) Protection	60	1	26
Network Sandboxing	138	9	
Application Control	154	37	
DDoS Defense	70	18	27
Non-Signature based Malware Analysis	74	2	28
Malware Defense	124	8	
Cyber Attack Modeling and Attack Generation	80	28	29
Network IPS (Intrusion Prevention System)	111	11	30
Host-based Intrusion Prevention System (HIPS)	157	17	
Next-Generation IPS	92	5	
Network Traffic Analysis	127	34	
Deep Packet Analyzing	67	39	
Boundary Defense (Perimeter Security)	161	24	
Network Security Policy Management	156	46	
Next-Generation Firewalls	72	27	
Content-Aware DLP for Email	112	45	31
Secure Web Gateway	155	15	32
Automated Reverse Engineering	51	64	33
Deception Technology (e.g. honeypots)	59	72	34
IaaS (Infrastructure as a Service) Container Encryption	66	82	35
Cloud Access Security Brokers	91	96	
Biometric Authentication Methods	77	73	36
Risk Management (IT, Digital, Vendor, Operational, Industrial, Social)	95	78	37

4.7 Second Focus Group Meeting

The second focus group meeting was held again in the SSB's facilities with the participation of 14 experts from Turkish Armed Forces, government, academia, and cybersecurity companies. Three more experts participated in the activities after the meeting by filling the necessary forms using the internet.

This meeting was dedicated to the Delphi study. Delphi statements and questions were listed as shown in a snapshot in Table 40. Delphi questions were categorized into four groups:

(1) Expert Level: Expert; Non-Expert.

(2) Importance for Turkey: Contribution to National Security; Contribution to Economy.

(3) Implementation Timeframe: 2019-2023; 2024-2029; 2030-2035; 2036-2040; 2040+.

(4) Implementation Method: R&D Investment; Technology Transfer; Foreign Company Cooperation; COTS or Open Source Use.

Table 40: Snapshot of the Delphi Statements and Questions

No	Technology No	Delphi Statement	Expert Level		Importance for Turkey (Enter score 1 to 5) 1: Not important 5: Very high		Implementation Timeframe					Implementation Method (Select up to 2 of them)			
			Expert	Non-Expert	Contribution to National Security	Contribution to Economy	2019-2023	2024-2029	2030-2035	2036-2040	2040+	R&D Investment	Technology Transfer	Foreign Company Cooperation	COTS or Open Source Use
1	18, 26	The technological level has been reached to protect the embedded systems against cyber attacks and to perform security tests of all kinds of electronic circuits (chips, micro-electronic circuits, etc.).													
2	1, 2, 6, 9, 10 57, 61	Crypto algorithms, technology and modules (software, hardware) that cannot be cracked by super computers and quantum computers (quantum safe) have been developed and started to be used in operational environments.													

In the workshop, participants reviewed the researcher's 37 Delphi statements and they were requested to add theirs. During the workshop, participants did not fill out the Delphi questions for statements but just reviewed. They added 54 additional Delphi statements. Participants' statements and the final set of statements are in Appendix D.

4.8 Prioritization of Delphi Statements Study with Experts

Delphi statements that are the outcome of second focus group meeting were sent to 16 experts, including the ones participated in the second focus group meeting, through e-mail and they answered the questions per statements. Researcher's 37 statements and 10 statements chosen from the focus group meeting (total 47 statements) were sent to 16 experts to get their assessments. Prioritization of Delphi statements was carried out in two rounds.

As shown in the snapshot in Table 41, the second round of prioritization Delphi list contained the previous scores and experts were requested to reassess the statements based on the first round's scores.

Table 41: Snapshot of Second Delphi Round with Focus Group

No	Delphi Statement	Expert Level		Importance for Turkey (Enter score 1 to 5) 1: Not important 5: Very high		Implementation Timeframe					Implementation Method (Select up to 2 of them)			
		Expert	Non-Expert	Contribution to National Security	Contribution to Economy	2019-2023	2024-2029	2030-2035	2036-2040	2040+	R&D Investment	Technology Transfer	Foreign Company Cooperation	COTS or Open Source Use
1	The technological level has been reached to protect the embedded systems against cyber attacks and to perform security tests of all kinds of electronic circuits (chips, micro-electronic circuits, etc.).	5	8	4,85	3,69	0	2	9	2	0	12	1	11	1
	Your assessment in the first round													
	Your current assessment													
2	Crypto algorithms, technology and modules (software, hardware) that cannot be cracked by super computers and quantum computers (quantum safe) have been developed and started to be used in operational environments.	2	11	4,31	3,38	0	0	3	9	1	13	12	1	0
	Your assessment in the first round													
	Your current assessment													

Experts' weight was 0.6 while non-experts' was 0.4 and weight of contribution to national security was 0.6 while the weight of contribution to the economy was 0.4.

After the focus group's assessments, 25 statements were chosen (in Table 42, the cells with green background color) for the Delphi survey. For selection, top scored statements or more extensive scoped statements (e.g. D-14 in which 31st order and D-12 in which 36th order) were chosen by the researcher. Composite score was calculated by adding the 60% of security and 40% of the economy.

Table 42: Chosen Delphi Statements for Delphi Survey

Order	Delphi No	Contribution to Security	Contribution to Economy	Composite Score
1	D-3	4,71	4,43	4,60
2	D-15	4,95	3,75	4,47
3	D-5	4,94	3,59	4,40
4	D-1	4,79	3,74	4,37
5	D-8	5,00	3,23	4,29
6	D-27	4,44	3,95	4,24
7	D-9	4,06	4,51	4,24
8	D-29	4,50	3,84	4,24
9	D-26	4,36	4,03	4,23
10	D-28	4,13	4,29	4,19
11	D-30	3,92	4,44	4,13
12	D-23	4,08	4,13	4,10
13	D-39	4,55	3,42	4,10
14	D-16	3,89	4,37	4,08
15	D-42	4,45	3,53	4,08
16	D-31	4,10	3,97	4,05
17	D-21	3,98	4,05	4,01
18	D-25	4,21	3,67	3,99
19	D-2	4,42	3,33	3,99
20	D-11	3,68	4,42	3,98
21	D-22	4,32	3,46	3,98
22	D-44	4,41	3,29	3,96
23	D-47	3,84	4,06	3,93
24	D-4	3,94	3,86	3,91
25	D-35	3,76	4,08	3,89

Table 42 (Cont'd)

Order	Delphi No	Contribution to Security	Contribution to Economy	Composite Score
26	D-13	3,85	3,92	3,88
27	D-32	3,92	3,77	3,86
28	D-38	3,97	3,65	3,84
29	D-7	4,05	3,51	3,84
30	D-17	3,86	3,75	3,82
31	D-14	3,49	4,26	3,79
32	D-34	4,05	3,27	3,74
33	D-24	3,74	3,66	3,71
34	D-10	3,55	3,82	3,65
35	D-36	3,36	4,03	3,63
36	D-12	3,59	3,68	3,63
37	D-20	3,79	3,33	3,61
38	D-46	3,68	3,44	3,58
39	D-6	3,18	4,12	3,56
40	D-37	3,82	3,08	3,52
41	D-41	3,83	3,00	3,50
42	D-33	3,47	3,50	3,48
43	D-19	3,51	3,27	3,42
44	D-40	3,69	2,89	3,37
45	D-45	3,51	3,12	3,36
46	D-18	3,19	3,06	3,14
47	D-43	2,81	2,50	2,69

4.9 Delphi Survey

In order to reach as many as participants for the survey, e-mail addresses of faculty members of computer engineering departments in Turkey's universities were collected by researcher through official web sites of the universities.

Additionally, the researcher collected business cards from cybersecurity experts during cybersecurity conferences and events in Turkey within the thesis timeframe. Apart from these, experts and friends who were informed about the study provided new participants' contact addresses. Total about 1,900 participants were found and reached for the survey.

4.9.1 First Round

The first round of Delphi survey was conducted between 17 July and 12 August 2018. Standard e-mail messages were sent to participants to urge them to respond.

The message that is sent to participant is given in Appendix E in both Turkish and English languages.

Delphi survey was prepared in Google Forms platform. Participants accessed the forms through the link provided within e-mail messages. The forms are given in Appendix F.

General questions and top-scored 25 Delphi statements were included in the survey form. These Delphi statements are the capabilities that Turkey has to have to reach the desired cybersecurity vision and goals.

General questions in the first round:

(1) Your e-mail address: *(e-mail addresses were used to keep the record of participants)*

(2) Your Education: a) Associate degree; b) Bachelor degree; c) MS degree; d) Ph.D. degree; e) Postdoctoral degree

(3) Your cybersecurity experience: a) 0-5 years; b) 6-10 years; c) 11-15 years; d) 16-20 years; e) Over 21 years

(4) Your sector: a) Academia; b) Turkish Armed Forces; c) Government; d) Private Sector; e) Non-Governmental Organizations

Total of 150 people provided the answers. Participants' experience and education levels per sector are given in Table 43, Figure 17, Table 44 and Figure 18. It can be seen that more than half of the participants (78 people) are from academia, most of the participants (95 people) have less than 5 years' experience within cybersecurity field and most of the participants (48) have Master of Science (MS) degree.

Table 43: Participants' Experience per Sector (Round-1)

Sector	0-5 years	11-15 years	16-20 years	21+ years	6-10 years	Total
Academia	55	2	6	3	12	78
Government	7	2	0	0	3	12
Private Sector	17	4	6	2	5	34
Turkish Armed Forces	16	1	2		7	26
Total	95	9	14	5	27	150

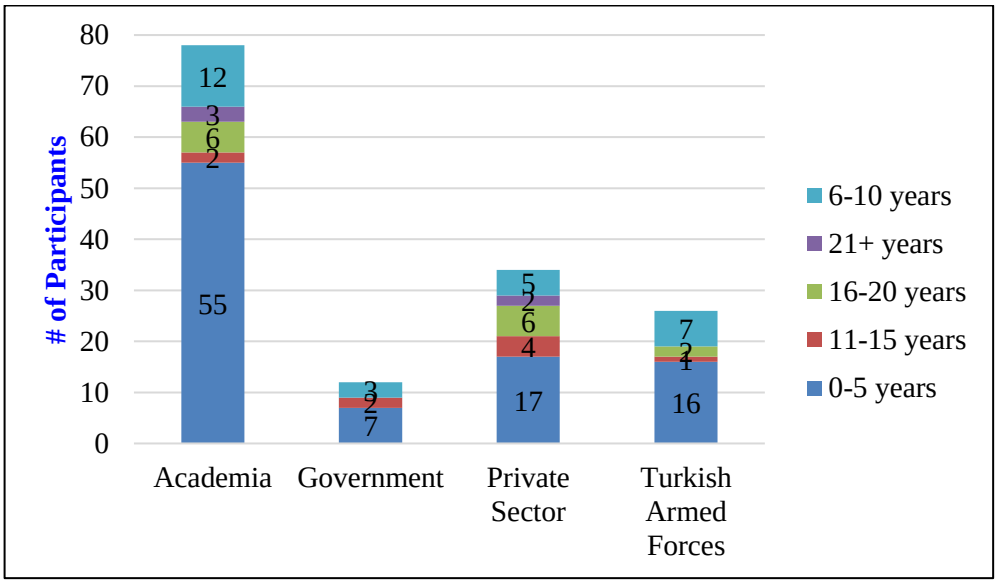


Figure 17: Participants' Experience per Sector (Round-1)

Table 44: Participants' Education Levels per Sector (Round-1)

Sector	Bachelor of Science (BS)	Master of Science (MS)	PhD	Post-doc	Total
Academia	6	18	32	22	78
Government	4	7	1	0	12
Private Sector	14	15	4	1	34
Turkish Armed Forces	15	8	2	1	26
Total	39	48	39	24	150

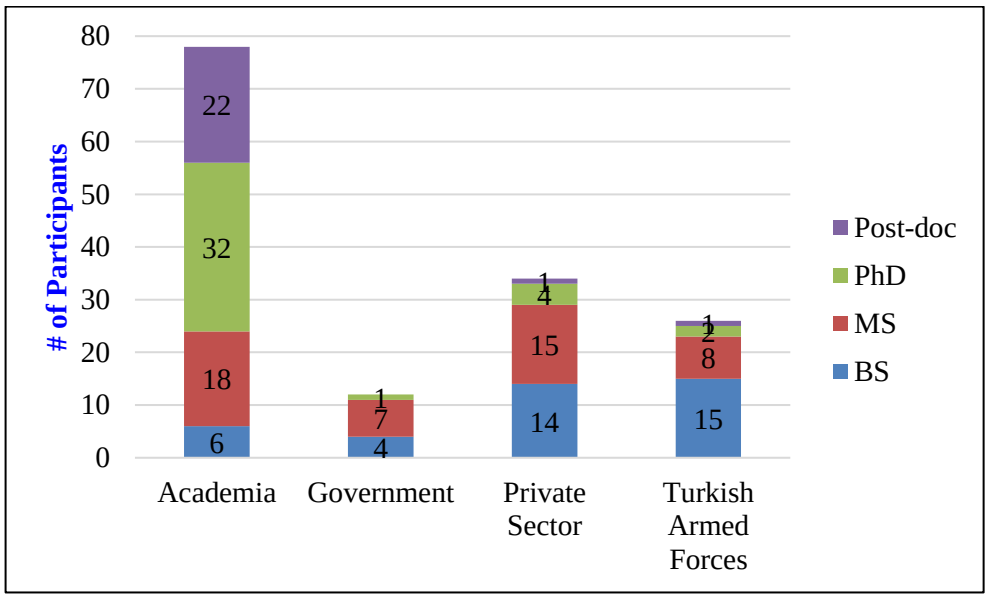


Figure 18: Participants' Education Levels per Sector (Round-1)

4.9.2 Second Round

The second round of Delphi survey was conducted with the same participants between 28 August and 26 September 2018. Total 91 participants out of 150 responded to the second round of the survey.

The second round of Delphi survey was also prepared in Google Forms platform. Statistics based on the answers of the first round in graphics were provided per Delphi statement as shown in Appendix G. Additionally, individual's previous answers were sent to participants by exploiting Google Forms' utilities through a script. Part of the source code of the script is provided in Appendix F.

Participants' education and experience levels per sector are given in Table 45, Figure 19, Table 46 and Figure 20. It can be seen that most of the participants (49 people) are from academia, most of the participants (56 people) have less than 5 years' experience within cybersecurity field and most of the participants (34) have Master of Science (MS) degree.

Table 45: Participants' Education Levels per Sector (Round-2)

Sector	Bachelor of Science (BS)	Master of Science (MS)	PhD	Post-doc	Total
Academia	3	14	19	13	49
Government	2	6	0	0	8
Private Sector	6	10	2	1	19
Turkish Armed Forces	8	4	2	1	15
Total	19	34	23	15	91

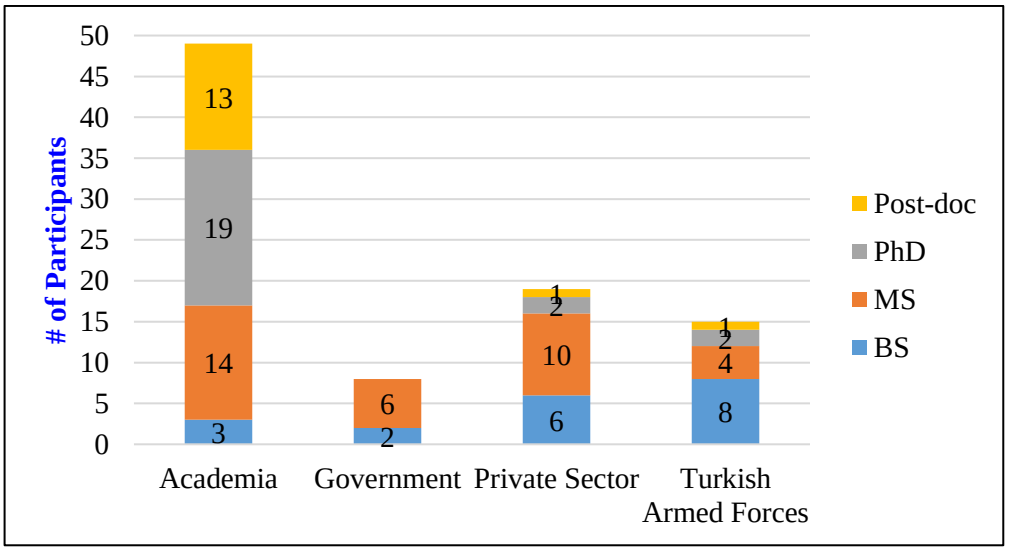


Figure 19: Participants' Education Levels per Sector (Round-2)

Table 46: Participants' Experience per Sector (Round-2)

Sector	0-5 years	6-10 years	11-15 years	16-20 years	21+ years	Total
Academia	35	9	1	3	1	49
Government	6	0	2	0	0	8
Private Sector	7	3	3	5	1	19
Turkish Armed Forces	8	6	1	0	0	15
Total	56	18	7	8	2	91

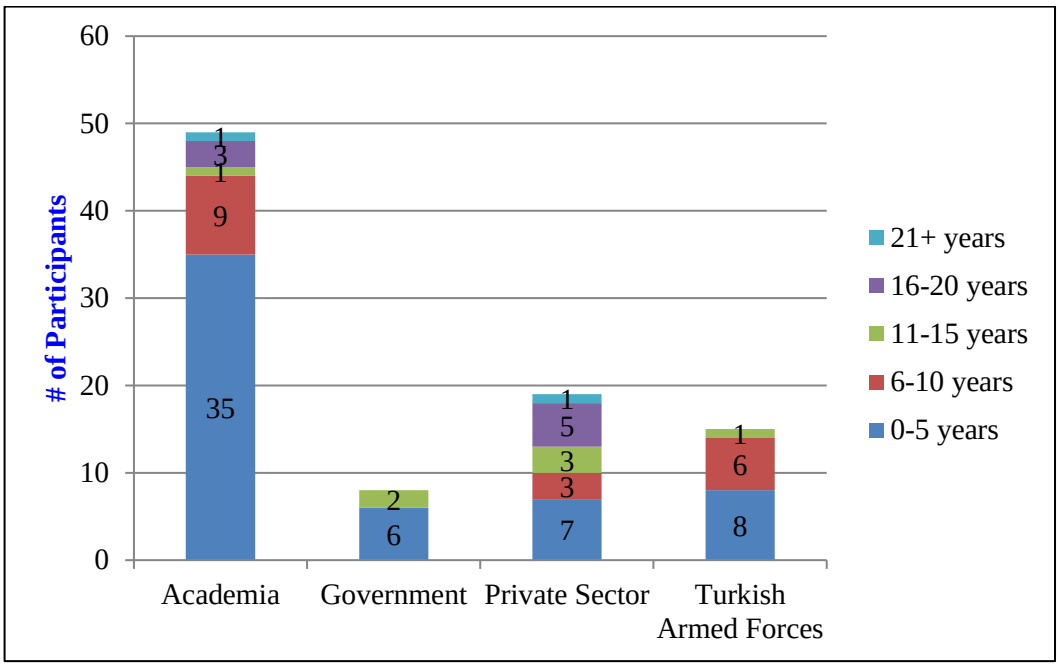


Figure 20: Participants' Experience per Sector (Round-2)

4.10 Scenario and Action Workshop

Scenario and action workshop was conducted with five experts on 17 December 2018. Steps of scenario workshop are as follows:

1) Identify the key drivers [major trends that are out of our control, STEEPLE (social, technological, economic, environmental, political, legal, and ethical) factors that are influencing the scenarios, SWOT (strengths, weaknesses, opportunities, trends) factors, etc.].

2) Identify uncertainties and impacts of key drivers.

3) Identify signposts (metrics or conditions that show the certain scenario path is unfolding).

4) Develop scenarios.

4.10.1 Key Drivers and Major Uncertainties

Scenarios are not build based on known or predictable trends but build on uncertainties, which are driving forces that affect future developments (WikiEducator, 2018b).

Uncertainties are major forces among key drivers, which have an impact on the current and future developments, are used as the foundations for creating foresight scenarios (WikiEducator, 2018b). In the scenario workshop, Impact-Uncertainty Matrix was exploited in order to determine the scenario drivers (Figure 21). The issues having high uncertainty and high impact (top-right cell of the matrix) are the candidates for the scenario drivers.

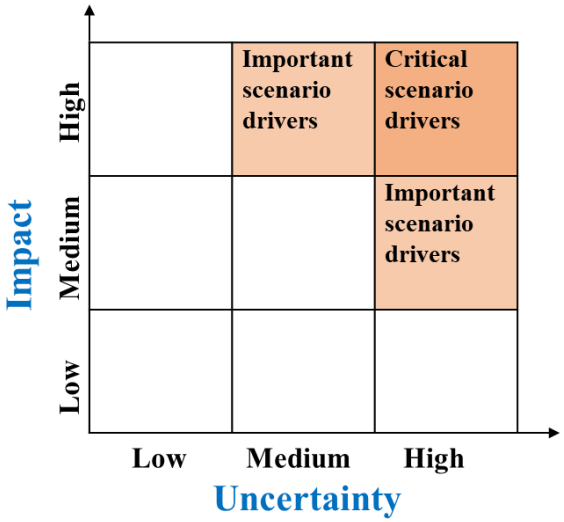


Figure 21: Impact-Uncertainty Matrix

4.10.2 Signposts

Signposts are indications or signals that a particular scenario is happening (Schwartz, 1991). These are helpful to determine which precautions and actions should be taken in order to attain the strategy defined in the scenario. Signposts provide early warning of the events that will occur in the future (Pherson, 2015).

4.10.3 Scenarios

Scenario is defined by Godet and Roubelat (1996) as a representation of future events that allows taking necessary actions for a future situation. A scenario is not just a prediction of a future or reality but a way to define the future to clarify present actions in the light of possible futures (Durance & Godet, 2010).

There are various approaches to scenario planning in the literature such as normative and explorative scenarios. Normative scenarios are goal-directed that are created from the snapshots of the futures ranging from desirable to feared ones while exploratory scenarios are concerned with trends and their possible reflections in the future (Amer, Daim, & Jetter, 2013).

Scenarios can be constructed on the levels of the driving forces that affect the future with their uncertainty and impact degree (WikiEducator, 2018a).

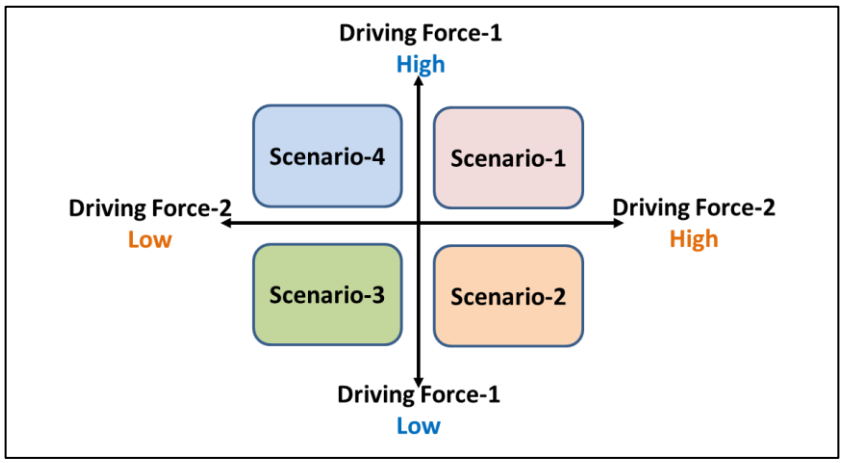


Figure 22: Driving Force Axes and Scenarios

In the workshop, two major driving forces (Driving Force-1: Commitment of Turkey; Driving Force-2: Global security and stability) were created as in Figure 22 as the axes of four different scenarios. Scenario details are given in the Findings and Analysis section of this document.

CHAPTER 5

FINDINGS AND ANALYSIS

5.1 Results of Vision Study

Vision study was carried out in the first focus group meeting by three groups formed during the workshop. 32 statements didn't get any vote from their own group members are shown in Table 47.

Table 47: Statements That Didn't Get Vote From Own Groups

international cooperation	advanced versions of Industry 4.0 applications	recruited workforce
private sector based	protected against external threats	trusted
totally autonomous	Conformant to international standards	fast
training and certification	3% of qualified workforce working in security area	privacy based
big data governance	in cooperation with other countries	awareness
netocratic rules are set	security of information resources	branding
reversed brain drain	mechanisms to provide security to Europe's IoT network	cyber rights
internet security in space	authority in cybersecurity market	secret
increasing R&D incentives	cybersecurity excellence center owner	Internet of Things
university-industry cooperation	80% of indigenous product development	quantum technologies
exporter of penetration test tools		artificial intelligence

Vision phrases of the groups and the number of occurrences of phrases can be shown in the following figures (Figure 23, Figure 24 and Figure 25).

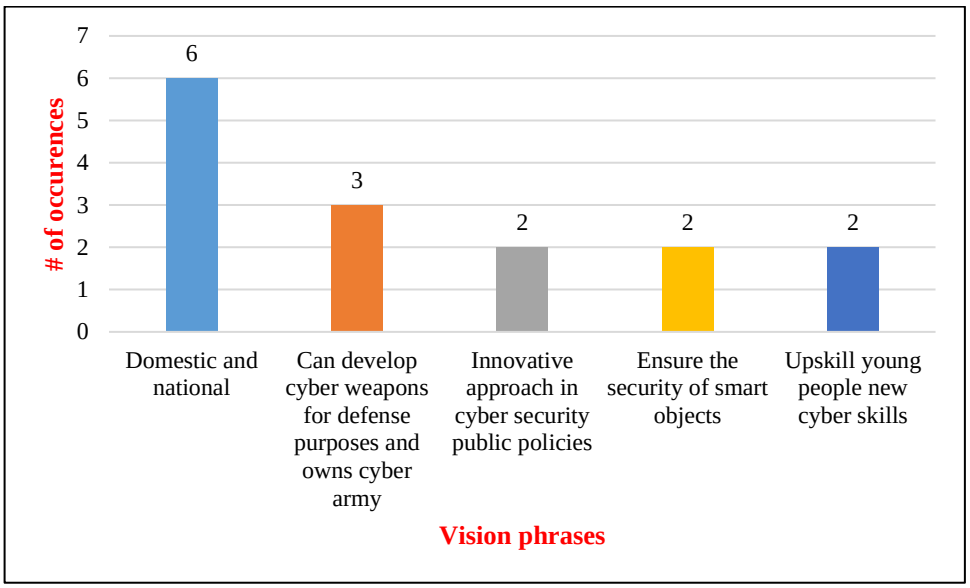


Figure 23: Vision Phrases and Number of Occurrences (Group-1)

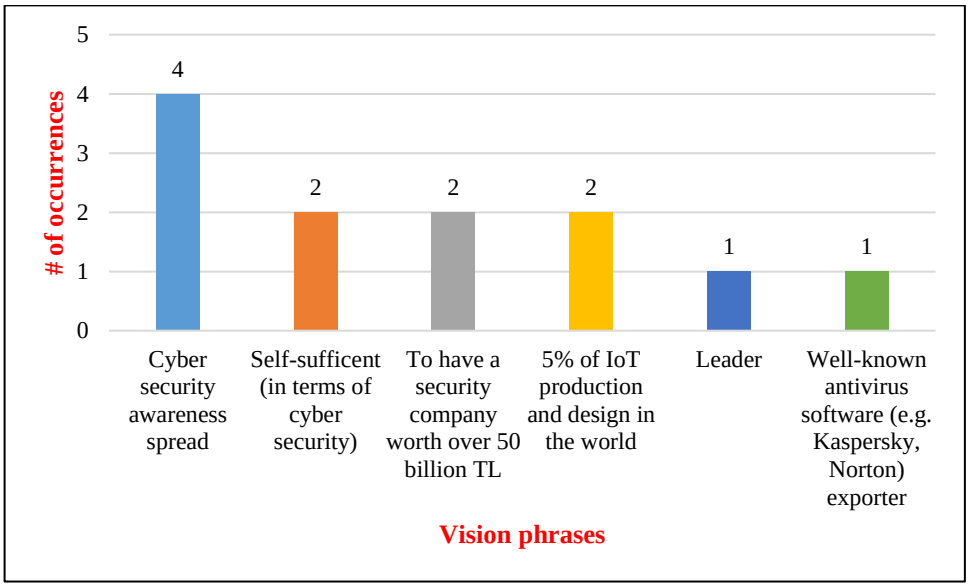


Figure 24: Vision Phrases and Number of Occurrences (Group-2)

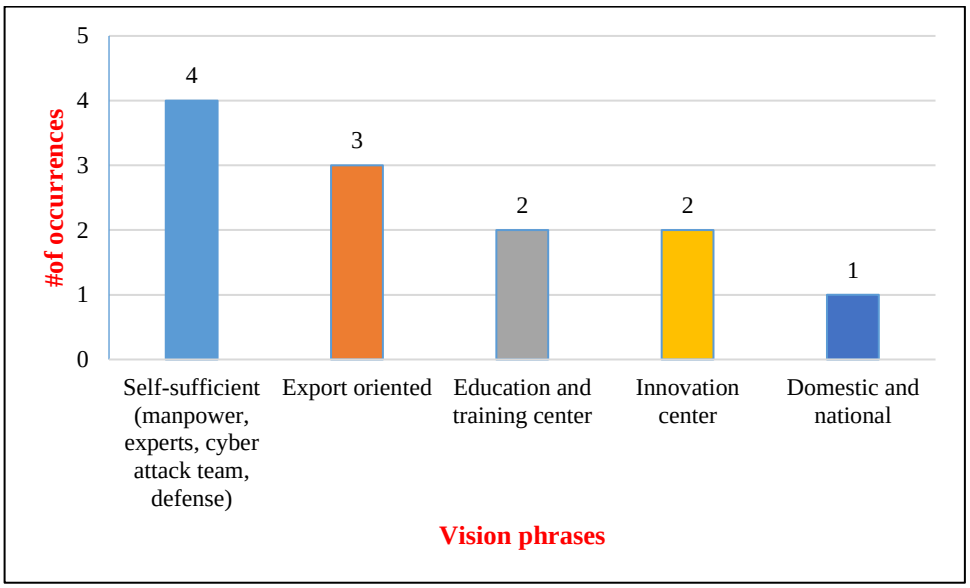


Figure 25: Vision Phrases and Number of Occurrences (Group-3)

Vision statements of the groups are as follows:

- The vision of Group-1: A country that adopts innovative approaches in cyber public policies, capable of safely developing cyber weapons, army and smart objects, capable of upskilling young people with new cyber skills, having domestic and national solutions.

- The vision of Group-2: To become a country that is a leader in the field of cybersecurity, self-sufficient, owns cybersecurity companies with a value of 50 billion TL, exports cybersecurity products and spread the awareness of cybersecurity to the public.

- The vision of Group-3: A country that is domestic, national and export-oriented, self-sufficient, producing the world's best cybersecurity technology, and becomes a center of education and innovation.

Cybersecurity vision of Turkey was set by combining three visions: To become an export-oriented and self-sufficient country, with the domestic and national cybersecurity technologies, having a strong cyber army, a center of education and innovation, where cybersecurity awareness is spread to the public.

5.2 Results of SWOT Analysis

Participants prioritized the prewritten SWOT issues prepared by the researcher and they were encouraged to add their statements. After the workshop, the issues were sorted by the researcher according to their priority scores given by the participants.

According to the results, weaknesses of Turkey is more than the strengths, on the other hand, opportunities are highly more than the threats. Numbers of the factors are depicted in Table 48 and Figure 26.

Table 48: Distribution of STEEPLE Factors by SWOT Factors

	Strengths	Weaknesses	Opportunities	Threats	**Total**
Social	7	10	11	2	**30**
Technological	1	11	25	2	**39**
Economic	1	1	6	6	**14**
Environmental	0	0	0	1	**1**
Political	5	5	11	3	**24**
Legal	2	3	2	1	**8**
Ethical	1	1	1	0	**3**
Total	**17**	**31**	**56**	**15**	**119**

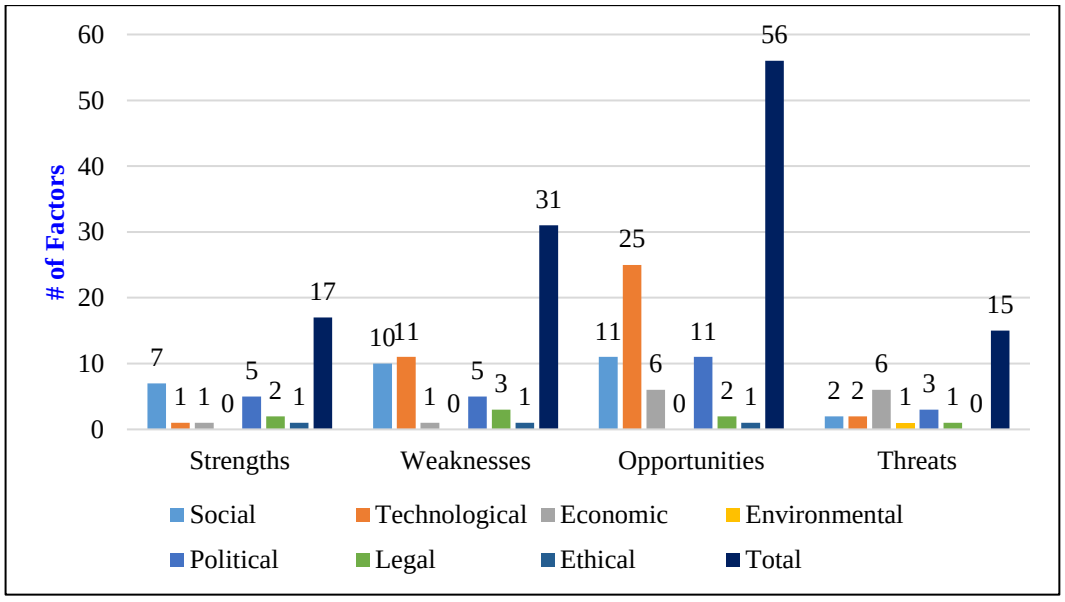


Figure 26: Distribution of STEEPLE Factors by SWOT Factors

5.2.1 Strengths

Participants added 10 more strengths to the current 7 strengths written by the researcher. Strengths of Turkey in terms of cybersecurity is given in Table 49 in the order of importance (priority) set by the participants.

Table 49: Strengths of Turkey in Terms of Cybersecurity

No	Factor	Strengths
S-1	Social	Young and entrepreneurial manpower
S-2	Social	A science and technology community integrated into the international community
S-3	Political	The existence of the institutions to realize the strategies (SSB, TUBITAK, Ministries, etc.)
S-4	Economic	Turkey's being among the 20 largest economies in the world
S-5	Political	Government's support for cybersecurity
S-6	Technological	An industry that is open to the international arena
S-7	Legal	Presence of legal infrastructure that protects personal data, ideas and works (Law of Intellectual and Artistic Works and Protection of Personal Data, etc.)
S-8	Social	Young manpower adopting technology
S-9	Political	Powerful political support for cybersecurity
S-10	Ethical	Having sense of nationalism and patriotism
S-11	Social	Manpower open to innovation
S-12	Political	The acceleration of the defense industry
S-13	Social	A society with practical approaches
S-14	Social	Education conditions and specifications
S-15	Political	Current relations with regional countries
S-16	Social	Being a role model for the countries in the region
S-17	Legal	The existence of Law No. 5651 (Internet)

5.2.2 Weaknesses

Participants added 13 more weaknesses to the current 18 issues written by the researcher. Weaknesses of Turkey in terms of cybersecurity is given in Table 50 in the order of importance (priority) set by the participants.

Table 50: Weaknesses of Turkey in Terms of Cybersecurity

No	Factor	Weaknesses
W-1	Social	Lack of skilled human resources
W-2	Political	Disruptions in education and training
W-3	Technological	Dependency on abroad in terms of information technologies (especially hardware) on which cybersecurity is built
W-4	Social	Institutions' not being aware of the real needs for cybersecurity
W-5	Technological	Lack of national products and technologies for information systems and cybersecurity
W-6	Social	Poor cooperation between public, industrial and academic community
W-7	Social	Lack of cooperation culture
W-8	Technological	Inadequate institutional competencies (organization, infrastructure, personnel, resources) in cybersecurity
W-9	Technological	Too many firms focusing on a limited number of specific cybersecurity products and services
W-10	Technological	Lack of research data
W-11	Technological	The low number of domestic products and functional diversity
W-12	Political	Failure to be successful in the implementation of cybersecurity strategy and action plans
W-13	Technological	Failure to implement certification and testing mechanisms
W-14	Social	Keeping cybersecurity as a secondary issue on the institutional basis
W-15	Social	Keeping cybersecurity as a secondary issue on a personal basis
W-16	Legal	Inadequate legislation to counter international cyber threats and cyber incidents
W-17	Economic	Lack of scale economy
W-18	Ethical	Personal deficiencies in compliance with the principles for the protection of ideas and works
W-19	Social	Lack of opportunities to attract a trained workforce
W-20	Social	Having the idea that an expensive product is better
W-21	Technological	Lack of scientific knowledge of cyberspace and technologies
W-22	Political	Shortage of universities and departments providing education in basic sciences
W-23	Political	Uncertainties in the country's cybersecurity organizational structure (leadership, responsibilities, etc.)
W-24	Legal	Problems in the functioning of legal mechanisms
W-25	Technological	Low cybersecurity product development capabilities
W-26	Technological	Lack of research methods
W-27	Social	Managers are not aware of cybersecurity needs and risks
W-28	Technological	Failure to follow new technologies
W-29	Social	Experienced manpower goes abroad
W-30	Political	Insufficiency of cooperation mechanisms
W-31	Legal	Noncompliance with international legislation

5.2.3 Opportunities

Participants added 11 more opportunities to the current 45 ones written by the researcher. Opportunities for Turkey in terms of cybersecurity is given in Table 51 in the order of importance set by the participants.

Table 51: Opportunities of Turkey in Terms of Cybersecurity

No	Factor	Opportunities
O-1	Social	Increased need for cybersecurity because of an increase in cyber threats and complexity
O-2	Political	Adoption of cybersecurity among elements of national security in many countries around the world, including Turkey
O-3	Social	Cybersecurity needs caused by social, technological, economic, environmental and political factors
O-4	Technological	The need for domestic products due to the nature of cybersecurity
O-5	Social	Increased use and penetration of technology in every area of life
O-6	Economic	The willingness of the public and private sector to invest in cybersecurity
O-7	Technological	The rapid development of cyber threats
O-8	Economic	The width of internal and external cybersecurity market
O-9	Social	The penetration of digital services through internet (health, shopping, information sharing, etc.)
O-10	Technological	Lack of institutionalization of cybersecurity systems
O-11	Political	Cyber events and crimes that the countries faced
O-12	Technological	Widespread use of smart objects (home, car, home goods, etc.)
O-13	Social	Widespread use of internet
O-14	Technological	The spread of robotics and autonomous systems
O-15	Technological	Widespread transition to cloud computing
O-16	Technological	Expansion of industrial control systems
O-17	Technological	Expansion of Industry 4.0 concepts (cyber-physical systems, big data, artificial intelligence, internet of things, etc.)
O-18	Technological	Widespread use of mobile and wireless systems
O-19	Social	Increased emphasis on privacy
O-20	Technological	The spread of online services
O-21	Technological	The spread of wearable smart objects
O-22	Technological	Importance of technologies to protect data privacy
O-23	Technological	Widespread use of crypto coins
O-24	Technological	AI, machine learning and methods of deep learning
O-25	Technological	Widespread use of global internet access

Table 51 (Cont'd)

No	Factor	Opportunities
O-26	Ethical	More emphasis on cybersecurity than cyber attack
O-27	Political	Use of cyber attacks as an element of power among states
O-28	Political	Cyber espionage actions of states become more complex
O-29	Technological	The spread of multi-factor authentication mechanisms
O-30	Political	The transition of countries to e-government and digitization
O-31	Political	Increasing the state's efforts and incentives to protect data (technological, personal, etc.)
O-32	Legal	Establishment and dissemination of national and international legislation on cybercrime
O-33	Legal	New arrangements in nations (e.g. USA) and country communities (e.g. European Union) for the compliance of the systems processing personal data with the security criteria
O-34	Political	Introducing restrictions on the sale of advanced cybersecurity products and technologies
O-35	Political	Increased state support for information technologies and cybersecurity
O-36	Technological	Systems become more complex as hardware and software
O-37	Technological	Vulnerabilities in software and hardware
O-38	Political	Increased state support for electronic and online technologies
O-39	Economic	The decrease in prices of electronic and online systems
O-40	Social	Public services through digital media
O-41	Economic	Facilitation of access to international markets due to global economic policies
O-42	Technological	The emergence of internet concept in space
O-43	Social	Increased online education and training activities
O-44	Social	Training needs for cybersecurity
O-45	Economic	Globalization of financial resources
O-46	Technological	Increasing the speed of technological development and transformations
O-47	Technological	Widespread use of human-machine interfaces
O-48	Technological	Increased interdependence and interaction between countries
O-49	Economic	Increased purchasing power in Turkey and in the world
O-50	Technological	Ability to provide cybersecurity services remotely
O-51	Social	Widespread use of social media
O-52	Social	Numerous universities and graduates in Turkey
O-53	Technological	Cybersecurity technologies are very recent and new
O-54	Technological	The rapid change of the cybersecurity sector
O-55	Political	Possibility to export product and services as a role-model to regional countries, especially Muslim countries
O-56	Political	Access to cooperation between Russia and geographical proximity

5.2.4 Threats

Participants added 3 more threats to the current 12 ones written by the researcher. Threats for Turkey in terms of cybersecurity is given in Table 52 in the order of importance set by the participants.

Table 52: Threats of Turkey in Terms of Cybersecurity

No	Factor	Threats
T-1	Political	Less investment in R&D than it should be
T-2	Social	Lack of confidence in domestic products
T-3	Technological	Failure to give sufficient importance to the national development of systems due to urgent supply demands
T-4	Legal	According to the public procurement legislation, the cost is evaluated before quality
T-5	Economic	Foreign products dominate most of the market
T-6	Economic	Inquire about the defense expenditures in the Western world
T-7	Political	Introducing restrictions on the sale of advanced cybersecurity products and technologies
T-8	Technological	The spread of technologies based on cloud computing and the dominance of foreign firms in this field
T-9	Social	Start to settle a culture that is eager to make easy money
T-10	Economic	International competition
T-11	Economic	The defense is expensive, the attack is cheap
T-12	Political	The geopolitical environment in which Turkey is located and the instability in the surrounding countries have the potential to affect foreign investors
T-13	Economic	Investments and partnerships of foreign companies in Turkey
T-14	Environmental	The energy consumption of crypto-money mining and its negative impact on the environment
T-15	Economic	Lack of economic support for companies

5.3 Results of STEEPLE Analysis

Social, technological, economic, environmental, political, legal and ethical (STEEPLE) factors of cybersecurity were prepared by the researcher and then participants were requested to add new ones and prioritize all issues during the workshop. Number of STEEPLE factors can be shown in Table 53 and Figure 27.

According to the results, total of 85 factors were identified by the researcher and participants. Technological factors have the highest share while ethical factors have the lowest.

Table 53: Number of STEEPLE Factors

	Pre-Written by Researcher	Added by Participants	**Total**
Social	11	6	**17**
Technological	19	11	**30**
Economic	6	8	**14**
Environmental	2	1	**3**
Political	8	6	**14**
Legal	3	2	**5**
Ethical	0	2	**2**
Total	**49**	**36**	**85**

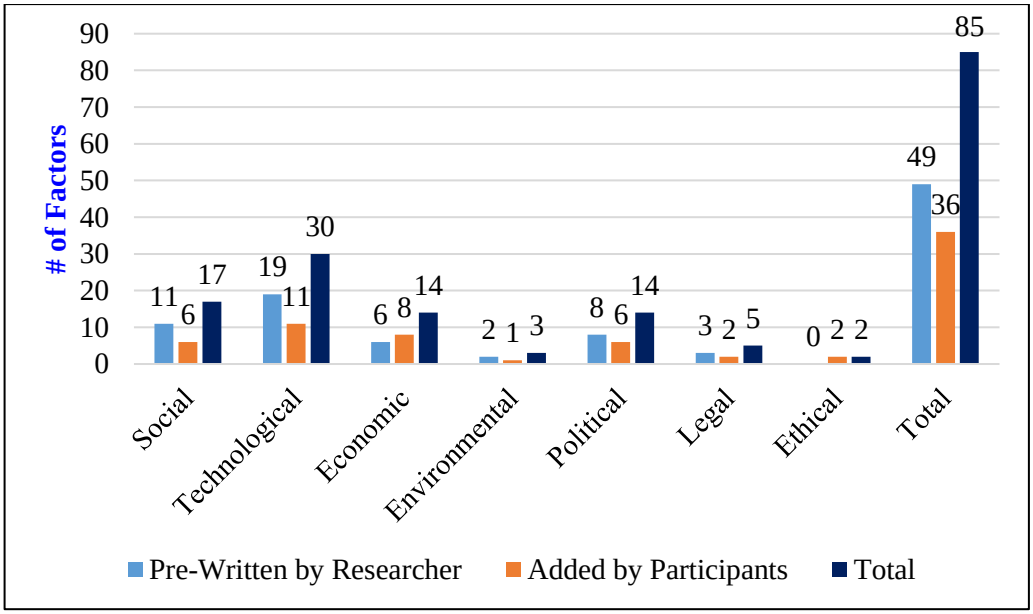


Figure 27: Number of STEEPLE Factors

In the following tables (from Table 54 to Table 60), STEEPLE factors are listed in the order of importance voted by the participants.

Table 54: Social Factors in Terms of Cybersecurity

No	Social Factors
1	Widespread use of smart things (home, car, household goods, etc.)
2	Increased need for cybersecurity because of the increase in cyber threats and complexity
3	Increased use and penetration of technology in every area of life
4	The penetration of internet and digital services into every aspect of life (health, shopping, information sharing, etc.)
5	Lack of confidence in domestic products
6	The penetration of robotic and autonomous systems into social life
7	Cybersecurity needs caused by social, technological, economic, environmental and political factors
8	Widespread use of the Internet
9	Increase in cybercrime
10	Public services through the digital environment (internet)
11	Widespread use of social media
12	Training needs for cybersecurity
13	Increased emphasis on privacy and security
14	Start to settle a culture that is eager to make easy money
15	Widespread use of mobile phones
16	Increase in online education and training activities
17	Numerous universities and graduates in Turkey

Table 55: Technological Factors in Terms of Cybersecurity

No	Technological Factors
1	The rapid development of cyber threats
2	Widespread use of smart things (home, car, household goods, etc.)
3	The need for domestic products due to the nature of cybersecurity
4	Increase in cyber threat sources and abilities
5	The spread of robotics and autonomous systems
6	Widespread transition to cloud computing
7	Failure to give sufficient importance to the national development of systems due to urgent supply demands

Table 55 (Cont'd)

No	Technological Factors
1	The rapid development of cyber threats
2	Widespread use of smart things (home, car, household goods, etc.)
3	The need for domestic products due to the nature of cybersecurity
4	Increase in cyber threat sources and abilities
5	The spread of robotics and autonomous systems
6	Widespread transition to cloud computing
7	Failure to give sufficient importance to the national development of systems due to urgent supply demands
8	Vulnerabilities in software and hardware
9	Expansion of Industry 4.0 concept (cyber-physical systems, big data, artificial intelligence, internet of things, etc.)
10	The proliferation of artificial intelligence, machine learning and methods of deep learning
11	The spread of technologies based on cloud computing and the dominance of foreign firms in this field
12	Lack of institutionalization of cybersecurity systems
13	Diffusion of online services
14	Faster technological developments and transformations
15	Widespread use of wearable smart objects
16	Ability to provide cybersecurity services remotely
17	Widespread use of crypto coins
18	Widespread use of mobile and wireless systems
19	Widespread use of global internet access
20	More complex systems in terms of hardware and software
21	Widespread use of human-machine interfaces
22	Increased technological interdependence and interaction between countries
23	Increase in importance of technologies to protect data security
24	More widespread behavior-based security mechanisms than signature-based security mechanisms
25	Expansion of industrial control systems
26	Widespread use of multi-factor authentication mechanisms
27	The impact of the private sector on technological developments in comparison with the state
28	The rapid change of the cybersecurity sector
29	Cybersecurity technologies are very recent and new
30	The emergence of internet concept in space

Table 56: Economic Factors in Terms of Cybersecurity

No	Economic Factors
1	Increased demand for online systems
2	The decrease in prices of electronic and online systems
3	Facilitation of access to international markets due to global economic policies
4	Globalization of financial resources
5	Increased purchasing power in Turkey and in the world
6	Inquire about the defense expenditures in the Western world
7	Funding cyber terrorism by black money
8	The defense is expensive, the attack is cheap
9	The width of internal and external cybersecurity market
10	The willingness of the public and private sector to invest in cybersecurity
11	Foreign products dominate most of the market
12	Investments and partnerships of foreign companies in Turkey
13	International competition
14	Lack of economic support for companies

Table 57: Environmental Factors in Terms of Cybersecurity

No	Environmental Factors
1	Widespread use of renewable energy
2	Increase in environmental awareness and the importance of the environment
3	The energy consumption of crypto-money mining and its negative impact on the environment

Table 58: Political Factors in Terms of Cybersecurity

No	Political Factors
1	Use of cyber attacks as an element of power among states
2	More complex cyber espionage actions of states
3	Adoption of cybersecurity among elements of national security in many countries around the world, including Turkey
4	The transition of countries to e-government and digitization
5	Increasing the state's efforts and incentives to protect data (technological, personal, etc.)
6	Introducing restrictions on the sale of advanced cybersecurity products and technologies

Table 58 (Cont'd)

No	Political Factors
7	Increased state support for information technologies and cybersecurity
8	Increased state support for electronic and online technologies
10	Access to cooperation between Russia and geographical proximity
11	Cyber events and crimes that the countries faced
12	Possibility to export product and services as a role-model to regional countries, especially Muslim countries
13	Less investment in R&D than it should be
14	The geopolitical environment in which Turkey is located and the instability in the surrounding countries have the potential to affect foreign investors

Table 59: Legal Factors in Terms of Cybersecurity

No	Legal Factors
1	Establishment and dissemination of national and international legislation on cybercrime
2	New arrangements in nations (e.g. USA) and international communities (e.g. European Union) for the compliance of systems with personal data to the security criteria
3	Taking steps to protect intellectual property rights
4	Uncertainties regarding international law on the cyber domain
5	According to the public procurement legislation, the cost is evaluated before quality

Table 60: Ethical Factors in Terms of Cybersecurity

No	Ethical Factors
1	In the Internet environment, the sensitivity of the privacy of people is lower than the real environment
2	More emphasis on cybersecurity than cyber attack

5.4 Results of Cybersecurity Trends Survey

A cybersecurity survey was conducted with the experts in the first workshop. Questions and results are given in the following paragraphs.

In order to determine the rankings given by participants, average and standard deviation of the scores per item (country, attack type, sector, and technology) were calculated. Then Z-scores standardization was applied to compare the scores of the items. Aggregations of standardization scores per item were sorted in order to sort the final scores. After calculating scores, experts' lists and non-experts' list were analyzed separately. Then, all lists combined and analyzed where applicable, without giving any weight to the experts' lists.

Question-1: What do you think will happen in the next 5 years in which countries will come out in cyber attacks?

Results: 5 experts and 9 non-experts answered the questions. Results are shown in Table 61.

Table 61: Trends Survey - Top Cyber Attack Source Countries

Experts' Rankings	Country
1	China
2	Russia
3	USA
4	Israel
5	Germany
6	India
7	UK
8	Syria

Non-Experts' Rankings	Country
1	China
2	Russia
3	USA
4	North Korea
5	Israel
6	India
7	Iran
8	Netherlands
9	UK
10	Hungary

Final Ranks	Country
1	China
2	Russia
3	USA
4	Israel
5	North Korea
6	India
7	UK
8	Germany
9	Iran
10	Syria
11	Netherlands
12	Hungary

Question-2: Which countries will be the target of cyber attacks in the next 5 years?

Results: 5 experts and 9 non-experts answered the questions. Results are shown in Table 62.

Table 62: Trends Survey - Top Cyber Attack Target Countries

Experts' Rankings	Country
1	USA
2	Russia
3	China
4	Germany
5	Israel
6	Turkey
7	Iran
8	UK

Non-Experts' Rankings	Country
1	USA
2	Russia
3	Turkey
4	China
5	Iran
6	India
7	Korea
8	Germany
9	UK
10	Saudi Arabia
11	France
12	Canada

Final Ranks	Country
1	USA
2	Russia
3	China
4	Turkey
5	India
6	Iran
7	Korea
8	UK
9	Germany
10	Israel
11	North Korea
12	Japan
13	Ukraine
14	Saudi Arabia
15	France
16	Canada

Question-3: What types of cyber attacks will be effective in the next 5 years?

Results: 7 experts and 5 non-experts answered the question. Results are shown in Table 63.

Table 63: Trends Survey – Top Cyber Attack Types

Experts' Rankings	Attacks
1	Cyber espionage
2	Data breaches
3	Ransomware
4	Malware
5	Phishing
6	Insider threat
7	Information leakage
8	Denial of service

Non-Experts' Rankings	Attacks
1	Information leakage
2	Phishing
3	Web application attacks
4	Cyber espionage
5	Identity theft
6	Spam
7	Ransomware
8	Web-based attacks

Table 63 (Cont'd)

Experts' Rankings	Attacks
9	Botnets
10	Web-based attacks
11	Exploit kits
12	Identity theft
13	Spam
14	Web application attacks

Non-Experts' Rankings	Attacks
9	Malware
10	Botnets
11	Insider threat
12	Physical manipulation (theft/loss)
13	Denial of service
14	Data breaches

Question-4: What sectors will be the target of cybersecurity attacks in the next 5 years? (Write to the list by prioritizing. You can use the table below or add new sectors by yourself.)

Results: 4 experts and 10 non-experts answered the question. Results are shown in Table 64.

Table 64: Trends Survey – Top Cyber Attack Target Sectors

Experts' Rankings	Sector
1	Government
2	Energy (oil, electricity, etc.)
3	Telecom
4	Banking/Finance
5	Armed forces
6	Health
7	Critical infrastructures
8	Defense industry
9	Transportation
10	Manufacturing
11	Technology
12	Automotive
13	Food

Non-Experts' Rankings	Sector
1	Energy (oil, electricity, etc.)
2	Defense industry
3	Government
4	Telecom
5	Banking/Finance
6	Critical infrastructures
7	Armed forces
8	Health
9	Technology
10	Medicine
11	Transportation
12	Manufacturing
13	Automotive
14	Food
15	Education
16	Entertainment

Question-5: In your opinion, what technologies (except for cybersecurity technologies) will affect cybersecurity most in the next 5 years?

Results: 5 experts and 8 non-experts answered the question. Results are shown in Table 65.

Table 65: Trends Survey – Technologies that Affect Cybersecurity

Experts' Rankings	Technology
1	Cloud Computing
2	Blockchain
3	IoT Platform
4	Big Data
5	Artificial Intelligence
6	Deep Learning
7	Wireless (4G, 5G)
8	Machine Learning
9	Quantum Computing
10	Cognitive Computing
11	Wearable Devices
12	Smart Cars
13	Smart Robots
14	Micro Data Centers
15	Brain-Computer Interface
16	Smart Workspace
17	Commercial UAVs
18	Autonomous Vehicles
19	Virtual Reality

Non-Experts' Rankings	Technology
1	Big Data
2	Artificial Intelligence
3	IoT Platform
4	Machine Learning
5	Cloud Computing
6	Blockchain
7	Wearable Devices
8	Quantum Computing
9	Edge Computing
10	Smart Robots
11	Virtual Reality
12	Wireless (4G, 5G)
13	Smart Cars
14	Cognitive Computing
15	Deep Learning
16	Commercial UAVs
17	Digital Twin
18	Micro Data Centers
19	Autonomous Vehicles
20	Smart Home
21	Brain-Computer Interface

Question-6: What other questions could be asked in a cybersecurity trends survey?

Results: 9 additional questions were offered by participants. These questions can be used in a cybersecurity trend survey.

- In which cybersecurity technologies is our country the best?

- Which cybersecurity technologies are the fastest to develop in our country?
- What are the most critical types of cybersecurity technologies for our country?
- Which security technologies will be the most important in the next 5 years?
- In which cybersecurity domains should the first domestic and national products be developed in our country?
- Which technologies benefit our country economically?
- What are the most critical types of cybersecurity attacks for our country?
- Which types of attacks may our country face?
- Which information technologies or cybersecurity technologies will emerge as destructive technology in the next 5 years?

5.5 Results of Key/Critical Technologies Study

Key/Critical technologies study was carried out by 22 experts after the first focus group meeting. Technology list was sent to participants and they weight technology groups and technologies according to three criteria: 1) Meeting national security needs, 2) Supporting the development of the national science, technology and innovation infrastructure, 3) World-class competitiveness, collaboration or mutual dependence.

Experts were also requested to add additional cybersecurity technologies that do not exist in the current list. None of the experts provided new technology to the list.

Experts were requested to compare and weight the criteria by using AHP for the ranking of technologies. Weights of criteria are given in Table 66.

Table 66: Weights of Criteria for Technology Selection

Criteria	Weight
Meeting national security needs	0,490944
World-class competitiveness, collaboration or mutual dependence	0,213479
Supporting the development of the national science, technology and innovation infrastructure	0,295577

The result of the technology scores is depicted in Appendix C in the order of the composite scores. Participant's scores for the technologies are also given by splitting experts' and non-experts' scores as well. Composite scores were calculated by using weights of the criteria and weights of the expertise levels [*Level=1 (Poor):0.075460; Level=2 (Medium):0.333821; Level=3 (Good):0.590719*] as determined just after the first focus group meeting during "technology prioritization" study. The difference in ranks between experts' scores and non-experts' scores are also calculated as shown in Appendix C.

5.5.1 Analysis of Technology Scores

Results of the technology scores were analyzed from Table 67 to Table 70 based on the ranks given by experts and non-experts. From the tables, it can be seen that 2 technologies were scored by both experts and non-experts in top 10 technologies, 3 technologies in top 20, 8 technologies in top 30, 17 technologies in top 50. For creating Delphi statements, these scores were taken into account and top 50 technologies in either group (experts and non-experts) and top 100 technologies in both groups were selected.

Table 67: Technologies in Top 10 by Experts and Non-Experts

Technologies	Rank (Experts)	Rank (Non-Experts)
Quantum-Safe Cryptographic Algorithms	2	4
Quantum Cryptography	5	3

Table 68: Technologies in Top 20 by Experts and Non-Experts

Technologies	Order (Experts)	Order (Non-Experts)
Quantum-Safe Cryptographic Algorithms	2	4
Quantum Cryptography	5	3
Blockchain for Identity & Access Management	15	20

Table 69: Technologies in Top 30 by Experts and Non-Experts

Technologies	Rank (Experts)	Rank (Non-Experts)
Quantum-Safe Cryptographic Algorithms	2	4
Cyber-Physical Systems (CPS) Security	3	22
Quantum Cryptography	5	3
Secure Aviation Protocols and Architecture	6	29
Blockchain for Identity & Access Management	15	20
Cryptographic Chips and Modules	19	21
Blockchain for Data Security	24	30
Cybersecurity Training and Exercise Systems	26	7

Table 70: Technologies in Top 50 by Experts and Non-Experts

Technologies	Rank (Experts)	Rank (Non-Experts)
Microelectronics Security Tests	1	33
Quantum-Safe Cryptographic Algorithms	2	4
Cyber-Physical Systems (CPS) Security	3	22
Quantum Cryptography	5	3
Secure Aviation Protocols and Architecture	6	29
Cyber Offense	11	42
New Generation (4G, 5G, etc.) Wireless Security	12	36
Blockchain for Identity & Access Management	15	20
Hardware Trusted Platform Module (TPM)	18	49
Cryptographic Chips and Modules	19	21
Secure IoT Routing Protocols	20	50
Blockchain Security	23	48
Blockchain for Data Security	24	30

Table 70 (Cont'd)

Technologies	Rank (Experts)	Rank (Non-Experts)
Cybersecurity Training and Exercise Systems	26	7
Big Data Security	30	38
Cybersecurity Testbed	44	31
Cyber Forensics (stand-alone, mobile, disk, memory)	48	16
Incident Response and Management	50	40

5.6 Turkey's Cybersecurity Technology Review

In the review study, Turkish universities and companies were analyzed in order to find out the cybersecurity-related courses, cybersecurity products, and cybersecurity services.

5.6.1 Cybersecurity Courses in Universities of Turkey

Universities in Turkey were analyzed to find out cybersecurity-related departments and courses. The results are shown in Table 71 and details were given in the following sub-sections.

Table 71: Statistics for Cybersecurity at Turkish Universities

Topic	Value
Number of universities that have computer engineering, computer sciences, informatics engineering or software engineering departments	114
Number of associate degrees (two-years) related to cybersecurity	10
Number of universities that teach cybersecurity-related courses in undergraduate programs	88
Number of universities that have cybersecurity graduate programs	20
Number of total courses given in undergraduate programs	171
Number of different courses given in undergraduate programs	67
Number of topics given in undergraduate program syllabus	34
Number of total courses given in graduate programs	322
Number of different courses given in graduate programs	215
Number of topics given in graduate program syllabus	114

5.6.1.1 Undergraduate Programs

In Turkey, 114 universities have computer engineering, computer sciences, informatics engineering or software engineering departments in 2019. These departments have generally “hardware” and “software” sections. Universities that have cybersecurity related undergraduate departments or degrees are as follows:

- Total 10 universities (Bilgi University, Bülent Ecevit University, Ondokuz Mayıs University, Selçuk University, Isparta Applied Sciences University, Karabük University, Erzincan BY University, İzmir Economy University, Batman University, and Beykoz University) have a two-year vocational degree (associate degree) on information security technologies.

- Fırat University has a digital forensics Bachelor of Science (BS) program.

- Avrasya University, Turkish-German University, and Yaşar University have cybersecurity or informatics security options under BS programs.

- 77% of universities (88 of 114) have cybersecurity related courses in the syllabus of undergraduate programs.

In 2018-2019 Fall and Spring semesters, there are 171 cybersecurity related courses in undergraduate programs of Turkish universities and 67 of them are unique as listed in Appendix H (see Table H.1) in alphabetical order.

Cybersecurity courses were analyzed by the researcher and 34 different cybersecurity topics (see Table 72) were discovered through the following approach:

- Some of the courses were split into two different ones (e.g. “computer and network security” were split into two courses “computer security” and “network security”).

- Some of the courses were grouped under the same name (e.g. “secure application development” and “secure coding” were handled under “secure software development”).

- Levels of the courses were overlooked (e.g. “introduction to cybersecurity” and “advanced topics in cybersecurity” courses were handled as a single course “cybersecurity”).

Among the courses, 7 of them are compulsory (“C” column at the table) and the rest are elective (“E” column at the table). Network security, cryptology/cryptography, information security, cybersecurity, data security, and information systems security are the courses that are mostly taught at Turkish universities’ undergraduate programs.

Table 72: Cybersecurity Topics in Undergraduate Programs (Turkey)

Courses	E	C	# of Universities
Network Security	46	1	47
Cryptography/Cryptology	42	1	43
Information Security	23	-	23
Cybersecurity	19	-	19
Data Security	10	-	10
Information Systems Security	9	1	10
Computer Security	8	1	9
Secure Software Development	3	-	3
Computer Systems Security	2	-	2
Encryption	2	-	2
Application Security	1	-	1
Blockchain	1	-	1
Cloud Computing Security	1	-	1
Communication Security	1	-	1
Computer Security and Ethics	1	-	1
Critical Infrastructures and Security	1	-	1
Cryptographic Algorithms and Systems	1	-	1
Cyber Attacks	1	-	1
Cyber Forensic	1	-	1
Cyber-Physical Systems Security	1	-	1
Cyberwarfare	1	-	1
Database Security	1	-	1
Energy Security	1	-	1
Homeland Security	-	1	1

Table 72 (Cont'd)

Courses	E	C	# of Universities
Informatics Security	-	1	1
IT and Security Governance	1	-	1
Operating Systems Security	1	-	1
Secure Application Engineering	1	-	1
Security Management	1	-	1
Security Systems and Protocols	1	-	1
Server Programming and Security	1	-	1
Software Security	-	1	1
Systems Security	1	-	1
Web Application Security	1	-	1

5.6.1.2 Graduate Programs

As of 2019, 20 universities have cybersecurity-related graduate programs as listed in Table 73.

Table 73: Cybersecurity Related Graduate Departments (Turkey)

No	University	Department	Degree
1	Adana Science and Technology University	Cybersecurity Digital Forensics	MS
2	Air Force Academy	Cybersecurity	MS
3	Bahçeşehir University	Cybersecurity	MS
4	Fırat University	Digital Forensic Engineering	MS
5	Gebze Technical University	Cybersecurity	MS
6	Hacettepe University	Information Security	MS
7	Işık University	Cybersecurity	MS
8	İstanbul Şehir University	Information Security Engineering	MS
9	İstanbul Technical University	Information Security Engineering and Cryptography	MS/PhD
10	İstanbul Ticaret University	Cybersecurity	MS

Table 73 (Cont'd)

No	University	Department	Degree
11	Kadir Has University	Cybersecurity	MS
12	KTO Karatay University	Digital Forensic Engineering	MS
13	Marmara University	Cybersecurity	MS
14	Middle East Technical University	Cybersecurity	MS
15	Naval Academy	Cybersecurity	MS
16	Sabancı University	Cybersecurity	MS/PhD
17	Sakarya University	Cybersecurity	MS/PhD
18	Süleyman Demirel University	Cybersecurity	MS
19	TOBB University of Economics and Technology	Cybersecurity	MS
20	Turkish Military Academy	Cybersecurity	MS

In Turkey, in 2018-2019 Fall and Spring semesters, there are 322 cybersecurity related courses in graduate programs (MS and Ph.D.) of the universities and 215 of them are unique as listed in Appendix H (see Table H.2) in alphabetical order.

After analyzing the cybersecurity courses by the same approach in undergraduate programs, 114 different cybersecurity topics were found and listed in Table 74 in the order of number of universities that the courses were included in the syllabus.

Among the course topics, 30 of them are compulsory ("C" column at the table) and the rest are elective ("E" column at the table).

Network security, cryptology (cryptography), cybersecurity, computer security, and information security are the courses that are mostly taught at Turkish universities' graduate programs.

Compulsory courses are only in the syllabus of the "cybersecurity" and "information security" graduate programs while "computer engineering" and "software engineering" graduate programs have elective courses.

Table 74: Cybersecurity Topics in Graduate Programs (Turkey)

Courses	E	C	# of Universities
Network Security	43	2	45
Cryptology (Cryptography)	40	3	43
Cybersecurity	15	4	19
Computer Security	18	-	18
Information Security	14	4	18
Secure Software Development	11	-	11
Cybersecurity: Law and Ethics	10	-	10
Data Security	11	-	11
Information Security Management	9	1	10
Penetration Testing	8	-	8
Malware Analysis	7	-	7
Software Security	7	-	7
Cyberwarfare	6	-	6
Digital Forensics	5	1	6
Information Systems Security	5	1	6
Blockchain: Security and Applications	5	-	5
Cloud Computing Security	5	-	5
Cryptanalysis	5	-	5
Database Security	5	-	5
Encryption	4	1	5
Internet Security	4	1	5
Wireless Network Security	4	1	5
Intrusion Detection and Prevention	3	1	4
Web Security	4	-	4
Big Data Security	3	-	3
Biometrics	3	-	3
Cryptocurrencies	3	-	3
Data Mining for Cybersecurity	3	-	3
e-Commerce Security	2	1	3
Mobile Security	3	-	3
Network Forensics	3	-	3
Number Theory for Cryptography	3	-	3
Operating System Security	3	-	3
Operating Systems Security	3	-	3
Vulnerability Analysis	3	-	3
Authentication in Cybersecurity	2	-	2
Data Mining in Information Security	2	-	2
Encryption Algorithms	1	1	2

Table 74 (Cont'd)

Courses	E	C	# of Universities
Ethical Hacking	2	-	2
Information Assurance	2	-	2
Internet Security Protocols	2	-	2
IoT Security	1	1	2
Network Defense Systems	2	-	2
Public Key Cryptography	2	-	2
Risk Management	2	-	2
Security Analysis	2	-	2
Security and Privacy	2	-	2
Security Assessment	2	-	2
Symmetric Encryption Algorithms	2	-	2
System Security	1	1	2
TCP/IP Security	2	-	2
Advanced Asymmetrical Cryptosystems	1	-	1
Advanced Symmetrical Cryptosystems	1	-	1
C4I and Information Warfare	1	-	1
Computer Forensics	1	-	1
Cryptographic Microprocessor Design	1	-	1
Cyber Data Analytics	1	-	1
Cyber Defense	1	-	1
Cyber Offense and Defense Methods	-	1	1
Cyber Warfare	1	-	1
Cybercrime Analysis Hardware	-	1	1
Cybercrime Analysis Software	-	1	1
Cybercrime Hardware	-	1	1
Cybercrimes and Preventive Measures	1	-	1
Cybercrimes and the Applications in the Turkish Laws	-	1	1
Cyber-Physical Systems Security	1	-	1
Data Encryption	1	-	1
Data Recovery Techniques	1	-	1
Decryption	1	-	1
Digital Evidences and Computer Crimes	-	1	1
Digital Signature	1	-	1
Emergency Response to Cyber Attacks	-	1	1
Encryption Systems	1	-	1
End User Security	-	1	1
Forensics Information Security and Technical Review	1	-	1
Formal Methods for Safety and Security	1	-	1
Hacker Ethics	1	-	1

Table 74 (Cont'd)

Courses	E	C	# of Universities
Hash Functions and Message Authentication Codes	1	-	1
Human Factors in Cyber-Physical Systems	1	-	1
Information Hiding Techniques	1	-	1
Information Security and Crypto Applications with Java	1	-	1
Information Security Audit and Assurance	1	-	1
Information Security Management System	-	1	1
Information Systems Security Management	1	-	1
Information Warfare	1	-	1
Internet Crimes and Data Mining	1	-	1
Machine Learning for Cybersecurity	1	-	1
Machine Learning for Cybersecurity	1	-	1
Machine Learning in Security	1	-	1
Machine Learning Methods for Cybersecurity	1	-	1
Malware Detection	1	-	1
Network Traffic Analysis	1	-	1
Network Vulnerability Analysis	-	1	1
Online Crime Investigation	-	1	1
Pair-based Cryptography	1	-	1
Privacy in Internet and Mobile Networks	1	-	1
Privacy Preserved Data Management	1	-	1
Programming Language Security	1	-	1
Quantum Cryptography	1	-	1
Reverse Engineering	1	-	1
Secure Card Applications	1	-	1
Secure Implementation and Side Channel Analysis	1	-	1
Security Event Management	-	1	1
Security in Embedded Systems	1	-	1
Security Products Management	-	1	1
Security Products Monitoring	-	1	1
Security Protocols	1	-	1
Signal Intelligence	1	-	1
Software Vulnerability Analysis	-	1	1
Stochastic Analysis in Cybersecurity Systems	1	-	1
Stream Ciphers	1	-	1
Vulnerability Scanning and Prevention	1	-	1
Web Application Security	1	-	1
Wireless and Ad-Hoc Network Security	1	-	1

5.6.2 Cybersecurity Companies, Products, and Services in Turkey

Companies in Turkey were analyzed to discover whether they have cybersecurity products or they have cybersecurity services such as being supplier of products, consultancy or training. Almost 3,000 companies' web pages were visited to collect the information in the study. According to the results, as of April 2019, there are 90 companies that have cybersecurity products and 96 companies that have cybersecurity services, which makes a total 186.

Defense Industries Presidency (SSB) started an initiative in 2018 to create Turkish Cybersecurity Cluster (Türkiye Siber Güvenlik Kümelenmesi) for improving and prospering cybersecurity companies in Turkey and the most prominent companies of Turkey became member of the cluster (SSB, 2019). The membership process is still proceeding. There are 54 companies that have cybersecurity products, 20 companies that have cybersecurity services, 4 technology development regions or technology transfer centers (Bilkent Cyberpark, İTÜ NOVA, ODTÜ Teknokent, and Teknopark İstanbul) and 17 companies without any product or services in the cluster, which constituting total 95 companies. Almost half of the cybersecurity companies are not a member of the cluster yet.

There are 61 active technology development regions (science and technology parks i.e. technoparks) in Turkey. In 18 technoparks, companies have cybersecurity products and cybersecurity service companies in 25 technoparks, constitutes a total 29 technoparks having companies with cybersecurity products or services. List of technoparks with products or services is in Appendix H.

Among 169 cybersecurity technologies, 66 of them have been addressed in Turkish cybersecurity products and 16 technologies are partly realized while 87 technologies remain almost untouched or were not realized in a product. Distribution of technology realization status within Turkish cybersecurity products is depicted in Figure 28 with numbers and percentage. List of technologies and the information whether Turkish companies has addressed in the products is provided in Appendix H.

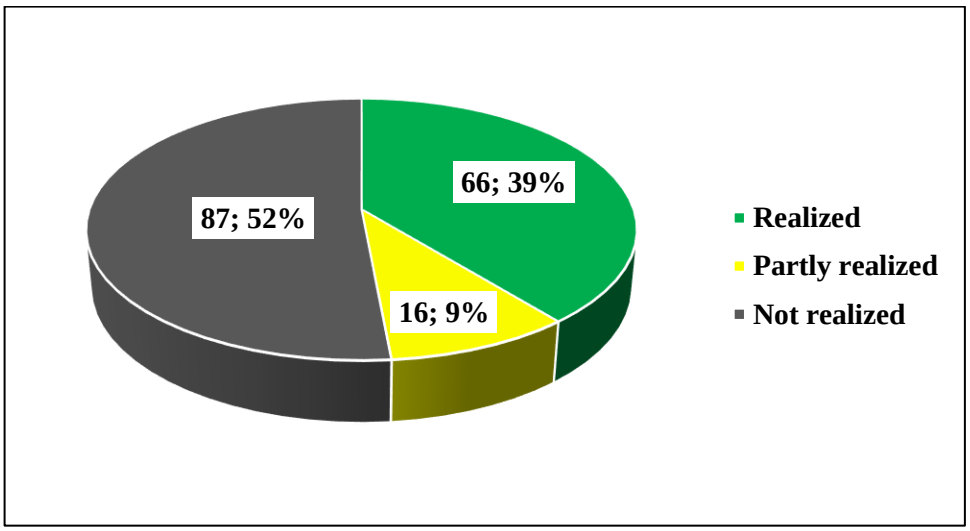


Figure 28: Cybersecurity Technologies Offered in Turkish Products

Turkish Cybersecurity Cluster's financial turnover is about $300 million and the objective is to double this number in 2019. These companies' export revenue is $41 million. The average age of the companies is six and they have nearly 4,400 personnel.

Statistics about the Turkish cybersecurity companies, products and services are listed in Table 75.

Table 75: Statistics for Turkish Cybersecurity Company, Product and Services

Topic	Value
Number of Turkish companies having cybersecurity products	90
Number of companies that are member of Turkish Cybersecurity Cluster (TCC)	95
Number of TCC members having cybersecurity products	54 (60%)
Number of Turkish companies having cybersecurity services	96
Number of TCC members having cybersecurity services	20 (21%)
Number of Turkish cybersecurity products	176
Number of Turkish cybersecurity services	395
Number of technoparks in Turkey (Technology Development Regions)	61
Number of technoparks in Turkey having companies with cybersecurity products or services	29 (47%)
Number of technologies used in Turkish cybersecurity products	66 (39%)

Cybersecurity products were analyzed based on cybersecurity technology groups. Table 76 lists the products in the order of product counts. Most of the products are related to Network Security, Identity & Access Management, Cybersecurity Event Management, Internet Security, Cyber Intelligence Cybersecurity Risk and Compliance Management and Data Security. Four of the groups [Industrial Control (SCADA) Systems Security, Operating Systems and Container Security, Cybersecurity for Autonomous and Smart Platforms and Hardware Security] do not have any products therein. 66% of the product owner companies are the member of the cluster.

Table 76: Turkish Cybersecurity Products Groups

Group	Technopark and Cluster Member	Only Cluster Member	Only Technopark Member	Not Member	Total Products
Network Security	12	7	8	3	30
Identity & Access Management	6	4	8	2	20
Cybersecurity Event Management	10	4	2	2	18
Internet Security	5	4	5	2	16
Cybersecurity Operations	7	5	2	2	16
Cyber Intelligence	2	5	4	2	13
Cybersecurity Risk and Compliance Management	6	4	1	0	11
Data Security	4	3	1	2	10
Messaging and Communication Security	6	1	0	1	8
Endpoint Security	4	2	1	0	7
Cybersecurity Analytics	1	2	1	2	6
Application Security	3	1	1	0	5
Mobile Devices Security	4	1	0	0	5
Cyber Forensics	1	1	0	3	5
Cloud Computing Security	1	0	0	2	3
Firmware Security	0	0	2	0	2
Internet of Things (IoT) Security	0	0	1	0	1
Industrial Control (SCADA) Systems Security	0	0	0	0	0
Operating Systems and Container Security	0	0	0	0	0
Cybersecurity for Autonomous and Smart Platforms	0	0	0	0	0
Hardware Security	0	0	0	0	0
Total Products	72	44	37	23	176

Cybersecurity services were also analyzed. Table 77 lists the services in the order of service counts. Consultancy, Cybersecurity Risk and Compliance Management, training and network security are the most common services. There are no services in five groups [Industrial Control (SCADA) Systems Security, Operating Systems and Container Security, Cybersecurity for Autonomous and Smart Platforms, Hardware Security and Firmware Security]. Only 37% of the service companies are the member of the cluster, which shows that an attempt is needed to reach those remaining companies.

Table 77: Turkish Cybersecurity Services Groups

Group	Technopark and Cluster Member	Only Cluster Member	Only Technopark Member	Not Member	Total Services
Consultancy	15	18	44	20	97
Cybersecurity Risk and Compliance Management	10	11	21	13	55
Training	10	14	15	13	52
Network Security	7	8	19	9	43
Endpoint Security	0	4	9	5	18
Application Security	4	3	9	2	18
Cybersecurity Event Management	3	7	5	2	17
Cybersecurity Operations	3	5	6	2	16
Data Security	1	2	5	6	14
Internet Security	2	1	8	2	13
Cyber Forensics	1	4	3	5	13
Cybersecurity Analytics	4	3	1	1	9
Identity & Access Management	0	1	5	2	8
Messaging and Communication Security	1	2	3	1	7
Cyber Intelligence	0	2	3	2	7
Internet of Things (IoT) Security	1	1	1	1	4
Mobile Devices Security	0	0	1	2	3
Cloud Computing Security	1	0	0	0	1
Industrial Control (SCADA) Systems Security	0	0	0	0	0
Operating Systems and Container Security	0	0	0	0	0
Cybersecurity for Autonomous and Smart Platforms	0	0	0	0	0
Hardware Security	0	0	0	0	0
Firmware Security	0	0	0	0	0
Total Services	63	86	158	88	395

5.7 Results of Delphi Survey

In this study, a two-round Delphi survey was conducted through internet. Almost 1900 people were reached. 150 people completed the survey in the first round and 91 of them responded in the second round.

Composite scores of Delphi statements were calculated by weighting security scores by 0.6 and economy scores by 0.4. Likewise, the weight of experts' inputs was 0.6 while non-experts' was 0.4. Results of first and second Delphi rounds are shown in Table 78 in the order of composite scores.

Table 78: Scores of Delphi Rounds (in the order of composite scores)

Delphi Round 1			
Delphi No	**Security**	**Economy**	**Composite Score**
D-29	4,86	4,27	4,62
D-8	4,90	4,10	4,58
D-31	4,52	4,66	4,57
D-1	4,81	4,06	4,51
D-39	4,64	4,27	4,49
D-4	4,74	4,12	4,49
D-9	4,57	4,34	4,48
D-27	4,74	4,09	4,48
D-2	4,55	4,32	4,46
D-12	4,50	4,40	4,46
D-22	4,54	4,32	4,45
D-14	4,63	4,16	4,44
D-26	4,47	4,41	4,44
D-47	4,53	4,28	4,43
D-23	4,43	4,43	4,43
D-16	4,63	4,08	4,41
D-5	4,46	4,32	4,40
D-28	4,51	4,13	4,36
D-25	4,55	4,07	4,35
D-35	4,63	3,92	4,35
D-13	4,45	4,06	4,30
D-3	4,43	4,10	4,29
D-15	4,32	4,21	4,28
D-30	4,24	4,02	4,15
D-21	4,20	4,06	4,15

Delphi Round 2			
Delphi No	**Security**	**Economy**	**Composite Score**
D-1	4,93	4,21	4,64
D-8	4,94	4,13	4,61
D-29	4,81	4,31	4,61
D-39	4,77	4,31	4,59
D-31	4,53	4,66	4,58
D-14	4,75	4,29	4,57
D-2	4,67	4,38	4,55
D-26	4,52	4,51	4,51
D-4	4,75	4,12	4,50
D-27	4,75	4,12	4,50
D-47	4,62	4,31	4,50
D-9	4,61	4,32	4,49
D-12	4,51	4,46	4,49
D-22	4,53	4,34	4,46
D-28	4,57	4,26	4,44
D-16	4,67	4,08	4,43
D-35	4,75	3,94	4,43
D-13	4,56	4,25	4,43
D-25	4,64	4,10	4,42
D-23	4,41	4,40	4,41
D-5	4,40	4,35	4,38
D-15	4,36	4,36	4,36
D-3	4,47	4,17	4,35
D-30	4,32	4,05	4,21
D-21	4,06	3,95	4,01

In Figure 29 and Figure 30, the distribution of the scores is depicted in security and economy axes.

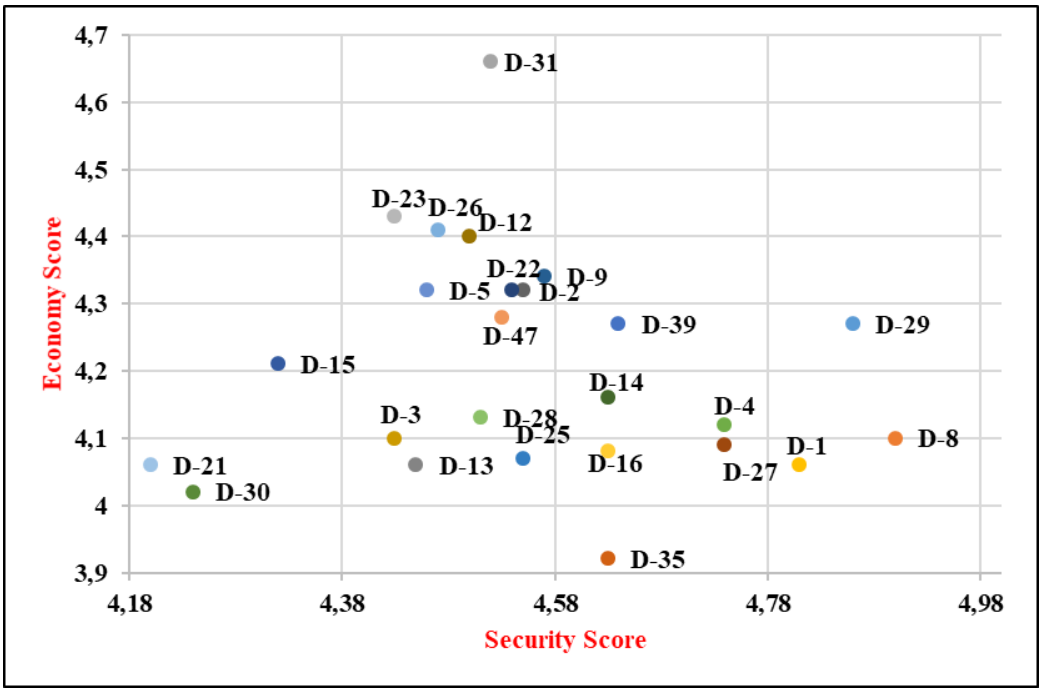


Figure 29: Distribution of Delphi Statements' Scores (Round-1)

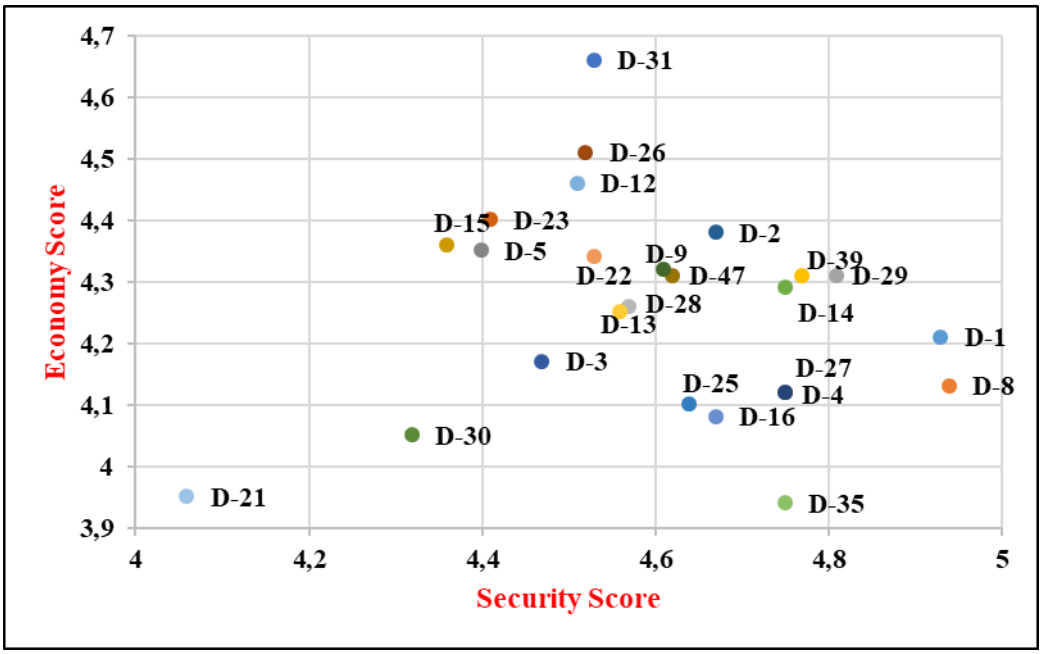


Figure 30: Distribution of Delphi Statements' Scores (Round-2)

In a Delphi study, spectrum of inputs between rounds is analyzed in order to check whether consensus reached in the survey (Dalkey, 1969). Therefore, the distribution of the answers between rounds is calculated and depicted in the tables in Appendix G. Moreover, since the number of participants is different in rounds (150 people in the first round, 91 people in the second round), the percentage of the answers are more meaningful to show the preference of the participants. Here, Table 79 was put here to show the interpretation of the tables. Green color refers to an increase in the scores per item in the second round while red color refers to a decrease in second round scores.

Table 79: Distribution of Answers in Delphi Rounds (Sample)

Question # .b (Security)	1	2	3	4	5
Round-1	0,0%	3,0%	11,9%	29,9%	55,2%
Round-2	0,0%	2,8%	6,9%	29,2%	61,1%
*Question # .*c (Economy)	1	2	3	4	5
Round-1	0,0%	4,5%	17,9%	38,8%	38,8%
Round-2	0,0%	4,2%	16,7%	37,5%	41,7%
*Question # .*d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	58,2%	32,8%	7,5%	1,5%	0,0%
Round-2	56,9%	36,1%	5,6%	1,4%	0,0%

*Question # .*e (Method)	Round-1	Round-2
R&D Investment	50,4%	52,4%
Technology Transfer	19,3%	18,3%
Foreign Company Cooperation	11,8%	9,5%
COTS or Open Source Use	18,5%	19,8%

5.7.1 Statistics of the Results

Some statistics for Delphi rounds in terms of security and economy scores are depicted in the following tables (from Table 80 to Table 83).

Table 80: Statistics of Round 1 (Security Scores)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Valid	122	127	127	131	126	116	126	114	120	106	104	112	119	118	106	115	124	101	126	120	104	94	115	101	104
Missing	28	23	23	19	24	34	24	36	30	44	46	38	31	32	44	35	26	49	24	30	46	56	35	49	46
Mean	4,4	4,3	4,4	4,8	4,9	4,7	4,6	4,9	4,5	4,5	4,3	4,4	4,6	4,6	4,5	4,2	4,6	4,5	4,5	4,5	4,7	4,6	4,4	4,6	4,5
Std. Dev.	0,8	0,8	0,7	0,6	0,5	0,5	0,7	0,4	0,7	0,7	0,9	0,8	0,6	0,7	0,8	1	0,6	0,7	0,7	0,8	0,6	0,8	0,8	0,7	0,8
Variance	0,6	0,7	0,5	0,3	0,2	0,3	0,5	0,2	0,5	0,4	0,7	0,6	0,4	0,5	0,7	0,9	0,4	0,5	0,5	0,6	0,4	0,6	0,7	0,4	0,6
Range	3	3	2	3	3	2	4	2	2	2	3	4	3	4	4	4	2	3	3	3	3	4	4	3	4
Min	2	2	3	2	2	3	1	3	3	3	2	1	2	1	1	1	3	2	2	2	2	1	1	2	1
Max	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Table 81: Statistics of Round 1 (Economy Scores)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Valid	122	127	127	130	126	116	124	114	120	105	104	112	119	118	105	115	124	100	126	120	104	92	114	101	104
Missing	28	23	23	20	24	34	26	36	30	45	46	38	31	32	45	35	26	50	24	30	46	58	36	49	46
Mean	4,1	4,2	4,3	4,1	4,2	4,2	4,3	4,3	4,4	4,2	4,1	4,4	4,3	4,1	4,6	4,1	4,1	4,3	4,3	4,3	4,1	3,9	4,1	4,2	4,4
Std. Dev.	0,9	0,8	0,8	1	1	0,9	0,8	1	0,8	0,9	0,9	0,8	0,9	1	0,7	1	1	0,8	0,9	0,9	1,1	1,2	1	0,9	0,9
Variance	0,8	0,7	0,7	1	1,1	0,9	0,7	1	0,6	0,7	0,9	0,6	0,8	1	0,4	1	0,9	0,6	0,8	0,8	1,1	1,3	0,9	0,9	0,8
Range	4	4	4	4	4	4	3	4	3	3	4	4	3	4	3	4	3	3	4	4	4	4	4	3	4
Min	1	1	1	1	1	1	2	1	2	2	1	1	2	1	2	1	2	2	1	1	1	1	1	2	1
Max	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Table 82: Statistics of Round 2 (Security Scores)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Valid	85	86	85	86	84	83	86	80	85	74	75	79	82	84	76	80	85	70	83	79	75	65	81	71	76
Missing	6	5	6	5	7	8	5	11	6	17	16	12	9	7	15	11	6	21	8	12	16	26	10	20	15
Mean	4,4	4,3	4,4	4,9	4,9	4,7	4,6	4,8	4,5	4,5	4,3	4,4	4,8	4,7	4,5	4,1	4,6	4,6	4,5	4,6	4,7	4,7	4,5	4,7	4,5
Std. Dev.	0,9	0,8	0,8	0,4	0,4	0,6	0,7	0,5	0,8	0,6	0,9	0,8	0,5	0,7	0,8	1	0,6	0,6	0,7	0,8	0,6	0,7	0,8	0,6	0,7
Variance	0,8	0,6	0,6	0,1	0,2	0,3	0,5	0,3	0,6	0,4	0,8	0,6	0,2	0,5	0,6	1	0,3	0,4	0,5	0,6	0,4	0,5	0,7	0,3	0,5
Range	4	3	3	3	3	3	4	4	3	2	3	4	2	4	4	4	2	2	3	3	3	4	4	2	4
Min	1	2	2	2	2	2	1	1	2	3	2	1	3	1	1	1	3	3	2	2	2	1	1	3	1
Max	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Table 83: Statistics of Round 2 (Economy Scores)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Valid	86	86	85	86	84	82	86	80	85	74	74	79	82	84	76	80	85	70	84	79	75	64	81	71	75
Missing	5	5	6	5	7	9	5	11	6	17	17	12	9	7	15	11	6	21	7	12	16	27	10	20	16
Mean	4,1	4,3	4,3	4,2	4,2	4,2	4,3	4,4	4,5	4,3	4,1	4,5	4,3	4,1	4,6	4	4,1	4,4	4,4	4,3	4,1	4	4,2	4,2	4,4
Std. Dev.	0,9	0,8	0,8	0,9	1	0,9	0,8	0,9	0,7	0,7	0,9	0,8	0,8	1	0,7	0,9	0,9	0,8	0,8	0,8	1	1,2	0,9	0,8	0,8
Variance	0,9	0,6	0,7	0,9	1	0,9	0,7	0,8	0,6	0,5	0,9	0,6	0,7	1,1	0,5	0,9	0,8	0,6	0,7	0,6	1	1,4	0,8	0,7	0,7
Range	4	3	4	4	4	4	3	3	3	2	4	4	3	4	3	4	3	3	4	3	4	4	3	3	4
Min	1	2	1	1	1	1	2	2	2	3	1	1	2	1	2	1	2	2	1	2	1	1	2	2	1
Max	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

5.7.2 Consensus Between Rounds

The Delphi is a technique that was developed as a means for attaining consensus (Thangaratinam & Redman, 2005). This is achieved through iterations. In order to check whether the consensus between rounds achieved, rankings of the Delphi statements in both first and second round were compared (see Table 84).

Table 84: Comparison of Ranks between Delphi Rounds

Delphi No	Rank in Round-1	Rank in Round-2	Difference
D-1	4	1	3
D-2	9	7	2
D-3	22	23	1
D-4	6	9	3
D-5	17	21	4
D-8	2	2	0
D-9	7	12	5
D-12	10	13	3
D-13	21	18	3
D-14	12	6	6
D-15	23	22	1
D-16	16	16	0
D-21	25	25	0
D-22	11	14	3
D-23	15	20	5
D-25	19	19	0
D-26	13	8	5
D-27	8	10	2
D-28	18	15	3
D-29	1	3	2
D-30	24	24	0
D-31	3	5	2
D-35	20	17	3
D-39	5	4	1
D-47	14	11	3

Differences in the rankings of the Delphi statements between rounds is depicted in Figure 31. For example, it can be seen that five statements have the same rank in both rounds (Left-most bar in the figure with “0” value showing zero difference of

ranks in both rounds). The biggest difference in rankings between the rounds is six owing to the statement D-14 (virtualization security).

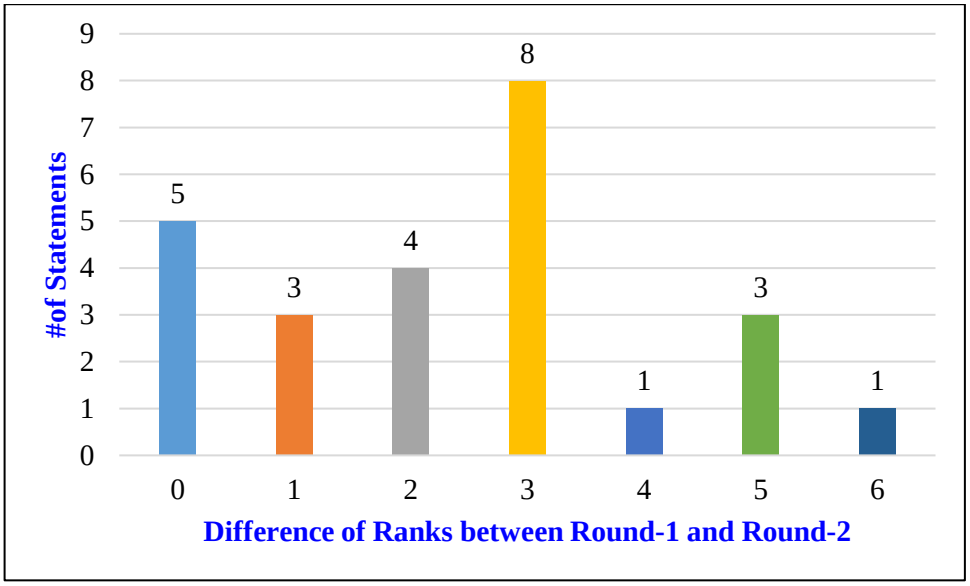


Figure 31: Differences in the Rankings of the Delphi Statements between Rounds

It can also be seen in Figure 32 that, rankings of the statements in rounds are very close. In the figure, the y-axis (left) shows the rankings and x-axis (bottom) shows the Delphi statements. The similarity of the patterns of the lines, which connect the rankings, is the sign of proximity of the rankings and thoughts. It can be concluded that the consensus between the Delphi rounds was achieved.

Additionally, consensus per question was formulated as follows: If the percentage of the top scored option is greater than the mean percentage of total scores and sum of top scored option and second top scored option is greater than % 50 then the consensus is achieved. Total percentage of top two scored options shows the degree of consensus where “medium” is between 50% - 70%, “high” is between 70% - 90% and “very high” is between 90% - 100%. Results show that in 21 questions, the degree of consensus is “very high”, the degree is “high” in 60 questions and degree is “medium” in 19 questions (see Table 85).

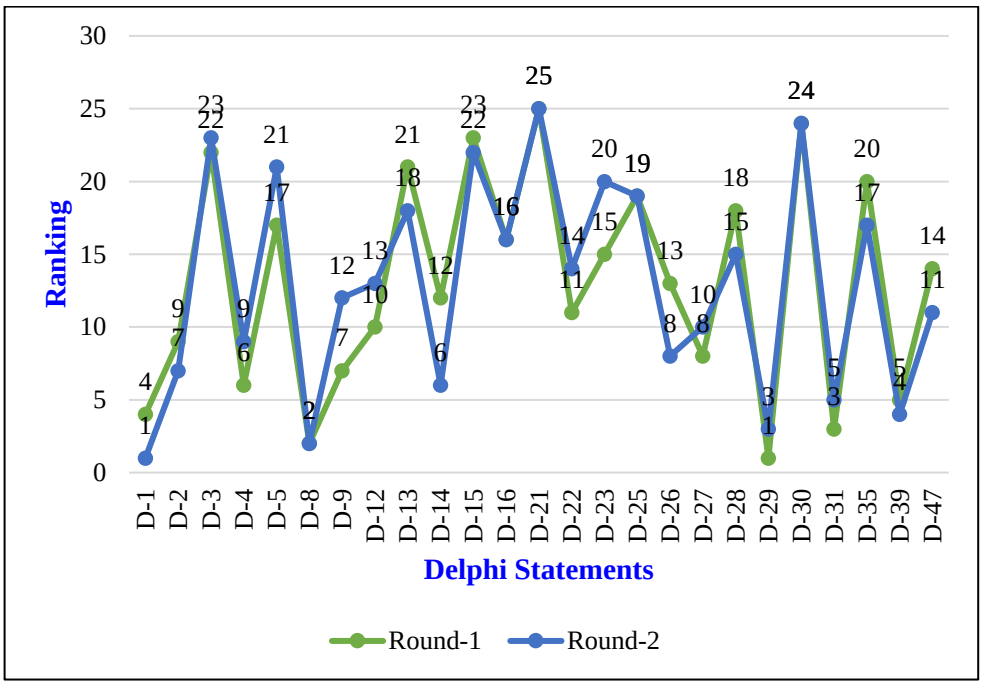


Figure 32: Rankings of the Delphi Statements

Table 85: Degree of Consensus in the Participants' Preference

Question	% of Top Scored Option	% of Second Top Scored Option	Total % of Top Two Scored Options	Consensus
1b (Security)	61,1	29,2	90,3	Very High
1c (Economy)	41,7	37,5	79,2	High
1d (Timeframe)	56,9	36,1	93,0	Very High
1e (Method)	52,4	19,8	72,2	High
2b (Security)	50,6	35,1	85,7	High
2c (Economy)	46,8	40,3	87,1	High
2d (Timeframe)	68,8	27,3	96,1	Very High
2e (Method)	46,2	21,7	67,9	Medium
3b (Security)	58,4	26	84,4	High
3c (Economy)	50,6	37,7	88,3	High
3d (Timeframe)	50	35,9	85,9	High
3e (Method)	46,9	24,5	71,4	High
4b (Security)	94,9	3,8	98,7	High
4c (Economy)	44,3	25,3	69,6	Medium
4d (Timeframe)	51,9	25,3	77,2	High
4e (Method)	48,2	17,7	65,9	High

Table 85 (Cont'd)

Question	% of Top Scored Option	% of Second Top Scored Option	Total % of Top Two Scored Options	Consensus
5b (Security)	95,9	2,7	98,6	Very High
5c (Economy)	45,9	29,7	75,6	High
5d (Timeframe)	31,1	27	58,1	Medium
5e (Method)	53	25	78,0	High
6b (Security)	79,7	17,2	96,9	Very High
6c (Economy)	46,9	25	71,9	High
6d (Timeframe)	43,8	23,4	67,2	Medium
6e (Method)	48,7	38,5	87,2	High
7b (Security)	70,5	24,4	94,9	Very High
7c (Economy)	52,6	30,8	83,4	High
7d (Timeframe)	35,9	30,8	66,7	Medium
7e (Method)	49,3	26,1	75,4	High
8b (Security)	86,4	12,1	98,5	Very High
8c (Economy)	51,5	34,8	86,3	High
8d (Timeframe)	34,8	34,8	69,6	Medium
8e (Method)	48,8	33,3	82,1	High
9b (Security)	63	27,4	90,4	Very High
9c (Economy)	64,4	24,7	89,1	High
9d (Timeframe)	39,7	32,9	72,6	High
9e (Method)	45,9	26,7	72,6	High
10b (Security)	60,9	34,4	95,3	Very High
10c (Economy)	42,2	42,2	84,4	High
10d (Timeframe)	34,4	31,3	65,7	Medium
10e (Method)	47,1	23,1	70,2	High
11b (Security)	54,7	25	79,7	High
11c (Economy)	43,8	35,9	79,7	High
11d (Timeframe)	31,3	29,7	61,0	Medium
11e (Method)	46,7	19,2	65,9	Medium
12b (Security)	53,6	36,2	89,8	High
12c (Economy)	56,5	34,8	91,3	Very High
12d (Timeframe)	37,7	27,5	65,2	Medium
12e (Method)	47,2	22,8	70,0	High
13b (Security)	77,8	22,2	100,0	Very High
13c (Economy)	50	33,3	83,3	High
13d (Timeframe)	40,3	33,3	73,6	High
13e (Method)	48,1	23,7	71,8	High

Table 85 (Cont'd)

Question	% of Top Scored Option	% of Second Top Scored Option	Total % of Top Two Scored Options	Consensus
14b (Security)	75,6	20,5	96,1	Very High
14c (Economy)	48,7	23,1	71,8	High
14d (Timeframe)	30,8	29,5	60,3	Medium
14e (Method)	50	25,7	75,7	High
15b (Security)	66,2	24,6	90,8	Very High
15c (Economy)	69,2	24,6	93,8	Very High
15d (Timeframe)	32,3	27,7	60,0	Medium
15e (Method)	49,6	27,3	76,9	High
16b (Security)	43,2	32,4	75,6	High
16c (Economy)	37,8	33,8	71,6	High
16d (Timeframe)	55,4	18,9	74,3	High
16e (Method)	47,4	23,4	70,8	High
17b (Security)	70	25	95,0	Very High
17c (Economy)	38,8	38,8	77,6	High
17d (Timeframe)	43,8	32,5	76,3	High
17e (Method)	49	26,5	75,5	High
18b (Security)	71,9	20,3	92,2	Very High
18c (Economy)	51,6	35,9	87,5	High
18d (Timeframe)	32,8	29,7	62,5	Medium
18e (Method)	48,3	26,3	74,6	High
19b (Security)	65	22,5	87,5	High
19c (Economy)	53,8	32,5	86,3	High
19d (Timeframe)	36,3	36,3	72,6	High
19e (Method)	47,3	20,9	68,2	Medium
20b (Security)	73,7	18,4	92,1	Very High
20c (Economy)	50	35,5	85,5	High
20d (Timeframe)	50	22,4	72,4	High
20e (Method)	51,1	20,4	71,5	High
21b (Security)	83,8	7,4	91,2	Very High
21c (Economy)	50	23,5	73,5	High
21d (Timeframe)	29,4	27,9	57,3	Medium
21e (Method)	51,7	25,8	77,5	High
22b (Security)	83,3	13	96,3	Very High
22c (Economy)	48,1	29,6	77,7	High
22d (Timeframe)	40,7	25,9	66,6	Medium
22e (Method)	50,5	27,8	78,3	High

Table 85 (Cont'd)

Question	% of Top Scored Option	% of Second Top Scored Option	Total % of Top Two Scored Options	Consensus
23b (Security)	69,3	21,3	90,6	Very High
23c (Economy)	49,3	26,7	76,0	High
23d (Timeframe)	38,7	29,3	68,0	Medium
23e (Method)	47,8	22,8	70,6	High
24b (Security)	76,2	22,2	98,4	Very High
24c (Economy)	46	34,9	80,9	High
24d (Timeframe)	31,7	28,6	60,3	Medium
24e (Method)	50,9	27,7	78,6	High
25b (Security)	62,1	30,3	92,4	High
25c (Economy)	63,6	24,2	87,8	High
25d (Timeframe)	31,8	24,2	56,0	Medium
25e (Method)	50,8	27,4	78,2	High

5.7.3 Reliability Analysis

The reliability analysis of the factors formed by the questions in the questionnaire was investigated by Cronbach's Alpha values by utilizing SPSS Statistics program. The fact that this ratio is 0.70 or above indicates that the variables are measured reliably (Nunally, 1978). As it can be seen from the tables below (Table 86 and Table 87), since the Cronbach's Alpha values of the factors are greater than 0.70, it can be said that the variables are measured reliably in the Delphi survey.

Table 86: Reliability of Delphi Survey (First Round)

Item	Case Processing Summary		Reliability Statistics		
	Valid N*	Excluded N	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
Security	53	97	.945	.949	25
Economy	53	97	.955	.956	25
Timeframe	52	98	.974	.975	25
Whole Survey	50	100	.952	.956	75

(*): N: Number of participants for the specific rounds.

Table 87: Reliability of Delphi Survey (Second Round)

Item	Case Processing Summary		Reliability Statistics		
	Valid N*	Excluded N	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
Security	43	48	.882	.890	24
Economy	45	46	.944	.946	25
Timeframe	45	46	.957	.957	25
Whole Survey	43	48	.937	.938	74

(*): N: Number of participants for the specific rounds.

5.8 Results of Scenario and Action Workshop

5.8.1 Key Drivers and Uncertainties

Key drivers and uncertainties have been identified through brainstorming as in Table 88. It can be seen from Table 88, Key Driver 10 (KD10) is not in the area that is either impact or uncertainty is high, making KD10 a “trend” rather than a “key driver”.

Table 88: Key Drivers and Uncertainties

No	Key Drivers	Impact	Uncertainty
KD1	Turkey’s R&D budget assigned for cybersecurity and related technological areas	High	Medium
KD2	Turkey’s incentives and investments for cybersecurity	High	Medium
KD3	The political and economic stability of Turkey	High	Medium
KD4	Employment of experienced workforce in Turkey for cybersecurity	High	Medium
KD5	Turkish private sector’s venture and entrepreneurship	High	High
KD6	Stability within Turkey’s neighborhood (Middle East, Caucasia, Balkans)	High	High
KD7	Global economic stability	High	High
KD8	Fluctuation and decreasing demands in cybersecurity product and service market	High	Medium

Table 88 (Cont'd)

No	Key Drivers	Impact	Uncertainty
KD9	Stability of global security and peace	High	High
KD10	Negative effects of free cybersecurity services	Medium	Low
KD11	New powerful foreign competitors as new actors in the global cybersecurity market	High	Medium
KD12	Nations deciding domestic and national cybersecurity software, hardware and services	High	Medium
KD13	The outbreak of global monopolies in cybersecurity domain	High	High

In Figure 33, the impact and uncertainty matrix is depicted. Five of the drivers are in the high part of the matrix while seven factors have medium uncertainty and high impact.

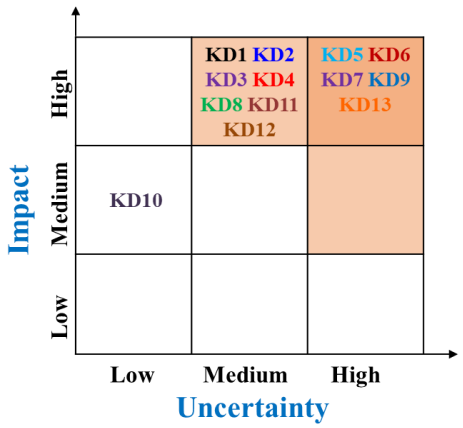


Figure 33: Key Drivers and Uncertainties

5.8.2 Signposts

Signposts are the indicators to see which scenario is unfolding. The recommended signposts (Table 89) are not decisive indicators but can be reasonable signs that demonstrate which scenario is unfolded in the future in terms of Turkey's commitments and global peace and stability. Signposts were given for the countries that dominate the global cybersecurity market in the world.

Table 89: Signposts for Cybersecurity Foresight Scenarios

No	Signpost
1	Global Cybersecurity Index
2	Global Innovation Index
3	Global Competitiveness Index
4	Ease of Doing Business Index
5	Information and Communication Technologies Development Index
6	Gross Domestic Expenditure on R&D (GERD)
7	Turkish National Science, Technology and Innovation Indicators - GERD Details (Labor cost, capital cost) - R&D Personnel Counts
8	Others: - The political and economic stability of Turkey - Stability within Turkey's neighborhood (Middle East, Caucasia, Balkans) - Fluctuation and decreasing demands in cybersecurity product and service market - Global economic stability - Stability of global security and peace - New powerful foreign competitors as new actors in the global cybersecurity market - Nations deciding domestic and national cybersecurity software, hardware and services - The outbreak of global monopolies in cybersecurity domain

Global cybersecurity market was about 152 billion US dollars in 2018 and the market is expected to reach 250 billion US dollars in 2023 (Statista, 2018). According to Strategic Defense Intelligence (2015), USA, China, UK, France, Russian Federation (RF), Israel, Brazil, India, Australia, Saudi Arabia have the highest market share in the world. North America (the USA and Canada) dominated the cybersecurity market (39.5% share of the global market in 2015) because of the outstanding companies serving advanced solutions and services to all sectors. In the Asia Pacific, countries like China and India are expected to penetrate the markets owing to the digitization in all of the sectors. UK, Germany, Japan, and Brazil are the prominent countries for the global market share (Grand View Research, 2018). In some countries, cybersecurity is dominating the export sector or high tech sector. For example, according to the report from the UK Government (Department for International Trade, 2017), cybersecurity became the largest security export category in the UK in 2015 and 2016 with £1.5 billion and 34% share. Israeli cybersecurity sector has 8% global market share and 20% of all

high-tech firms in the country are dealing with cybersecurity, making it Israel's biggest sector (Globes-Israel, 2016).

5.8.2.1 Global Cybersecurity Index

Measurement of cybersecurity status and progress over time is important to align the strategy and policies and to determine future scenarios. There are various cybersecurity indices measuring the cybersecurity postures of the countries. These indices were developed by international organizations, think tanks and private sector organizations. List of the indices are as follows (ITU, 2015): Global Cybersecurity Index; Cyber Maturity in the Asia-Pacific Region; The Cyber Index: International Security Trends and Realities; Cybersecurity: The Vexed Question of Global Rules; Cybersecurity Policy Making at a Turning point; Cyber Operations Maturity Framework; Cyber Readiness Index 2.0; Cybersecurity Intelligence Index; Index of Cybersecurity; Cybersecurity Index; Gibson Index; Information Risk Maturity Index 2014; Risk and Responsibility in a Hyperconnected World; Cybersecurity Capability Maturity Model; Cyber Power Index; EU Cybersecurity Dashboard.

Global Cybersecurity Index (GCI) is an index that measures the commitment of the countries to cybersecurity (ITU, 2017). GCI measures five pillars of cybersecurity shown in Table 90.

There are three main categories of the GCI score according to the commitments and scores of the countries:

- ***Initiating stage***: 96 countries, GCI score less than the 50^{th} percentile,
- ***Maturing stage***: 77 countries (Turkey is in this stage together with Brazil, China, Israel, Italy, and India), GCI score between the 50^{th} and 89^{th} percentile,
- ***Leading stage***: 21 countries (Australia, Canada, Egypt, Estonia, Finland, France, Georgia, Japan, Korea, Malaysia, Mauritius, Netherlands, New Zealand,

Norway, Oman, Russian Federation, Singapore, Sweden, Switzerland, UK, USA), GCI score in the 90th percentile.

Table 90: Global Cybersecurity Index (GCI) Framework

Legal	Technical	Organizational	Capacity Building	Cooperation
Cybercriminal legislation	National CIRT	Strategy	Standardization bodies	Intra-state cooperation
Cybersecurity regulation	Sectoral CIRT	Responsible agency	Good practices	Multilateral agreements
Cybersecurity training	Government CIRT	Cybersecurity metrics	R&D programs	International fora participation
	Standards for Organizations		Public awareness campaigns	Public-private partnerships
	Certifications for professionals		Professional training courses	Inter-agency partnerships
	Child online protection		National education programs and academic curricula	
			Incentive mechanisms	
			Home-grown cybersecurity industry	

In order to keep the commitment high and attain the desired goals and strategies, Turkey should try to take measures to progress into the “leading stage”.

5.8.2.2 Global Innovation Index

The Global Innovation Index (GII) is a global index created by INSEAD (Institut Européen d'Administration des Affaires or European Institute of Business Administration), Cornell University and the World Intellectual Property Organization (WIPO) and their partners (Dutta, Lanvin, & Wunsch-Vincent, 2018). The GII provides detailed metrics for over 120 countries, representing over 90% of the world’s population and over 95% of the world’s GDP (Gross Domestic Products) in current US dollars.

Four values are calculated in GII: the overall GII, the Innovation Efficiency Ratio and the Input and Output Sub-Indices (Table 91). The brief explanation of the values are as follows:

- The overall GII score is the average of the Input and Output Sub-Index scores.

- The Innovation Input Sub-Index is composed of 5 inputs that are elements of the national economy and innovation: Institutions, Human capital and research, Infrastructure, Market sophistication, and Business sophistication.

- The Innovation Output Sub-Index is comprised of two output pillars: Knowledge and technology outputs and Creative outputs.

- The Innovation Efficiency Ratio is calculated by dividing the Output Sub-Index score to the Input Sub-Index score. Each pillar is divided into three sub-items containing total of 80 individual indicators.

Table 91: Global Innovation Index Framework

Global Innovation Index (average)						
Innovation Efficiency Ratio (ratio)						
Innovation Input Sub-Index					Innovation Output Sub-Index	
Institutions	Human capital & research	Infrastructure	Market sophistication	Business sophistication	Knowledge & technology outputs	Creative outputs
Political environment	Education	ICTs	Credit	Knowledge workers	Knowledge creation	Intangible assets
Regulatory environment	Tertiary education	General infrastructure	Investment	Innovation linkages	Knowledge impact	Creative goods & services
Business environment	R&D	Ecological sustainability	Trade & competition	Knowledge absorption	Knowledge diffusion	Online creativity

In Table 92, GII scores of countries that have the biggest global shares in cybersecurity market are shown together with Turkey in the order of 2018 scores. Even though there is no correlation between the GII scores and being dominant in cybersecurity sector, Turkey should have the commitment to rise up to top 20 in order to get benefit and leverage of innovations in cybersecurity sector.

Table 92: GII Scores (in the order of 2018 scores)

Country	2016	2017	2018
UK	3	5	4
USA	4	4	6
Germany	10	9	9
Israel	21	17	11
Korea	11	11	12
Japan	16	14	13
France	18	15	16
China	25	22	17
Canada	15	18	18
Australia	19	23	20
Russia	43	45	46
Turkey	42	43	50
India	66	60	57
Brazil	69	69	64

5.8.2.3 Global Competitiveness Index (GCI)

The World Economic Forum, an independent international organization, lists the countries according to their competitiveness with the Global Competitiveness Index (GCI). According to the GCI 2018 report (see Table 93), Turkey ranks 61st among 140 countries with a 61.60 score (World Economic Forum, 2018).

Table 93: Global Competitiveness Index (GCI) (2018)

Country	**Rank**	**Score**
USA	1	85,6
Germany	3	82,8
Japan	5	82,5
UK	8	82,0
Canada	12	79,9
Australia	14	78,9
Korea	15	78,8
France	17	78,0
Israel	20	76,6
China	28	72,6
Russia	43	65,6
India	58	62,0
Turkey	61	61,6
Brazil	72	59,5

5.8.2.4 Ease of Doing Business Index

The Business Conduct Project, which is carried out in cooperation with the World Bank and the International Financial Institution, aims to improve the legal regulations in global business. The index takes the following items into account (The World Bank, 2018):

- Business extent of disclosure index (0=less to 10=more disclosure)
- New businesses registered (number)
- New business density (new registrations per 1,000 people ages 15-64)
- Distance to frontier score (0=lowest performance to 100=frontier)
- Time to import (days)
- Losses due to theft and vandalism (% of annual sales of affected firms)
- Time required to register property (days)
- Firms that do not report all sales for tax purposes (% of firms)

Looking at the ease of business index in 2018, New Zealand is at the top of the list. Turkey's rank is 43rd in 190 countries (see Table 94).

Table 94: Ease of Doing Business Index (2018)

Country	Rank
Korea	5
USA	8
UK	9
Australia	18
Canada	22
Germany	24
Russia	31
France	32
Japan	39
Turkey	43
China	46
Israel	49
India	77
Brazil	109

5.8.2.5 Information and Communication Technologies Development Index

The International Telecommunication Union (ITU) publishes a report called "Measuring Information Society" which includes the Information and Communication Technologies (ICT) Development Index (IDI). IDI measures 11 ICT indicators in three clusters (ITU, 2018b):

- ICT access (ICT readiness):
  - (1) Fixed-telephone subscriptions/100 inhabitants
  - (2) Mobile-cellular telephone subscriptions/100 inhabitants
  - (3) International Internet bandwidth (bits/s) per user
  - (4) Percentage of households with a computer
  - (5) Percentage of households with Internet access
- ICT use (ICT intensity):
  - (6) Percentage of individuals using the Internet
  - (7) Fixed (wired)-broadband subscriptions per 100 inhabitants
  - (8) Wireless broadband subscriptions per 100 inhabitants
- ICT skills:
  - (9) Adult literacy rate
  - (10) Gross enrollment ratio secondary level
  - (11) Gross enrollment ratio tertiary level

In the IDI, which includes 176 countries, Iceland was first in 2017, followed by Korea and Switzerland. In 2017 (see Table 95), Turkey ranked 67th among 176 countries (ITU, 2018a).

Table 95: ICT Development Index (2017)

Country	Rank
Korea	2
UK	5
Japan	10
Germany	12
Australia	14
France	15
USA	16
Israel	23
Canada	29
Russia	45
Brazil	66
Turkey	67
China	80
India	134

5.8.2.6 Gross Domestic Expenditure on R&D (GERD)

Gross domestic expenditure on R&D (GERD) includes domestic expenditure on research and development in a given year in terms of percentage of GDP (Eurostat, 2018). In Table 96 and Figure 34, GERD of countries that have bigger cybersecurity market shares can be shown (UNESCO Institute for Statistics, 2018). The Organization for Economic Cooperation and Development (OECD) countries' average of GERD as a percentage of GDP is 2,33 (OECD, 2018).

Table 96: GERD of Cybersecurity Leaders and Turkey

Country	2015	2016
Israel	4,27	4,25
Korea	4,22	4,24
Japan	3,29	3,15
Germany	2,92	2,94
USA	2,74	2,74
France	2,27	2,25
China	2,06	2,11

Table 96 (Cont'd)

Country	2015	2016
Australia	1,93	1,93
UK	1,67	1,69
Canada	1,66	1,61
Brazil	1,28	1,28
Russia	1,10	1,10
Turkey	0,88	0,94
India	0,62	0,62

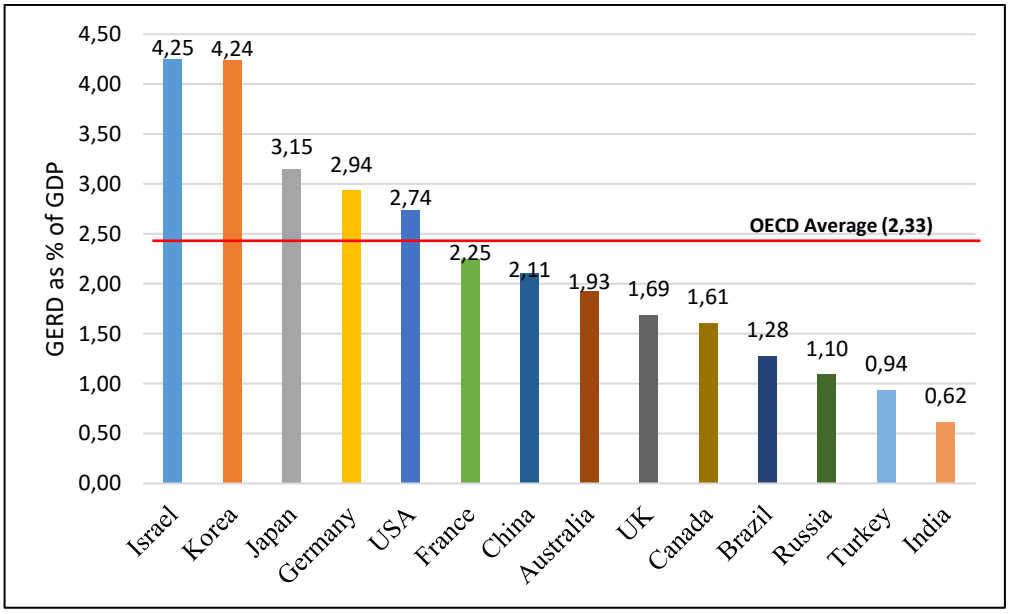


Figure 34: GERD for Cybersecurity Leaders and Turkey (2016)

5.8.2.7 Turkish National Science, Technology and Innovation Indicators

Among Turkish national, science, technology and innovation indicators, GERD as a percentage of GDP, R&D personnel headcount details and GERD as a percentage of GDP in years can be seen in Table 97, in Figure 35 (TÜBİTAK, 2018) and in Table 98 (TUİK, 2018).

R&D investments for cybersecurity and related sectors and the number of people working for cybersecurity industry are very important to penetrate and dominate the cybersecurity markets in the world.

Table 97: GERD Details of Turkey

		2015	2016	2017
GERD / GDP (%)		0,88	0,94	0,96
Total R&D Expenditure (TL)		**20,6**	**24,6**	**29,8**
	Labor costs (Turkish Lira -TL)	11,0	12,3	15,1
	Other current cost (TL)	7,2	9,5	11,6
	Capital cost (TL)	2,4	2,8	3,1
General government		**21,3**	**23,4**	**28,6**
	Labor costs (TL)	9,8	11,0	12,2
	Other current cost (TL)	6,0	8,0	10,7
	Capital cost (TL)	5,5	4,3	5,7
Higher education sector		**8,2**	**8,9**	**10,0**
	Labor costs (TL)	4,8	4,8	5,0
	Other current cost (TL)	2,5	2,9	3,6
	Capital cost (TL)	0,8	1,2	1,4

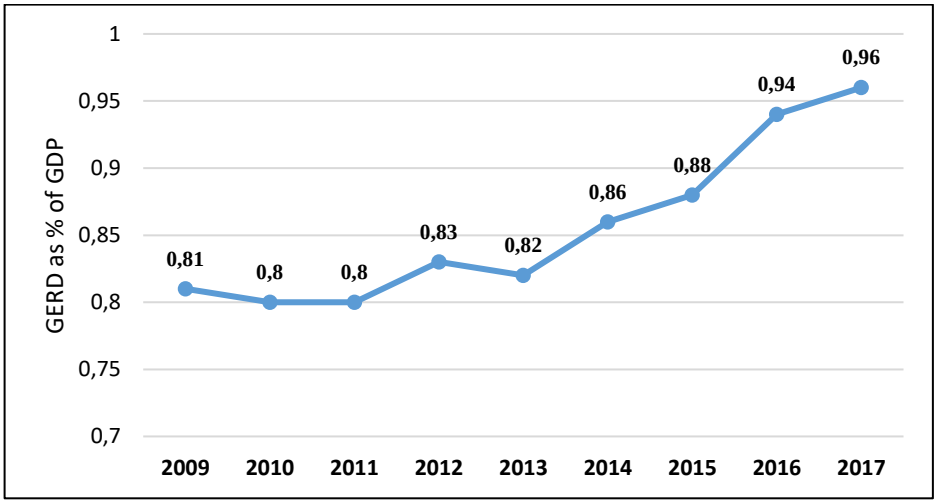


Figure 35: GERD as a Percentage of GDP for Turkey

Table 98: Details of R&D Personnel Headcounts in Turkey

		2015	2016	2017
R&D personnel (Headcount)		**224 284**	**242 213**	**266 478**
	Financial and non-financial corporations	77 551	83 873	101 404
	General government	14 217	13 372	12 828
	Higher education sector	132 516	144 968	152 246
R&D personnel (Full Time Equivalent)		**122 288**	**136 953**	**153 552**
	Financial and non-financial corporations	66 667	72 579	87 918
	General government	12 328	11 799	11 345
	Higher education sector	43 293	52 576	54 289

5.8.2.8 Others

Other signposts can be inferred from the identified key drivers. Substantial changes in the following key drivers will directly affect the success of the investments and decisions in terms of cybersecurity domain:

- The political and economic stability of Turkey
- Stability within Turkey's neighborhood (Middle East, Caucasia, Balkans)
- Fluctuation and decreasing demands in cybersecurity product and service market
- Global economic stability
- Stability of global security and peace
- New powerful foreign competitors as new actors in the global cybersecurity market
- Nations deciding domestic and national cybersecurity software, hardware and services
- The outbreak of global monopolies in cybersecurity domain.

5.8.3 Scenarios

According to the results of the key drivers and uncertainties analysis, four scenarios were created along with two axes as shown in Figure 36.

"Commitment of Turkey" encompasses all the drivers that are related to Turkey's desire, resolution and real steps to attain the cybersecurity vision while "Global Security and Stability" refers to the drivers related to the environment in which Turkey has to face challenges while progressing towards the achieving cybersecurity goals.

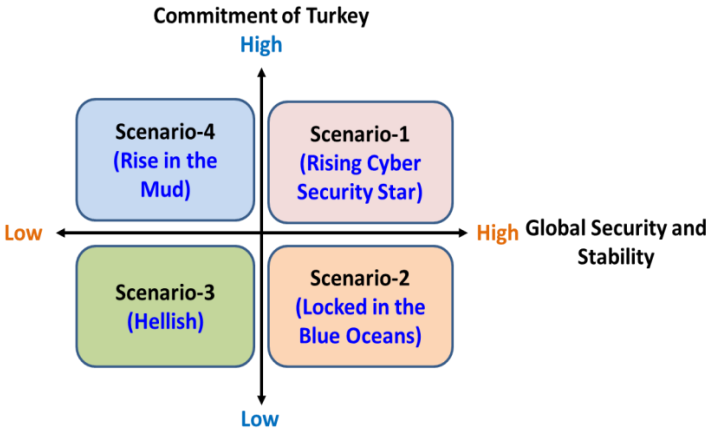


Figure 36: Driving Forces Axes and Scenarios

5.8.3.1 Scenario-1: Rising Cybersecurity Star

- The commitment of Turkey: Turkey has increased the expenditure on R&D, especially for cybersecurity technologies and product development activities. GERD as a percentage of GDP is over OECD countries' average and it is nearly 2.5%. R&D personnel headcount has been doubled in all sectors (higher education, industry, and government) and cybersecurity became the leader sector among high tech sectors. The country became security service and product exporter owing to the investments and incentives in both hardware and software projects directly or indirectly influencing cybersecurity domain. Turkey's political and economic conditions are stable. It attracts experienced scientist from world.

- Global Security and Stability: Global economy is in a stable condition while there is competition between economic leaders such as the USA, China, Germany, and Japan. There is no conventional war between countries in the world that can have adverse effects on the markets. There is no big scale conflict in the vicinity of Turkey except for small-scale terrorist activities that do not influence

Turkey's penetration into the cybersecurity markets within the border countries and all over the world.

5.8.3.2 Scenario-2: Locked in the Blue Oceans

- The commitment of Turkey: Turkey is trying to invest in cybersecurity projects but there is not enough budget assigned to the R&D for high technologies, especially for cybersecurity domain. GERD is stuck around 1%. The national education system and academia do not have enough motivation and effort to raise skillful generations and to foster scientific developments. Government is trying to incentivize cybersecurity ventures just to survive the sector but not for a breakthrough that requires high resources in terms of experienced workforce and substantial funds. The country is stable in terms of political governance while there are problems in terms of the act of law and human rights that keep foreign entrepreneurs away from investing in Turkey.

- Global Security and Stability: It is same as in Scenario-1.

5.8.3.3 Scenario-3: Hellish

- The commitment of Turkey: It is same as in Scenario-2.

- Global Security and Stability: There are excessive fluctuations in the macroeconomic systems and indicators. The global financial system is not working properly. Countries took strict decisions in order to use national cybersecurity products that hinder or complicate foreign countries' entrance into the markets. There are conflicts especially in the border countries or in the regions where Turkey has an influence on cultural, political and hence economic dimensions.

5.8.3.4 Scenario-4: Rise in the Mud

- The commitment of Turkey: It is same as in Scenario-1.

- Global Security and Stability: It is same as in Scenario-3.

5.8.3.5 Allocation of Delphi Statements to Scenarios:

Delphi statements were allocated to the scenarios as shown in Table 99.

Table 99: Scenario – Delphi Statement Allocation

Scenario	Statements
Scenario-1	All of 91 Delphi statements
Scenario-2	Top 47 Delphi statements (these statements were chosen by focus group experts)
Scenario-3	Top 25 Delphi statements 7 of 25 statements (D-3, D-11, D-21, D-23, D-30, D-31, D-47) deferred to the next time frames
Scenario-4	All of 91 Delphi statements 9 of 91 statements (D-3, D-11, D-21, D-23, D-30, D-31, D-47, D-89, D-90) deferred to the next time frames

Scenario-1: All of the Delphi statements (91 statements) are included in this scenario.

Scenario-2: Since commitment of Turkey is low, only the top 47 Delphi statements, which were handled within the focus group, are included in this scenario.

Scenario-3: This is the worst case because both Turkey's desire to reach the cybersecurity vision is low and global security and economic conditions are inconvenient. Only top 25 Delphi statements, which were sent to Delphi survey, are included in this scenario. Furthermore, realization timeframe of Delphi statements that require integration with international organizations and penetration into the global cybersecurity markets are deferred to the next timeframe. For example, D-23 (*Cybersecurity tools and mechanisms through software modules and systems have been developed, and these products have at least 5 % of the world market dominated.*) requires penetration into the global cybersecurity market and since global security and stability is low, the timeframe of D-23 is

deferred from 2024-2029 to 2030-2035. The statements that conform to this case are D-3, D-11, D-21, D-23, D-30, D-31, and D-47.

Scenario-4: Since Turkey's commitment is high, all of the Delphi statements (91 statements) are included in this scenario. On the other hand, as in Scenario-3, because of the global security and stability is low, realization timeframe of Delphi statements that require integration with international organizations and penetration into the global cybersecurity markets are deferred to the next timeframe. The statements that conform to this case are D-3, D-11, D-21, D-23, D-30, D-31, D-47, D-89, and D-90.

5.8.4 Cybersecurity Actions for Turkey

Brainstorming method was used to capture the actions to prosper cybersecurity and reach the desired vision. Actions were generated to mitigate the weaknesses of Turkey in terms of cybersecurity, to avoid threats, and to take advantage of opportunities defined in the previous focus group meeting.

Total of 50 actions were defined in workshop. The researcher updated and tweaked the actions based on the results of the analysis on universities and companies. The distributions of the actions based on the factors are depicted in Figure 37.

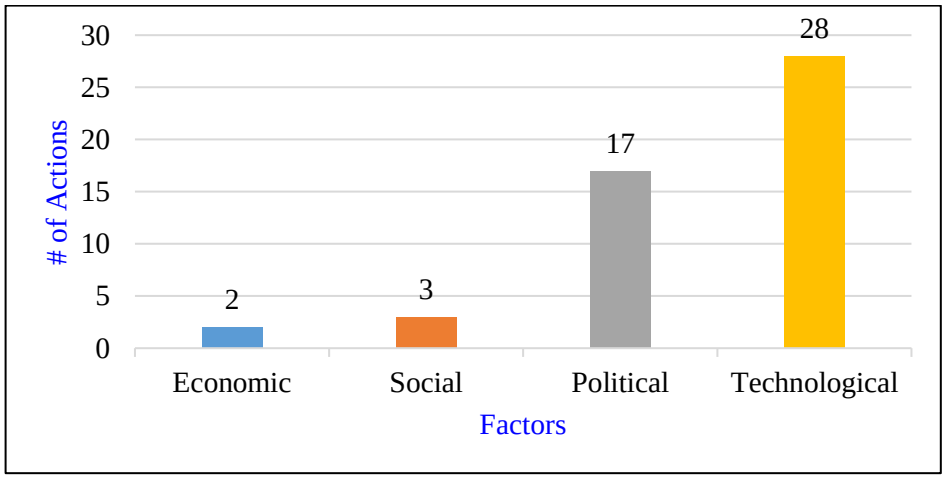


Figure 37: Distributions of the Actions based on the Factors

CHAPTER 6

CONCLUSION

The fundamental aim of this thesis is to carry out technology foresight for Turkey in the following 20 years until the year 2040 and to decide solid policy recommendations according to the results of cybersecurity technology foresight by applying generic foresight model FPM (Foresight Periscope Model) and FORESIGHT framework created by Yüksel and Çifci (2017). In the study, trend analysis, Delphi survey, focus group, and scenario techniques are used as underlying foresight methods.

Technology is penetrating into every part of daily life, reliance on technological appliances and breakthroughs is expanding and this reliance conveys new vulnerabilities and threats to security. Cyberspace, which is the domain that connects networks and systems, becomes a vital area and the target of the emerging threats. As the cyberspace grows into the far-flung network, security aspects (i.e. cybersecurity) culminated to protect the systems and to maintain the availability. Cybersecurity is the measures and activities to protect cyberspace from the threats and provide information and information systems available, integral and confidential.

Cybersecurity is one of the fastest growing and largest technology sectors. According to the forecasts on cybersecurity economy over the next years from various sources, global spending on cybersecurity products will exceed one trillion dollars and the need for cybersecurity professionals will increase.

Cyberspace is a borderless environment that connects all actors including individuals, organizations, systems, and nations. cybersecurity becomes the priority issue because of the growing dependence on cyberspace. Number,

severity, and complexity of cyber attacks and cyber threats are increasing gradually. Proper cybersecurity strategy is essential in order to manage risks, to counter cyber attacks, to protect people's, organizations' and country's privacy and security in the cyberspace, to retain business operations, to maintain connection with the world and to survive in the digital domain. In order to preserve the ability to leverage cyberspace, it is essential to develop policies, strategies, and plans to address cybersecurity.

In Turkey, cybersecurity field was paid attention in the government level for almost 15 years and it can be stated that official projects and actions were started by e-Transformation Turkey Project back to 2003 (Çifci, 2017). Later on, several studies were carried out until today. The most important steps related to cybersecurity are Turkey's National Cybersecurity Strategy and Action Plan 2013-2014 and National Cybersecurity Strategy and Action Plan 2016-2019. The methodology of the mentioned works was meetings, workshops, seminars and conferences with experts, which lacks technology foresight methodologies.

Technology Foresight (TF) is a standardized approach of looking into long-run future of science, technology, economy, and society to determine strategic research areas and identify emerging technologies that may bring significant economic and social gains (Martin, 1995). Yüksel and Çifci (2017) define foresight as "a systematic and multidisciplinary process with proper methodology combinations for identifying technological, economic and social areas to prioritize investments and research in order to determine medium or long term future strategies by using all level of resources from organizational to international". TF provides approaches to specify indispensable science and technology topics, it suggests means to integrate research and development activities with economic and social needs and it helps interaction and common understanding among TF participants (Martin & Johnston, 1999).

In the literature and practice, there are diverse TF approaches, frameworks, and models to follow in foresight studies. Foresight Periscope Model (FPM), which is developed by Yüksel and Çifci (2017), is a new technology foresight approach, which has three interdependent modules, Resources, Methodology and Futures

Strategies. The model is inspired by periscope's modules, that is, "resources" and "methodology" are underside modules that enable an organization to see alternative futures and provide "futures strategies" to follow in order to survive and compete in the environment. A generic foresight functional framework with nine sequential steps (Framing, Obtaining, Reviewing, Establishing, Synthesizing, Illustrating, Guiding, Handling, Tracking) named 'FORESIGHT' is also developed by Yüksel and Çifci (2017) to be used in integration with FPM. Functions in the FORESIGHT framework are matched with the steps of common foresight frameworks in the literature with respect to their actions and artifacts within specific steps.

FORESIGHT framework does not enforce specific methods for the foresight activities. However, a bunch of suitable methods is suggested within each functional stage to carry through the activities needed in the stages.

FPM is a foresight model that simplifies foresight activities from the start to the finish. Similar to the periscope device used in submarines, the model aims to determine future strategies as clearly as possible by depending on the resources and methodologies underside. "Angle of sight" refers to "scope of foresight", "range" refers to "time horizon of foresight", "resolution capacity" implies "effective determination of alternative futures" and "skillful and trained users" match with "foresight experts". In the FPM, tangible and intangible resources and their footprints in organizational, sectoral, national and international levels are the determining factors of the methods. Selection of proper method combinations is highly reliant on the resources and the nature of the foresight study. Future strategies are the alternative futures among which the desired or the possible future exists. "Resources" constitutes the base of the model, "methodology" is selected according to the resources, aim and scope of the foresight study and "future strategies" are determined based on the results of the activities performed through chosen methodology. FPM does not impose or enforce a specific means and methods to tackle and oversee the futures strategies. Suitable methods suggested in the FORESIGHT framework steps can be utilized to identify, create, carry out and track the future strategies.

The needs of organizations and technological developments shape foresight generations. Foresight has been divided into five generations in the literature based on goal, scope, methods, actors, and context. Any exercise of foresight may have the characteristics of one or more generations. Çifci and Yüksel (2018) suggest new (sixth) foresight generation, named Foresight 6.0, focusing on Industry 4.0 and beyond, Society 5.0, netocracy, cyberspace, biotechnology and more values and ethics in a chaordic social dimension. Prevalence of cyberspace through networks and increasing power of communication through internet makes the netocracy be rising management concept in networked societies. This generation provides more effective implementation of foresight exercises through facilitating the participation of diverse stakeholders on global scope through the network. Foresight data can be obtained online; big data can be utilized. This new foresight generation also utilizes artificial intelligence and machine learning within the foresight process.

In this study, cybersecurity technology list and technology taxonomy were created using technology taxonomy of Turkish Presidency of Defense Industries (Savunma Sanayii Başkanlığı -SSB), cybersecurity technology and product taxonomy of the Scientific and Technological Research Council of Turkey (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu -TÜBİTAK) and cybersecurity product lists of international companies. Cybersecurity technology taxonomy, which has 169 underpinning technologies under 15 system-related technologies and 6 systems/product technologies, was created in order to have the most extensive and inclusive list under right categories that can address the academic and industrial cybersecurity technology and product lists. List of technologies was sent to experts for prioritization. 169 cybersecurity technologies were weighted against the three criteria (meeting national security needs; supporting the development of the national science, technology and innovation infrastructure; world-class competitiveness, collaboration or mutual dependence).

Total three focus group meetings were conducted throughout the study with the participation of nearly 25 different experts from Turkish Armed Forces, government, academia, and cybersecurity companies.

The first focus group meeting was held in the SSB's facilities with the participation of 17 experts. Vision study, SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, STEEPLE (Social, Technological, Economic, Environmental, Political, Legal, and Ethical) analysis and cybersecurity trends survey have been achieved in the meeting.

Cybersecurity vision of Turkey was set by the experts as: To become an export-oriented and self-sufficient country, with the domestic and national cybersecurity technologies, having a strong cyber army, a center of education and innovation, where cybersecurity awareness is spread to the public.

Participants prioritized the researcher's pre-written SWOT issues and were encouraged to add their statements. Following the meeting, the issues were sorted by the researcher according to the participants ' priority scores. Turkey's weaknesses are more than the strengths, according to the results, while opportunities are much more than threats, on the other hand. Total 119 (17 strengths, 31 weaknesses, 56 opportunities, and 15 threats) issues were defined.

STEEPLE factors for cybersecurity were prepared by the researcher and then participants were asked to add new ones and prioritize all issues during the meeting. According to the results, total of 85 factors (17 social, 30 technological, 14 economic, 3 environmental, 14 political, 5 legal and 2 ethical) were identified by the researcher and participants. Technological factors have the highest proportion while the lowest are ethical factors.

According to the trends survey, which is performed in the first focus group meeting, Turkey will not be among the top 10 cyber attackers while it will be at 4th rank in terms of cyber attack targets. Cyber espionage, information leakage, data breaches, ransomware, malware, phishing, cyber espionage, denial of service, botnets, web-based attacks, identity theft, and web application attacks would be among the top attack types. Government, energy, telecom, banking and finance, armed forces, defense industry, critical infrastructures, health, technology, transportation, manufacturing and medicine sectors will be the target of attacks. Cloud computing, big data, artificial intelligence, IoT, deep learning, machine

learning, blockchain, wireless, quantum computing, cognitive computing, wearable devices, smart things (appliances, workspace, houses, cars, cities etc.), micro data centers, brain-computer interface, commercial unmanned air vehicles, autonomous vehicles and virtual reality are among the technologies that affect the cybersecurity technologies.

After the first focus group meeting, the researcher created Delphi statements based on the participants' cybersecurity technology scores. The researcher wrote Delphi statements in a way to include selected top-scored technologies. In order to address as many technologies as possible, similar technologies were grouped.

The second meeting of the focus group was held again with the participation of 14 experts in the facilities of the SSB. This meeting was devoted to the Delphi exercise. Participants reviewed the 37 Delphi statements of the researcher in the workshop. They were also urged to cover all of the 169 technologies that they think a capability shall be attained based on those technologies. During the workshop, participants added 54 additional Delphi statements.

Delphi statements resulting from the second focus group meeting were sent by e-mail to the experts and they answered to the questions per statements. The 37 statements of the researcher and 10 statements selected from the focus group meeting (total 47 statements) were evaluated. Delphi statements have been prioritized by the experts. 25 statements were selected for the Delphi survey after the evaluations of the focus group.

In the study, a two-round Delphi survey was completed through internet. Nearly 1,900 people were reached. Using Google Forms, the survey was conducted. 25 Delphi statements were sent to the voting participants. Contribution to the economy and contribution to security were scored from 1 to 5, the timeframe of realization and methods of realization were also requested.

The first round of Delphi survey took place between 17 July and 12 August 2018. E-mail addresses of faculty members of computer engineering departments in Turkish universities were collected by researcher through official university

websites in order to reach as many participants as possible for the survey. In addition, during cybersecurity conferences and events in Turkey, the researcher collected business cards from cybersecurity experts within the timeframe of the thesis. Besides these, the contact addresses of new participants were provided by experts and friends informed about the study. Total about 1,900 participants were reached for the survey. Total of 150 people responded the first round of the survey.

The second round of Delphi survey was completed with the same participants between 28 August and 26 September 2018. Total 91 participants out of 150 responded to the second round of the survey.

According to the results, consensus between the Delphi rounds was attained. Reliability analysis of the factors formed by the questions in the questionnaire was investigated by Cronbach's Alpha values by utilizing SPSS Statistics software. Reliability of the first round was 0.952 (Cronbach's Alpha) while it is 0.937 in the second round, which reveals the variables are measured reliably in the survey. Statements' contribution to security scores ranged from 4.3 to 4.9 while it is 3.9 to 4.6 for economy scores. As the result of this study, the prioritization of 25 Delphi statements based on their contribution to security and economy scores, and timeframe and methods of realization per statement were obtained.

An analysis was performed to find out the cybersecurity-related courses and programs in order to discover the conditions and circumstances of Turkish universities in the cybersecurity field. In Turkey, 114 universities have computer engineering, computer sciences, informatics engineering or software engineering departments as of 2019. Total 10 universities have a two-year vocational degree (associate degree) on information security technologies. The four-year departments have generally "hardware" and "software" sections while one university has digital forensics and three have cybersecurity or informatics security options under Bachelor of Science (BS) programs. 77% of universities (88 of 114) have cybersecurity related courses in the syllabus of undergraduate programs. In 2018-2019 Fall and Spring semesters, there are 171 cybersecurity related courses in undergraduate programs (67 of them are unique) with 34 different cybersecurity topics. 20 universities have cybersecurity-related graduate programs (MS and

Ph.D.) and three of them have Ph.D. programs while others have only MS programs. There are 322 cybersecurity related courses (215 of them are unique) in graduate programs (MS and Ph.D.) with 114 different cybersecurity topics. Network security, cryptology, information security, cybersecurity, data security, and information systems security are the courses that are mostly taught at Turkish universities' undergraduate and graduate programs.

Companies in Turkey were also analyzed to discover whether they have cybersecurity products or they are in cybersecurity service sectors. Almost 3,000 companies' web pages were visited to compile the data for the study. According to the results, there are 90 companies that have cybersecurity products and 96 companies that have cybersecurity services, which makes a total 186. Most of the products are related to Network Security, Identity & Access Management, Cybersecurity Event Management, Internet Security, Cyber Intelligence, Cybersecurity Risk and Compliance Management and Data Security. Companies are not dealing with some cybersecurity technology groups such as Industrial Control (SCADA) Systems Security, Operating Systems and Container Security, Cybersecurity for Autonomous and Smart Platforms and Hardware Security groups. When it comes to cybersecurity services, Consultancy, Cybersecurity Risk and Compliance Management, Training and Network Security are the most common services while there is no service in Industrial Control Systems Security, Operating Systems and Container Security, Cybersecurity for Autonomous and Smart Platforms, Hardware Security and Firmware Security fields.

Turkish Cybersecurity Cluster (Türkiye Siber Güvenlik Kümelenmesi) was created by SSB in 2018 to support cybersecurity companies in Turkey. Almost half of the companies (95 of 186) are the member of the cluster while the membership process is still proceeding. There are 61 active technology development regions (science and technology parks i.e. technoparks) in Turkey. There are cybersecurity companies in just about half of the technoparks. Turkish Cybersecurity Cluster's financial turnover is about $300 million and the objective is to double this number in 2019. These companies' export revenue is $41 million. The average age of the companies is six and they have nearly 4,400 personnel.

Scenario and action workshop was conducted with five experts on 17 December 2018. Key drivers, which are substantial trends that are out of our control, were defined. Then uncertainties and impacts of the key drivers were identified to determine the alternative scenarios. Signposts, which are not decisive but reasonable indicators, metrics or conditions, were suggested to reveal which scenario path is unfolding at the current time. Global Cybersecurity Index, Global Innovation Index, Gross Domestic Expenditure on R&D (GERD) and R&D Personnel Counts are the examples of the signposts. Four scenarios were created along with two axes named "Commitment of Turkey" and "Global Security and Stability". "Commitment of Turkey" includes all the drivers related to Turkey's aspiration and real paces to reach the cybersecurity vision while "Global Security and Stability" refers to the worldwide drivers in which Turkey has to confront challenges and take risks while reaching the cybersecurity objectives. Scenarios were named as Rising Cybersecurity Star, Locked in the Blue Oceans, Hellish, and Rise in the Mud. Delphi statements were apportioned to the scenarios based on the conditions, resources, and political and economic power to accomplish the capabilities implied in the statements. Apart from the scenarios containing Delphi statements (i.e. cybersecurity capabilities), action items to improve cybersecurity in Turkey were delineated. Total 50 actions were defined to overcome the weaknesses and threats, and to take advantage of strengths and opportunities.

According to the results of the study, it can be seen that there is a long way for Turkey to attain the goals of cybersecurity technologies, education, products and services and research and development. In order to reach the vision defined within the scope of the study, it is necessary to carry out the determined action items in a pertinacious manner and to perform the works and investments related to the capabilities and technologies in the roadmaps included in the scenarios. In addition, it is vital that technology foresight studies for cybersecurity should be regularly repeated and necessary corrections and improvements should be applied by evaluating the results of the projects, initiatives, and investments.

REFERENCES

Akaike, S. (2016). Foresight and evidence based policy making in Japan. *The 2nd Asian Innovation Forum (AIF)*, 1–35. Retrieved from www.asianinnovation.org/!Board/down.php?wd=1&bf_code=78

Aktharsha, U. S. (2010). A Theory of Knowledge Management. *Journal of Contemporary Research in Management*, *5*(3), 103–119. Retrieved from http://adh.sagepub.com/content/2/1/38.short

Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures*, *46*(Summer), 23–40. https://doi.org/10.1016/j.futures.2012.10.003

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

BMBF. (2018). BMBF Foresight. Retrieved October 26, 2018, from https://www.bmbf.de/en/bmbf-foresight-1419.html

Cambridge Dictionary. (2018). Framework. Retrieved October 18, 2018, from https://dictionary.cambridge.org/dictionary/english/framework

Casas, L., & Talavera, B. (2008). Future-Oriented Technology Analysis (FTA) - Impacts and Implications for Policy and Decision Making. In *Book of abstracts from the 3rd International Seville Conference on Future-Oriented Technology Analysis (FTA)* (pp. 1–222). https://doi.org/10.2791/50885

Chen, H., Wakeland, W., & Yu, J. (2012). A two-stage technology foresight model with system dynamics simulation and its application in the Chinese ICT industry. *Technological Forecasting and Social Change*, *79*(7), 1254–1267. https://doi.org/10.1016/j.techfore.2012.02.007

Chen, S., & Chang, B.-G. (2012). The Effects of Absoprtive Capacity and Decision Speed on Organizational Innovation: A Study of Organizational Structure as an Antecedent Variable. *Contemporary Management Research*, *8*(1), 27–50. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=76286684&site=ehost-live

Choi, M., & Choi, H. (2015). Foresight for Science and Technology Priority Setting in Korea. *Foresight and STI Governance*, *9*(3), 54–65. https://doi.org/10.17323/1995-459X.2015.3.54.65

Ciarli, T., Coad, A., & Rafols, I. (2013). *Quantitative Analysis of Technology Futures. Part 1: Techniques, Contexts, and Organizations*.

Çifci, H. (2017). *Her Yönüyle Siber Savaş* (2'nd Ed.). Ankara: TÜBİTAK.

Çifci, H., & Yüksel, N. (2018). Foresight 6.0: The New Generation of Technology Foresight. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1–5). https://doi.org/10.1109/ICE.2018.8436350

Coates, V., Farooque, M., Klavans, R., Lapid, K., Linstone, H. A., Pistorius, C., & Porter, A. L. (2001). On the Future of Technological Forecasting. *Technological Forecasting and Social Change*, *67*(1), 1–17. https://doi.org/10.1016/S0040-1625(00)00122-0

Conway, M. (2015). *Foresight: an Introduction*. Thinking Futures.

Cuhls, K. (2003a). From forecasting to foresight processes—new participative foresight activities in Germany. *Forecast*, *22*, 93–111. https://doi.org/10.1002/for.848

Cuhls, K. (2003b). Government Foresight Activities in Germany: The Futur Process. *Institute for Systems and Innovation Research*.

Cuhls, K. (2010). The German BMBF Foresight Process. *European Foresight Platform*, (174).

Cuhls, K. (2016). The role of foresight in identifying and responding to grand challenges. Fraunhofer.

Cyber Security Council. (2016). European Foresight Cyber Security Meeting.

Dalkey, N. C. (1969). *The Delphi Method: An experimental study of group opinion*. *Futures* (Vol. 1). https://doi.org/10.1016/S0016-3287(69)80025-X

Davenport, T. H., & Prusak, L. (1998). Working knowledge: How organizations manage what they know. *IEEE Engineering Management Review*.

https://doi.org/10.1109/EMR.2003.1267012

Department for International Trade. (2017). *UK Defence and Security Export Statistics 2016*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/631343/UK_defence_and_security_export_statistics_2016_Final_Version.pdf

Dreyer, I., & Stang, G. (2013). Foresight in governments – practices and trends around the world. *Yearbook of European Security YES 2013*, 7–32.

Durance, P., & Godet, M. (2010). Scenario building: Uses and abuses. *Technological Forecasting and Social Change*, *77*(9), 1488–1492. https://doi.org/10.1016/j.techfore.2010.06.007

Dutta, S., Lanvin, B., & Wunsch-Vincent, S. (2018). *Global Innovation Index 2018*. Retrieved from https://www.globalinnovationindex.org

ENISA. (2012). National Cyber Security Strategies - Practical Guide on Development and Execution, (December), 15. https://doi.org/10.2824/3903

European Commission. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *European Commission*, 20. https://doi.org/10.4271/2010-01-1021

Eurostat. (2018). GDP. Retrieved January 2, 2019, from https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Gross_domestic_expenditure_on_R_%26_D_(GERD)

Fortune. (2016). Lloyd's CEO: Cyber attacks cost companies $400 billion every year. Retrieved June 9, 2017, from http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds

French Government. (2018). Key Technologies 2020. Retrieved November 8, 2018, from https://www.entreprises.gouv.fr/politique-et-enjeux/technologies-cles-2020

Georghiou, L., Harper, J. C., Keenan, M., Miles, I., & Popper, R. (2008). *The Handbook of Technology Foresight: Concepts and Practice*. Cheltenham, UK: Edward Elgar Publishing, Inc.

Georghiou, L., & Keenan, M. (2006). Evaluation of national foresight activities: Assessing rationale, process and impact. *Technological Forecasting and Social Change*, *73*(7), 761–777. https://doi.org/10.1016/j.techfore.2005.08.003

Glenn, J. C. (1994). Introduction to the Futures Research Methods Series. *Futures Research Methodology - Version 2.0*, 1–45. Retrieved from http://mp.cim3.net/file/project/mp-sofi-sd/reference/01-Introduction.PDF

Globes-Israel. (2016). Israeli cybersecurity grabs 8% global market share. Retrieved December 23, 2018, from https://en.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669

Godet, M. (2000). The Art of Scenarios and Strategic Planning: Tools and Pitfalls. *Technological Forecasting and Social Change*, *65*(1), 3–22. https://doi.org/10.1016/S0040-1625(99)00120-1

Godet, M., & Roubelat, F. (1996). Creating the future: The use and misuse of scenarios. *Long Range Planning*, *29*(2), 164–171.

Goffin, K., & Mitchell, R. (2010). *Innovation Management - Strategy and Implementation using the Pentathlon Framework*. Palgrave Macmillan.

Government Office for Science. (2017). Technology and Innovation Futures 2017, 194. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288571/10-1252an-technology-and-innovation-futures-annex.pdf

Grand View Research. (2018). Cyber Security Market Research Report. Retrieved December 23, 2018, from https://www.grandviewresearch.com/industry-analysis/cyber-security-market

Grupp, H., & Linstone, H. A. (1999). National technology foresight activities around the globe: Resurrection and new paradigms. *Technological Forecasting and Social Change*, *60*(1), 85–94. https://doi.org/10.1016/S0040-1625(98)00039-0

Haegeman, K., Marinelli, E., Scapolo, F., Ricci, A., & Sokolov, A. (2013). Quantitative and qualitative approaches in Future-oriented Technology Analysis (FTA): From combination to integration? *Technological Forecasting and Social Change*, *80*(3), 386–397. https://doi.org/10.1016/j.techfore.2012.10.002

Haig, Alexander M., J. (1984). *Caveat: Realism, Reagan, and Foreign Policy*. London: Weidenfeld and Nicolson.

Hammett, P. (2005). Strategic Foresight: A Critical Leadership Competency. *Leadership Advance Online*, (IV), 1–7.

Hao, Q. M., Kasper, H., & Muehlbacher, J. (2012). How does Organizational Structure Influence Performance Through Learning and Innovation in Austria and China. *Chinese Management Studies*, *6*(1), 36–52. https://doi.org/10.1108/17506141211213717

Harayama, Y. (2016). Society 5.0: Aiming for a New Human-centered Society. *Japan SPOTLIGHT*, *27*(July / August 2088), 8–13.

Harper, J. C. (2013). *Impact of Technology Foresight*. *NESTA Compendium of Evidence on Innovation Policy Intervention*.

Hines, A. (2016). Let 's Talk about Success: A Proposed Foresight Outcomes Framework for Organizational Futurists. *Journal of Futures Studies*, *20*(4), 1–20. https://doi.org/10.6531/JFS.2016.20(4).A1

Hines, A., & Bishop, P. (2007). *Thinking about the Future:Guidelines for Strategic Foresight*. Washington, DC: Social Technologies LLC.

Hines, A., & Bishop, P. C. (2013). Framework foresight: Exploring futures the Houston way. *Futures*, *51*, 31–49. https://doi.org/10.1016/j.futures.2013.05.002

Hiratsuka, H. (2016). The 5th Science and Technology Basic Plan and Gunma University. *The Journal of the Institute of Electrical Engineers of Japan*, *136*(8), 519–519. https://doi.org/10.1541/ieejjournal.136.519

Horton, A. (1999). A Simple Guide to Successful Foresight. *Foresight*, *1*(1), 5–9.

IBM. (2018). IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses. Retrieved November 12, 2018, from https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

Inayatullah, S. (2001). Epistemology and Methodology in the Study of the Future. *Global Transformations and World Futures*, *II*.

ITU. (2015). Index of Cybersecurity Indices. Retrieved December 23, 2018, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf

ITU. (2017). *Global Cybersecurity Index 2017*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2018a). ICT Development Index 2017. Retrieved December 25, 2018, from http://www.itu.int/net4/itu-d/idi/2017/index.html

ITU. (2018b). The ICT Development Index (IDI): conceptual framework and methodology. Retrieved December 25, 2018, from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx

Jemala, M. (2010). Evolution of foresight in the global historical context. *Foresight*, *12*(4), 65–81. https://doi.org/10.1108/14636681011063004

Keidanren. (2016). Toward realization of the new economy and society. *Policy & Action*. Retrieved from http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf

KISTEP. (2017). *The 5 th Science and Technology Foresight (2016-2040)*. Seoul. Retrieved from http://www.kistep.re.kr/en/

KISTEP. (2018a). Foresight and Future Strategy for Science & Technology. Retrieved October 27, 2018, from http://www.kistep.re.kr/en/c2/sub1.jsp

KISTEP. (2018b). KISTEP 10 Emerging Technologies. Retrieved October 27, 2018, from http://www.kistep.re.kr/en/c3/sub4.jsp?

Linstone, H. A. (2011). Three eras of technology foresight. *Technovation*, *31*(2–3), 69–76. https://doi.org/10.1016/j.technovation.2010.10.001

Loveridge, D. (1996). Technology foresight and models of the future. In *CEC ASTPP Network Conference Ideas in Progress*. Rovaniemi. Retrieved from https://php.portals.mbs.ac.uk/Portals/49/docs/dloveridge/futmodpdf%7B_%7Dwp4.PDF

Luhmann, N. (2006). System as difference. *Organization*, *13*(1), 37–57.

Marciano, V. M. (1995). The Origins and Development of Human Resource Management. *Academy of Management Journal*, *1995*(1), 223–227.

Martin, B. R. (1995). Foresight in science and technology. *Technology Analysis and Strategic Management*, *7*(2), 139–168.

Martin, B. R. (2001). Technology Foresight in a Rapidly Globalizing Economy. In *International Conference on Technology Foresight for Central and Eastern Europe and the Newly Independent States*. Vienna.

Martin, B. R. (2010). The origins of the concept of "foresight" in science and technology: An insider's perspective. *Technological Forecasting and Social Change*, *77*(9), 1438–1447. https://doi.org/10.1016/j.techfore.2010.06.009

Martin, B. R., & Johnston, R. (1999). Technology Foresight for Wiring Up the National Innovation System-Experiences in Britain, Australia, and New Zealand. *Technological Forecasting and Social Change*, *60*(1), 37–54. https://doi.org/10.1016/S0040-1625(98)00022-5

McAfee. (2015). *Threat Reports - August*. Retrieved from www.mcafee.com

Meredith, J. R., & Mantel, S. J. (1995). Technological Forecasting.

Miles, I. (2002). Appraisal of Alternative Methods and Procedures for Producing Regional Foresight. *Mobilising the Regional Foresight Potential for an Enlarged EU*, (May).

Miles, I., & Keenan, M. (2002). *Practical Guide To Regional Foresight in the UK*.

Miles, I., & Keenan, M. (2003). Overview of Methods used in Foresight. In *Technology Foresight for Organizers* (pp. E1–E16). Ankara: UNIDO SCIENTIFIC AND TECHNICAL RESEARCH COUNCIL OF TURKEY (TÜBİTAK).

Ministère De L'Économie. (2017). Technologies Clés 2020 Préparer L'Industrie Du Futur. *Ministère De L'Économie*.

Ministry of Transport and Infrastructure. (2012). *National Cyber Security Strategy and 2013-2014 Action Plan*. Ankara. Retrieved from http://www.ubak.gov.tr/

Ministry of Transport and Infrastructure. (2016). *National Cyber Security Strategy*

2016-2019. Ankara. Retrieved from http://www.ubak.gov.tr/

Misa, T. J. (2009). *History of Technology*. *A Companion to the Philosophy of Technology*. West Sussex, UK: Blackwell Publishing.

Molas-Gallart, J. (1997). Which way to go? Defence technology and the diversity of 'dual-use'' technology transfer.' *Research Policy*, *26*, 367–385. https://doi.org/10.1016/S0048-7333(97)00023-1

Moll, P. (1996). The Thirst for Certainty: Futures Studies in Europe and the United States. *Knowledge Base of Futures Studies*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Thirst+for+Certainty:+Futures+Studies+in+Europe+and+the+United+States#0

Morgan, S. (2017). Cybersecurity Ventures. Retrieved June 4, 2017, from http://cybersecurityventures.com/

Nah, F., Siau, K., Tian, Y., & Ling, M. (2002). Knowledge Management Mechanisms in E-Commerce: A Study of Online Retailing and Auction Sites. *Journal of Computer Information Systems*, *42*(5), 119–128. https://doi.org/10.1080/08874417.2002.11647616

National Research Center for Science and Technology for Development. (2005). *China's Report of Technology Foresight*. Retrieved from www.foresight.org.cn

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *NIST*, 1–41. https://doi.org/10.1109/JPROC.2011.2165269

NISTEP. (2010). *The 9th Delphi Survey*. Tokyo. Retrieved from http://www.nistep.go.jp/HP_E/researchworks/02_foresight/index.html

NISTEP. (2015). *The 10th Science and Technology Foresight*. Tokyo. Retrieved from http://www.nistep.go.jp/HP_E/researchworks/02_foresight/index.html

NISTEP. (2018). Science and Technology Foresight in Japan. Retrieved October 20, 2018, from http://www.nistep.go.jp/en/?page_id=56#target01

Nonaka, I., & Takeuchi, H. (1995). *The Knowledge-Creating Companies: How Japanese Companies Create the Dynamics of Innovation*. New York: Oxford University Press.

OECD. (2018). Gross domestic spending on R&D. Retrieved December 25, 2018, from https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

Office of Science and Technology. (2004). *Foresight Cyber Trust and Crime Prevention Project*.

Ogasawara, A. (2015). 1st Preliminary Report on The 10th Science and Technology Foresight Survey, 1–40. Retrieved from http://www.nistep.go.jp/wp/wp-content/uploads/2-1_Ogasawara.pdf

Okuwada, K. (2010). Toward a new type of science and technology foresight. In *AUGUR Challenges for Europe in the world of 2030 Sharing visions on Europe in 2030: lessons from comparative approaches of recent foresight exercises*. Brussels.

Phaal, R., Farrukh, C. J. P., & Probert, D. R. (2001). Technology Roadmapping: linking technology resources to business objectives. *International Journal of Technology Management*. https://doi.org/10.1504/IJTM.2003.003140

Pherson, R. H. (2015). Strategic Foresight Nine Techniques for Business and Intelligence Analysis. Retrieved from http://www.globalytica.com/wp-content/uploads/2016/03/Strategic-Foresight_Nine-Techniques.pdf

Popper, R. (2008a). Foresight Methodology : an overview and more...

Popper, R. (2008b). How are foresight methods selected? *Foresight*, *10*(6), 62–89. https://doi.org/10.1108/14636680810918586

Popper, R. (2010). Foresight experiences and output in Europe and Latin America.

Popper, R., Georghiou, L., Keenan, M., & Miles, I. (2010). *Evaluating Foresight Fully-Fledged Evaluation of the Colombian Technology Foresight (CTFP)*. Universidad del Valle (Colombia).

Popper, R., Keenan, M., Miles, I., Butter, M., & Sainz, G. (2007). *Global foresight outlook 2007*.

Porter, A. L. (2010). Technology foresight: types and methods. *International Journal of Foresight and Innovation Policy*, *6*(1), 36–45. https://doi.org/10.1504/IJFIP.2010.032664

Porter, A. L., Ashton, W. B., Clar, G., Coates, J. F., Cuhls, K., Cunningham, S. W., … Thissen, W. (2004). Technology futures analysis: Toward integration of the field and new methods. *Technological Forecasting and Social Change*, *71*(3), 287–303. https://doi.org/10.1016/j.techfore.2003.11.004

Rant, M. (2004). How Organizational Structure Affects Organizational Learning Process and Organizational Effectivness? Retrieved from http://proquest.umi.com/pqdweb?did=1500155801&Fmt=7&clientId=3224&RQT=309&VName=PQD

Ray, J. M. (2003). *Designing a Knowledge Management System: A Sensemaking Perspective*. The Pennsylvania State University. Retrieved from http://search.proquest.com.ezproxy.apollolibrary.com/dissertations/docview/305306495/abstract/13D66A22BE227BCB2B0/14?accountid=35812

Reger, G. (2001). Technology Foresight in Companies: From an Indicator to a Network and Process Perspective. *Technology Analysis & Strategic Management*, *13*(4), 533–553.

Ringland, G. (2010). The role of scenarios in strategic foresight. *Technological Forecasting and Social Change*, *77*(9), 1493–1498. https://doi.org/10.1016/j.techfore.2010.06.010

Rodriguez, P. J., & Ordóñez de Pablos, P. (2003). Knowledge management and organizational competitiveness: A framework for human capital analysis. *Journal of Knowledge Management*, *7*(3), 82–91. https://doi.org/10.1108/13673270310485640

Rogers, E. M. (1995). *Diffusion of Innovations*. *New York Free Press*. https://doi.org/citeulike-article-id:126680

Rongping, M., & Zhongbao, R. (2008). Technology Foresight towards 2020 in China: the Practice and its Impacts. *Technology Analysis and Strategic Management*, *20*(3), 287–307. https://doi.org/10.1080/09537320801999587

Saaty, T. L. (1980). *The Analytic Hierarchy Process*. New York: McGraw-Hill.

Sardar, Z. (2010). The Namesake: Futures; futures studies; futurology; futuristic; foresight-What's in a name? *Futures*, *42*(3), 177–184. https://doi.org/10.1016/j.futures.2009.11.001

Saritas, O. (2006). *Systems Thinking for Foresight (Doctoral Dissertation)*. The

University of Manchester.

Saritas, O. (2011). Sytemic Foresight Methodology. In *Forth International Seville Conference on Future-Oriented Technology Analysis (FTA) FTA and Grand Societal Challenges – Shaping and Driving Structural and Systemic Transformations* (p. 34).

Saunila, M., & Ukko, J. (2012). A Conceptual Framework for the Measurement of Innovation Capability and its Effects. *Baltic Journal of Management*, *7*(4), 355–375. https://doi.org/10.1108/17465261211272139

Schatzmann, J., Schäfer, R., & Eichelbaum, F. (2013). Foresight 2.0 - Definition, overview & evaluation. *European Journal of Futures Research*, *1*(1), 15. https://doi.org/10.1007/s40309-013-0015-4

Schein, E. H. (1992). *Organizational Culture and Leadership*. San Francisco, CA: Jossey-Bass.

Schmidt, J. M. (2015). Policy, planning, intelligence and foresight in government organizations. *Foresight*, *17*(5), 489–511. https://doi.org/10.1108/FS-12-2014-0081

Schultz, W. L. (1997). The Foresight Fan: Systemic Approaches to Foresight. *Part of the King's Fund European Symposium - Health Futures: Tools to Create Tomorrow's Health System*, (November).

Schwartz, P. (1991). *The Art of the Long View*. New York: Doubleday.

Şentürk, H., Çil, C. Z., & Sağıroğlu, Ş. (2012). Cyber Security Analysis of Turkey. *International Journal of Information Security Science*, *1*(4), 112–125. Retrieved from http://ijiss.org/ijiss/index.php/ijiss/article/download/18/112-125

Shengkai, S., Chang, W., Chao, S., & Yu, P. (2017). Japan's 10th Technology Foresight: Insights and Enlightenment. *Chinese Journal of Engineering Science*, *19*(1), 133. https://doi.org/10.15302/J-SSCAE-2017.01.019

Shrake, D. L., Elfner, L. E., Hummon, W., Janson, R. W., & Free, M. (2006). What is Science? *Ohio Academy of Science*, *106*(4), 130–135. https://doi.org/10.1119/1.2351388

Slaughter, R. A. (1995). *The Foresight Principle: Cultural Recovery in the 21st Century*. London: Adamantine Press.

Slaughter, R. A. (1997). Developing and applying strategic foresight. *ABN Report*, *5*, 13–27.

Smith, J. E., & Saritas, O. (2008). Science and technology foresight baker's dozen: a pocket primer of comparative and combined foresight methods. *Foresight*, *13*(3), 79–96. https://doi.org/10.1108/14636681111126265

Sokolov, A. (2018). Foresight in Russia Technology Foresight system in Russia, (March).

Sokolov, A., & Chulok, A. (2014). Russian S & T Foresight 2030 : Looking for New Drivers of Growth. *5th International Conference on Future-Oriented Technology Analysis (FTA) - Engage Today to Shape Tomorrow Brussels, 27-28 November 2014*.

Srivastava, S., & Misra, M. (2014). Developing Evaluation Matrix for Critical Success Factors in Technology Forecasting. *Global Business Review*, *15*(2), 363–380. https://doi.org/10.1177/0972150914523598

SSB. (2017). *Savunma Sanayii Teknoloji Taksonomisi*. Ankara. Retrieved from www.ssb.gov.tr

SSB. (2019). Türkiye Siber Güvenlik Kümelenmesi. Retrieved March 1, 2019, from https://siberkume.org.tr/

Statista. (2018). Size of the cyber security market worldwide. Retrieved December 23, 2018, from https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size

Steed, G., & Tiffin, S. (1986). A National Consultation on Emerging Technology. In *Science Council of Canada*. Ottawa.

Strategic Defense Intelligence. (2015). *The Global Cyber security Market 2015–2025*.

Symantec. (2016). *Threat Report*. *Internet Security Threat Report*. Retrieved from www.symantec.com

Thangaratinam, S., & Redman, C. W. (2005). The Delphi technique. *The Obstetrician & Gynaecologist*, *7*(2), 120–125. https://doi.org/10.1576/toag.7.2.120.27071

The European Foresight Platform. (2010). *France 2025*. Retrieved from http://www.foresight-platform.eu/

The White House. (2015). National Security Strategy, 32. Retrieved from https://www.whitehouse.gov/

The World Bank. (2018). Rankings & Ease of Doing Business Score. Retrieved December 26, 2018, from http://www.doingbusiness.org/en/rankings

Tilley, F., & Fuller, T. (2000). Foresighting methods and their role in researching small firms and sustainability. *Futures*, *32*, 149–161. Retrieved from file:///Users/nurdan/Downloads/Foresight/Foresighting methods and their role in researching small firms and sustainability (Tilley&Fuller-2010).pdf

TÜBİTAK. (2003). *Kritik Teknoloji Ağacı*. Retrieved from https://www.tubitak.gov.tr/

TÜBİTAK. (2004a). *Bilgi ve İletişim Teknolojileri Paneli*. Retrieved from https://www.tubitak.gov.tr/

TÜBİTAK. (2004b). *Ulusal Bilim ve Teknoloji Politikaları - 2003-2023 Strateji Belgesi*. *Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi*. Retrieved from https://www.tubitak.gov.tr/tubitak_content_files/vizyon2023/Vizyon2023_Strateji_Belgesi.pdf

TÜBİTAK. (2017). *Siber Güvenlik Teknoloji ve Ürün Taksonomisi*. Retrieved from https://www.tubitak.gov.tr/

TÜBİTAK. (2018). BTY İstatistikleri (STI Statistics). Retrieved December 26, 2018, from https://www.tubitak.gov.tr/tr/kurumsal/politikalar/icerik-bty-istatistikleri

TUİK. (2018). Basic Statistics. Retrieved December 25, 2018, from http://www.tuik.gov.tr/UstMenu.do?metod=temelist

UNESCO Institute for Statistics. (2018). UIS.Stat. Retrieved January 2, 2019,

from http://data.uis.unesco.org

UNIDO. (2004). *Foresight Methodologies: Training Module 2*. Retrieved from http://www.tc.cz/files/istec_publications/text-book-2-revised-cf.pdf

UNIDO. (2005a). *Technology Foresight Manual- Organization and Methods* (Vol. 1). https://doi.org/10.1038/186062a0

UNIDO. (2005b). *Technology Foresight Manual-Technology Foresight in Action*. https://doi.org/10.1111/j.1467-9299.1960.tb01252.x

US Joint Chief of Staff. (2013). Joint Publication 3-12: Cyberspace Operations, *12*(February 2013), 62. Retrieved from www.e-publishing.af.mil

Voros, J. (2001). A Primer on Futures Studies. *Prospect: The Foresight Bulletin*, *6*(1).

Voros, J. (2003). A generic foresight process framework. *Foresight*, *5*(3), 10–21. https://doi.org/10.1108/14636680310698379

Voros, J. (2005). A generalised "layered methodology" framework. *Foresight: The Journal of Futures Studies, Strategic Thinking and Policy*, *7*(2), 28–40. https://doi.org/10.1108/14636680510700094

WikiEducator. (2018a). Anatomy of a scenario. Retrieved December 16, 2018, from http://wikieducator.org/Introduction_to_scenario_planning/Anatomy_of_a_scenario#Components_of_a_deductive_scenario

WikiEducator. (2018b). Uncertainties. Retrieved December 16, 2018, from http://wikieducator.org/Drivers_of_change_in_education/Uncertainties

World Economic Forum. (2018). *The Global Competitiveness Report 2017–2018*. Retrieved from http://www3.weforum.org/docs/GCR2017-2018/05FullReport/TheGlobalCompetitivenessReport2017–2018.pdf

Xu, S. (2012). Management & Engineering Study on the Natural Science and Technology Resources Share Mechanism. *Management & Engineering*, *07*, 47–82. https://doi.org/10.5503/J.ME.2012.07.007

Yüksel, N., & Çifci, H. (2017). A New Model for Technology Foresight :

Foresight Periscope Model (FPM). In *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 807–817).

Yüksel, N., Çifci, H., & Çakir, S. (2017). New Foresight Generation and Framework of Foresight. In *2nd World Conference on Technology, Innovation and Entrepreneurship* (pp. 224–233). https://doi.org/10.17261/Pressacademia.2017.593

Zweck, A., Braun, M., Erdmann, L., Hirt, M., & Kimpeler, S. (2015). Forschungs- und Technologieperspektiven 2030, *2*, 288. Retrieved from https://www.zukunft-verstehen.de/application/files/5214/7983/3485/VDI_Band_2.pdf

Zweck, A., Holtmannspötter, D., Braun, M., Erdmann, L., Hirt, M., & Kimpeler, S. (2017). *Stories from the Future 2030 Volume 3 of results from the search phase of BMBF Foresight Cycle II* (Vol. 3).

Zweck, A., Holtmannspötter, D., Braun, M., Hirt, M., Kimpeler, S., & Warnke, P. (2017). *Social Changes 2030 Volume 1 of results from the search phase of BMBF Foresight Cycle II* (Vol. 1).

APPENDICES

APPENDIX A: LIST OF PARTICIPANTS

Table A.1: First Focus Group Members

Sector	Organization	# of People
Academia	Middle East Technical University	2
	Bilkent University	1
	Public Administration Institute for Turkey and the Middle East (TODAİE; closed down in July 2018)	1
Turkish Armed Forces	Ministry of National Defense (MSB)	3
	Turkish Air Force	1
Government	Presidency of Defense Industries (SSB)	2
	TÜBİTAK (Scientific and Technological Research Council of Turkey)	2
Turkish Armed Forces Foundation	ASELSAN	1
	HAVELSAN	1
Private Sector	Barikat	1
	Bilge SGT	1
	STM	1
	Total	**17**

Table A.2: Technology Prioritization Study Participants

Sector	Organization	# of People
Academia	Middle East Technical University	2
	Gazi University	1
Turkish Armed Forces	Turkish Air Force	3
Government	Presidency of Defense Industries (SSB)	2
	TÜBİTAK (Scientific and Technological Research Council of Turkey)	2
Private Sector	NETAŞ	1
	Barikat	1
	sayTEC	1
	EVOTRİO	1
	Labris	4
	Biznet	1
	Bilishim Cybersecurity and Artificial Intelligence LLC	1
	Bilge SGT	1
	STM	1
	Total	**22**

Table A.3: Second Focus Group Members

Sector	Organization	# of People
Academia	Middle East Technical University	3
Turkish Armed Forces	Ministry of National Defense (MSB)	1
	Turkish Air Force	2
Government	National Defense Council (MGK)	1
	TÜBİTAK (Scientific and Technological Research Council of Turkey)	2
Turkish Armed Forces Foundation	ASELSAN	3
Private Sector	Barikat	1
	EVETRİO	1
	Total	**14**

Table A.4: Prioritization of Delphi Statements Study with Experts

Sector	Organization	# of People
Academia	Middle East Technical University	3
Turkish Armed Forces	Turkish Air Force	3
Government	National Defense Council (MGK)	1
	TÜBİTAK (Scientific and Technological Research Council of Turkey)	2
Turkish Armed Forces Foundation	ASELSAN	3
	HAVELSAN	1
Private Sector	Barikat	1
	Bilishim Cybersecurity and Artificial Intelligence LLC	1
	STM	1
	Total	**16**

Table A.5: Universities to which Delphi Survey (Round-1) Sent

University	# of People
A. Gül University	18
Adana Science and Technology University	17
Ahi Evran University	3
Akdeniz University	7
Amasya University	8
Anadolu University	27
Ankara University	15
Antalya Bilim University	8
Artvin Çoruh University	10
Atatürk University	19
Atılım University	16
Avrasya University	5
Bahçeşehir University	10
Balıkesir University	6
Bartın University	7
Başkent University	20
Batman University	8
Bayburt University	5
Beykent University	4
Bilgi University	9

Table A.5 (Cont'd)

University	# of People
Bilkent University	25
Bingöl University	7
Bosphorus University	37
Bursa Technical University	5
Bülent Ecevit University	9
Celal Bayar University	10
Cumhuriyet University	11
Çanakkale Onsekiz Mart University	14
Çankaya University	16
Çukurova University	13
Dicle University	3
Doğuş University	12
Dokuz Eylül University	29
Dumlupınar University	10
Düzce University	16
Ege University	31
Erciyes University	8
Erzincan University	8
Erzurum Technical University	6
Fatih Sultan Mehmet University	31
Fırat University	24
Galatasaray University	20
Gazi University	24
Gaziantep University	2
Gebze Technical University	25
Gelişim University	31
Gümüşhane University	10
Hacettepe University	49
Hakkari University	2
Haliç University	7
Harran University	14
Hasan Kalyoncu University	11
Hitit University	4
Iğdır University	7
Işık University	14
İnönü University	18
İskenderun Technical University	14

Table A.5 (Cont'd)

University	# of People
İstanbul Arel University	6
İstanbul Aydın University	14
İstanbul Esenyurt University	7
İstanbul Gedik University	5
İstanbul Kültür University	10
İstanbul Medeniyet University	5
İstanbul Sabahattin Zaim University	13
İstanbul Şehir University	12
İstanbul Technical University	56
İstanbul Ticaret University	6
İstanbul University	27
İstinye University	13
İzmir Institute of Technology	37
İzmir Kâtip Çelebi University	3
İzmir University of Economics	14
Kafkas University	1
Kahramanmaraş Sütçü İmam University	5
Karabük University	31
Karadeniz Technical University	29
Karamanoğlu Mehmetbey University	4
Kastamonu University	5
Kırıkkale University	12
Kırklareli University	8
Kocaeli University	26
Koç University	9
Koç University	8
Konya Necmettin Erbakan University	13
KTO Karatay University	8
Marmara University	13
MEF University	6
Mehmet Akif Ersoy University	6
Mersin University	9
Middle East Technical University	73
Muğla Sıtkı Koçman University	11
Munzur University	12
Muş Alparslan University	12
Namık Kemal University	15

Table A.5 (Cont'd)

University	# of People
Niğde Ömer Halisdemir University	16
Okan University	10
Ondokuz Mayıs University	6
Osmangazi University	21
Özyeğin University	13
Pamukkale University	13
Piri Reis University	2
Sabancı University	12
Sakarya University	35
Selçuk University	25
Siirt University	8
Süleyman Demirel University	14
TED University	13
TOBB University of Economics and Technology	15
Tokat Gaziosmanpaşa University	9
Toros University	7
Trakya University	22
Turkish - German University	65
Uludağ University	6
University of Turkish Aeronautical Association	9
Üsküdar University	7
Van Yüzüncü Yıl University	3
Yalova University	14
Yaşar University	13
Yeditepe University	11
Yıldız Technical University	45
Yozgat Bozok University	5
Total	**1756**

Table A.6: Number of People to which Delphi Survey (Round-1) Sent

Sector	Organization	# of People
Academia	*(120 universities)*	1756
Turkish Armed Forces	Turkish Air Force, Turkish Land Forces, Turkish Naval Forces	45
Government	MGK, TÜBİTAK, BTK (Information and Communication Technology Authority)	12
Turkish Armed Forces Foundation	ASELSAN, HAVELSAN, TA (Turkish Aerospace)	10
Private Sector	*(29 different companies)*	43
	Total	**1866**

Table A.7: Universities Answered Delphi Survey (Round-1)

University	# of People
Adana Science and Technology University	1
Air Force Academy	1
Alparslan University	2
Anadolu University	1
Ankara University	1
Atatürk University	1
Bahçeşehir University	2
Balıkesir University	1
Bartın University	1
Başkent University	1
Beykent University	1
Bosphorus University	1
Bozok University	1
Bülent Ecevit University	3
Celal Bayar University	1
Çanakkale Onsekiz Mart University	2
Doğuş University	1
Dumlupınar University	2
Erciyes University	1
Erzincan University	1

Table A.7 (Cont'd)

University	**# of People**
Erzurum Technical University	2
Fatih Sultan Mehmet University	1
Galatasaray University	1
Gazi University	1
Gebze Technical University	3
Gelişim University	3
Hacettepe University	1
Hitit University	1
Iğdır University	1
İnonü University	1
İstanbul Gedik University	1
İstanbul Technical University	1
İstanbul University	2
İzmir University of Economics	1
Karadeniz Technical University	3
Karatay University	1
Kastamonu University	2
Kırıkkale University	1
Middle East Technical University	2
Muğla Sıtkı Koçman University	1
Namın Kemal University	2
Niğde Ömer Halisdemir University	1
Ondokuz Mayıs University	1
Osmangazi University	2
Süleyman Demirel University	1
TOBB University of Economics and Technology	1
Toros University	1
Turkish-German University	1
Uludağ University	2
Yaşar University	4
Yeditepe University	1
Not specified	5
Total	**78**

Table A.8: Number of People Answered Delphi Survey (Round-1)

Sector	Organization	# of People
Academia	*(50 universities listed in the previous table)*	78
Turkish Armed Forces	Turkish Air Force, Turkish Land Forces, Turkish Naval Forces	26
Government	MGK, TÜBİTAK, BTK (Information and Communication Technology Authority)	11
Turkish Armed Forces Foundation	ASELSAN, HAVELSAN, TA (Turkish Aerospace)	5
Private Sector	*(Since the name of participants' employee organizations weren't requested in the survey, name of the companies couldn't be found except for some inferred from e-mail extensions.)*	31
	Total	**151**

Table A.9: Universities Answered Delphi Survey (Round-2)

University	# of People
Adana Science and Technology University	1
Air Force Academy	1
Alparslan University	1
Balıkesir University	1
Bartın University	1
Başkent University	1
Bozok University	1
Bülent Ecevit University	2
Celal Bayar University	1
Çanakkale Onsekiz Mart University	1
Dumlupınar University	1
Erciyes University	1
Erzincan University	1
Erzurum Technical University	2
Galatasaray University	1
Gebze Technical University	1
Gelişim University	3
Hitit University	1
Iğdır University	1
İstanbul Gedik University	1

Table A.9 (Cont'd)

University	# of People
İstanbul Technical University	1
İzmir University of Economics	1
Karabük University	1
Karadeniz Technical University	1
Kastamonu University	2
Kırıkkale University	1
Middle East Technical University	1
Muğla Sıtkı Koçman University	1
Namın Kemal University	2
Ondokuz Mayıs University	2
Osmangazi University	2
TOBB University of Economics and Technology	1
Toros University	1
Uludağ University	1
Yaşar University	4
Not Specified	3

Table A.10: Number of People Answered Delphi Survey (Round-2)

Sector	Organization	# of People
Academia	*(35 universities listed in the previous table)*	49
Turkish Armed Forces	Turkish Air Force, Turkish Land Forces, Turkish Naval Forces	15
Government	MGK, TÜBİTAK, BTK (Information and Communication Technology Authority)	8
Turkish Armed Forces Foundation	ASELSAN, HAVELSAN	2
Private Sector	*(Since the name of participants' employee organizations weren't requested in the survey, name of the companies couldn't be found except for some inferred from e-mail extensions.)*	17
	Total	**91**

APPENDIX B: TECHNOLOGY TAXONOMY

Table B.1: Technology Groups (Used as Taxonomy Header in the next Table)

	No	
Group A (Underpinning Technologies)		
Group B (Systems Related Technologies)	1	Network Security
	2	Endpoint Detection and Protection
	3	Identity and Access Management (IAM)
	4	Messaging and Communication Security
	5	Data Security
	6	Cloud Computing Security
	7	Application Security
	8	Internet Security
	9	Mobile Devices Security
	10	Industrial Control (SCADA) Systems Security
	11	Internet of Things (IoT) Security
	12	Operating Systems and Container Security
	13	Cybersecurity for Autonomous and Smart Platforms
	14	Hardware Security
	15	Firmware Security
Group C (Systems/Products)	1	Cybersecurity Analytics
	2	Cyber Intelligence
	3	Cybersecurity Operations
	4	Cybersecurity Event Management
	5	Cyber Forensics
	6	Cybersecurity Risk and Compliance Management

Table B.2: Cybersecurity Technology Taxonomy

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
1	Network Security Policy Management	X							X													
2	Network Access Control	X							X													
3	Software-Defined Security	X							X													
4	Network Monitoring	X							X													
5	Firewall as a Service	X							X													
6	Next-Generation Firewalls	X							X													
7	Stateful Firewalls	X							X													
8	Network IPS (Intrusion Prevention System)	X							X													
9	Next-Generation IPS	X							X													
10	DDoS Defense	X							X													
11	Unified Threat Management (UTM)	X							X													
12	Software-Defined Perimeter	X							X													
13	Security in the Switch	X							X													
14	Unidirectional Security Gateways	X							X													
15	Boundary Defense (Perimeter Security)	X							X													
16	Wireless Devices Security	X		X	X					X												
17	Moving Target (MT) Defense	X																	X	X	X	
18	Secure Web Gateways	X						X	X													
19	Remote Browser		X					X	X													
20	Application Control		X					X														
21	Network Sandboxing		X						X													
22	Non-Signature based Malware Analysis		X					X														

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
23	Advanced Persistent Threat (APT) Protection	X	X						X	X	X	X		X								
24	Malware Defense	X	X					X	X	X	X	X	X	X								
25	Host-based Intrusion Prevention System (HIPS)		X																			
26	Device Control		X	X		X				X	X	X										
27	Process and Data Isolation		X				X															
28	Hardware Roots of Trust		X		X	X	X	X	X	X	X	X	X	X	X	X						
29	Virtualized Roots of Trust		X		X	X	X	X	X	X	X	X	X	X	X	X						
30	Network and Protocol Based Isolation Technologies	X				X	X	X	X		X	X	X									
31	Enterprise Key Management			X																		
32	Key Management as a Service			X																		
33	Identity Governance and Administration (IGA)			X																		
34	Federated Identity Management			X																		
35	Blockchain for Identity & Access Management			X																		
36	Common Access Cards			X																		
37	Biometric Authentication Methods			X																		
38	Phone-as-a-Token Authentication Methods			X																		
39	Mobile Single Sign-On			X						X												
40	X.509 Tokens for User Authentication			X																		
41	Identification as a Service (IDaaS)			X																		
42	Strong Authentication for Enterprise Access			X																		
43	Digital Signature			X	X																	
44	Privileged Access Management			X																		

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
45	Externalized Authorization Management			X	X																	
46	Mobile-Apt User Authentication Methods			X																		
47	System for Cross-domain Identity Management (SCIM)			X																		
48	Attribute-Based Access Control (ABAC)			X																		
49	Multifactor Authentication			X	X																	
50	New Generation User and Object Identification and Access Control Technologies			X	X																	
51	Context-Aware Network Access Control	X		X					X													
52	Secure e-Voting Systems			X																		
53	Mobile Voice Protection				X					X												
54	Secure Texting				X																	
55	Mobile Virtual Private Networks				X					X												
56	Crypto Analysis				X												X	X			X	
57	Secure Aviation Protocols and Architecture													X								
58	Encryption Algorithms	X			X	X		X	X	X	X	X	X	X	X	X			X			
59	Encryption Technologies	X			X	X		X	X	X	X	X	X	X	X	X			X			
60	Cryptographic Chips and Modules	X			X	X		X	X	X	X	X		X	X	X			X			
61	Quantum Cryptography	X			X	X																
62	Quantum-Safe Cryptographic Algorithms	X			X	X																
63	Lightweight Cryptography	X			X	X				X	X	X		X								
64	Cyber-Physical Systems (CPS) Security									X	X	X		X								
65	Secure IoT Routing Protocols										X	X										

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
66	Distributed Trust Mechanisms						X				X	X										
67	Fog Computing Security	X	X			X	X		X		X	X										
68	New Generation (4G, 5G etc.) Wireless Security	X			X					X												
69	Privacy in IoT									X	X	X										
70	Virtual Trusted Platform Module (vTPM)									X	X	X	X	X								
71	Hardware Trusted Platform Module (TPM)									X	X	X	X	X	X	X						
72	Wearable Technologies Security													X								
73	Static and Dynamic Data Masking					X																
74	Format Preserving Encryption					X																
75	Information Dispersal Algorithms					X																
76	Tokenization					X																
77	Interoperable Storage Encryption					X																
78	Trusted Portable Storage Security					X																
79	Blockchain for Data Security					X																
80	Privacy Management Technologies and Tools			X		X	X			X												
81	Data Sanitization and Disposal					X				X												
82	Data Loss Prevention (DLP)					X																
83	Content-Aware DLP for Email					X																
84	Content-Aware Mobile DLP					X				X												
85	Data Recovery					X															X	
86	Database Security (Audit, Protection, Encryption)					X																

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
87	Big Data Security					X																
88	Contextual Verification for Information Integrity					X																
89	Cloud Access Security Brokers						X															
90	High-Assurance Hypervisors						X						X									
91	Cloud Data Protection Gateways						X															
92	SaaS (Software as a Service) Platform Security Management						X															
93	IaaS (Infrastructure as a Service) Container Encryption						X															
94	Virtualization Security						X						X									
95	Pervasive Trust Services (Distributed Trust, Blockchain-like Architectures etc.)					X	X				X	X										
96	Hypervisor Security						X						X									
97	Fully Homomorphic Encryption				X	X	X															
98	Runtime Application Self-Protection (RASP)							X														
99	Application Shielding							X														
100	Web Application Firewalls (WAF)							X	X													
101	Mediated Application Programming Interfaces (APIs)							X														
102	Application Security as a Service							X														
103	Application Obfuscation							X														
104	Embedded Software and Systems Security							X							X	X						
105	Vulnerability Assessment	X						X	X		X	X		X	X	X						X

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
106	Application Vulnerability Correlation							X														X
107	Network Penetration Testing Tools	X						X	X													X
108	Crowdsourced Security Testing Platforms							X									X					X
109	Interactive Application Security Testing							X														
110	Mobile Application Security Testing							X		X												
111	Static Application Security Testing (SAST)							X														
112	Fuzz Testing	X						X					X									
113	Dynamic Application Security Testing (DAST)							X														
114	Software Development Life Cycle Security							X														X
115	DevSecOps							X														X
116	Content Monitors and Filters	X						X	X													
117	Web Page Integrity and Monitor							X	X													
118	Autocode Generators and Correct by Construction							X	X	X	X	X	X									
119	SaaS based Mobile Device Management (MDM)									X	X	X										
120	Enterprise Mobility Management (EMM) Security									X												X
121	Bring Your Own Device (BYOD) Security		X							X												
122	User Authentication to Mobile Devices									X												
123	Mobile Threat Defense									X												
124	Protected Mobile Browsers									X												
125	Mobile Platform Health Checks									X												X
126	Trusted Mobile Environments									X												X

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
127	Mobile Vulnerability Management Tools									X												X
128	Consumer Mobile Security Apps									X	X	X										
129	IoT Authentication										X	X										
130	Operational Technology Security										X	X		X								
131	Blockchain Security				X	X																
132	Removable Devices Security		X			X									X	X						
133	Microelectronics Security Tests														X	X						
134	Polymorphic Computing Architecture									X	X	X	X	X	X	X						
135	Separation Kernel												X		X	X						
136	User and Entity Behavior Analytics			X							X	X					X	X				
137	Network Traffic Analysis	X							X								X	X				
138	Threat Intelligence Platforms																X	X				
139	Fraud Detection and Transaction Security				X	X			X								X					
140	Deception Technology (e.g. honeypots)	X							X								X	X	X			
141	Security Information and Event Management (SIEM)																		X	X	X	
142	Privacy-Preserving Machine Learning				X	X	X															
143	Threat Analytics																X	X	X	X	X	
144	Data Farming based Threat Analytics																X	X	X	X		
145	Crowdsourced Threat Intelligence and Protection	X	X														X	X	X			
146	Incident Response and Management																		X	X		
147	Cyber Forensics (stand-alone, mobile, disk, memory)																X		X		X	

Table B.2 (Cont'd)

No	Underpinning Technologies	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
148	Network-based Cyber Forensics																X		X		X	
149	Dynamic Network/Computer Forensics																X		X		X	
150	Model-Driven Cyber Defense																		X	X		
151	Cyber Offense																		X			
152	Deep Packet Analyzing	X			X				X								X	X	X	X	X	
153	Cyber Attack Modeling and Attack Generation																X	X	X	X	X	
154	Cybersecurity Training and Exercise Systems																		X	X	X	
155	Cyber Analytics and Decision Support Systems																		X	X	X	
156	Cybersecurity Testbed																		X	X	X	
157	Cybersecurity Sense-Making																		X	X	X	
158	Penetration Testing																					X
159	Cyber Automated Response																		X	X	X	
160	Vulnerability Management																					X
161	Model-based Dynamic Risk Assessment																					X
162	Certification and Accreditation																					X
163	Cybersecurity Assessment and Evaluation																					X
164	Configuration Auditing												X		X	X						X
165	Automated Reverse Engineering							X									X		X			
166	Software Composition Analysis							X					X			X						X
167	Information Security Management System																		X	X	X	X
168	Formal Verification of Security Mechanisms																					X
169	Risk Management																					X

APPENDIX C: TECHNOLOGY SCORES

Table C.1: Technology Scores

Composite Rank	Technology Number in Taxonomy	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Expert' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
1	61	Quantum Cryptography	3	19	89,4	5	86,6	3	2	87,1
2	62	Quantum-Safe Cryptographic Algorithms	4	18	92,8	2	85,0	4	2	86,9
3	154	Cybersecurity Training and Exercise Systems	15	6	84,5	26	82,1	7	19	84,0
4	151	Cyber Offense	12	9	87,6	11	75,4	42	31	83,4
5	64	Cyber-Physical Systems (CPS) Security	6	15	90,9	3	78,9	22	19	83,3
6	59	Encryption Technologies	12	10	88,4	8	72,4	74	66	82,5
7	23	Advanced Persistent Threat (APT) Protection	13	8	80,3	59	87,4	1	58	82,4
8	35	Blockchain for Identity & Access Management	6	16	87,2	15	79,0	20	5	81,9
9	58	Encryption Algorithms	10	12	88,4	7	73,9	53	46	81,8
10	60	Cryptographic Chips and Modules	5	17	86,1	19	79,0	21	2	81,1
11	22	Non-Signature based Malware Analysis	14	7	78,6	73	87,3	2	71	80,9
12	147	Cyber Forensics (stand-alone, mobile, disk, memory)	8	13	81,9	47	79,7	16	31	80,8
13	159	Cyber Automated Response	9	12	80,7	55	80,5	12	43	80,6
14	79	Blockchain for Data Security	7	15	85,3	24	76,3	30	6	79,9
15	156	Cybersecurity Testbed	11	10	82,1	43	76,2	31	12	79,8
16	155	Cyber Analytics and Decision Support Systems	12	9	78,8	72	81,8	10	62	79,8
17	68	New Generation (4G, 5G etc.) Wireless Security	5	16	87,6	12	76,0	36	24	79,6
18	104	Embedded Software and Systems Security	5	16	80,1	62	79,4	19	43	79,6
19	9	Next-Generation IPS	12	9	77,1	90	84,1	5	85	79,5
20	146	Incident Response and Management	11	10	81,8	49	75,7	40	9	79,4
21	158	Penetration Testing	13	8	82,4	40	72,4	75	35	79,4
22	10	DDoS Defense	15	6	79,1	69	79,5	18	51	79,2
23	131	Blockchain Security	7	15	85,3	23	74,4	48	25	78,8
24	87	Big Data Security	6	15	84,0	30	75,8	38	8	78,8
25	57	Secure Aviation Protocols and Architecture	2	20	88,5	6	77,4	29	23	78,8
26	133	Microelectronics Security Tests	2	19	95,8	1	76,2	33	32	78,8
27	163	Cyber Security Assessment and Evaluation	9	12	82,7	39	74,1	51	12	78,6

Table C.1 (Cont'd)

Composite Rank	Technology Number in Taxonomy	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Expert' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
28	6	Next-Generation Firewalls	13	8	78,8	71	77,9	27	44	78,6
29	63	Lightweight Cryptography	6	16	89,8	4	72,4	76	72	78,5
30	152	Deep Packet Analyzing	11	10	79,7	66	75,7	39	27	78,2
31	143	Threat Analytics	11	10	77,9	81	78,5	23	58	78,1
32	105	Vulnerability Assessment	12	9	79,6	67	75,2	43	24	78,1
33	149	Dynamic Network/Computer Forensics	6	15	78,2	77	78,0	26	51	78,1
34	65	Secure IoT Routing Protocols	5	16	85,9	20	74,3	50	30	77,9
35	148	Network-based Cyber Forensics	8	13	75,0	108	80,5	13	95	77,9
36	153	Cyber Attack Modeling and Attack Generation	12	9	78,0	79	77,6	28	51	77,9
37	150	Model-Driven Cyber Defense	6	15	80,1	61	76,0	35	26	77,5
38	71	Hardware Trusted Platform Module (TPM)	4	17	86,2	18	74,4	49	31	77,4
39	3	Software-Defined Security	10	10	81,9	44	70,5	87	43	77,3
40	160	Vulnerability Management	15	6	77,7	84	75,1	44	40	77,1
41	145	Crowdsourced Threat Intelligence and Protection	5	16	78,5	75	76,2	32	43	76,9
42	66	Distributed Trust Mechanisms	6	15	82,3	41	73,7	60	19	76,8
43	138	Threat Intelligence Platforms	11	10	81,8	48	68,7	113	65	76,8
44	8	Network IPS (Intrusion Prevention System)	13	8	74,9	109	80,9	11	98	76,7
45	96	Hypervisor Security	4	17	84,3	27	74,0	52	25	76,6
46	140	Deception Technology (e.g. honeypots)	9	12	80,3	58	72,6	72	14	76,6
47	130	Operational Technology Security	5	16	85,0	25	72,8	71	46	76,6
48	80	Privacy Management Technologies and Tools	4	17	86,7	16	73,1	67	51	76,6
49	86	Database Security (Audit, Protection, Encryption)	7	14	77,7	83	75,7	41	42	76,5
50	144	Data Farming based Threat Analytics	4	17	84,3	28	73,7	58	30	76,4
51	142	Privacy-Preserving Machine Learning	4	17	83,6	32	73,7	59	27	76,2
52	141	Security Information and Event Management (SIEM)	15	6	74,1	116	83,5	6	110	76,1
53	157	Cyber Security Sense-Making	7	14	70,3	134	80,2	14	120	76,0
54	164	Configuration Auditing	7	14	83,4	35	70,6	86	51	76,0
55	24	Malware Defense	12	9	72,7	122	82,0	8	114	75,9
56	165	Automated Reverse Engineering	5	16	81,1	50	73,3	64	14	75,7
57	54	Secure Texting	5	16	69,5	140	78,3	25	115	75,6
58	107	Network Penetration Testing Tools	13	8	76,3	97	73,5	63	34	75,5
59	95	Pervasive Trust Services (Distributed Trust, Blockchain-like Architectures etc.)	4	17	83,8	31	72,3	77	46	75,3

Table C.1 (Cont'd)

Composite Rank	Technology Number in Taxonomy	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Expert' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
60	98	Runtime Application Self-Protection (RASP)	4	17	85,7	22	71,6	83	61	75,1
61	97	Fully Homomorphic Encryption	4	17	85,7	21	71,5	84	63	75,1
62	139	Fraud Detection and Transaction Security	8	13	79,9	64	70,7	85	21	75,0
63	169	Risk Management (IT, Digital, Vendor, Operational, Industrial, Social)	11	10	76,7	93	72,3	78	15	75,0
64	74	Format Preserving Encryption	3	18	83,1	36	73,1	69	33	75,0
65	83	Content-Aware DLP for Email	7	14	74,9	110	74,9	45	65	74,9
66	70	Virtual Trusted Platform Module (vTPM)	4	17	87,4	13	70,5	88	75	74,8
67	53	Mobile Voice Protection	4	17	75,6	102	74,5	47	55	74,8
68	16	Wireless Devices Security	6	15	86,4	17	68,1	121	104	74,8
69	82	Data Loss Prevention (DLP)	11	10	75,3	105	73,9	54	51	74,7
70	21	Network Sandboxing	11	10	70,1	136	81,9	9	127	74,7
71	112	Fuzz Testing	5	16	77,9	80	73,1	66	14	74,6
72	37	Biometric Authentication Methods	6	16	78,5	76	72,5	73	3	74,6
73	94	Virtualization Security	6	15	83,4	34	69,3	107	73	74,5
74	106	Application Vulnerability Correlation	11	10	77,6	85	69,4	106	21	74,4
75	99	Application Shielding	4	17	87,8	10	69,8	101	91	74,4
76	55	Mobile Virtual Private Networks	7	14	82,1	42	68,0	123	81	73,9
77	100	Web Application Firewall (WAF)	12	9	75,9	100	69,8	100	0	73,8
78	137	Network Traffic Analysis	12	9	72,3	125	76,1	34	91	73,6
79	12	Software-Defined Perimeter	5	16	74,7	113	73,1	68	45	73,6
80	162	Certification and Accreditation	7	14	73,4	119	73,2	65	54	73,3
81	93	IaaS (Infrastructure as a Service) Container Encryption	3	18	79,8	65	71,7	82	17	73,3
82	88	Contextual Verification for Information Integrity	4	17	81,9	45	70,3	94	49	73,3
83	111	Static Application Security Testing (SAST)	8	13	77,7	82	68,8	110	28	73,0
84	5	Firewall as a Service	11	10	74,6	115	70,5	90	25	73,0
85	69	Privacy in IoT	5	16	87,4	14	66,2	139	125	72,8
86	14	Unidirectional Security Gateway	5	16	70,9	132	73,5	62	70	72,7
87	84	Content-Aware Mobile DLP	6	15	70,3	133	73,9	56	77	72,6
88	110	Mobile Application Security Testing	7	14	79,0	70	67,9	124	54	72,6
89	17	Moving Target (MT) Defense	6	15	79,2	68	68,7	114	46	72,5
90	161	Model-based Dynamic Risk Assessment	7	14	80,6	56	66,7	135	79	72,5
91	28	Hardware Roots of Trust	3	18	80,8	54	70,5	89	35	72,5
92	29	Virtualized Roots of Trust	2	19	75,3	104	72,0	79	25	72,4

Table C.1 (Cont'd)

Composite Rank	Technology Number in Taxonomy	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Expert' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
93	167	Information Security Management System	13	8	72,7	123	70,4	92	31	72,0
94	126	Trusted Mobile Environments	4	17	80,5	57	69,1	108	51	72,0
95	25	Host-based Intrusion Prevention System (HIPS)	9	12	64,9	155	79,6	17	138	72,0
96	72	Wearable Technologies Security	3	18	88,0	9	68,1	120	111	72,0
97	56	Crypto Analysis	6	16	76,0	98	69,5	102	4	71,8
98	75	Information Dispersal Algorithms	3	18	78,6	74	70,0	98	24	71,7
99	127	Mobile Vulnerability Management Tools	6	15	82,8	38	65,0	143	105	71,5
100	50	New Generation User and Object Identification and Access Control Technologies	8	13	82,9	37	61,4	156	119	71,5
101	42	Strong Authentication for Enterprise Access	8	14	75,1	107	68,4	118	11	71,4
102	32	Key Management as a Service	2	19	66,7	151	71,9	80	71	71,2
103	114	Software Development Life Cycle Security	13	8	70,2	135	73,6	61	74	71,2
104	15	Boundary Defense (Perimeter Security)	9	12	64,4	159	78,5	24	135	71,1
105	90	High-Assurance Hypervisors	4	17	75,8	101	69,5	103	2	71,1
106	2	Network Access Control	11	10	73,0	120	68,1	122	2	71,1
107	18	Secure Web Gateway	12	9	66,4	153	80,0	15	138	71,1
108	13	Security in the Switch	7	14	68,5	144	72,8	70	74	71,0
109	67	Fog Computing Security	6	15	77,4	87	67,3	132	45	71,0
110	33	Identity Governance and Administration (IGA)	5	16	80,8	53	66,6	137	84	71,0
111	11	Unified Threat Management (UTM)	10	11	72,5	124	68,8	111	13	70,8
112	136	User and Entity Behavior Analytics	6	14	76,3	96	67,4	131	35	70,8
113	27	Process and Data Isolation	8	13	71,3	130	70,0	97	33	70,6
114	168	Formal Verification of Security Mechanisms	5	16	76,6	94	67,9	126	32	70,6
115	123	Mobile Threat Defense	8	13	77,0	92	64,8	147	55	70,5
116	113	Dynamic Application Security Testing (DAST)	7	14	72,1	128	69,4	105	23	70,5
117	43	Electronic Signature	10	11	72,9	121	67,3	133	12	70,5
118	103	Application Obfuscation	5	16	80,2	60	66,0	141	81	70,4
119	49	Multifactor Authentication	9	12	70,1	137	70,5	91	46	70,3
120	1	Network Security Policy Management	9	13	65,7	154	74,8	46	108	70,3
121	31	Enterprise Key Management	9	12	75,2	106	64,8	146	40	70,2
122	78	Trusted Portable Storage Security	2	19	81,9	46	68,4	117	71	70,2
123	77	Interoperable Storage Encryption	1	20	83,5	33	69,1	109	76	70,0
124	73	Static and Dynamic Data Masking	5	16	75,4	103	67,5	130	27	70,0

Table C.1 (Cont'd)

Composite Rank	Technology Number in Taxonomy	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Expert' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
125	81	Data Sanitization and Disposal	5	16	81,1	51	64,9	145	94	69,9
126	51	Context-Aware Network Access Control	6	15	69,8	138	69,9	99	39	69,9
127	115	DevSecOps	8	13	72,1	127	67,8	129	2	69,8
128	20	Application Control	12	9	66,6	152	76,0	37	115	69,8
129	85	Data Recovery	6	15	74,8	111	66,8	134	23	69,7
130	102	Application Security as a Service	6	15	71,3	131	68,7	112	19	69,7
131	76	Tokenization	4	17	74,7	114	67,9	125	11	69,6
132	89	Cloud Access Security Brokers	5	16	68,2	147	70,1	95	52	69,5
133	52	Secure e-voting Systems	2	19	41,2	169	73,8	57	112	69,5
134	4	Network Monitoring	14	7	69,0	143	70,4	93	50	69,3
135	92	SaaS (Software as a Service) Platform Security Management	4	17	79,9	63	65,7	142	79	69,3
136	30	Network and Protocol Based Isolation Technologies	9	12	64,6	158	73,9	55	103	69,1
137	7	Stateful Firewall	14	7	68,1	148	71,7	81	67	69,0
138	129	IoT Authentication	4	17	84,2	29	63,6	153	124	68,8
139	135	Separation Kernel	4	17	69,8	139	68,2	119	20	68,6
140	166	Software Composition Analysis	3	18	77,3	88	66,3	138	50	68,4
141	19	Remote Browser	5	16	76,0	99	64,9	144	45	68,3
142	34	Federated Identity Management	4	17	74,7	112	66,1	140	28	68,2
143	108	Crowdsourced Security Testing Platforms	4	17	63,7	160	69,4	104	56	68,0
144	132	Removable Devices Security	4	17	68,2	146	67,8	127	19	67,9
145	116	Content Monitors and Filters	11	10	67,1	150	68,4	116	34	67,6
146	26	Device Control	10	11	67,3	149	67,8	128	21	67,5
147	109	Interactive Application Security Testing	5	16	61,8	162	70,1	96	66	67,5
148	134	Polymorphic Computing Architecture	3	18	80,9	52	63,8	150	98	67,2
149	91	Cloud Data Protection Gateway	5	15	72,2	126	64,5	149	23	67,0
150	101	Mediated APIs	3	18	76,4	95	64,6	148	53	66,9
151	120	Enterprise Mobility Management (EMM) Security	3	18	78,1	78	63,4	154	76	66,2
152	125	Mobile Platform Health Checks	4	17	71,8	129	63,8	151	22	65,9
153	48	Attribute-Based Access Control (ABAC)	3	18	54,7	166	68,5	115	51	65,8
154	124	Protected Mobile Browsers	4	17	77,2	89	61,8	155	66	65,7
155	44	Privileged Access Management	6	15	69,0	142	63,7	152	10	65,6
156	118	Autocode Generators and Correct by Construction	5	16	77,1	91	57,7	162	71	63,7
157	41	Identification as a Service (IDaaS)	4	17	73,8	118	59,4	159	41	63,0

Table C.1 (Cont'd)

Composite Rank	Technology Number in Taxonomy	Technology	# of Experts	# of Non-Experts	Experts' Score	Experts' Rank	Non-Expert' Score	Non-Experts' Rank	Difference in Ranks	Composite Score
158	122	User Authentication to Mobile Devices	7	13	69,1	141	57,7	161	20	62,7
159	117	Web Page Integrity and Monitor	9	12	68,4	145	54,9	165	20	61,9
160	119	SaaS based Mobile Device Management (MDM)	4	17	64,7	157	60,1	157	0	61,3
161	128	Consumer Mobile Security Apps	5	16	73,9	117	55,5	164	47	61,2
162	121	Bring Your Own Device (BYOD)	7	14	53,6	167	66,6	136	31	61,1
163	36	Common Access Card	3	18	64,8	156	60,0	158	2	60,9
164	40	X.509 Tokens for User Authentication	7	14	60,8	164	56,7	163	1	58,4
165	47	System for Cross-domain Identity Management (SCIM)	3	18	77,5	86	52,6	167	81	57,5
166	39	Mobile Single Sign-On	9	12	52,6	168	59,2	160	8	55,8
167	46	Mobile-Apt User Authentication Methods	2	19	61,0	163	53,4	166	3	54,4
168	38	Phone-as-a-Token Authentication Methods	4	17	62,1	161	51,8	168	7	54,4
169	45	Externalized Authorization Management	1	20	57,0	165	50,7	169	4	51,1

APPENDIX D: DELPHI STATEMENTS

List of Delphi Statements Created by Researcher and Experts

D-1: The technological level has been reached to protect the embedded systems against cyber attacks and to perform security tests of all kinds of electronic circuits (chips, micro-electronic circuits, etc.).

D-2: Crypto algorithms, technology and modules (software, hardware) that cannot be cracked by super computers and quantum computers (quantum safe) have been developed and started to be used in operational environments.

D-3: Technologies and systems have been developed to provide cybersecurity for cyber-physical systems (systems and networks of smart things, factory production control systems, industrial internet and industrial control systems) and our country has been among the top 5 countries selling products in the world.

D-4: The lightweight cryptography systems that can be used in very small systems that can be connected to the network have been developed and used in the products of international brands.

D-5: To provide cybersecurity of manned and unmanned aircraft systems and air traffic control systems (navigation systems, air traffic networks, flight control systems, etc.), cybersecurity protocols and architectures have been developed and started to be used.

D-6: Cybersecurity technologies and systems for wearable technologies (watches, glasses, dresses, artificial organs, various sensors, etc.) have been developed and used in the products of international brands.

D-7: In order to prevent application-level attacks, applications such as application shielding and Runtime Application Self-Protection (RASP), which use artificial intelligence, machine learning and deep learning techniques, have been developed.

D-8: A high level of cyber-attack techniques, technologies and systems have been developed to compete with countries with high-level cyber-attack and defense capabilities in the world (e.g., the US, Russia, China) and a powerful cyber army has been established at this level.

D-9: Technologies have been developed for the cybersecurity of wireless devices (computers, network devices, mobile phones, cameras, etc.) as well as for new generation wireless communication technologies (5G and later) and have been used in international products.

D-10: The Trusted Platform Module (TPM) is designed as a virtual (virtual) and physical (chip) device and used in international market equipment to ensure reliable operations and secure encryption in information systems hardware.

D-11: Protocols, technologies and applications have been developed to ensure privacy, authentication and communication security in the Internet of Things devices and networks, and our country is among the top 10 countries with the largest market share in this area.

D-12: The blockchain and new generation of applications and techniques have been developed and used in order to provide the user and object identity and access control and data security to the highest level.

D-13: Cybersecurity testing, training and drill systems for international training institutions and international cybersecurity drills have been developed and our country has become a global cybersecurity training and innovation center.

D-14: Techniques and technologies (virtualization security, hypervisor security) have been developed to rise the cybersecurity levels of virtual operating systems and are integrated into internationally distributed products.

D-15: The infrastructure, software, hardware, techniques and technologies have been developed to collect, analyze and provide decision support for cyber threat intelligence (threats, tools, resources, targets, etc.) covering all countries in the world.

D-16: Techniques (audit, encryption etc.) technology, software and hardware to provide cybersecurity for big data, other database and data therein has been developed and marketed internationally.

D-17: Advanced techniques, technologies and applications (such as distributed trust, blockchain-like architectures, etc.) have been developed and implemented to provide the trust mechanism among many objects (devices, networks, users).

D-18: Techniques and technologies to protect privacy in machine learning applications have been developed.

D-19: Advanced software, hardware and technologies (user authentication, unbreakable encryption, high performance, etc.) have been developed to ensure security of portable memory devices (USB sticks, external disks, disk units, etc.).

D-20: Techniques and technologies that provide change detection and configuration auditing between servers, applications, databases and network devices and in the internal and public cloud infrastructure have been developed and used.

D-21: In mobile and on premise systems, new generation techniques, technologies and applications have been developed to perform vulnerability management and cybersecurity assessment and evaluation and these have been among the top 5 technological products preferred in this field.

D-22: A new generation of techniques (within/external to system, on-site/remote, manual/automatic, with artificial intelligence etc.) for penetration testing, tools and technologies have been developed.

D-23: Cybersecurity tools and mechanisms (e.g. firewall, security gateway, guard, router, etc.) through software modules and systems (software-defined security) have been developed, and these products have at least 5 % of the world market dominated.

D-24: A variety of technics, software, hardware and technologies for cyber forensic of all kinds of information system devices (computers, telephones, smart objects, etc.) and information storage units (RAM, disk, etc.) have been developed and introduced to the international market.

D-25: New generation technologies and systems to respond cyber events quickly, effectively and automatically (including incident response, automated response and model-driven cyber defense), and to manage these events (incident management) have been developed and used.

D-26: Software, hardware and technologies (e.g. isolation, sandboxing, virtualization, application control, etc.) to protect systems against Advanced Persistent Threats (APTs) have been developed and marketed to the world markets.

D-27: New generation of technics and technologies that can protect systems from Distributed Denial of Service (DDoS) attacks from millions of different locations have been developed and introduced to the markets around the world.

D-28: Software and hardware that can protect systems against all kinds of malicious software (viruses, worms, trojans, rootkits, etc.) through both signature and anomaly based (behavior based, non-signature based) methods have been developed and started to be marketed internationally.

D-29: Intelligent cyber-attack systems with self-learning capability (with machine learning, deep learning, etc.) that can model cyber attacks have been developed both for testing and for real automatic attack capability.

D-30: Cybersecurity systems (firewall, web application firewall, intrusion prevention system, etc.) to analyze communication network traffic (deep packet inspection, etc.) and to take automatic measures against this traffic have been developed and become the top 10 preferred brands in the international markets.

D-31: Data Loss Prevention (DLP) techniques and systems have been developed and are among the top 10 products in the world.

D-32: New generation techniques and systems have been developed and used to protect web servers and web-based systems against cyber attacks.

D-33: Advanced techniques and technologies that enable reverse engineering have been developed and used.

D-34: Advanced deception techniques and systems (honeypot etc.) have been developed and used to protect the systems from attacks and to identify the technics and movements of the attackers.

D-35: Cloud computing security technics (encryption, access brokers, etc.) and technologies have been developed and used.

D-36: Biometric (retina, fingerprint, face, voice, etc.) authentication systems have been developed and presented to international markets.

D-37: Cybersecurity risk management methodologies, techniques and tools have been developed and used.

List of Delphi Statements Created by Experts in Second Focus Group Meeting

D-38: Quantum satellites based on quantum switches have been developed and deployed in deep space to provide internet service from space.

D-39: Flying systems (airplanes, helicopters, unmanned aerial vehicles, etc.) have gained cyber attack capability.

D-40: Reliable digital infrastructures and systems have been developed for secure election, community vision collection and survey.

D-41: Cyber attack systems that mimic human behavior have been developed.

D-42: Cognitive-based network infrastructures have been developed to identify the source of cyber attacks and enable immediate counter-attack.

D-43: The technological level to understand the signals (possibly cryptographic) coming from space has been reached.

D-44: Artificial intelligence software has been developed which designs non-breakable cryptographic algorithms resistant to quantum machines.

D-45: Visualization systems have been developed, which visualize and process the security logs and enable them to be understood easily by analysts.

D-46: Cybersecurity systems have been developed to secure human-machine communication.

D-47: Durable and rapidly recoverable systems that increase the immunity of artificial intelligence systems (robots etc.) have been developed and become among the top 10 countries in the world.

D-48: Cybersecurity risks in all developed products are considered and cybersecurity is embedded in the products.

D-49: Smart technologies have been developed to detect bio-printing (voice, fingerprint) and use them in cyber attacks.

D-50: Machine-based deep learning technologies have been developed that generate behavioral profiles using big data, and create intelligent cyber defense and attack strategies based on these profiles.

D-51: Quantum processor and quantum computer have been developed and used in crypto analysis.

D-52: Secure memory (USB, hard disk, etc.) technologies which use plasma infrastructure and which self-destruct mechanism for tempering were developed.

D-53: Embedded systems have reached the technological level that can use the embedded chip-based boundary scan standards (IEEE 1149.6, IEEE 1581, etc.) that enable the security tests of micro-electronic chips on the integrated circuit board with only a few access points.

D-54: Artificial intelligence test software and hardware has been developed for security testing using cybersecurity systems (networked devices, embedded systems, etc.) or using self-developed attack methods.

D-55: A cryptographic algorithm that cannot be broken by quantum computers has been designed, based on a new mathematical problem that will be difficult to be

solved, can be run quickly, and will take up little space in memory (which can be integrated into small systems).

D-56: The national cyber shield and cyber defense system that has cyber attack ability were implemented.

D-57: Systems that can continuously monitor the potential of the cyber attack of robots have been implemented.

D-58: Systems that provide the security of the system/limbs integrated into the human body have been developed.

D-59: Intelligent city monitoring and security systems have been developed.

D-60: By analyzing the legislation and laws and analyzing the scenarios that may occur, models that determine potential cybersecurity vulnerabilities have been developed.

D-61: Cybersecurity solutions have been developed that can provide all kinds of privacy of individuals (not being followed, not monitoring data, storing personal information, etc.).

D-62: Anonymized cybersecurity intelligence data collection (from all members of society if necessary) infrastructure has been developed and put into use.

D-63: All of the security systems based on difficult to solve problems have been broken by developing quantum computer technology.

D-64: Country elections are made online, using blockchain and similar techniques.

D-65: The security mechanisms of 6G mobile systems are designed and reached in the top 5 in the international market.

D-66: Intelligent (autonomous) defense systems have been developed that perceive the cyber attacks to be done through cyber intelligence and misdirect the target and/or stop the operation.

D-67: Advanced machine learning based intrusion detection systems have been developed which can detect zero-day attacks with at least 95% performance.

D-68: Software has been developed to detect the first leakage point of the attacked data.

D-69: Autonomous crypto analysis ability is gained.

D-70: Systems that can detect and use cybersecurity vulnerabilities in software and systems have been developed.

D-71: The ability of cyber attack to autonomous systems has been developed.

D-72: Cybersecurity of autonomous systems is ensured.

D-73: Dynamic cyber-deception technologies have been developed in software-based network technologies and made compatible with 5G infrastructure.

D-74: Virtual firewalls and virtualized system security technologies have been installed.

D-75: SIEM systems have been developed which collect system and security records from network and server systems and detect security breaches.

D-76: Systems have been developed to monitor and report the compatibility of network, system and security devices with the baseline.

D-77: A test structure has been developed for organizations and companies to test their own security against DDoS attacks.

D-78: E-commerce and banking systems have been developed to detect and prevent fraud and illegal transactions.

D-78: Secure biometric authentication mechanisms have been developed for access to sensitive data hosting systems.

D-80: Training and certification programs, which are valid in national and international levels and have been attended by students from abroad, have been developed.

D-81: SDLC (Software Development Life Cycle) processes have been started to be given in the universities with programming lessons and secure software production has been ensured.

D-82: Domestic and national boundary protection technologies have been developed and a serious decline has occurred in cybersecurity incidents.

D-83: Systems have been developed to detect weaknesses in our national systems and internationally available software.

D-84: Cybersecurity systems have been developed to ensure the security of communication between satellites.

D-85: Technologies for the cybersecurity of personal aircrafts have been developed.

D-86: Signal analysis (possibly encrypted) technologies have been developed and become leading country in the region.

D-87: Holographic design security is among the top 5 technologies.

D-88: Machine system software that malware cannot enter has been developed.

D-89: Identity management and authorization systems based on behavioral and cognitive methods and models have been developed and became the leader in the region and entered the top 10 countries in the world.

D-90: With the cognitive and behavioral models, user-specific cyber immunity and continuous improvement (self-paced learning, continuous improvement) systems have been developed, became the leader in the region and entered the top 10 countries in the world.

D-91: Cybersecurity awareness training packages have been developed that can be used locally and globally.

APPENDIX E: MESSAGES TO DELPHI SURVEY PARTICIPANTS

E-Mail Message to Call for Delphi Survey Round-1 (Turkish)

Değerli hocam günaydın,
Bu çalışma için 15 dakikanızı ayırmanız mümkün mü?

ODTÜ'de Doç.Dr. Serhat ÇAKIR ile doktora tezi olarak **Türkiye'nin Siber Güvenlik Öngörüsü-2040** konusunu çalışmaktayız.

Anket 2 tur olarak gerçekleştirilecektir. 15 gün sürecek olan ilk tur sonuçları anketi dolduran herkesle paylaşılacak ve ilk turun tamamlanmasını takiben, ikinci turda aynı anket tekrar değerlendirilmek üzere ilk tura katılanlara gönderilecektir.

Anketin daha tutarlı olması için mümkün olduğu kadar fazla kişiye ulaştırılması önemlidir. **Bu açıdan, size gönderdiğim bu e-maili siber güvenlik alanında bilgi sahibi olan tanıdıklarınıza da iletmenizi istirham ediyorum.**

Anketin Ağustos ayında yapılacak **ikinci turunu tamamlayan HERKESE** TÜBİTAK tarafından basılan ve tarafımdan yazılmış olan **Her Yönüyle Siber Savaş** kitabı hediye edilecektir.

Bu çalışmada isimler ve kişi bazındaki cevaplar başka kimse ile paylaşılmayacak ve gizli tutulacaktır.

Akademik çalışmaya yaptığınız katkılardan dolayı çok teşekkür eder, saygılarımı sunarım.

Anketin Linki: https://docs.google.com/forms/d/e/1FAIpQLSdwxDFzEgEBFoo449-0m29dwRWNxXrH652Yoe3qT_CHTVsbLw/viewform

Önemli Notlar:
1. Anketi cep telefonundan da doldurmak mümkündür.
2. Anket 15-20 dakikada doldurulabilmektedir.
3. Siber güvenlik konusunda uzman olmaya gerek yoktur. Bilgi sahibi olmak yeterlidir.

Hasan ÇİFCİ
İletişim:
İş Tel : 0312 414 xxxx
Cep Tel : 0546 781 xxxx

E-Mail Message to Call for Delphi Round-1 (English)

Good morning dear sir,

Could you please make 15 minutes for this study?

We work with Assoc.Prof. Serhat Çakır (METU) on **Turkey's Cybersecurity Foresight-2040** subject as a PhD thesis.

The survey will be held in 2 rounds. The results of the first round, which will last for 15 days, will be shared with all who completed the survey and following the completion of the first round, the same survey will be sent to the participants of first round for re-evaluation in the second round.

It is important to reach as many people as possible to make the questionnaire more consistent. In this respect, **I request you to forward this e-mail to your acquaintances and colleagues in the field of cybersecurity.**

The people **who complete the second round of the survey** planned in August will be presented a book named "**All Aspects of Cyber Warfare**" written by myself and published by TUBITAK.

In this study, the names and personal answers will not be shared with anyone else and will be kept confidential.

I would like to thank you very much for your contribution to the academic study.

Survey's Link: https://docs.google.com/forms/d/e/1FAIpQLSdwxDFzEgEBFoo449-0m29dwRWNxXrH652Yoe3qT_CHTVsbLw/viewform

Important notes:

1. It is also possible to fill out the survey on the mobile phone.
2. The survey can be completed in 15-20 minutes.
3. There is **no need to be an expert** in cybersecurity. Knowledge is sufficient.

Hasan ÇİFCİ
Contact:
Work Phone : 0312 414 xxxx
Mobile Phone: 0546 781 xxxx

E-Mail Message to Call for Delphi Round-2 (Turkish)

Türkiye'nin Siber Güvenlik Öngörüsü-2040 anketinin ilk turuna katıldığınız için çok teşekkür ederim.

İkinci ve son turda, ilk turdaki soruların aynısı, istatistiklerle birlikte yer almaktadır.

Ankette ilk turda verdiğiniz cevaplar işaretlenmiştir.

Özellikle uzmanların verdiği cevaplara bakarak, dilerseniz ilk turdaki cevaplarınızı değiştirebilirsiniz.

Cevaplarınız aynıysa, işaretleme yapmadan sonraki soruya geçebilirsiniz.

Bu çalışmada isimler ve kişi bazındaki cevaplar başka kimse ile paylaşılmayacak ve gizli tutulacaktır.

Akademik çalışmaya yaptığınız katkılardan dolayı çok teşekkür eder, saygılarımı sunarım.

Anketin Linki: https://docs.google.com/forms/d/e/1FAIpQLScGCnDmEiWx50-fZZibJxTaiM1fqygx2NMGeUCruGsE57fVJg/viewform?edit2=2_ABaOnuet4ANQpOVj4yideXPkHlDPgQZbFqwwrGFz3lzZqnq5tquIusUaNpMkm7I

Önemli Notlar:
1. Anketi cep telefonundan da doldurmak mümkündür.
2. Anket 10-15 dakikada doldurulabilmektedir.

Size "**Her Yönüyle Siber Savaş**" kitabımı gönderebilmem için, anketi doldurduktan sonra **adınızı**, **soyadınızı** ve **adresinizi** içeren bir e-postayı bana gönderebilir misiniz?

Hasan ÇİFCİ

E-Mail Message to Call for Delphi Round-2 (English)

Thank you very much for participating to the first round of the **Turkey's Cybersecurity Foresight-2040** survey.

In this second (and final round), the same questions as in the first round take place together with the statistics.

Your answers in the first round of the survey are marked.

Especially by looking at the answers given by experts, you can change your answers you gave in the first round.

If your answers are the same, you can proceed to the next question without marking.

In this study, the names and personal answers will not be shared with anyone else and will be kept confidential.

I would like to thank you very much for your contribution to the academic study.

Survey's Link: https://docs.google.com/forms/d/e/1FAIpQLScGCnDmEiWx50-fZZibJxTaiM1fqygx2NMGeUCruGsE57fVJg/viewform?edit2=2_ABaOnuet4ANQpOVj4yideXPkHlDPgQZbFqwwrGFz3lzZqnq5tquIusUaNpMkm7I

Important notes:
1. It is also possible to fill out the survey on the mobile phone.
2. The questionnaire can be filled in 10-15 minutes.

Can you send me an e-mail with your name, surname, and address after filling out the questionnaire so that I can send you my book "**All Aspects of Cyber Warfare**"?

Hasan ÇİFCİ

APPENDIX F: SURVEY FORMS

Cybersecurity Trends Survey:

Q-1: What do you think will happen in the next 5 years in which countries will come out in cyber attacks? (Write 5 countries sequentially)

Select either: …. I am expert of this subject
…. I have information about the subject

No	Country (Attacker)
1	
2	
3	
4	
5	

Q-2: Which countries will be the target of cyber attacks in the next 5 years? (Write 5 countries sequentially)

Select either: …. I am expert of this subject
…. I have information about the subject

No	Country (Target)
1	
2	
3	
4	
5	

Q-3: What types of cyber attacks will be effective in the next 5 years? (Write to the list by prioritizing. You can use the table below or add a new attack type yourself.)

Select either: …. I am expert of this subject
…. I have information about the subject

Malware	Denial of service	Spam	Data breaches
Web-based attacks	Physical manipulation (theft/loss)	Ransomware	Identity theft
Web application attacks	Phishing	Cyber espionage	Information leakage
Botnets	Insider threat (malicious, accidental)	Exploit kits	

No	Attack Type	No	Attack Type
1		6	
2		7	
3		8	
4		9	
5		10	

Q-4: What sectors will be the target of cybersecurity attacks in the next 5 years? (Write to the list by prioritizing. You can use the table below or add new sectors by yourself.)

Select either: …. I am expert of this subject
…. I have information about the subject

Government	Health	Education	Critical infrastructures
Banking/Finance	Energy	Technology	Defense industry
Telecom	Production facilities	Leisure	Transportation
Medicine/Drugs	Food	Automotive	Defense

No	Target Sectors	No	Target Sectors
1		6	
2		7	
3		8	
4		9	
5		10	

Q-5: In your opinion, what technologies (except for cybersecurity technologies) will affect cybersecurity most in the next 5 years? (Write to the list by prioritizing. You can use the table below or add new technology by yourself.)

Select either: …. I am expert of this subject
…. I have information about the subject

Artificial Intelligence	Big Data	Blockchain	Edge Computing
Deep Learning	Augmented Reality	Digital Twin	Brain-Computer Interface
Machine Learning	Virtual Reality	IoT Platform	Autonomous Vehicles
Cloud Computing	Cognitive Computing	Smart Workspace	Wireless (4G, 5G)
Micro Data Centers	Smart Cars	Smart Home	Cognitive Computing
Smart Robots	Quantum Computing	Commercial UAVs	Wearable Devices

No	Technology	No	Technology
1		6	
2		7	
3		8	
4		9	
5		10	

Q-6: What other questions could be asked in a cybersecurity trends survey?

a. ……
b. ……
c. ……
d. ……
e. ……

Delphi Survey - First Round:

Turkey's Cybersecurity Foresight Survey (Round-1)

This survey contains 25 questions related to cybersecurity.

Survey can be completed in 15-20 minutes.

Since the survey will be two-rounds, it is essential to issue your real e-mail address.

Thank you for your contribution to my academic studies.

Hasan ÇİFCİ (e-mail: hasan.cifci@metu.edu.tr)

* Required

Email address *: ……..

General Questions

Your educational background *

- O Associate degree
- O Bachelor of science
- O Master of science
- O PhD
- O Post-doctoral

Your cybersecurity experience *

- O 0-5 years
- O 6-10 years
- O 11-15 years
- O 16-20 years
- O Over 21 years

Your sector *

- O Academia
- O Turkish Armed Forces
- O Government
- O Private Sector
- O Non-Governmental Organization

Cybersecurity Questions

Question-1: The lightweight cryptography systems that can be used in very small systems that can be connected to the network have been developed and used in the products of international brands.

1.a: Expertise Level

- O Expert
- O I have opinion
- O I don't have any idea *(Don't answer questions, press NEXT at the bottom of the page)*

1.b: Contribution to National Security (1: Not important; 5: Very important)

Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

1.c: Contribution to Economy (1: Not important; 5: Very important)

Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

1.d: Realization Timeframe

- O 2019-2023
- O 2024-2029
- O 2030-2035
- O 2036-2040
- O After 2040

1.e: Realization Method (You can choose up to two)

- ☐ Research and Development
- ☐ Technology Transfer
- ☐ Foreign Company Cooperation
- ☐ COTS or Open Source Use

BACK **NEXT** *Page 2 of 26*

(All of the Delphi statements have the same questions… Only first and last question were given here in order not to repeat the Delphi statements which were already given in previous appendix of this thesis document)

Question-25: *Durable and rapidly recoverable systems that increase the immunity of artificial intelligence systems (robots etc.) have been developed and become among the top 10 countries in the world.*

25.a: Expertise Level

- O Expert
- O I have opinion
- O I don't have any idea

25.b: Contribution to National Security (1: Not important; 5: Very important)

Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

25.c: Contribution to Economy (1: Not important; 5: Very important)

Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

25.d: Realization Timeframe

- O 2019-2023
- O 2024-2029
- O 2030-2035
- O 2036-2040
- O After 2040

25.e: Realization Method (You can choose up to two)

- ☐ Research and Development
- ☐ Technology Transfer
- ☐ Foreign Company Cooperation
- ☐ COTS or Open Source Use

O Send me a copy of my responses.

BACK **SUBMIT** *Page 26 of 26*

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service

Google Forms

Delphi Survey - Second Round:

In the second round, participants were able to see their responses in the first round through Google Forms scripts written by the researcher. With the help of this script, every participant received individual Google Forms survey pages with their responses checked and they were able to change their answers to the questions. Piece of source code is given below:

```
var formURL = 'https://docs.google.com/forms/d/veSqE/viewform';
var sheetName = 'Siber Sablon';
…
function getEditResponseUrls(){
  var ss = SpreadsheetApp.getActiveSpreadsheet();
  var sheet = ss.getSheets()[0];
  var lastCol = sheet.getLastColumn()
  var rng = sheet.getRange(1,1,1,lastCol);
  var headers = rng.getValues();
  var columnIndex = headers[0].indexOf(columnName);
  var form = FormApp.openByUrl(formURL);
  …
  for(var i = startRow-1; i < data.length; i++) {
    if(data[i][0] != '' && data[i][columnIndex] == '') {
      var timestamp = data[i][0];
      var formSubmitted = form.getResponses(timestamp);
      …
      if(formSubmitted.length < 1) continue;
      var editResponseUrl = formSubmitted[0].getEditResponseUrl();
      sheet.getRange(i+1, columnIndex+1).setValue(editResponseUrl);
}
```

Turkey's Cybersecurity Foresight Survey (Round-2)

PLEASE READ THIS SECTION…

In this survey, the same questions as in the first round are included with the statistics.

The answers you gave in the first round were marked.

Especially by looking at the answers given by experts, you can change your answers that you gave in the first round.

If your answers are the same, you can proceed to the next question without marking.

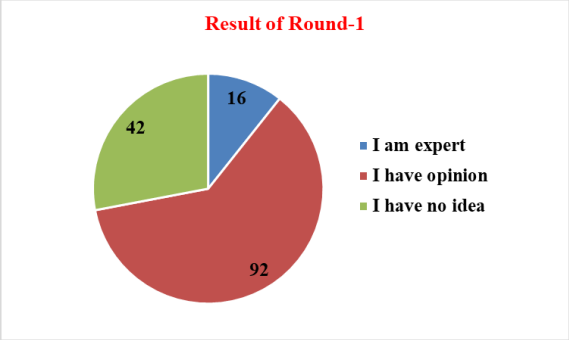
IMPORTANT NOTE:

Proceed to the next section if you don't have any idea about the question.

Cybersecurity Questions

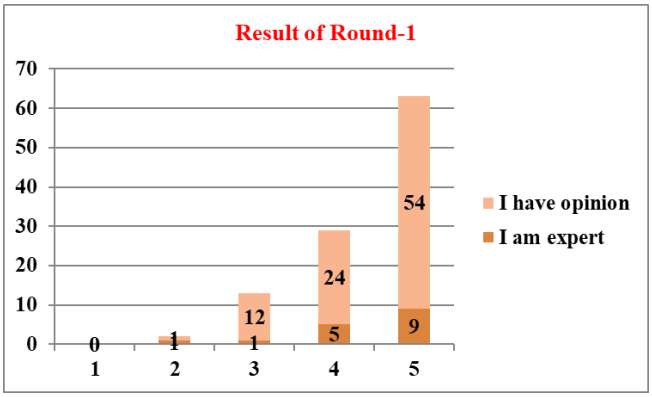
Question-1: The lightweight cryptography systems that can be used in very small systems that can be connected to the network have been developed and used in the products of international brands.

1.a: Expertise Level



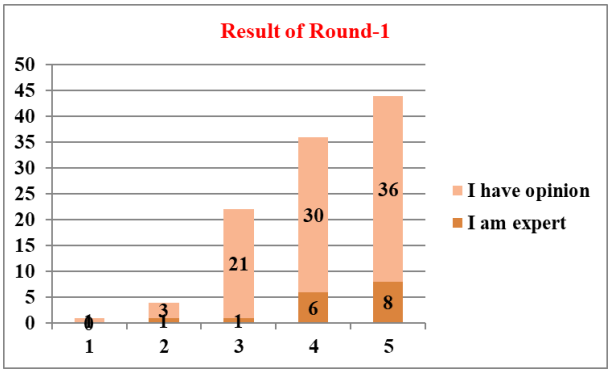
O Expert
O I have opinion
O I don't have any idea *(Don't answer questions, press NEXT at the bottom of the page)*

1.b: Contribution to National Security (1: Not important; 5: Very important)



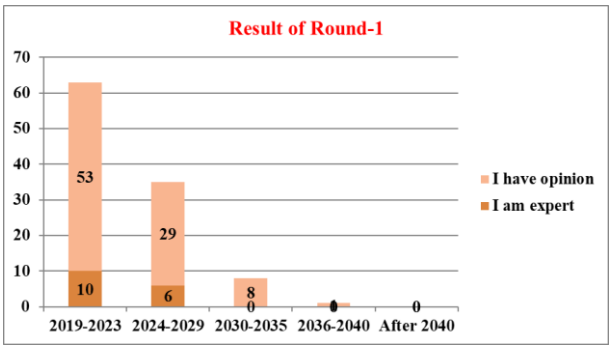
Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

1.c: Contribution to Economy (1: Not important; 5: Very important)



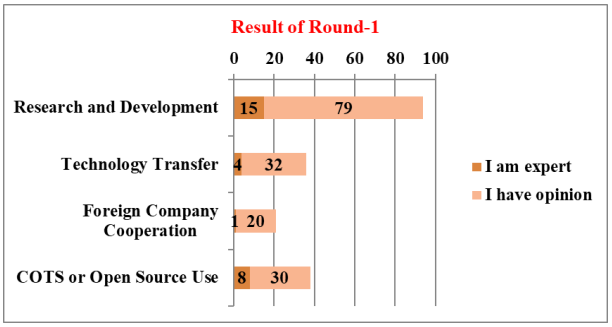
Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

1.d: Realization Timeframe



O 2019-2023
O 2024-2029
O 2030-2035
O 2036-2040
O After 2040

1.e: Realization Method (You can choose up to two)



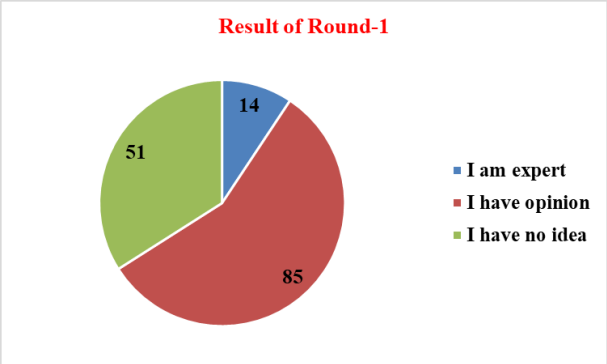
☐ Research and Development
☐ Technology Transfer
☐ Foreign Company Cooperation
☐ COTS or Open Source Use

BACK **NEXT** *Page 2 of 26*

(All of the Delphi statements have the same questions… Only first and last question were given here in order not to repeat the Delphi statements which were already given in previous appendix of this thesis document)

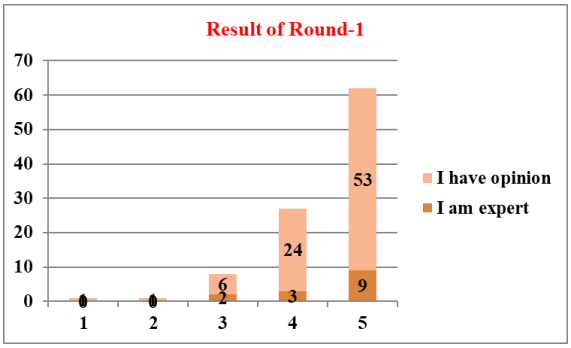
Question-25: ***Durable and rapidly recoverable systems that increase the immunity of artificial intelligence systems (robots etc.) have been developed and become among the top 10 countries in the world.***

25.a: Expertise Level



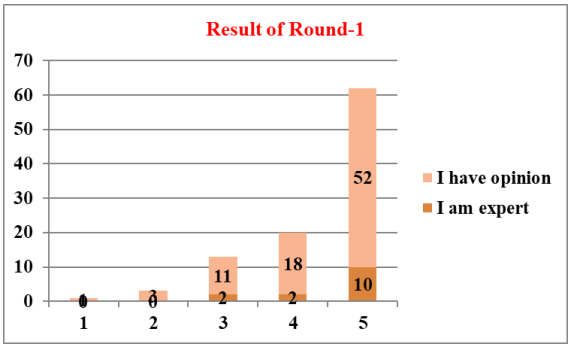
O Expert
O I have opinion
O I don't have any idea

25.b: Contribution to National Security (1: Not important; 5: Very important)



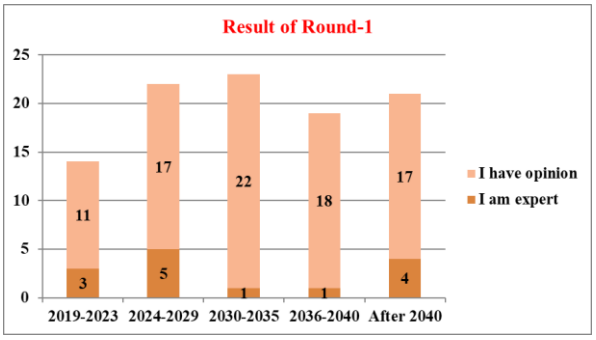
Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

25.c: Contribution to Economy (1: Not important; 5: Very important)



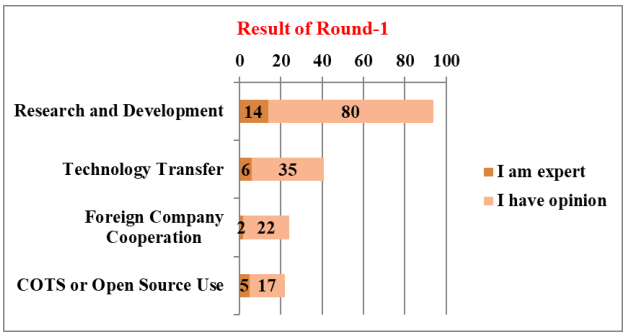
Not important	1	2	3	4	5	Very important
	O	O	O	O	O	

25.d: Realization Timeframe



O 2019-2023
O 2024-2029
O 2030-2035
O 2036-2040
O After 2040

25.e: Realization Method (You can choose up to two)



☐ Research and Development
☐ Technology Transfer
☐ Foreign Company Cooperation
☐ COTS or Open Source Use

O Send me a copy of my responses.

BACK **SUBMIT** *Page 26 of 26*

APPENDIX G: DISTRIBUTION OF ANSWERS IN DELPHI ROUNDS

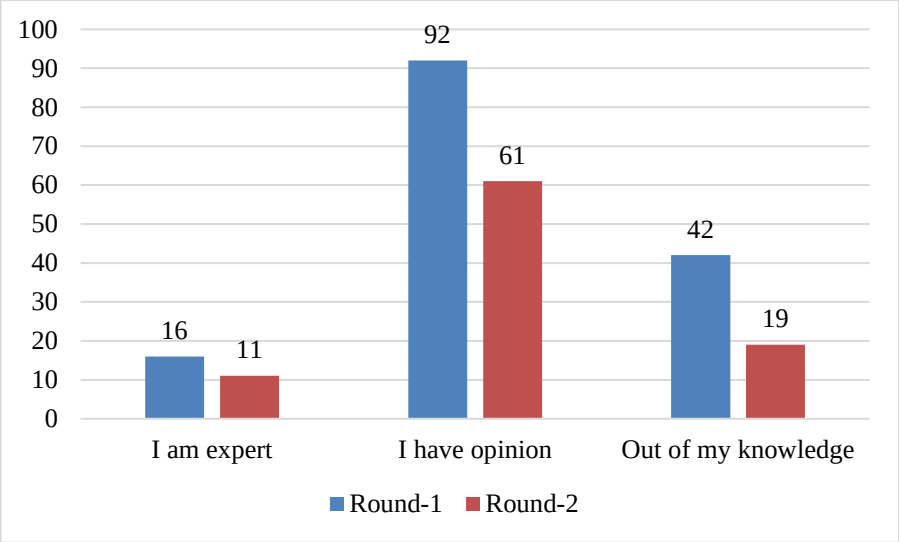


Figure G.1: Distribution of Expertise Levels (Statement-1)

Table G.1: Distribution of Answers in Delphi Rounds (Statement-1)

1b (Security)	1	2	3	4	5
Round-1	0,0%	3,0%	11,9%	29,9%	55,2%
Round-2	0,0%	2,8%	6,9%	29,2%	61,1%
1c (Economy)	1	2	3	4	5
Round-1	0,0%	4,5%	17,9%	38,8%	38,8%
Round-2	0,0%	4,2%	16,7%	37,5%	41,7%
1d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	58,2%	32,8%	7,5%	1,5%	0,0%
Round-2	56,9%	36,1%	5,6%	1,4%	0,0%

1e (Method)	Round-1	Round-2
R&D Investment	50,4%	52,4%
Technology Transfer	19,3%	18,3%
Foreign Company Cooperation	11,8%	9,5%
COTS or Open Source Use	18,5%	19,8%

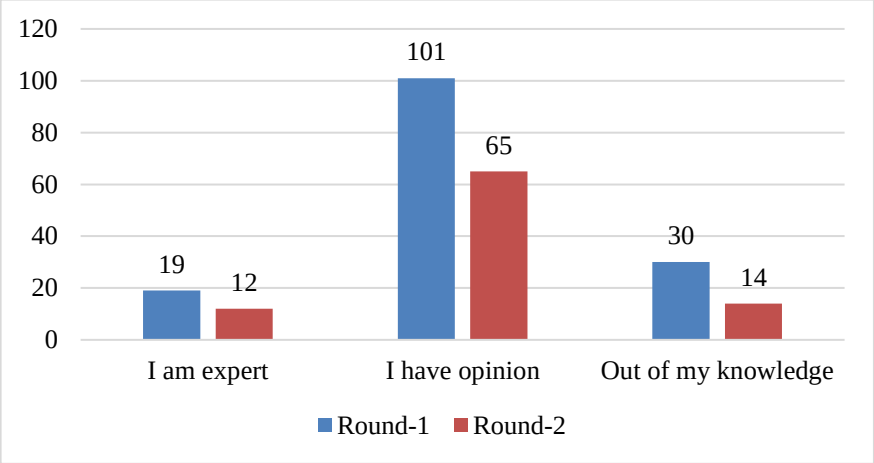


Figure G.2: Distribution of Expertise Levels (Statement-2)

Table G.2: Distribution of Answers in Delphi Rounds (Statement-2)

2b (Security)	1	2	3	4	5
Round-1	0,0%	1,3%	17,3%	33,3%	48,0%
Round-2	0,0%	1,3%	13,0%	35,1%	50,6%
2c (Economy)	1	2	3	4	5
Round-1	0,0%	4,0%	14,7%	38,7%	42,7%
Round-2	0,0%	2,6%	10,4%	40,3%	46,8%
2d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	70,7%	24,0%	4,0%	1,3%	0,0%
Round-2	68,8%	27,3%	2,6%	1,3%	0,0%

2e (Method)	Round-1	Round-2
R&D Investment	44,3%	46,2%
Technology Transfer	22,1%	21,7%
Foreign Company Cooperation	15,0%	12,6%
COTS or Open Source Use	18,6%	19,6%

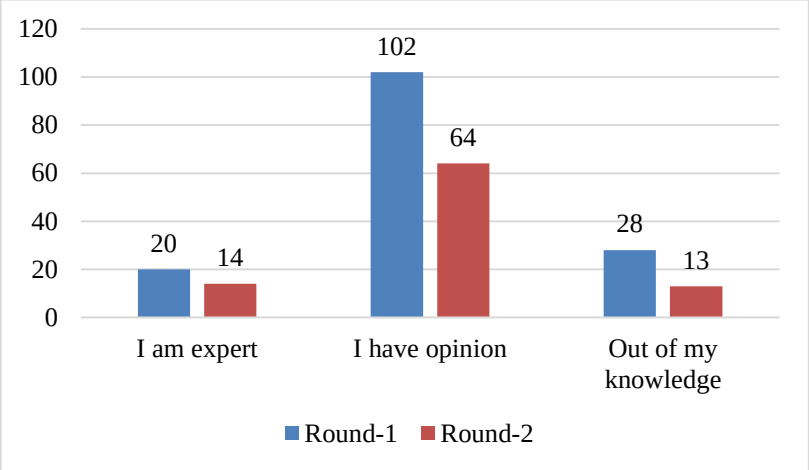


Figure G.3: Distribution of Expertise Levels (Statement-3)

Table G.3: Distribution of Answers in Delphi Rounds (Statement-3)

3b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	15,8%	27,6%	56,6%
Round-2	0,0%	2,6%	13,0%	26,0%	58,4%
3c (Economy)	1	2	3	4	5
Round-1	1,3%	1,3%	13,2%	36,8%	47,4%
Round-2	1,3%	2,6%	7,8%	37,7%	50,6%
3d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	50,6%	31,2%	15,6%	2,6%	0,0%
Round-2	50,0%	35,9%	12,8%	1,3%	0,0%

3e (Method)	Round-1	Round-2
R&D Investment	45,6%	46,9%
Technology Transfer	23,8%	24,5%
Foreign Company Cooperation	12,9%	9,5%
COTS or Open Source Use	17,7%	19,0%

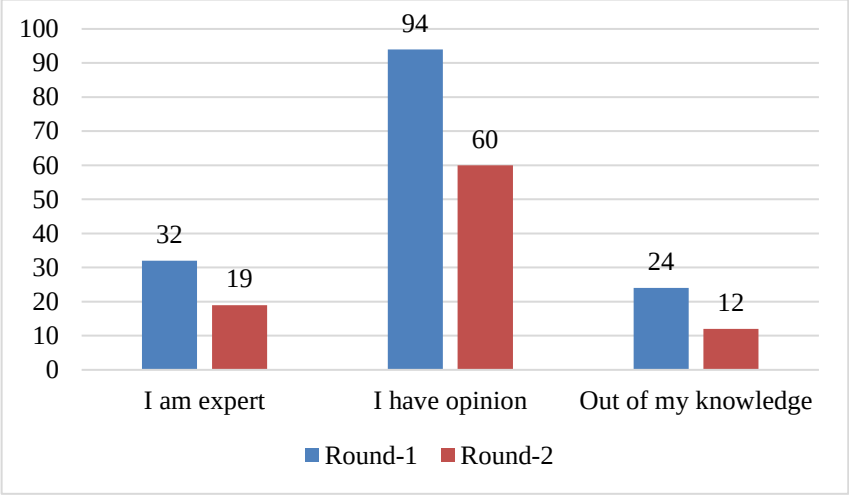


Figure G.4: Distribution of Expertise Levels (Statement-4)

Table G.4: Distribution of Answers in Delphi Rounds (Statement-4)

4b (Security)	1	2	3	4	5
Round-1	0,0%	1,3%	3,8%	5,1%	89,9%
Round-2	0,0%	1,3%	0,0%	3,8%	94,9%
4c (Economy)	1	2	3	4	5
Round-1	2,5%	3,8%	25,3%	24,1%	44,3%
Round-2	1,3%	3,8%	17,7%	27,8%	49,4%
4d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	51,9%	25,3%	12,7%	2,5%	7,6%
Round-2	51,9%	30,4%	10,1%	2,5%	5,1%

4e (Method)	Round-1	Round-2
R&D Investment	47,5%	48,2%
Technology Transfer	18,0%	17,0%
Foreign Company Cooperation	19,4%	17,0%
COTS or Open Source Use	15,1%	17,7%

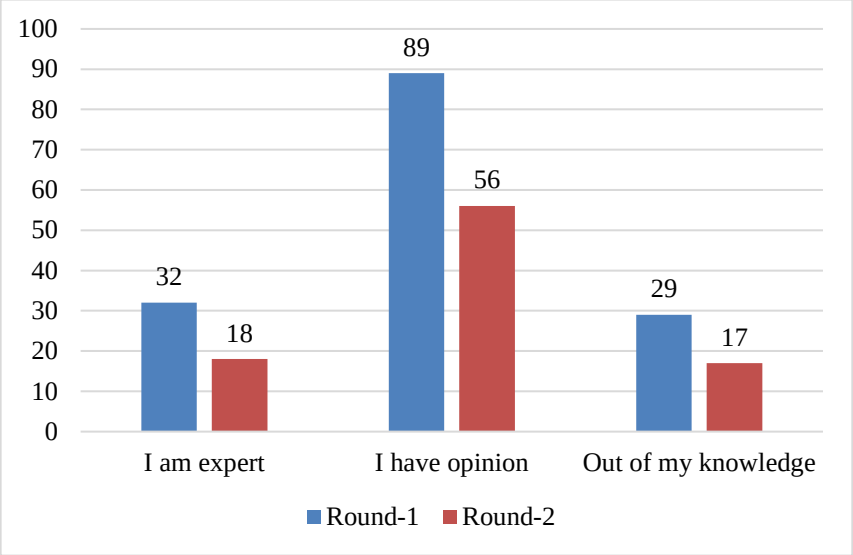


Figure G.5: Distribution of Expertise Levels (Statement-5)

Table G.5: Distribution of Answers in Delphi Rounds (Statement-5)

5b (Security)	1	2	3	4	5
Round-1	0,0%	1,4%	1,4%	4,1%	93,2%
Round-2	0,0%	1,4%	0,0%	2,7%	95,9%
5c (Economy)	1	2	3	4	5
Round-1	1,4%	5,4%	17,6%	29,7%	45,9%
Round-2	1,4%	6,8%	13,5%	27,0%	51,4%
5d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	27,0%	31,1%	20,3%	6,8%	14,9%
Round-2	27,0%	32,4%	20,3%	8,1%	12,2%

5e (Method)	Round-1	Round-2
R&D Investment	51,9%	53,0%
Technology Transfer	18,3%	16,7%
Foreign Company Cooperation	6,9%	5,3%
COTS or Open Source Use	22,9%	25,0%

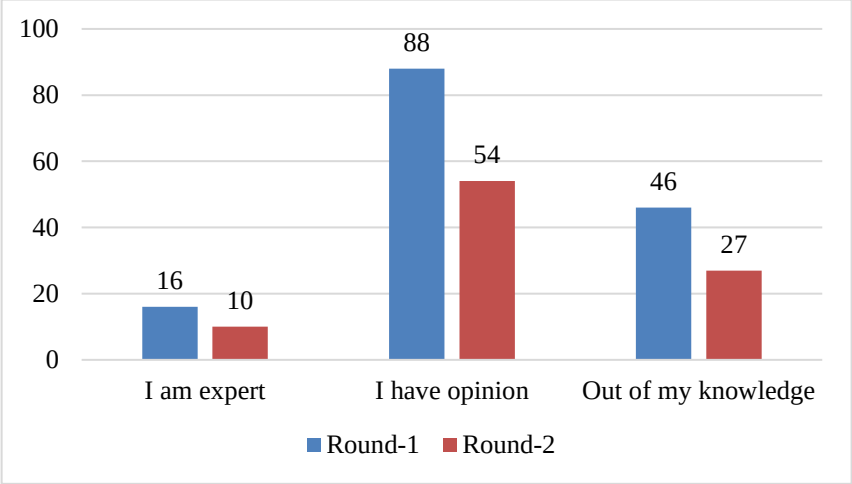


Figure G.6: Distribution of Expertise Levels (Statement-6)

Table G.6: Distribution of Answers in Delphi Rounds (Statement-6)

6b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	3,1%	23,4%	73,4%
Round-2	0,0%	0,0%	3,1%	17,2%	79,7%
6c (Economy)	1	2	3	4	5
Round-1	1,6%	7,8%	18,8%	25,0%	46,9%
Round-2	1,6%	4,7%	20,3%	23,4%	50,0%
6d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	25,4%	36,5%	19,0%	11,1%	7,9%
Round-2	23,4%	43,8%	21,9%	7,8%	3,1%

6e (Method)	Round-1	Round-2
R&D Investment	48,7%	48,7%
Technology Transfer	35,7%	38,5%
Foreign Company Cooperation	9,6%	7,7%
COTS or Open Source Use	6,1%	5,1%

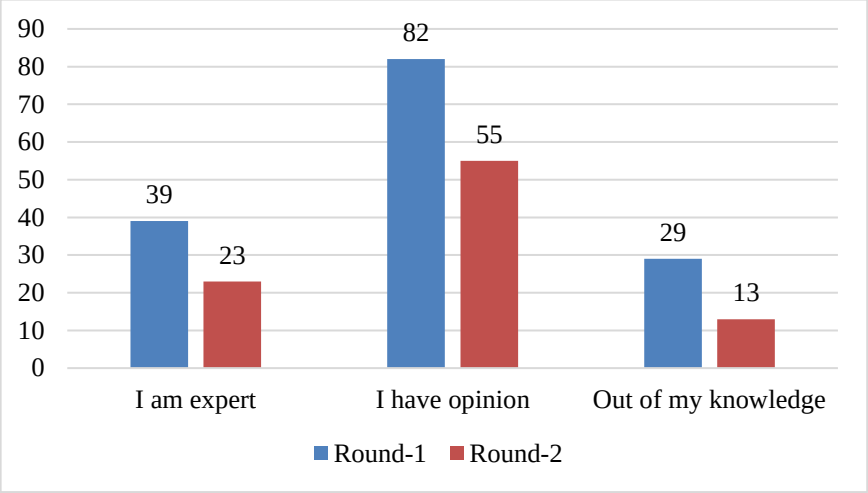


Figure G.7: Distribution of Expertise Levels (Statement-7)

Table G.7: Distribution of Answers in Delphi Rounds (Statement-7)

7b (Security)	1	2	3	4	5
Round-1	1,3%	0,0%	3,9%	29,9%	64,9%
Round-2	1,3%	0,0%	3,8%	24,4%	70,5%
7c (Economy)	1	2	3	4	5
Round-1	0,0%	3,9%	14,5%	32,9%	48,7%
Round-2	0,0%	3,8%	12,8%	30,8%	52,6%
7d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	35,1%	23,4%	20,8%	13,0%	7,8%
Round-2	35,9%	30,8%	23,1%	6,4%	3,8%

7e (Method)	Round-1	Round-2
R&D Investment	48,9%	49,3%
Technology Transfer	25,2%	26,1%
Foreign Company Cooperation	12,2%	9,9%
COTS or Open Source Use	13,7%	14,8%

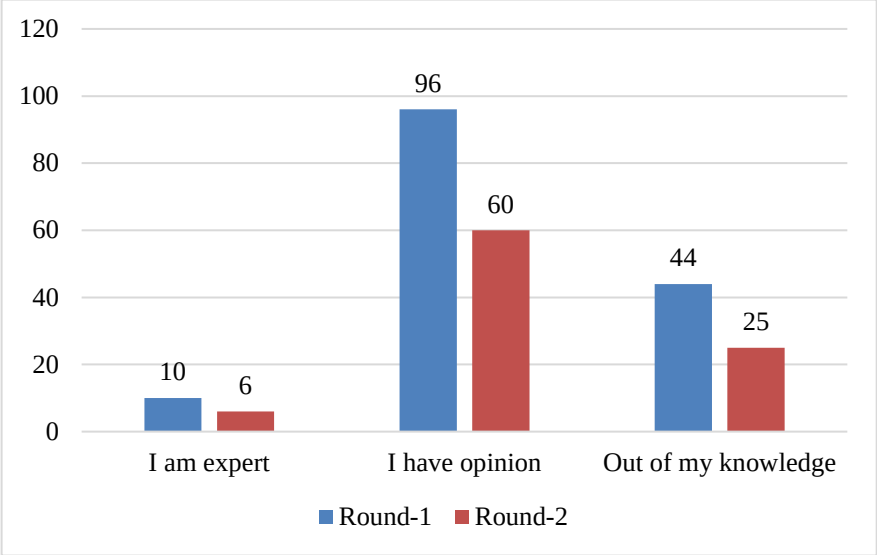


Figure G.8: Distribution of Expertise Levels (Statement-8)

Table G.8: Distribution of Answers in Delphi Rounds (Statement-8)

8b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	0,0%	15,2%	84,8%
Round-2	1,5%	0,0%	0,0%	12,1%	86,4%
8c (Economy)	1	2	3	4	5
Round-1	0,0%	9,1%	10,6%	28,8%	51,5%
Round-2	0,0%	6,1%	7,6%	34,8%	51,5%
8d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	33,3%	31,8%	24,2%	4,5%	6,1%
Round-2	34,8%	34,8%	24,2%	3,0%	3,0%

8e (Method)	Round-1	Round-2
R&D Investment	47,9%	48,8%
Technology Transfer	30,3%	33,3%
Foreign Company Cooperation	16,0%	13,8%
COTS or Open Source Use	5,9%	4,1%

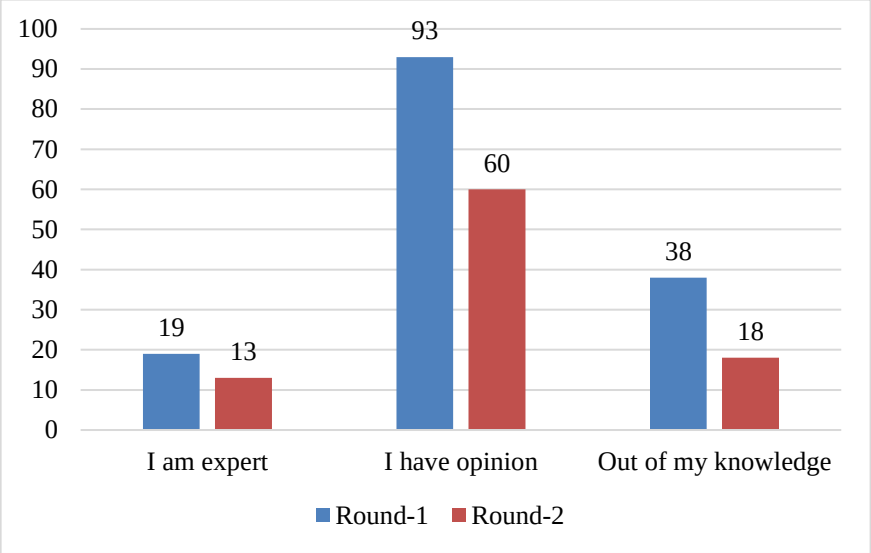


Figure G.9: Distribution of Expertise Levels (Statement-9)

Table G.9: Distribution of Answers in Delphi Rounds (Statement-9)

9b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	12,3%	30,1%	57,5%
Round-2	0,0%	0,0%	9,6%	27,4%	63,0%
9c (Economy)	1	2	3	4	5
Round-1	0,0%	4,1%	11,0%	24,7%	60,3%
Round-2	0,0%	1,4%	9,6%	24,7%	64,4%
9d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	41,1%	30,1%	20,5%	5,5%	2,7%
Round-2	39,7%	32,9%	21,9%	2,7%	2,7%

9e (Method)	Round-1	Round-2
R&D Investment	45,4%	45,9%
Technology Transfer	26,9%	26,7%
Foreign Company Cooperation	17,7%	17,0%
COTS or Open Source Use	10,0%	10,4%

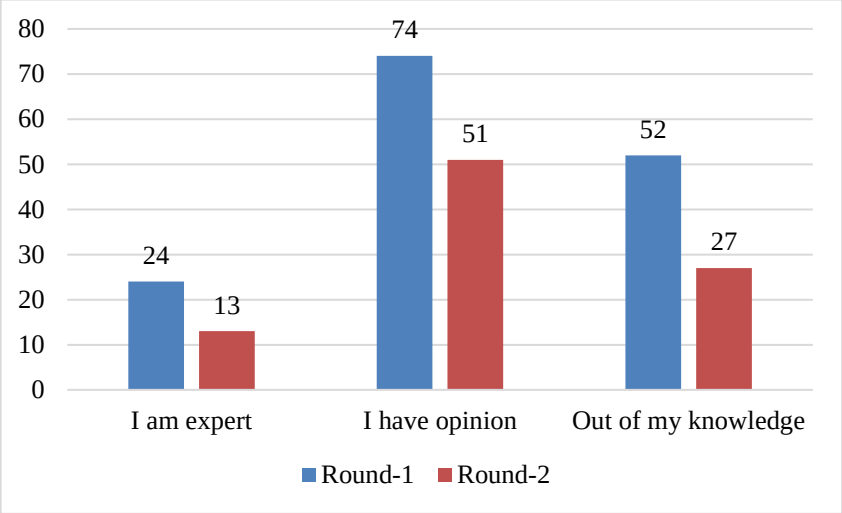


Figure G.10: Distribution of Expertise Levels (Statement-10)

Table G.10: Distribution of Answers in Delphi Rounds (Statement-10)

10b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	9,8%	32,8%	57,4%
Round-2	0,0%	0,0%	4,7%	34,4%	60,9%
10c (Economy)	1	2	3	4	5
Round-1	0,0%	0,0%	23,0%	36,1%	41,0%
Round-2	0,0%	0,0%	15,6%	42,2%	42,2%
10d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	29,5%	31,1%	26,2%	8,2%	4,9%
Round-2	31,3%	28,1%	34,4%	3,1%	3,1%

10e (Method)	Round-1	Round-2
R&D Investment	47,0%	47,1%
Technology Transfer	20,0%	19,0%
Foreign Company Cooperation	13,9%	10,7%
COTS or Open Source Use	19,1%	23,1%

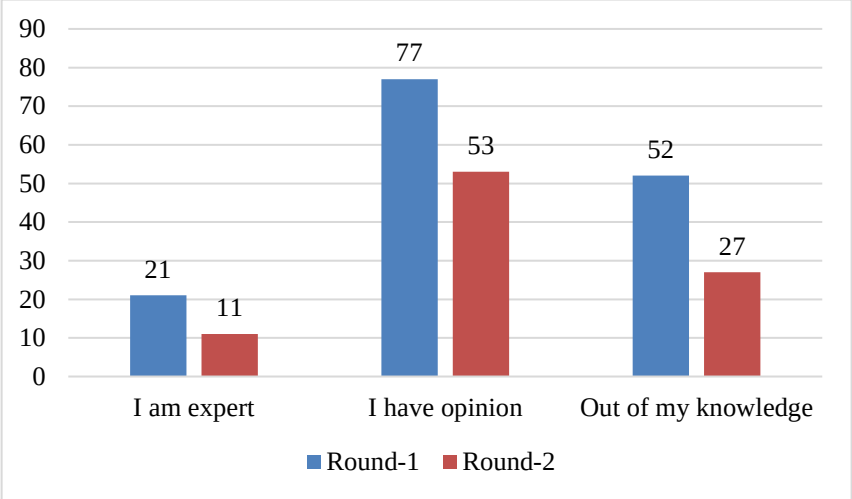


Figure G.11: Distribution of Expertise Levels (Statement-11)

Table G.11: Distribution of Answers in Delphi Rounds (Statement-11)

11b (Security)	1	2	3	4	5
Round-1	0,0%	3,2%	20,6%	28,6%	47,6%
Round-2	0,0%	1,6%	18,8%	25,0%	54,7%
11c (Economy)	1	2	3	4	5
Round-1	1,6%	6,3%	17,5%	38,1%	36,5%
Round-2	1,6%	3,1%	15,6%	43,8%	35,9%
11d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	29,0%	30,6%	25,8%	12,9%	1,6%
Round-2	29,7%	29,7%	31,3%	9,4%	0,0%

11e (Method)	Round-1	Round-2
R&D Investment	45,3%	46,7%
Technology Transfer	18,8%	19,2%
Foreign Company Cooperation	20,5%	17,5%
COTS or Open Source Use	15,4%	16,7%

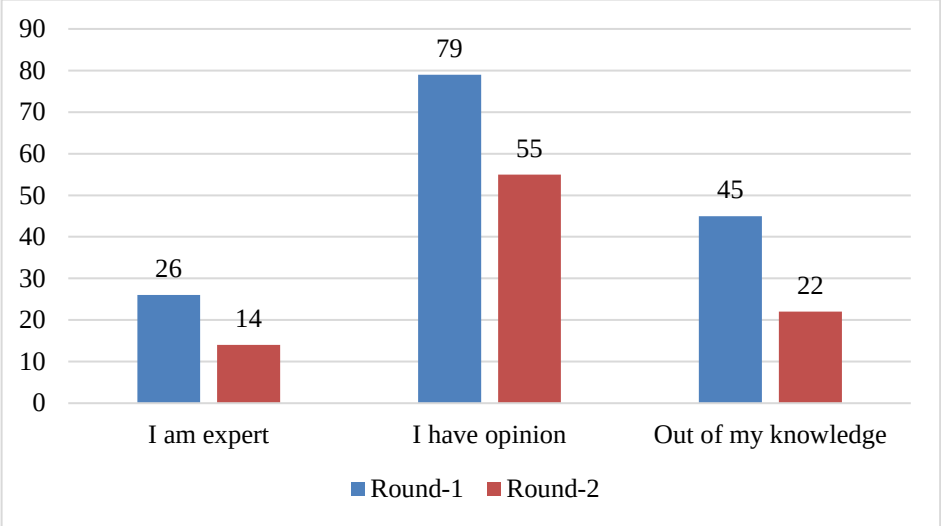


Figure G.12: Distribution of Expertise Levels (Statement-12)

Table G.12: Distribution of Answers in Delphi Rounds (Statement-12)

12b (Security)	1	2	3	4	5
Round-1	1,5%	2,9%	5,9%	39,7%	50,0%
Round-2	1,4%	1,4%	7,2%	36,2%	53,6%
12c (Economy)	1	2	3	4	5
Round-1	1,5%	1,5%	10,3%	32,4%	54,4%
Round-2	1,4%	1,4%	5,8%	34,8%	56,5%
12d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	14,7%	33,8%	23,5%	14,7%	13,2%
Round-2	13,0%	37,7%	27,5%	8,7%	13,0%

12e (Method)	Round-1	Round-2
R&D Investment	44,4%	47,2%
Technology Transfer	21,0%	22,8%
Foreign Company Cooperation	18,5%	15,0%
COTS or Open Source Use	16,1%	15,0%

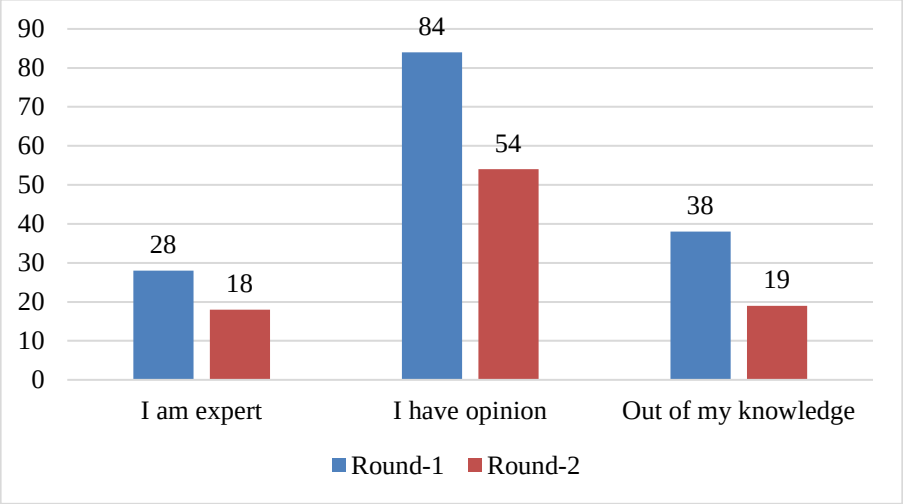


Figure G.13: Distribution of Expertise Levels (Statement-13)

Table G.13: Distribution of Answers in Delphi Rounds (Statement-13)

13b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	2,8%	26,4%	70,8%
Round-2	0,0%	0,0%	0,0%	22,2%	77,8%
13c (Economy)	1	2	3	4	5
Round-1	0,0%	4,2%	15,3%	34,7%	45,8%
Round-2	0,0%	2,8%	13,9%	33,3%	50,0%
13d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	37,5%	31,9%	13,9%	12,5%	4,2%
Round-2	40,3%	33,3%	15,3%	8,3%	2,8%

13e (Method)	Round-1	Round-2
R&D Investment	47,8%	48,1%
Technology Transfer	25,4%	23,7%
Foreign Company Cooperation	7,5%	6,7%
COTS or Open Source Use	19,4%	21,5%

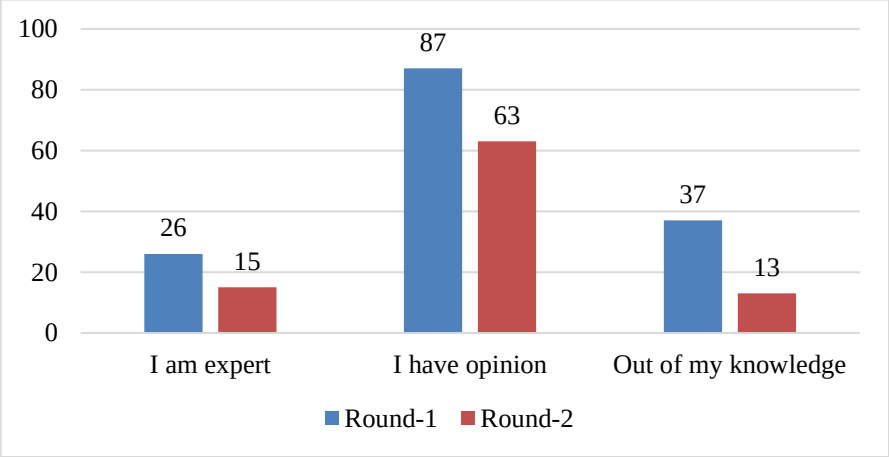


Figure G.14: Distribution of Expertise Levels (Statement-14)

Table G.14: Distribution of Answers in Delphi Rounds (Statement-14)

14b (Security)	1	2	3	4	5
Round-1	1,4%	1,4%	4,1%	23,0%	70,3%
Round-2	1,3%	1,3%	1,3%	20,5%	75,6%
14c (Economy)	1	2	3	4	5
Round-1	2,7%	6,8%	23,0%	25,7%	41,9%
Round-2	2,6%	5,1%	20,5%	23,1%	48,7%
14d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	25,7%	29,7%	24,3%	12,2%	8,1%
Round-2	29,5%	30,8%	25,6%	9,0%	5,1%

14e (Method)	Round-1	Round-2
R&D Investment	50,8%	50,0%
Technology Transfer	24,2%	25,7%
Foreign Company Cooperation	9,1%	5,6%
COTS or Open Source Use	15,9%	18,8%

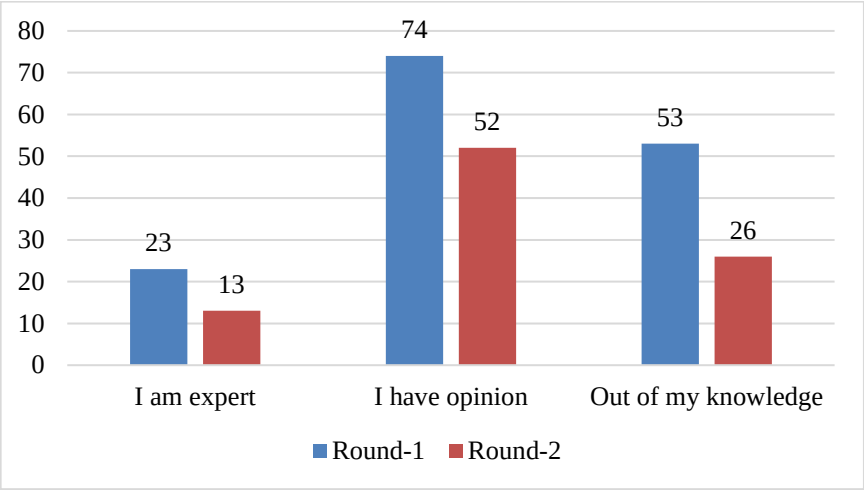


Figure G.15: Distribution of Expertise Levels (Statement-15)

Table G.15: Distribution of Answers in Delphi Rounds (Statement-15)

15b (Security)	1	2	3	4	5
Round-1	1,6%	0,0%	14,3%	22,2%	61,9%
Round-2	1,5%	0,0%	7,7%	24,6%	66,2%
15c (Economy)	1	2	3	4	5
Round-1	0,0%	1,6%	6,3%	27,0%	65,1%
Round-2	0,0%	1,5%	4,6%	24,6%	69,2%
15d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	9,5%	30,2%	23,8%	15,9%	20,6%
Round-2	9,2%	27,7%	32,3%	10,8%	20,0%

15e (Method)	Round-1	Round-2
R&D Investment	48,7%	49,6%
Technology Transfer	27,4%	27,3%
Foreign Company Cooperation	17,9%	15,7%
COTS or Open Source Use	6,0%	7,4%

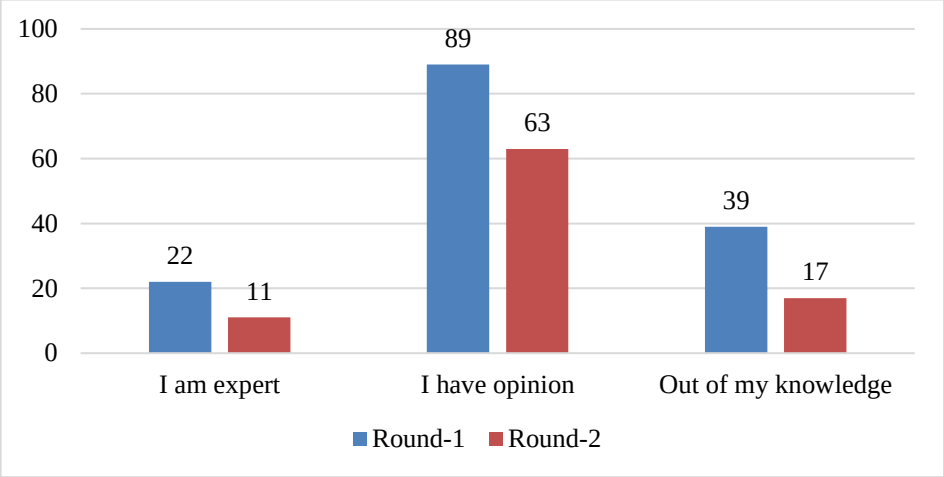


Figure G.16: Distribution of Expertise Levels (Statement-16)

Table G.16: Distribution of Answers in Delphi Rounds (Statement-16)

16b (Security)	1	2	3	4	5
Round-1	4,2%	1,4%	23,9%	29,6%	40,8%
Round-2	4,1%	1,4%	18,9%	32,4%	43,2%
16c (Economy)	1	2	3	4	5
Round-1	2,8%	5,6%	25,4%	33,8%	32,4%
Round-2	2,7%	2,7%	23,0%	37,8%	33,8%
16d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	47,9%	23,9%	19,7%	4,2%	4,2%
Round-2	55,4%	18,9%	18,9%	4,1%	2,7%

16e (Method)	Round-1	Round-2
R&D Investment	46,8%	47,4%
Technology Transfer	20,6%	20,4%
Foreign Company Cooperation	9,5%	8,8%
COTS or Open Source Use	23,0%	23,4%

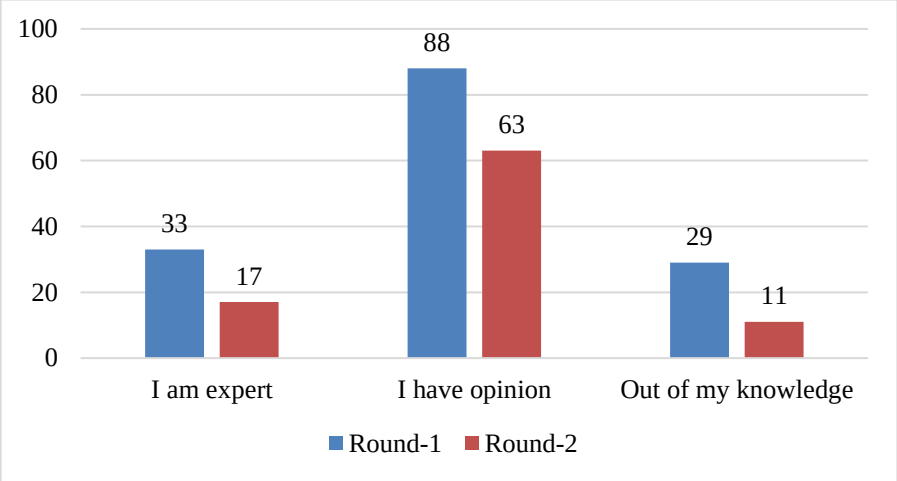


Figure G.17: Distribution of Expertise Levels (Statement-17)

Table G.17: Distribution of Answers in Delphi Rounds (Statement-17)

17b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	7,6%	25,3%	67,1%
Round-2	0,0%	0,0%	5,0%	25,0%	70,0%
17c (Economy)	1	2	3	4	5
Round-1	0,0%	7,6%	19,0%	36,7%	36,7%
Round-2	0,0%	6,3%	16,3%	38,8%	38,8%
17d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	41,0%	32,1%	17,9%	5,1%	3,8%
Round-2	43,8%	32,5%	18,8%	2,5%	2,5%

17e (Method)	Round-1	Round-2
R&D Investment	49,0%	49,0%
Technology Transfer	22,4%	19,2%
Foreign Company Cooperation	6,8%	5,3%
COTS or Open Source Use	21,8%	26,5%

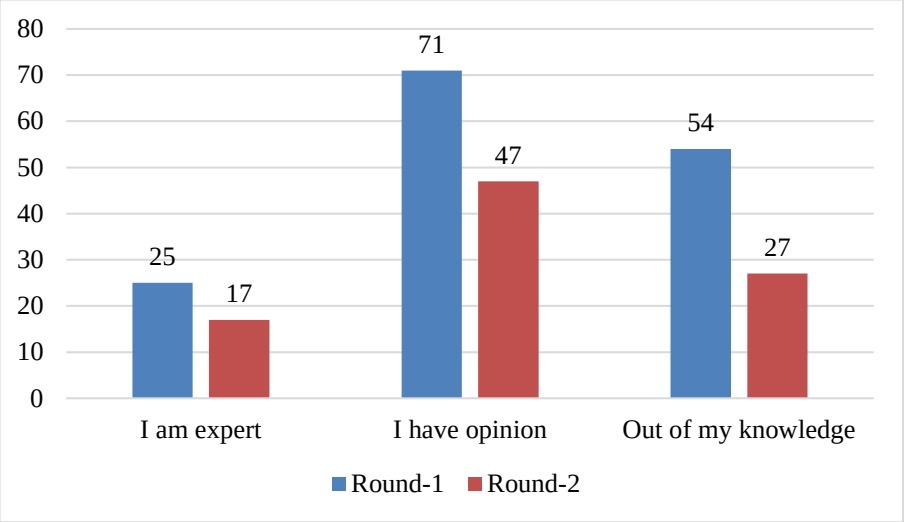


Figure G.18: Distribution of Expertise Levels (Statement-18)

Table G.18: Distribution of Answers in Delphi Rounds (Statement-18)

18b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	11,5%	23,0%	65,6%
Round-2	0,0%	0,0%	7,8%	20,3%	71,9%
18c (Economy)	1	2	3	4	5
Round-1	0,0%	3,3%	13,1%	34,4%	49,2%
Round-2	0,0%	3,1%	9,4%	35,9%	51,6%
18d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	26,2%	27,9%	32,8%	4,9%	8,2%
Round-2	29,7%	26,6%	32,8%	4,7%	6,3%

18e (Method)	Round-1	Round-2
R&D Investment	47,7%	48,3%
Technology Transfer	25,2%	26,3%
Foreign Company Cooperation	15,3%	11,9%
COTS or Open Source Use	11,7%	13,6%

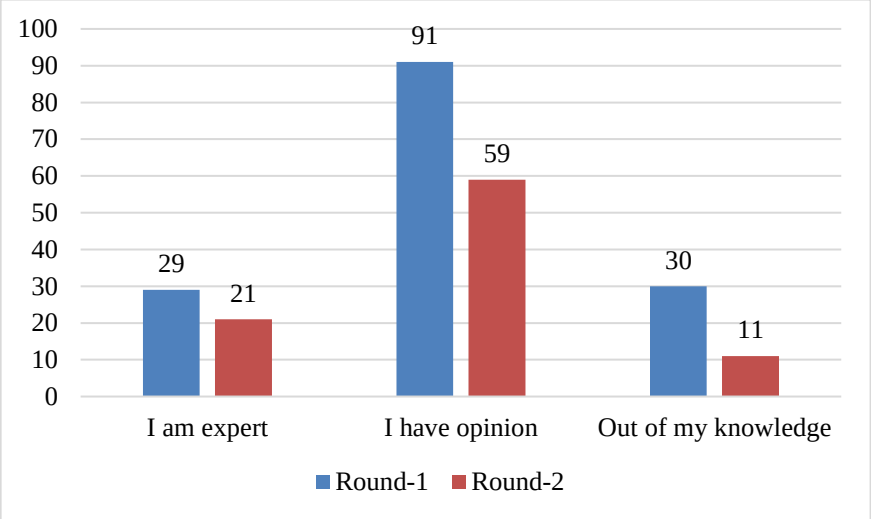


Figure G.19: Distribution of Expertise Levels (Statement-19)

Table G.19: Distribution of Answers in Delphi Rounds (Statement-19)

19b (Security)	1	2	3	4	5
Round-1	0,0%	1,3%	10,0%	23,8%	65,0%
Round-2	0,0%	1,3%	11,3%	22,5%	65,0%
19c (Economy)	1	2	3	4	5
Round-1	1,3%	3,8%	11,3%	31,3%	52,5%
Round-2	1,3%	2,5%	10,0%	32,5%	53,8%
19d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	32,5%	36,3%	23,8%	5,0%	2,5%
Round-2	36,3%	36,3%	23,8%	2,5%	1,3%

19e (Method)	Round-1	Round-2
R&D Investment	46,6%	47,3%
Technology Transfer	21,2%	20,9%
Foreign Company Cooperation	15,8%	13,5%
COTS or Open Source Use	16,4%	18,2%

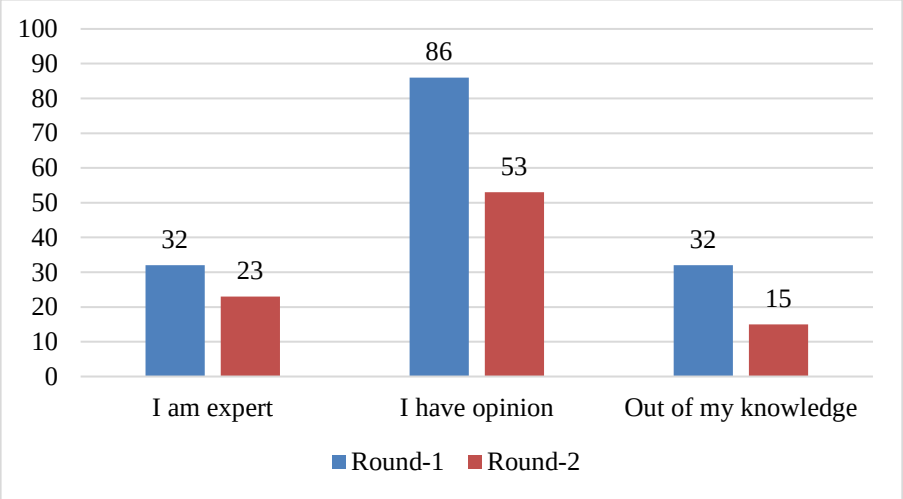


Figure G.20: Distribution of Expertise Levels (Statement-20)

Table G.20: Distribution of Answers in Delphi Rounds (Statement-20)

20b (Security)	1	2	3	4	5
Round-1	0,0%	4,1%	8,1%	20,3%	67,6%
Round-2	0,0%	5,3%	2,6%	18,4%	73,7%
20c (Economy)	1	2	3	4	5
Round-1	1,4%	2,7%	18,9%	31,1%	45,9%
Round-2	0,0%	2,6%	11,8%	35,5%	50,0%
20d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	48,0%	21,3%	21,3%	6,7%	2,7%
Round-2	50,0%	22,4%	19,7%	6,6%	1,3%

20e (Method)	Round-1	Round-2
R&D Investment	48,9%	51,1%
Technology Transfer	22,2%	20,4%
Foreign Company Cooperation	13,3%	9,5%
COTS or Open Source Use	15,6%	19,0%

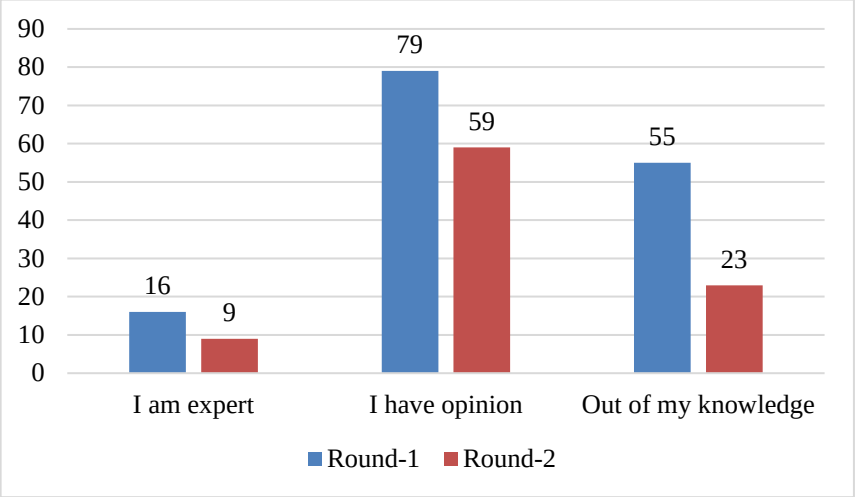


Figure G.21: Distribution of Expertise Levels (Statement-21)

Table G.21: Distribution of Answers in Delphi Rounds (Statement-21)

21b (Security)	1	2	3	4	5
Round-1	0,0%	1,6%	6,6%	8,2%	83,6%
Round-2	0,0%	1,5%	7,4%	7,4%	83,8%
21c (Economy)	1	2	3	4	5
Round-1	3,3%	8,2%	24,6%	18,0%	45,9%
Round-2	1,5%	4,4%	23,5%	20,6%	50,0%
21d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	14,8%	19,7%	24,6%	13,1%	27,9%
Round-2	13,2%	27,9%	29,4%	8,8%	20,6%

21e (Method)	Round-1	Round-2
R&D Investment	53,3%	51,7%
Technology Transfer	24,8%	25,8%
Foreign Company Cooperation	8,6%	9,2%
COTS or Open Source Use	13,3%	13,3%

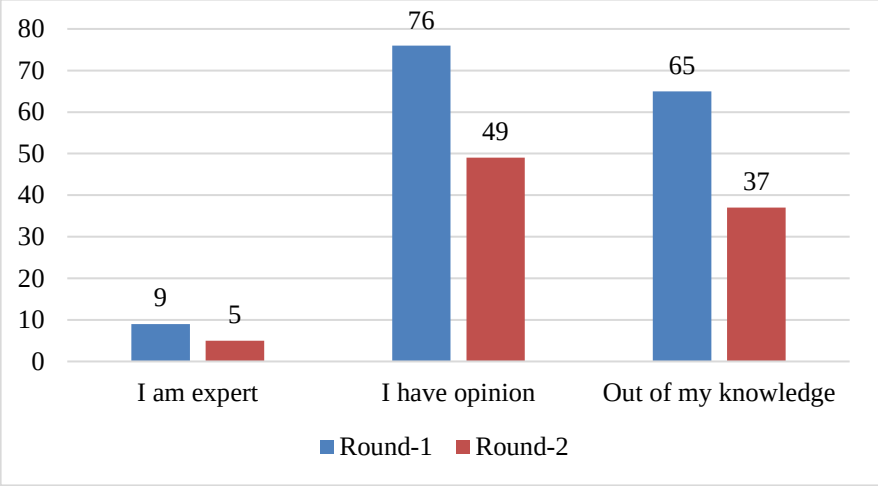


Figure G.22: Distribution of Expertise Levels (Statement-22)

Table G.22: Distribution of Answers in Delphi Rounds (Statement-22)

22b (Security)	1	2	3	4	5
Round-1	2,1%	2,1%	2,1%	18,8%	75,0%
Round-2	1,9%	0,0%	1,9%	13,0%	83,3%
22c (Economy)	1	2	3	4	5
Round-1	6,4%	6,4%	29,8%	12,8%	44,7%
Round-2	3,7%	7,4%	29,6%	11,1%	48,1%
22d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	20,8%	22,9%	33,3%	14,6%	8,3%
Round-2	18,5%	25,9%	40,7%	11,1%	3,7%

22e (Method)	Round-1	Round-2
R&D Investment	50,0%	50,5%
Technology Transfer	27,9%	27,8%
Foreign Company Cooperation	8,1%	6,2%
COTS or Open Source Use	14,0%	15,5%

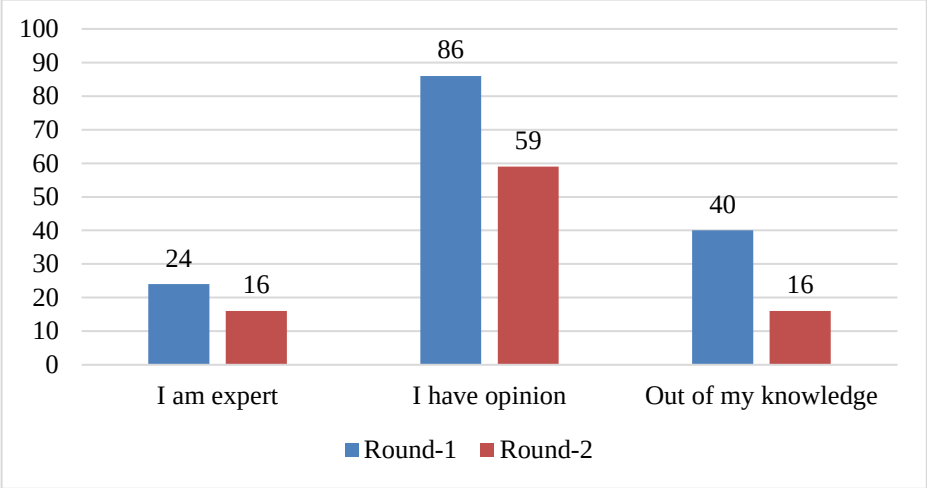


Figure G.23: Distribution of Expertise Levels (Statement-23)

Table G.23: Distribution of Answers in Delphi Rounds (Statement-23)

23b (Security)	1	2	3	4	5
Round-1	1,4%	2,7%	11,0%	20,5%	64,4%
Round-2	1,3%	2,7%	5,3%	21,3%	69,3%
23c (Economy)	1	2	3	4	5
Round-1	1,4%	4,1%	23,3%	26,0%	45,2%
Round-2	0,0%	2,7%	21,3%	26,7%	49,3%
23d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	30,6%	30,6%	12,5%	6,9%	19,4%
Round-2	29,3%	38,7%	12,0%	4,0%	16,0%

23e (Method)	Round-1	Round-2
R&D Investment	45,0%	47,8%
Technology Transfer	23,7%	22,8%
Foreign Company Cooperation	17,6%	14,7%
COTS or Open Source Use	13,7%	14,7%

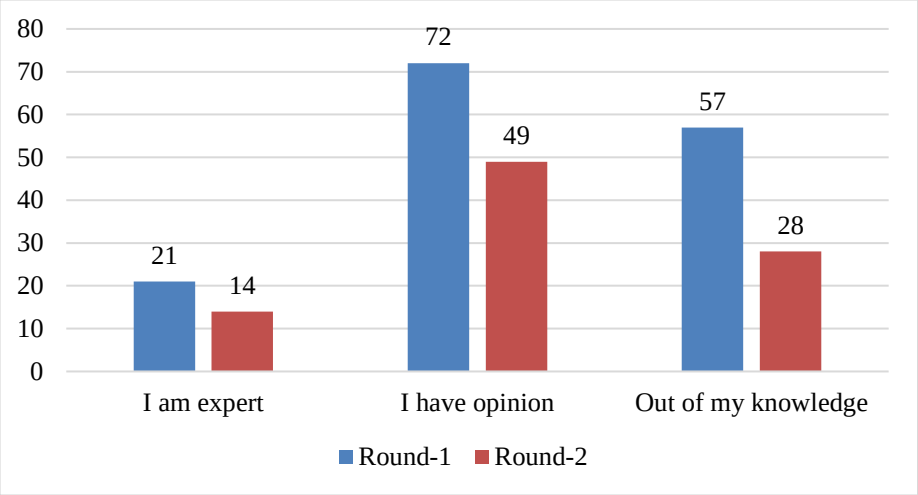


Figure G.24: Distribution of Expertise Levels (Statement-24)

Table G.24: Distribution of Answers in Delphi Rounds (Statement-24)

24b (Security)	1	2	3	4	5
Round-1	0,0%	0,0%	4,9%	19,7%	75,4%
Round-2	0,0%	0,0%	1,6%	22,2%	76,2%
24c (Economy)	1	2	3	4	5
Round-1	0,0%	4,9%	19,7%	27,9%	47,5%
Round-2	0,0%	3,2%	15,9%	34,9%	46,0%
24d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	19,7%	27,9%	27,9%	6,6%	18,0%
Round-2	20,6%	28,6%	31,7%	4,8%	14,3%

24e (Method)	Round-1	Round-2
R&D Investment	51,9%	50,9%
Technology Transfer	25,9%	27,7%
Foreign Company Cooperation	5,6%	3,6%
COTS or Open Source Use	16,7%	17,9%

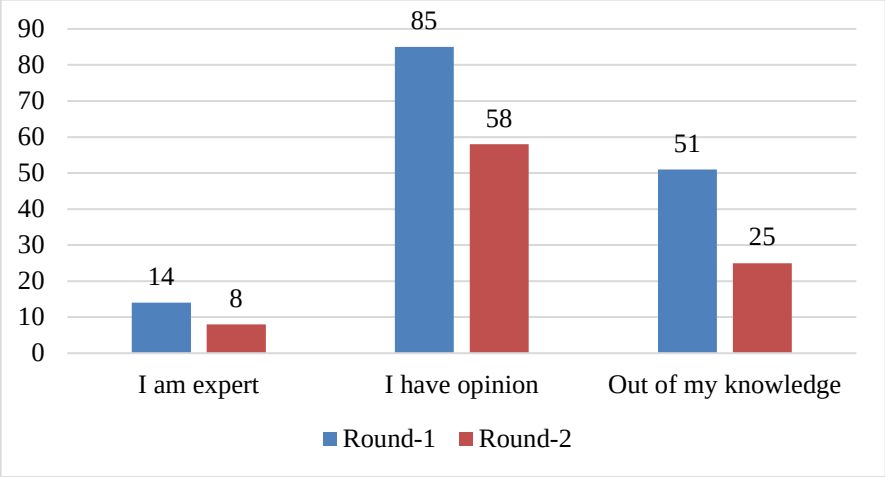


Figure G.25: Distribution of Expertise Levels (Statement-25)

Table G.25: Distribution of Answers in Delphi Rounds (Statement-25)

25b (Security)	1	2	3	4	5
Round-1	1,6%	1,6%	6,3%	34,9%	55,6%
Round-2	1,5%	0,0%	6,1%	30,3%	62,1%
25c (Economy)	1	2	3	4	5
Round-1	1,6%	3,2%	14,3%	22,2%	58,7%
Round-2	1,5%	1,5%	9,1%	24,2%	63,6%
25d (Timeframe)	2019-2023	2024-2029	2030-2035	2036-2040	2040 +
Round-1	9,5%	20,6%	25,4%	22,2%	22,2%
Round-2	7,6%	31,8%	24,2%	18,2%	18,2%

25e (Method)	Round-1	Round-2
R&D Investment	50,8%	50,8%
Technology Transfer	23,7%	27,4%
Foreign Company Cooperation	14,4%	12,1%
COTS or Open Source Use	11,0%	9,7%

APPENDIX H: TURKEY'S CYBERSECURITY TECHNOLOGY REVIEW

Cybersecurity Related Courses in the Universities of Turkey:

Table H.1: Cybersecurity Related Courses in Undergraduate Programs

Course Name	Course Name
Advanced Cryptography	Information Systems and Security
Cloud Computing and Security	Information Systems Security
Communication Security	Introduction to Cybersecurity
Computer and Network Security	Introduction to Blockchain
Computer Network Security	Introduction to Cryptography
Computer Security	Introduction to Cryptology
Computer Security and Ethics	Introduction to Cryptology and Computer Network Security
Computer Systems Security	Introduction to Cybersecurity
Critical Infrastructures and Security	Introduction to Data and Application Security
Cryptography and Network Security	Introduction to Data Security and Cryptography
Cryptographic Algorithms and Systems	Introduction to Encryption
Cryptographic Engineering	Introduction to Information Security
Cryptography	Introduction to Secure Coding
Cryptography and Security	Introduction to Systems Security
Cryptology	IT and Security Governance
Cryptology Basics	Modern Cryptography
Cyber Forensic	Network and Computer Security
Cyber Systems and Information Security	Network and Data Security
Cyber-Physical Systems and Security	Network and Information Security
Cybersecurity	Network Security
Cybersecurity and Energy Security	Network Security and Cyber Attack Management
Cybersecurity Fundamentals	Network Security and Encryption
Cyberwarfare and Cybersecurity	Network Security Principles
Data Protection and Security	Operating Systems Security
Data Security	Secure Application Engineering
Data Security and Cryptography	Secure Coding

Table H.1 (Cont'd)

Course Name	Course Name
Database Management and Security	Secure Programming Fundamentals
Encryption	Security Management
Homeland Security	Security Systems and Protocols
Informatics Security	Server Programming and Security
Information and Network Security	Software Security
Information Security	Special Topics in Computer Security Engineering
Information Security and Cryptography	Web Application Security

Table H.2: Cybersecurity Related Courses in Graduate Programs

Course Name	Course Name
Advanced Asymmetrical Cryptosystems	Cyber Systems and Information Security
Advanced Computer And Network Security	Cyber Warfare, Cybersecurity and Defense
Advanced Cryptography	Cyber Warfare and Security
Advanced Cryptography and Data Security	Cybercrime Analysis Hardware
Advanced Cryptology	Cybercrime Analysis Software
Advanced Encryption Systems and Decryption	Cybercrime Hardware
Advanced Information Security	Cybercrimes and Preventive Measures
Advanced Network Security	Cybercrimes and the Applications in the Turkish Laws
Advanced Symmetrical Cryptosystems	Cybersecurity
Advanced Topics in Computer and Network Security	Cybersecurity Law
Advanced Topics in Cryptography	Cybersecurity of Internet of Things
Advanced Topics in Network Security	Cybersecurity Planning and Management
Advanced Topics Network Security	Cybersecurity Primer
Applied Cryptanalysis	Cybersecurity: Ethics, Laws and Humanities
Applied Cryptography for Cybersecurity and Defense	Cyberwarfare
Applied Cryptology	Cyberwarfare and Security
Authentication in Cybersecurity	Cyberwarfare, Defense and Security
Big Data Security and Privacy	Data and Network Security
Biometric Systems and Authentication	Data Encryption and Network Security
Blockchain and Cryptocurrencies	Data Mining for Cybersecurity
Blockchain and Digital Coins	Data Mining in Information Security
Blockchain Technologies	Data Mining Methods in Security
Blockchain: Security and Applications	Data Recovery Techniques

Table H.2 (Cont'd)

Course Name	Course Name
C4I and Information Warfare	Data Security
Cloud Computing and Security	Data Security and Secure Software Development
Cloud Computing Security	Database and Software Security
Computational Number Theory	Database Security
Computer and Network Security	Digital Evidences and Computer Crimes
Computer Ethics	Digital Forensics
Computer Forensics	Digital Forensics and Emergency Response to Cyber Attacks
Computer Network Protocols and Network Security	Digital Signature Applications
Computer Network Security	E-Commerce Security
Computer Network Vulnerability Analysis	Encryption and Network Security
Computer Security	Encryption Techniques
Computer Security and Cryptography	Encryption: Algorithms and Applications
Computer System Security	End User Security
Computer Systems and Network Security	Enterprise Information Security
Critical Authentication Infrastructure and Applications	Ethical Hacking
Cryptanalysis	Forensics Information Security and Technical Review
Cryptographic Algorithms and Systems	Forensics Techniques and Law
Cryptographic Engineering	Formal Methods for Safety and Security
Cryptographic Methods	Hacker Ethics and Forensics
Cryptographic Microprocessor Design	Hash Functions and Message Authentication Codes
Cryptographic Protocols	Human Factors in Cyber Physical Systems
Cryptography	Information and Computer Security
Cryptography and Computer Security	Information and Network Security
Cryptography and Number Theory	Information Assurance and Secure Software Development
Cryptology	Information Hiding Techniques
Cryptology and Cybersecurity	Information Management and Security
Current Subjects in Informatics Security	Information Security
Cyber Data Analytics	Information Security and Crypto Applications with Java
Cyber Defense Technics and Control Mechanisms	Information Security and Encryption Techniques
Cyber Offense and Defense Methods	Information Security and Management
Information Security and Privacy	Pair-based Cryptography
Information Security Audit and Assurance	Penetration Test and Vulnerability Analysis
Information Security Law	Penetration Testing
Information Security Law and Policy	Penetration Testing and Security Assessments

Table H.2 (Cont'd)

Course Name	Course Name
Information Security Management	Penetration Testing and Vulnerability Analysis
Information Security Management System	Penetration Tests
Information Security Methods	Penetration Tests and Security Assessment
Information System Risk Management	Privacy in Internet and Mobile Networks
Information System Security Engineering	Privacy Preserved Data Management
Information Systems and Security	Programming Language Security
Information Systems Security	Public Key Cryptographic Systems
Information Systems Security and Management	Public Key Cryptography
Information Warfare	Quantum Cryptography and Applications
Internet and Data Security	Risk Management
Internet and e-Commerce Security	Secure Application Development
Internet Crimes and Data Mining	Secure Card Applications
Internet Security	Secure Coding and Software Security
Internet Security Protocols	Secure Implementation and Side Channel Analysis
Introduction to Biometrics	Secure Programming
Introduction to Cryptography	Secure Software Design and Programming
Introduction to Cryptography and Security Protocols	Secure Software Development
Introduction to Cryptography Engineering	Security and Privacy Engineering
Introduction to Cryptology	Security and Privacy in Big Data
Introduction to Cryptology and Computer Network Security	Security and Privacy in Wireless Networks
Introduction to Cybersecurity	Security Event Management
Introduction to Ethical Hacking	Security for Cloud Computing
Introduction to Information Security	Security for Cyber-Physical Systems and IoT
Introduction to Information Security and Cryptography	Security for Databases, Big Data and Social Data Processing
Intrusion Detection and Prevention	Security in Cloud Computing
Machine Learning for Cybersecurity	Security in Cloud Computing and Cryptography for Privacy
Machine Learning Methods for Cybersecurity	Security in Embedded Systems
Machine Learning Methods for Cybersecurity	Security in Wireless Networks
Machine Learning Methods in Security	Security of Symmetric Encryption Algorithms
Malware Analysis	Security Products Management
Malware Analysis and Detection	Security Products Monitoring
Malware Analysis and Reverse Engineering	Security, Law and Ethics
Malware Analysis: Tools and Techniques	Signal Intelligence
Malware and Software Vulnerability Analysis	Software and Web Security
Mobile Security	Software and Web Security
Modern Cryptography	Software Security

Table H.2 (Cont'd)

Course Name	Course Name
Network and Information Security	Software Vulnerability Analysis
Network and System Security	Special Topics in Information Security
Network and Web Security	Statistical Database Security
Network Defense Systems	Stochastic Analysis in Cybersecurity Systems
Network Forensics	Strategic Cybersecurity
Network Security	Stream Ciphers
Network Security and Encryption	Symmetric Encryption Algorithms and Security Analysis
Network Security and Network Forensics	TCP/IP Security
Network Traffic Analysis	The Legal Dimensions of Cybersecurity
Number Theory for Cryptography	Vulnerability Scanning and Prevention
Online Crime Investigation	Web Application Security
Operating System and Network Security	Wireless and Ad-Hoc Network Security
Operating System Security	Wireless Network Security
Operating Systems Security	

Note and Disclaimer

Product and company lists were mainly prepared based on the companies' web sites and last updated in April 2019. Please refer to company web sites for up-to-date information.

Table H.3: Turkish Cybersecurity Products (Used as Header for the Next Table)

Technopark	Turkish Cybersecurity Cluster Member (TCC)	Company	No	Network Security	Endpoint Security	Identity & Access Management	Messaging and Communication Security	Data Security	Cloud Computing Security	Application Security	Internet Security	Mobile Devices Security	Industrial Control (SCADA) Systems Security	Internet of Things (IoT) Security	Operating Systems and Container Security	Cybersecurity for Autonomous and Smart Platforms	Hardware Security	Firmware Security	Cybersecurity Analytics	Cyber Intelligence	Cybersecurity Operations	Cybersecurity Event Management	Cyber Forensics	Cybersecurity Risk and Compliance Management	Consultancy	Training
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Table H.4: Turkish Cybersecurity Products (Company - Product/Service Group Matrix)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	AltoSec Bilişim	X	Bilkent Cyberpark	S					S		P															
2	ALYO		ODTÜ Teknokent								P	S														
3	Argela	X	İTÜ Arı Teknokent ODTÜ Teknokent	P																						
4	arjeta		Göller Bölgesi	P																		S				
5	ArkSigner		Bilkent Cyberpark			P																				
6	ASELSAN	X	Teknopark Ankara	P		P	P	P																		
7	atarlabs	X	Bilkent Cyberpark																		P	P				
8	Ayesaş	X	ODTÜ Teknokent							P									P							
9	b!nalize	X																			P	P				
10	Barikat	X		P	S	S	S	S		S	S									P	S	S		P	S	S
11	BG-Tek	X	Ulutek	P		P															P	P		S		
12	Biznet Bilişim	X	ODTÜ Teknokent	S	P	P		S		S	S								S		S	S		P	S	S
13	BT Yazılım	X				P		P																		
14	BTrisk	X	Yıldız Teknokent																		P			P		S
15	BTYÖN	X						P													P			P	S	S
16	CHOMAR	X	Mersin Teknopark		P						P															
17	CRYPTTECH	X	Hacettepe Teknokent Yıldız Teknokent	P		P		P														P		P		
18	CTech	X	Teknopark İstanbul	P																	P	P		P		S
19	CUSTOS Solutions		Teknopark İstanbul		S		S	P			S															
20	DIFOSE	X																					P		S	
21	Digisecure																					S	P	S	S	

Table H.4 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
22	eBilge	X	Mersin Teknopark		P							P														
23	e-imzaTR		Hacettepe Teknokent			P																				
24	EMT Electronics				S			P				S											P		S	S
25	ENDPOINT LABS		Teknopark İstanbul	P			S			S	P												S	S	S	
26	ePati Bilişim	X	Mersin Teknopark	P							P											P				
27	Epsilon Grup	X	Teknopark Ankara			P																		S		
28	ForenSoft	X			P						P															
29	Gais Siber Güvenlik	X			S														P	P		S		P		
30	HAVELSAN	X	Bilişim Vadisi Hacettepe Teknokent ODTÜ Teknokent				P	P			P	P								P		P				
31	ICterra	X	ODTÜ Teknokent																			P			S	
32	INVICTUS		Teknopark İstanbul							S										P				S	S	S
33	ISR Bilgi Güvenliği (tina Security)	X		P																P	P		S	S	S	S
34	Kale Yazılım		ODTÜ Teknokent			P																				
35	Karmasis	X	Bilkent Cyberpark																			P			S	
36	Konneka		Bilkent Cyberpark	P							P											P			S	
37	Kripteks Forensics																						P			
38	Kriptex Security		Sakarya Teknokent			P																				
39	Kron	X	Bilkent Cyberpark	S		P																		P		
40	Labris	X	ODTÜ Teknokent	P			P				P										P	P			S	
41	Letta Grup		Bilişim Vadisi											P				P								

Table H.4 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
42	LİMATEK Sistem	X				P						P														
43	Logo Siber Güvenlik	X		P																						
44	Logsign																			S		P				
45	LOKİ Bilgi ve Güvenlik								P																	
46	Marta Teknoloji	X	Mersin Teknopark	P			P																		S	
47	MAY Cyber Technologies	X	ODTÜ Teknokent	P																	P	P			S	S
48	MIA Teknoloji		Gazi Teknopark			P														S						
49	MilSOFT	X	ODTÜ Teknokent	P			P	P		P																
50	nebula	X																		P	S	S		S	S	S
51	NETAŞ	X	ODTÜ Teknokent				P					P												S	S	S
52	Netsparker	X								P	P													S		
53	NRS Siber Güvenlik		Sakarya Teknokent							S	S									P	P			P	S	
54	NurD Yazılım		Ege Teknopark ODTÜ Teknokent Yıldız Teknokent	P	P						P															
55	ODC Business Solutions		Bilkent Cyberpark																P	P						
56	Okyanus Bilişim		Kocaeli Teknopark			P																				
57	onesTechnology		Ankara Ü. Teknokent			P																				
58	Onur Mühendislik	X		P																						
59	ÖLÇSAN	X				P																		S		S
60	PARTA Networks		Teknopark İzmir	P		P					P													S	S	S

Table H.4 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
61	Pavotek	X	Teknopark İstanbul	P																						
62	Picus Security	X	Hacettepe Teknokent																		P			P		
63	Pona			P																						
64	PRISMA CSI		Bilkent Cyberpark							P														S		S
65	Privia		Cumhuriyet Ü.	S																	P		S	S	S	S
66	PRODAFT																		P	P	P					
67	Qetra			P	S						P													S		
68	Rekare (r2)		Ulutek	P																		P			S	S
69	Roksit	X		P	P						P															
70	SARENTE		Bilişim Vadisi	P																						
71	Sarp Siber Güvenlik	X																						P		
72	Saykal Electronics		Bilişim Vadisi															P								
73	sayTEC	X		P			P	P																		
74	SemperTech	X																			P					
75	STM	X																	P	P	P	P			S	S
76	stratek		ODTÜ Teknokent			S																				
77	SWORDSEC	X	Teknopark Ankara							S				S					S	P		S		S	S	S
78	tac Consultancy		Yıldız Teknokent	P																						
79	TerraMedusa		Yıldız Teknokent																	P				S	S	S
80	Trapmine	X			S																					
81	TÜBİTAK BİLGEM			P		P	P	P	P		P								P	P				S	S	S
82	TÜBİTAK ULAKBİM					P															P	P				
83	TÜRKTRUST	X				P																			S	S

Table H.4 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
84	ULAK Haberleşme	X	ODTÜ Teknokent	P																						
85	Usishi Bilişim	X	Teknopark İstanbul						P																	
86	Verisis Veri ve İletişim	X	ODTÜ Teknokent																				P			
87	YATEM	X																				P				
88	YD Yazılım	X	ODTÜ Teknokent							P																
89	YÖNSİS	X		P							P											P				
90	Zemana	X	Bilkent Cyberpark		P							P														

Table H.5: Turkish Companies Having Cybersecurity Products (Company – Product Matrix)

No	Company	TCC	Technopark	Technology	Product
1	AltoSec Bilişim	X	Bilkent Cyberpark	WAF Software	AltoSec
2	ALYO		ODTÜ Teknokent	Browser Security	ALYO DRM
3	Argela	X	İTÜ Arı Teknokent ODTÜ Teknokent	Network Security	Argela SENS-PS, Argela SENS-CG
4	arjeta		Göller Bölgesi	Network Security	Xlog
5	ArkSigner		Bilkent Cyberpark	Digital Signature	ArkSigner

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
6	ASELSAN	X	Teknopark Ankara	Encryption Devices Secure Gateway (Air Gap) Secure Storage Secure Key Management Secure Satcom Phone	2064, 2034 SAHAB 2049, 2190 2070, 2080 2114
7	atarlabs	X	Bilkent Cyberpark	Security Orchestration, Automation and Response	Atar
8	Ayesaş	X	ODTÜ Teknokent	Software Testing	TRUVA
9	b!nalize	X		Evidence Collector for Incident Response	IREC-IR
10	Barikat	X		Cyber Intelligence DDoS Prevention Asset Management & Security	SIPER LODDOS ASMA
11	BG-Tek	X	Ulutek	BYOD Security Firewall Log Management Two-Factor Authentication	Coslat HotSpot Coslat Firewall Coslat Mirror Coslat 2FA
12	Biznet Bilişim	X	ODTÜ Teknokent	Infosec Management System Tool Digital Signature Vulnerability Management	ISMart SignArt BIZZY
13	BT Yazılım	X		Data Security and Authentication	securKEY
14	BTrisk	X	Yıldız Teknokent	InfoSec Management System	btrwatch
15	BTYÖN	X		InfoSec Management Tool Privacy	Optimate Solutions BGYS Optimate Solutions KVKK
16	CHOMAR	X	Mersin Teknopark	Anti-malware Endpoint Security Anti-malware & Web/E-mail Security	CHOMAR Antivirus CHOMAR Endpoint CHOMAR Internet Security

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
17	CRYPTTECH	X	Hacettepe Teknokent Yıldız Teknokent	SIEM Gateway Authorization Encryption Log Management Network Monitoring	CRYPTOSIM CRYPTOSPOT GiZ Encryption CRYPTOLOG UnitMON
18	CTech	X	Teknopark İstanbul	Cyber Exercise Platform Deep Packet Inspection Integrated Cybersecurity Solution	CyberRange CTech DPI CUSTOM ISM
19	CUSTOS Solutions		Teknopark İstanbul	Secure Data Storage	KRYPTOS
20	DIFOSE	X		Cyber Forensics	DIFOSE DF1, PCU, CRB, MFAS, CFAS
21	Digisecure			Computer Forensics	Forensafe
22	eBilge	X	Mersin Teknopark	Antivirus Secure Voice Call for Mobile Phones	CHOMAR Secure Call
23	e-imzaTR		Hacettepe Teknokent	Digital Signature	EİMZATR
24	EMT Electronics			Digital Forensics Secure Data Disposal	EMT VZ MultiMedia
25	ENDPOINT LABS		Teknopark İstanbul	UTM	Endpoint-Labs UTM
26	ePati Bilişim	X	Mersin Teknopark	Firewall L2 Tunneling Log Management	Antikor v2 Firewall Antikor v2 Layer2 Antikor Log
27	Epsilon Grup	X	Teknopark Ankara	Multifactor Authentication	Epsilon OTP
28	ForenSoft	X		Anti-malware (Gateway)	Siber Tehdit Kalkanı
29	Gais Siber Güvenlik	X		Penetration Testing Malware Analysis Cyber Intelligence Service	Gais Cloud-based Pentest fenriscan Peyk

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
30	HAVELSAN	X	Bilişim Vadisi Hacettepe Teknokent ODTÜ Teknokent	SIEM DLP WAF & Load Balancing Secure Communication Cyber Intelligence	HVL GÖZCÜ SIEM HVL BARİYER DLP HVL KALKAN WAF/LB İLETEE ASTARUS
31	ICterra	X	ODTÜ Teknokent	SIEM Integration	Suricata
32	INVICTUS		Teknopark İstanbul	Cyber Intelligence	USTA National Cyber Threat Network
33	ISR Bilgi Güvenliği (tina Security)	X		Intrusion Prevention System Honeypot Anti-malware	tina (Threat Intercepting Network Appliance)
34	Kale Yazılım		ODTÜ Teknokent	Authentication	EKDS (Elecronic ID Verification System)
35	Karmasis	X	Bilkent Cyberpark	Log Management	Infraskope
36	Konneka		Bilkent Cyberpark	Load Balancing and WAF GPS Firewall Log Manager Next Generation Firewall SSL/URL Filter	HAVELSAN Web Kalkanı Konneka LQGDOR Konneka Konneka
37	Kripteks Forensics			Digital Forensics	Kripteks Forensics
38	Kriptex Security		Sakarya Teknokent	Identity Verification	NIVST
39	Kron	X	Bilkent Cyberpark	Access Management Network Configuration Management Network Packet Broker	SINGLE CONNECT SINGLE COMMAND SINGLE CONTROL

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
40	Labris	X	ODTÜ Teknokent	UTM DDoS Prevention Secure Hotspot Log Manager	Labris UTM Harpp DDoS Mitigator Labris WAUTH+ Labris LOG
41	Letta Grup		Bilişim Vadisi	IoT/Firmware Security	MANAGEATM, MANAGELOCK
42	LİMATEK Sistem	X		Identity and Access Management Mobile Device Management	LimRAD HOTSPOT, LimRAD Auth LimRAD EMM / MDM
43	Logo Siber Güvenlik	X		Firewall	Berqnet
44	Logsign			SIEM, Log Management	Logsign
45	LOKİ Bilgi ve Güvenlik			Cloud Computing Security	LOKI
46	Marta Teknoloji	X	Mersin Teknopark	VOIP Firewall Network Analysis	SIPSEC Voip Firewall Lucia Network Analysis
47	MAY Cyber Technologies	X	ODTÜ Teknokent	Network Access Control Log Management Security Operation Center Net and System Monitoring Process Management	SCOP NET SCOP VISION SCOP SOC SCOP MON SCOP DESK
48	MIA Teknoloji		Gazi Teknopark	Biometrics & Authentication	MIA
49	MilSOFT	X	ODTÜ Teknokent	Software Integrity Protection Secure Gateway (Air Gap) Secure Communication	MilGUARD Mil-CDS Mil-DDS
50	nebula	X		Cyber Intelligence Service	N-SIS
51	NETAŞ	X	ODTÜ Teknokent	Secure VoIP Mobile Security	NOVA V-SPY, NOVA V-GATE NOVA S/COM
52	Netsparker	X		Web Application Security	Netsparker

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
53	NRS Siber Güvenlik		Sakarya Teknokent	Cyber Intelligence Vulnerability Management Risk Management Security Operation Center	NormShield - NSCTI NormShield - NSUVM NormShield - NSTS NormShield - NSSOC360
54	NurD Yazılım		Ege Teknopark ODTÜ Teknokent Yıldız Teknokent	UTM	Comodo Korugan
55	ODC Business Solutions		Bilkent Cyberpark	Secure Banking	SM Secure
56	Okyanus Bilişim		Kocaeli Teknopark	Secure Authentication Secure Login	O-KEY SECUREACCESS O-KEY IDENTITY
57	onesTechnology		Ankara Ü. Teknokent	Biometric Security	BioAffix
58	Onur Mühendislik	X		Crypto Gateway (to IP Device)	RIG-200SZ
59	ÖLÇSAN	X		Authentication Access Control	K!M EagleEye K!M KIMO, K!M FalconEye
60	PARTA Networks		Teknopark İzmir	Next Generation Firewall (Software) Network Security Authentication	PartaGuard TARGITAS PartaPoint
61	Pavotek	X	Teknopark İstanbul	Network Security	Pavotek Router, Switch, Modem, Access Point
62	Picus Security	X	Hacettepe Teknokent	Breach and Attack Simulation	Picus
63	Pona			Firewall	PONIVA
64	PRISMA CSI		Bilkent Cyberpark	Secure App Development	DOJO
65	Privia		Cumhuriyet Ü.	Cybersecurity Operation Center	AVCI

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
66	PRODAFT			Cyber Threat Intelligence Fraud Detection Threat Intelligence & Response	GPACT NoFraudThanks Raven
67	Qetra			Firewall	Qetra Firewall
68	Rekare (r2)		Ulutek	Firewall Log Management	Logix Firewall Logix Bridge
69	Roksit	X		Firewall DNS Security Anti-Malware	Roksit Secure DNS DNS and Threat visibility Roksit Threat Hunter
70	SARENTE		Bilişim Vadisi	Network Monitoring	Kron Single Monitor& Connect
71	Sarp Siber Güvenlik	X		Asset and Configuration Management	SOCRadar
72	Saykal Electronics		Bilişim Vadisi	Firmware Security	Saykal Embedded
73	sayTEC	X		VPN All in one Server Secure Voice and Multimedia	sayTRUST sayFUSE sayPHONE
74	SemperTech	X		Integrated Cybersecurity Secure Information Management Platform	Cybernate Bilgin
75	STM	X		Cybersecurity Decision Support System Cyber Fusion Center Security Operation Center	STM CyDecSys STM Fusion STM SOC
76	stratek		ODTÜ Teknokent	Digital Signature	SignCUBE
77	SWORDSEC	X	Teknopark Ankara	OSINT Collection	SwordEye
78	tac Consultancy		Yıldız Teknokent	Advanced SNMP	CSI Force
79	TerraMedusa		Yıldız Teknokent	Cyber Intelligence Service	TerraMedusa
80	Trapmine	X		Endpoint Security	Trapmine Endpoint Security

Table H.5 (Cont'd)

No	Company	TCC	Technopark	Technology	Product
81	TÜBİTAK BİLGEM			Identity Management Digital Signature IP Encryption Synchronous Data Encryption Secure Storage Secure Messaging Secure Card Crypto Management Cyber Threat Detection Honeypot DLP Secure Cloud Computing	Safir Kimlik, EKDS ESYA, KERMEN, İMZAGER IPKC SVKC SIR GMS, GMİ KEC, GEM EKADAS STAMS SORT VKÖS Safir
82	TÜBİTAK ULAKBİM			Integrated Cybersecurity Solution Identity Management	Ahtapot EnGerek
83	TÜRKTRUST	X		Digital Signature	Arnica, Castan, Platan, Tilia, Spira, Palma, Sekoya, Dianta
84	ULAK Haberleşme	X	ODTÜ Teknokent	Software Defined Network Security	MİLAT
85	Usishi Bilişim	X	Teknopark İstanbul	Cloud Computing Security	Buluthan
86	Verisis Veri ve İletişim	X	ODTÜ Teknokent	Digital Forensics	
87	YATEM	X		Log Management	LogCollector, LogStore
88	YD Yazılım	X	ODTÜ Teknokent	Software Code Analysis	BugStack.io
89	YÖNSİS	X		UTM	SNC ÇANAKKALE
90	Zemana	X	Bilkent Cyberpark	Anti-malware Anti Logger Mobile Antivirus Endpoint Security	Zemana

Table H.6: Cybersecurity Services in Turkey (Company – Service Matrix) (Used as Header for the Next Table)

No	Company	Cluster Member (TCC)	Technopark	Firewall	IDS/IPS	Load Balancing	SSL/VPN	Web/URL Filtering	WAF & Web Security	Network Access Control	DDoS Prevention	Log Management	Penetration Testing	Vulnerability Analysis	SIEM	Security Operation Center	Digital Signature	DLP	Red Team & Ethical Hacking	Malware Analysis	Anti-malware	Fraud Detection	Consultancy	Training
				1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**

Table H.7: Cybersecurity Services in Turkey (Company – Service Matrix)

No	Company	TCC	Technopark	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**
1	4B Yazılım		Yüzüncü Yıl Teknokent	S									S										S	S
2	ADEO Bilişim	X	Sakarya Teknokent										S	S									S	S
3	AGMLab		ODTÜ Teknokent																				S	
4	Akbim Bilgisayar		Adnan Menderes																		S			
5	aktek		Yıldız Teknokent	S	S		S	S		S											S		S	
6	Ankaraimza (@imza)		Hacettepe														S						S	
7	arquanum		İTÜ Arı Teknokent										S			S			S	S				

Table H.7 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
8	B&B Bilişim		Erciyes																				S	
9	BEAM Teknoloji												S	S									S	S
10	BGA Security																						S	S
11	Bilge SGT	X	Hacettepe										S						S	S			S	S
12	BilgeAdam		Bilkent Cyberpark İTÜ Arı Teknokent																					S
13	Bilishim												S	S		S							S	S
14	Bimser Çözüm		Kocaeli Teknopark																				S	
15	BlueCyt		Hacettepe											S		S								
16	BT Bilgi Teknolojileri									S														
17	Btm Arge		Konya Teknopark																				S	
18	Corvues Bilişim	X																					S	S
19	Cyber Struggle (SECHOB)	X	İTÜ Arı Teknokent																					S
20	CYBERAGE	X									S	S	S							S			S	S
21	CyberArts Bilişim	X																					S	
22	Cyberlab												S	S	S					S			S	S
23	cybernova		Samsun Teknopark										S										S	S
24	Cydets		Yüzüncü Yıl Teknokent										S										S	S
25	Cymsoft Bilişim	X								S			S										S	S

Table H.7 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
26	DEFENSEIN Siber Savunma		Sakarya Teknokent										S	S		S			S				S	S
27	dematek		InnoPark Konya									S												
28	DEMSISTEM													S									S	
29	DEREKA					S	S				S													
30	earth		Samsun Teknopark																				S	
31	EGY Bilişim		Yıldız Teknokent																					
32	EMFA Software & Colsuntancy												S	S									S	S
33	EMT Electronics																						S	S
34	EY Danışmanlık															S							S	
35	FBT		Yıldız Teknokent													S							S	
36	Globax Teknoloji		Yıldız Teknokent																				S	
37	InfoNet			S	S																		S	
38	Infoway						S																	
39	Innova		İTÜ Arı Teknokent																				S	
40	Invento		Boğaziçi										S	S									S	
41	Inventum		Boğaziçi										S	S									S	
42	Innotek		Bilişim Vadisi																		S			
43	innovera	X									S	S	S	S						S			S	
44	intersis		Erciyes	S				S	S	S					S									
45	intertech		ODTÜ Teknokent																				S	

Table H.7 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
46	inventiv												S											
47	KEPKUR		Yıldız Teknokent														S							
48	keytorc		Yıldız Teknokent																					
49	KoçSistem	X	ODTÜ Teknokent	S	S	S	S	S	S	S	S	S	S	S	S	S								
50	KuanTek		Bilişim Vadisi	S	S		S														S		S	
51	Lostar		Sakarya Teknokent										S	S					S				S	S
52	Morten																						S	S
53	MOS Academy																						S	S
54	NARLAB		Bilkent Cyberpark																				S	
55	National Keep		Hacettepe								S		S	S									S	S
56	Native Teknoloji		Teknopark İstanbul						S		S		S										S	
57	NETCOM		Erciyes										S		S						S			
58	Netkoru Bilişim	X	Fırat Teknokent	S																			S	S
59	NetSum		Bilişim Vadisi	S	S		S	S													S		S	
60	Networkmas			S			S		S									S					S	
61	Olle		Ankara Ü. Teknokent																				S	
62	PENTA Teknoloji			S																				
63	premierturk		Kocaeli Teknopark					S															S	
64	PwC												S										S	
65	RasyoTek		Düzce Teknopark																				S	

Table H.7 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
66	Ridia																S							
67	romeda		Bilişim Vadisi																				S	
68	RSA																						S	S
69	SBI Bilişim	X	Hacettepe										S							S			S	
70	SDataM		Samsun Teknopark									S									S		S	
71	Secrove	X									S												S	S
72	Securify	X	Teknopark Ankara																				S	
73	SEYBİT Siber Güvenlik			S	S					S				S				S						
74	Siber İstihbarat Akademisi																						S	S
75	Sibera		Kahramanmaraş																				S	
76	SmartValley (SAR Yazılım)		Teknopark İstanbul		S		S																S	S
77	Softsan Teknoloji	X	Kırıkkale Teknokent							S	S		S										S	
78	TDG Technology Dev.Group		Düzce Teknopark													S								
79	TechNarts		ODTÜ Teknokent																				S	
80	techSiN Solutions		Yıldız Teknokent										S	S									S	S
81	Tridea Siber Güvenlik	X								S			S										S	S
82	Troynetics		Teknopark İzmir																				S	
83	TRYSEC	X											S										S	S

Table H.7 (Cont'd)

No	Company	TCC	Technopark	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
84	TURKCELL	X		S	S	S					S				S	S				S		S	S	
85	Türk Telekom	X		S	S						S	S	S	S	S	S							S	
86	TÜRKSAT	X	Ankara Ü. Teknokent										S	S									S	
87	UITSEC	X									S		S			S							S	S
88	USGA Ulusal Siber Güvenlik Akademisi																						S	S
89	ÜniBim		Düzce Teknopark				S										S							
90	Verify			S	S	S		S						S										
91	verion		Yıldız Teknokent														S							
92	verisoft		Yıldız Teknokent																					
93	VMİ Danışmanlık																						S	
94	vMind		Yıldız Teknokent										S	S									S	
95	Wisnet		Mersin Teknopark	S	S		S	S															S	
96	Yediveren Bilişim		Zafer Teknopark	S																				

Table H.8: Cybersecurity Products/Service Matrix in Technoparks

No	Technopark	Product	Service
1	Adnan Menderes		X
2	Afyon-Uşak Zafer		X
3	Ankara Teknopark	X	X
4	Ankara (Bilkent Cyberpark)	X	X
5	Ankara Üniversitesi	X	X
6	Batı Akdeniz Teknokent		
7	Boğaziçi Üniversitesi		X
8	Bolu		
9	Bozok Üniversitesi		
10	Celal Bayar Üniversitesi		
11	Cumhuriyet	X	
12	Çanakkale		
13	Çorum		
14	Çukurova		
15	Dicle Üniversitesi		
16	Dokuz Eylül		
17	Düzce Teknopark		X
18	Ege Teknopark	X	
19	Erciyes Üniversitesi		X
20	Erzurum Ata Teknokent		
21	Eskişehir		
22	Fırat		X
23	Gazi Teknopark	X	
24	Gaziantep OSB		
25	Gaziantep Üniversitesi		
26	GOSB Teknopark		
27	Göller Bölgesi	X	
28	Hacettepe Üniversitesi	X	X
29	Harran Üniversitesi		
30	İstanbul	X	X
31	İstanbul Üniversitesi		
32	İTÜ Arı Teknokent	X	X
33	İzmir Bilim ve Teknoloji Parkı		
34	İzmir	X	X
35	Kahramanmaraş		X
36	Kapadokya		
37	Kırıkkale Üniversitesi		X
38	Kocaeli Üniversitesi	X	X
39	Konya		X

Table H.8 (Cont'd)

No	Technopark	Product	Service
40	Kütahya Dumlupınar Tasarım		
41	Malatya		
42	Marmara Üniversitesi		
43	Mehmet Akif Ersoy Üniversitesi		
44	Mersin	X	X
45	Muallimköy (Bilişim Vadisi)	X	X
46	Namık Kemal Üniversitesi		
47	Niğde Üniversitesi		
48	ODTÜ Teknokent	X	X
49	OSTİM Ekopark		
50	Pamukkale Üniversitesi		
51	Sakarya Üniversitesi	X	X
52	Samsun		X
53	Selçuk Üniversitesi		
54	Tokat		
55	Trabzon		
56	Trakya Üniversitesi Edirne		
57	TÜBİTAK Marmara Arş.Mrk.		
58	Ulutek	X	
59	Yıldız Teknik Üniversitesi	X	X
60	Yüzüncü Yıl Üniversitesi		X
61	Zonguldak		

Table H.9: Cybersecurity Products/Service Matrix in Technoparks[1]

Rank	Technology
1	Quantum Cryptography
2	Quantum-Safe Cryptographic Algorithms
3	Cybersecurity Training and Exercise Systems
4	Cyber Offense
5	Cyber-Physical Systems (CPS) Security
6	Encryption Technologies
7	Advanced Persistent Threat (APT) Protection
8	Blockchain for Identity & Access Management

[1] Technologies that were realized and addressed in products are in "green" color; technologies that are partly realized are in yellow color.

Table H.9 (Cont'd)

Rank	Technology
9	Encryption Algorithms
10	Cryptographic Chips and Modules
11	Non-Signature based Malware Analysis
12	Cyber Forensics (stand-alone, mobile, disk, memory)
13	Cyber Automated Response
14	Blockchain for Data Security
15	Cybersecurity Testbed
16	Cyber Analytics and Decision Support Systems
17	New Generation (4G, 5G etc.) Wireless Security
18	Embedded Software and Systems Security
19	Next-Generation IPS
20	Incident Response and Management
21	Penetration Testing
22	DDoS Defense
23	Blockchain Security
24	Big Data Security
25	Secure Aviation Protocols and Architecture
26	Microelectronics Security Tests
27	Cybersecurity Assessment and Evaluation
28	Next-Generation Firewalls
29	Lightweight Cryptography
30	Deep Packet Analyzing
31	Threat Analytics
32	Vulnerability Assessment
33	Dynamic Network/Computer Forensics
34	Secure IoT Routing Protocols
35	Network-based Cyber Forensics
36	Cyber Attack Modeling and Attack Generation
37	Model-Driven Cyber Defense
38	Hardware Trusted Platform Module (TPM)
39	Software-Defined Security
40	Vulnerability Management
41	Crowdsourced Threat Intelligence and Protection
42	Distributed Trust Mechanisms
43	Threat Intelligence Platforms
44	Network IPS (Intrusion Prevention System)
45	Hypervisor Security
46	Deception Technology (e.g. honeypots)
47	Operational Technology Security

Table H.9 (Cont'd)

Rank	Technology
48	Privacy Management Technologies and Tools
49	Database Security (Audit, Protection, Encryption)
50	Data Farming based Threat Analytics
51	Privacy-Preserving Machine Learning
52	Security Information and Event Management (SIEM)
53	Cybersecurity Sense-Making
54	Configuration Auditing
55	Malware Defense
56	Automated Reverse Engineering
57	Secure Texting
58	Network Penetration Testing Tools
59	Pervasive Trust Services (Distributed Trust, Blockchain-like Architectures etc.)
60	Runtime Application Self-Protection (RASP)
61	Fully Homomorphic Encryption
62	Fraud Detection and Transaction Security
63	Risk Management (IT, Digital, Vendor, Operational, Industrial, Social)
64	Format Preserving Encryption
65	Content-Aware DLP for Email
66	Virtual Trusted Platform Module (vTPM)
67	Mobile Voice Protection
68	Wireless Devices Security
69	Data Loss Prevention (DLP)
70	Network Sandboxing
71	Fuzz Testing
72	Biometric Authentication Methods
73	Virtualization Security
74	Application Vulnerability Correlation
75	Application Shielding
76	Mobile Virtual Private Networks
77	Web Application Firewall (WAF)
78	Network Traffic Analysis
79	Software-Defined Perimeter
80	Certification and Accreditation
81	IaaS (Infrastructure as a Service) Container Encryption
82	Contextual Verification for Information Integrity
83	Static Application Security Testing (SAST)
84	Firewall as a Service
85	Privacy in IoT
86	Unidirectional Security Gateway

Table H.9 (Cont'd)

Rank	Technology
87	Content-Aware Mobile DLP
88	Mobile Application Security Testing
89	Moving Target (MT) Defense
90	Model-based Dynamic Risk Assessment
91	Hardware Roots of Trust
92	Virtualized Roots of Trust
93	Information Security Management System
94	Trusted Mobile Environments
95	Host-based Intrusion Prevention System (HIPS)
96	Wearable Technologies Security
97	Crypto Analysis
98	Information Dispersal Algorithms
99	Mobile Vulnerability Management Tools
100	New Generation User and Object Identification and Access Control Technologies
101	Strong Authentication for Enterprise Access
102	Key Management as a Service
103	Software Development Life Cycle Security
104	Boundary Defense (Perimeter Security)
105	High-Assurance Hypervisors
106	Network Access Control
107	Secure Web Gateway
108	Security in the Switch
109	Fog Computing Security
110	Identity Governance and Administration (IGA)
111	Unified Threat Management (UTM)
112	User and Entity Behavior Analytics
113	Process and Data Isolation
114	Formal Verification of Security Mechanisms
115	Mobile Threat Defense
116	Dynamic Application Security Testing (DAST)
117	Digital Signature
118	Application Obfuscation
119	Multifactor Authentication
120	Network Security Policy Management
121	Enterprise Key Management
122	Trusted Portable Storage Security
123	Interoperable Storage Encryption
124	Static and Dynamic Data Masking
125	Data Sanitization and Disposal

Table H.9 (Cont'd)

Rank	Technology
126	Context-Aware Network Access Control
127	DevSecOps
128	Application Control
129	Data Recovery
130	Application Security as a Service
131	Tokenization
132	Cloud Access Security Brokers
133	Secure e-voting Systems
134	Network Monitoring
135	SaaS (Software as a Service) Platform Security Management
136	Network and Protocol Based Isolation Technologies
137	Stateful Firewall
138	IoT Authentication
139	Separation Kernel
140	Software Composition Analysis
141	Remote Browser
142	Federated Identity Management
143	Crowdsourced Security Testing Platforms
144	Removable Devices Security
145	Content Monitors and Filters
146	Device Control
147	Interactive Application Security Testing
148	Polymorphic Computing Architecture
149	Cloud Data Protection Gateway
150	Mediated APIs
151	Enterprise Mobility Management (EMM) Security
152	Mobile Platform Health Checks
153	Attribute-Based Access Control (ABAC)
154	Protected Mobile Browsers
155	Privileged Access Management
156	Autocode Generators and Correct by Construction
157	Identification as a Service (IDaaS)
158	User Authentication to Mobile Devices
159	Web Page Integrity and Monitor
160	SaaS based Mobile Device Management (MDM)
161	Consumer Mobile Security Apps
162	Bring Your Own Device (BYOD)
163	Common Access Card
164	X.509 Tokens for User Authentication

Table H.9 (Cont'd)

Rank	Technology
165	System for Cross-domain Identity Management (SCIM)
166	Mobile Single Sign-On
167	Mobile-Apt User Authentication Methods
168	Phone-as-a-Token Authentication Methods
169	Externalized Authorization Management

Table I.1: Actions

No	STEEPLE	Action
1	Economic	Cybersecurity companies' turnover should be increased at least by 20% in 2 years.
2	Economic	For cybersecurity R&D projects, at least an annual budget of 10 million dollars should be allocated to SSB and TÜBİTAK.
3	Political	In order to improve exporting, incentives (financial support, tax reduction, etc.) and credit should be provided to exporter companies.
4	Political	In order to increase the export of cybersecurity products, at least 5 countries should be selected for target markets and special studies should be carried out for each country.
5	Political	Cybersecurity firms should attend at least one international fair each year and advertise their products. For this purpose, 10,000+ US dollars funding support should be provided by government to the producer companies.
6	Political	In order to increase the number of patents in the field of cybersecurity, fund support should be provided depending on the quality of patents.
7	Political	The number of people working in the field of cybersecurity should be increased by at least 10% each year (at least 500 people per year).
8	Political	In order to expand the cybersecurity product portfolio, companies should be provided with techno-venture capital to work in areas where there is no supplier.
9	Political	Promotional activities should be carried out to register all companies working in cybersecurity sector to cybersecurity Cluster.
10	Political	At least 2 posts for cybersecurity experts should be added to the information processing organizations in government institutions.

Table I.1 (Cont'd)

No	STEEPLE	Action
11	Political	A political, social, legal and economic environment should be established to keep the qualified labor force in our country.
12	Political	In Turkey, the cybersecurity distribution of tasks should be rearranged in the highest-level institutions (Ministry of Internal Affairs, Turkish Armed Forces, National Intelligence Organization, National Computer Emergency Response Center, Information and Communication Technologies Authority etc.).
13	Political	In the next 5 years, the ratio of R&D investments to GDP should be increased to at least 2%.
14	Political	Every year 5 companies should be supported to open overseas branches in reputable technology or business centers abroad.
15	Political	In public institutions, examination fees for cybersecurity certification of the personnel working in cybersecurity and information technologies departments should be paid by the government.
16	Political	Cybersecurity job descriptions and workforce catalog should be established and therefore the definitions of the tasks to be performed and the certificates to be taken should be standardized.
17	Political	Technology awards should be given to successful companies in cybersecurity technologies annually (with the criteria of product export, patents etc.).
18	Political	In order to increase the number of cybersecurity companies to 3 times in the next 5 years (from 180 to 540) sectoral planning and incentives should be provided to establish at least 10 cybersecurity firms in each technopark.
19	Political	The use of certified national cybersecurity products in certain infrastructures and systems should be mandatory.
20	Social	Cybersecurity awareness conferences should be organized at each university once a year for academic personnel and students.
21	Social	Cybersecurity human resource inventory should be created by SSB.
22	Social	Public service ads (short films) should be made and promoted in the national media in order to improve the awareness of cybersecurity in the society.
23	Technological	An independent testing and certification center should be founded for the quality, testing and certification of cybersecurity products.
24	Technological	R&D and product development studies should be carried out for cybersecurity areas, which are not used in Turkish cybersecurity products or not being worked on.

Table I.1 (Cont'd)

No	STEEPLE	Action
24	Technological	R&D and product development studies should be carried out for cybersecurity areas, which are not used in Turkish cybersecurity products or not being worked on.
25	Technological	Under the auspices of SSB, cybersecurity technology foresights should be carried out every two years.
26	Technological	Among the cybersecurity products produced in the world, the successful ones should be identified, their common characteristics should be revealed and the national products should be improved accordingly.
27	Technological	International cybersecurity conventions and fairs should be organized annually by the organizations such as SSB, TÜBİTAK, Ministry of Industry and Technology and Ministry of Infrastructure Ministry.
28	Technological	To convene foreign academia and cybersecurity sectors, international cybersecurity seminars and fairs should be organized annually by two Turkish universities determined by the Higher Education Council (YÖK).
29	Technological	Each year, 5 cybersecurity R&D projects should be initiated by 5-company joint venture.
30	Technological	Each month, voluntary companies and universities should be assigned to arrange a cybersecurity competition (capture the flag, hacking competition, etc.), and sponsorships should be found for financial support.
31	Technological	At least once a year the international cybersecurity competition should be organized with a spectacular name (such as Hack-Tur-Key).
32	Technological	Cybersecurity experts should be provided with at least 3 new courses each year.
33	Technological	Cybersecurity technical high schools should be established in 10 major provinces of Turkey.
34	Technological	Cybersecurity sections should be added to existing sections in technical high schools.
35	Technological	Cybersecurity departments should be created within the computer engineering departments of at least 10 universities.
36	Technological	At least one compulsory cybersecurity course should be given in the computer engineering and software engineering departments of universities.
37	Technological	The number of cybersecurity graduate departments in universities should be doubled (from 20 to 40).
38	Technological	The number of cybersecurity doctoral programs in universities should be increased to 10 (currently 3).
39	Technological	Cybersecurity technology taxonomy should be created and updated continuously (for this purpose, taxonomy formed in this thesis can be used.).

Table I.1 (Cont'd)

No	STEEPLE	Action
40	Technological	In accordance with the cybersecurity taxonomy, companies and products must be classified. This activity was conducted in this thesis. Periodic updating of this activity should be ensured.
41	Technological	A monthly journal, which contains only scientific papers regarding cybersecurity and registered in the Science Citation Index, should be published.
42	Technological	Each year, 200 Master of Science students 100 PhD students and 50 post-doctoral students should be sent abroad. At least half of the education expenses should be paid by the government. In order to have these students worked in Turkish universities of companies for at least 2 years; legal arrangements should be set within the law.
43	Technological	In order to compete with international counterparts and increase the product quality level, cybersecurity products produced in our country should meet the international standards and obtain widespread certifications.
44	Technological	Investments should be made in information and communication technologies (edge computing, quantum computing, cloud computing, wireless etc.) that facilitates and provides infrastructure for cybersecurity technologies.
45	Technological	Technologies that are directly interacts with or have effects on cybersecurity (artificial intelligence, big data, deep learning, augmented reality, brain-computer interface, machine learning, virtual reality, IoT, autonomous vehicles, cloud computing, smart robots, wearable devices etc.) should be worked.
46	Technological	Cybersecurity internship programs should be established and students in the computer or software engineering departments of universities should be encouraged to do internship in Cybersecurity Cluster member companies.
47	Technological	An international cybersecurity training center, consisting of at least 50 experts with expertise in different fields, should be established, providing English cybersecurity training and certification.
48	Technological	Turkish Standards Institution (TSE) or TÜBİTAK BİLGEM should establish a unit such as NIST (National Institute of Standards and Technologies) in the USA to prepare cybersecurity guidelines.
49	Technological	Product integration studies should be done to create "cybersecurity product family" among Turkish cybersecurity firms and integrated solutions, which address widespread security needs, should be put forward.
50	Technological	A joint cybersecurity laboratory should be established by at least 5 companies specialized in different cybersecurity product groups to work on all kinds of cybersecurity products and malware analysis.

Notes for Roadmap Table for Scenarios:

1) All of Delphi statements' first realization method is "Research and Development". In the following scenario tables, only the second high-scored methods are given.

2) Abbreviations: TT: "Technology Transfer"; COTS: "COTS or Open Source Use"; FCC: "Foreign Company Cooperation"

3) Scenario – Delphi stamen allocation is shown in Table I.2. For simplicity, only the roadmap table for Scenario-1 is given. The other roadmaps can be inferred from the Table I.2.

Table I.2: Scenario – Delphi Statement Allocation

Scenario	Statements
Scenario-1	All of 91 Delphi statements
Scenario-2	Top 47 Delphi statements (these statements were chosen by focus group experts)
Scenario-3	Top 25 Delphi statements 7 of 25 statements (D-3, D-11, D-21, D-23, D-30, D-31, D-47) are deferred to the next timeframes
Scenario-4	All of 91 Delphi statements 9 of 91 statements (D-3, D-11, D-21, D-23, D-30, D-31, D-47, D-89, D-90) are deferred to the next timeframes

Table I.2: Roadmap for Scenario-1

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
1	D-1	The technological level has been reached to protect the embedded systems against cyber attacks and to perform security tests of all kinds of electronic circuits (chips, micro-electronic circuits, etc.).		X				TT	104; 133; 166; 168
2	D-8	A high level of cyber-attack techniques, technologies and systems have been developed to compete with countries with high-level cyber-attack and defense capabilities in the world (e.g., the US, Russia, China) and a powerful cyber army has been established at this level.		X				COTS	151
3	D-29	Intelligent cyber-attack systems with self-learning capability (with machine learning, deep learning, etc.) that can model cyber attacks have been developed both for testing and for real automatic attack capability.		X				TT	153
4	D-39	Flying systems (airplanes, helicopters, unmanned aerial vehicles, etc.) have gained cyber attack capability.			X			TT	57; 151
5	D-31	Data Loss Prevention (DLP) techniques and systems have been developed and are among the top 10 products in the world.			X			TT	26; 82; 83; 84
6	D-14	Techniques and technologies (virtualization security, hypervisor security) have been developed to rise the cybersecurity levels of virtual operating systems and are integrated into internationally distributed products.			X			FCC	90; 94; 96; 135
7	D-2	Crypto algorithms, technology and modules (software, hardware) that cannot be cracked by super computers and quantum computers (quantum safe) have been developed and started to be used in operational environments.			X			TT	54; 58; 59; 60; 61; 62; 97
8	D-26	Software, hardware and technologies (e.g. isolation, sandboxing, virtualization, application control, etc.) to protect systems against Advanced Persistent Threats (APTs) have been developed and marketed to the world markets.			X			TT	20; 21; 23; 166

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
9	D-4	The lightweight cryptography systems that can be used in very small systems that can be connected to the network have been developed and used in the products of international brands.	X					COTS	63
10	D-27	New generation of technics and technologies that can protect systems from Distributed Denial of Service (DDoS) attacks from millions of different locations have been developed and introduced to the markets around the world.	X					TT	10
11	D-47	Durable and rapidly recoverable systems that increase the immunity of artificial intelligence systems (robots etc.) have been developed and become among the top 10 countries in the world.		X				TT	24
12	D-9	Technologies have been developed for the cybersecurity of wireless devices (computers, network devices, mobile phones, cameras, etc.) as well as for new generation wireless communication technologies (5G and later) and have been used in international products.	X					TT	16; 39; 46; 53; 55; 68; 110; 119; 120; 121; 122; 123; 124; 125; 126; 128
13	D-12	The blockchain and new generation of applications and techniques have been developed and used in order to provide the user and object identity and access control and data security to the highest level.	X					COTS	27; 35; 44; 50; 79; 131

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
14	D-22	A new generation of techniques (within/external to system, on-site/remote, manual/automatic, with artificial intelligence etc.) for penetration testing, tools and technologies have been developed.	X					COTS	107; 158
15	D-28	Software and hardware that can protect systems against all kinds of malicious software (viruses, worms, trojans, rootkits, etc.) through both signature and anomaly based (behavior based, non-signature based) methods have been developed and started to be marketed internationally.		X				TT	22; 24
16	D-16	Techniques (audit, encryption etc.) technology, software and hardware to provide cybersecurity for big data, other database and data therein has been developed and marketed internationally.	X					TT	27; 30; 56; 73; 74; 75; 76; 86; 87; 88
17	D-35	Cloud computing security technics (encryption, access brokers, etc.) and technologies have been developed and used.	X					TT	89; 91; 92; 93
18	D-13	Cybersecurity testing, training and drill systems for international training institutions and international cybersecurity drills have been developed and our country has become a global cybersecurity training and innovation center.		X				TT	154
19	D-25	New generation technologies and systems to respond cyber events quickly, effectively and automatically (including incident response, automated response and model-driven cyber defense), and to manage these events (incident management) have been developed and used.	X					TT	141; 146; 150; 157; 159; 167

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
20	D-23	Cybersecurity tools and mechanisms (e.g. firewall, security gateway, guard, router, etc.) through software modules and systems (software-defined security) have been developed, and these products have at least 5 % of the world market dominated.		X				TT	3
21	D-5	To provide cybersecurity of manned and unmanned aircraft systems and air traffic control systems (navigation systems, air traffic networks, flight control systems, etc.), cybersecurity protocols and architectures have been developed and started to be used.	X					TT	57
22	D-15	The infrastructure, software, hardware, techniques and technologies have been developed to collect, analyze and provide decision support for cyber threat intelligence (threats, tools, resources, targets, etc.) covering all countries in the world.	X					FCC	138; 143; 144; 145; 155
23	D-3	Technologies and systems have been developed to provide cybersecurity for cyber-physical systems (systems and networks of smart things, factory production control systems, industrial internet and industrial control systems) and our country has been among the top 5 countries selling products in the world.			X			TT	64; 130
24	D-30	Cybersecurity systems (firewall, web application firewall, intrusion prevention system, etc.) to analyze communication network traffic (deep packet inspection, etc.) and to take automatic measures against this traffic have been developed and become the top 10 preferred brands in the international markets.	X					TT	4; 5; 6; 7; 8; 9; 11; 13; 15; 25; 51; 137; 152

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
25	D-21	In mobile and on premise systems, new generation techniques, technologies and applications have been developed to perform vulnerability management and cybersecurity assessment and evaluation and these have been among the top 5 technological products preferred in this field.			X			TT	105; 127; 160; 163
26	D-42	Cognitive-based network infrastructures have been developed to identify the source of cyber attacks and enable immediate counter-attack.			X			TT	1; 159
27	D-11	Protocols, technologies and applications have been developed to ensure privacy, authentication and communication security in the Internet of Things devices and networks, and our country is among the top 10 countries with the largest market share in this area.			X			TT	26; 65; 69; 80; 129; 139
28	D-44	Artificial intelligence software has been developed which designs non-breakable cryptographic algorithms resistant to quantum machines.					X	TT	58; 61; 62
29	D-32	New generation techniques and systems have been developed and used to protect web servers and web-based systems against cyber attacks.		X				COTS	18; 19; 100; 116; 117; 118
30	D-38	Quantum satellites based on quantum switches have been developed and deployed in deep space to provide internet service from space.					X	FCC	61; 1; 2
31	D-7	In order to prevent application-level attacks, applications such as application shielding and Runtime Application Self-Protection (RASP), which use artificial intelligence, machine learning and deep learning techniques, have been developed.			X			TT	98; 99; 101; 102; 103; 106
32	D-17	Advanced techniques, technologies and applications (such as distributed trust, blockchain-like architectures, etc.) have been developed and implemented to provide the trust mechanism among many objects (devices, networks, users).			X			COTS	66; 95; 131; 166

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
33	D-34	Advanced deception techniques and systems (honeypot etc.) have been developed and used to protect the systems from attacks and to identify the technics and movements of the attackers.		X				TT	140
34	D-24	A variety of technics, software, hardware and technologies for cyber forensic of all kinds of information system devices (computers, telephones, smart objects, etc.) and information storage units (RAM, disk, etc.) have been developed and introduced to the international market.		X				COTS	147; 148; 149
35	D-10	The Trusted Platform Module (TPM) is designed as a virtual (virtual) and physical (chip) device and used in international market equipment to ensure reliable operations and secure encryption in information systems hardware.				X		TT	28; 29; 70; 71
36	D-36	Biometric (retina, fingerprint, face, voice, etc.) authentication systems have been developed and presented to international markets.		X				TT	37
37	D-20	Techniques and technologies that provide change detection and configuration auditing between servers, applications, databases and network devices and in the internal and public cloud infrastructure have been developed and used.	X					COTS	164
38	D-46	Cybersecurity systems have been developed to secure human-machine communication.			X			TT	43; 45; 50
39	D-6	Cybersecurity technologies and systems for wearable technologies (watches, glasses, dresses, artificial organs, various sensors, etc.) have been developed and used in the products of international brands.	X					COTS	72
40	D-37	Cybersecurity risk management methodologies, techniques and tools have been developed and used.	X					COTS	161; 169
41	D-41	Cyber attack systems that mimic human behavior have been developed.				X		TT	151; 153

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
42	D-33	Advanced techniques and technologies that enable reverse engineering have been developed and used.				X		COTS	165
43	D-19	Advanced software, hardware and technologies (user authentication, unbreakable encryption, high performance, etc.) have been developed to ensure security of portable memory devices (USB sticks, external disks, disk units, etc.).		X				COTS	77; 78; 81; 85; 132
44	D-40	Reliable digital infrastructures and systems have been developed for secure election, community vision collection and survey.		X				COTS	43; 49; 52
45	D-45	Visualization systems have been developed, which visualize and process the security logs and enable them to be understood easily by analysts.	X					COTS	141; 146
46	D-18	Techniques and technologies to protect privacy in machine learning applications have been developed.		X				COTS	142
47	D-43	The technological level to understand the signals (possibly cryptographic) coming from space has been reached.					X	TT	58; 59
48	D-54	Artificial intelligence test software and hardware has been developed for security testing using cybersecurity systems (networked devices, embedded systems, etc.) or using self-developed attack methods.		X				TT	107; 108; 109; 110; 111; 112; 113; 153
49	D-69	Autonomous crypto analysis ability is gained.				X		FCC	56; 58; 59
50	D-56	The national cyber shield and cyber defense system that has cyber attack ability were implemented.				X		TT	17; 150; 151; 159; 162

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
51	D-53	Embedded systems have reached the technological level that can use the embedded chip-based boundary scan standards (IEEE 1149.6, IEEE 1581, etc.) that enable the security tests of micro-electronic chips on the integrated circuit board with only a few access points.			X			TT	133
52	D-55	A cryptographic algorithm that cannot be broken by quantum computers has been designed, based on a new mathematical problem that will be difficult to be solved, can be run quickly, and will take up little space in memory (which can be integrated into small systems).				X		TT	58; 63
53	D-70	Systems that can detect and use cybersecurity vulnerabilities in software and systems have been developed.		X				COTS	105; 159; 160
54	D-72	Cybersecurity of autonomous systems is ensured.					X	COTS	24; 66; 67; 134; 162
55	D-63	All of the security systems based on difficult to solve problems have been broken by developing quantum computer technology.					X	TT	56; 61; 62
56	D-82	Domestic and national boundary protection technologies have been developed and a serious decline has occurred in cybersecurity incidents.		X				TT	12; 14; 15
57	D-86	Signal analysis (possibly encrypted) technologies have been developed and become leading country in the region.				X		TT	56; 59
58	D-51	Quantum processors and quantum computers have been developed and used in crypto analysis.				X		TT	56
59	D-62	Anonymized cybersecurity intelligence data collection (from all members of society if necessary) infrastructure has been developed and put into use.		X				COTS	138; 144; 145

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
60	D-66	Intelligent (autonomous) defense systems have been developed that perceive the cyber attacks to be done through cyber intelligence and misdirect the target and/or stop the operation.			X			TT	140; 159
61	D-73	Dynamic cyber-deception technologies have been developed in software-based network technologies and made compatible with 5G infrastructure.		X				TT	68; 140
62	D-81	SDLC (Software Development Life Cycle) processes have been started to be given in the universities with programming lessons and secure software production has been ensured.		X				COTS	114; 115; 162
63	D-91	Cybersecurity awareness training packages have been developed that can be used locally and globally.		X				COTS	154
64	D-65	The security mechanisms of 6G mobile systems are designed and reached in the top 5 in the international market.		X				TT	16; 68
65	D-67	Advanced machine learning based intrusion detection systems have been developed which can detect zero-day attacks with at least 95% performance.			X			TT	9
66	D-85	Technologies for the cybersecurity of personal aircrafts have been developed.			X			TT	57
67	D-90	With the cognitive and behavioral models, user-specific cyber immunity and continuous improvement (self-paced learning, continuous improvement) systems have been developed, became the leader in the region and entered the top 10 countries in the world.				X		TT	24; 136
68	D-61	Cybersecurity solutions have been developed that can provide all kinds of privacy of individuals (not being followed, not monitoring data, storing personal information, etc.).			X			TT	80

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
69	D-80	Training and certification programs, which are valid in national and international levels and have been attended by students from abroad, have been developed.		X				FCC	154
70	D-83	Systems have been developed to detect weaknesses in our national systems and internationally available software.		X				COTS	105; 160; 108; 109; 112
71	D-57	Systems that can continuously monitor the potential of the cyber attack of robots have been implemented.			X			TT	24; 64; 134
72	D-50	Machine-based deep learning technologies have been developed that generate behavioral profiles using big data and create intelligent cyber defense and attack strategies based on these profiles.				X		TT	17; 151; 153; 159
73	D-59	Intelligent city monitoring and security systems have been developed.			X			TT	64; 69; 134
74	D-76	Systems have been developed to monitor and report the compatibility of network, system and security devices with the baseline.	X					COTS	1; 164
75	D-49	Smart technologies have been developed to detect bio-printing (voice, fingerprint) and use them in cyber attacks.		X				TT	37; 151
76	D-71	The ability of cyber attack to autonomous systems has been developed.		X				COTS	64; 151
77	D-84	Cybersecurity systems have been developed to ensure the security of communication between satellites.				X		TT	58; 59; 60; 63
78	D-89	Identity management and authorization systems based on behavioral and cognitive methods and models have been developed and became the leader in the region and entered the top 10 countries in the world.				X		FCC	31; 32; 33; 34; 35; 36; 38; 40; 41; 42; 47; 48; 50

Table I.2 (Cont'd)

Order	Delphi No	Delphi Statement	2019-2023	2024-2029	2030-2035	2036-2040	2040 +	Method	Technologies
79	D-52	Secure memory (USB, hard disk, etc.) technologies which use plasma infrastructure and which self-destruct mechanism for tempering were developed.			X			TT	77; 78; 81
80	D-68	Software has been developed to detect the first leakage point of the attacked data.			X			TT	147; 148; 152; 155
81	D-79	Secure biometric authentication mechanisms have been developed for access to sensitive data hosting systems.		X				TT	37
82	D-58	Systems that provide the security of the system/limbs integrated into the human body have been developed.					X	TT	24; 64
83	D-60	By analyzing the legislation and laws and analyzing the scenarios that may occur, models that determine potential cybersecurity vulnerabilities have been developed.		X				TT	105; 160
84	D-75	SIEM systems have been developed which collect system and security records from network and server systems and detect security breaches.	X					COTS	141
85	D-87	Holographic design security is among the top 5 technologies.			X			TT	115
86	D-77	A test structure has been developed for organizations and companies to test their own security against DDoS attacks.	X					COTS	10; 156
87	D-88	Machine system software that malware cannot enter has been developed.					X	TT	24; 64
88	D-78	E-commerce and banking systems have been developed to detect and prevent fraud and illegal transactions.		X				TT	139
89	D-48	Cybersecurity risks in all developed products are considered and cybersecurity is embedded in the products.		X				TT	114; 115; 169
90	D-74	Virtual firewalls and virtualized system security technologies have been installed.		X				COTS	3; 94; 96
91	D-64	Country elections are made online, using blockchain and similar techniques.					X	COTS	52

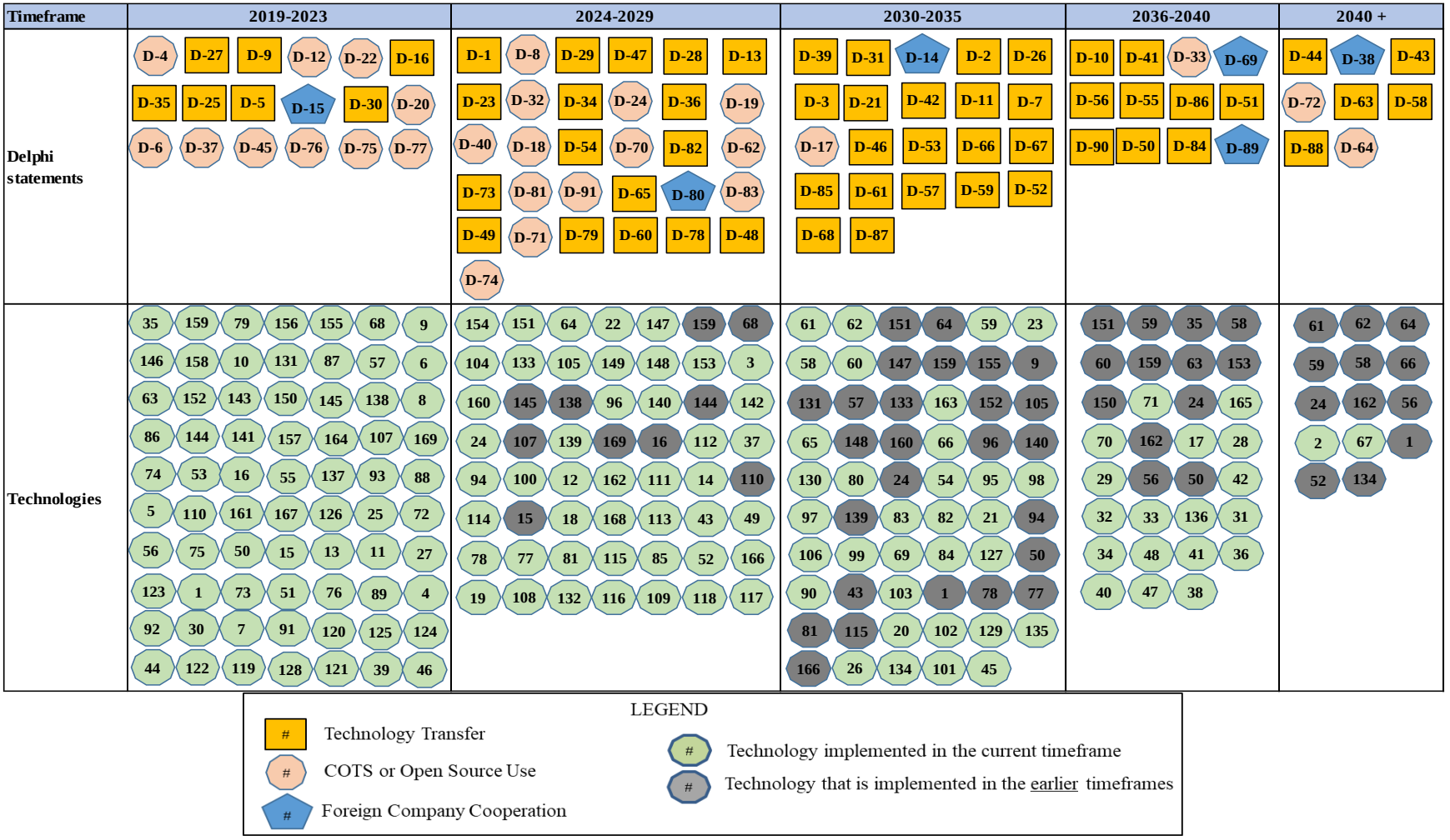


Figure I.1: Roadmap for Scenario-1

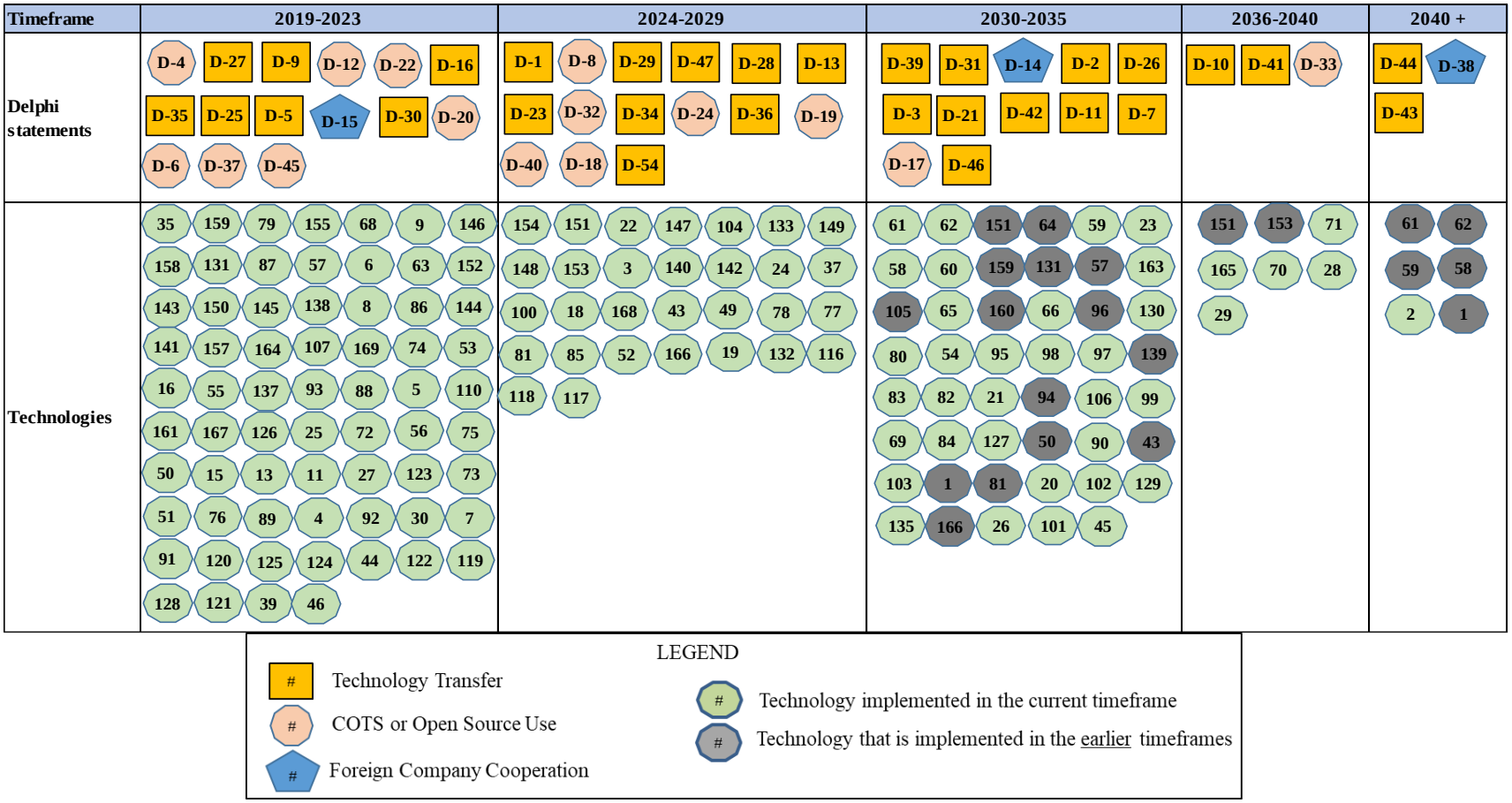


Figure I.2: Roadmap for Scenario-2

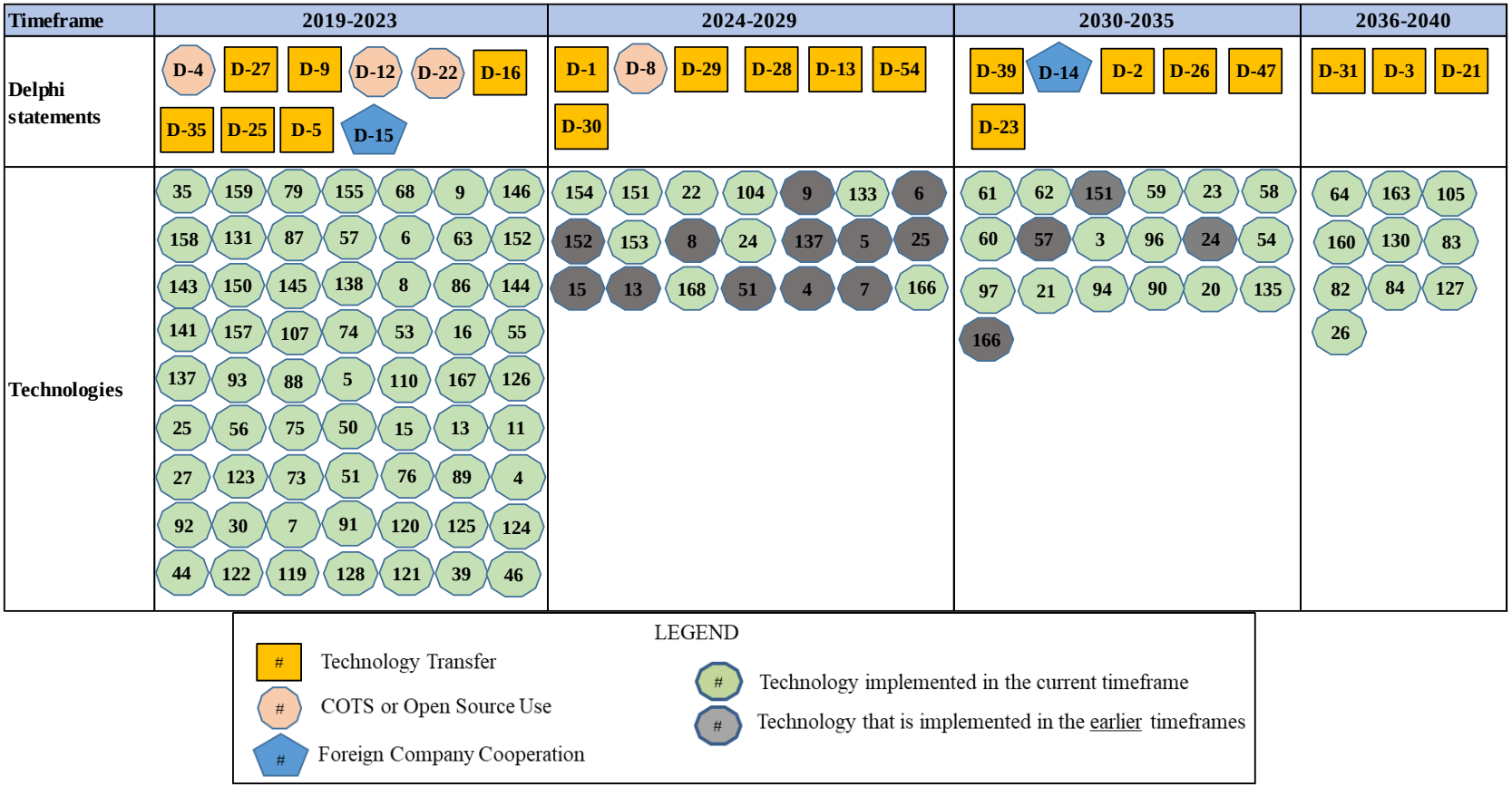


Figure I.3: Roadmap for Scenario-3

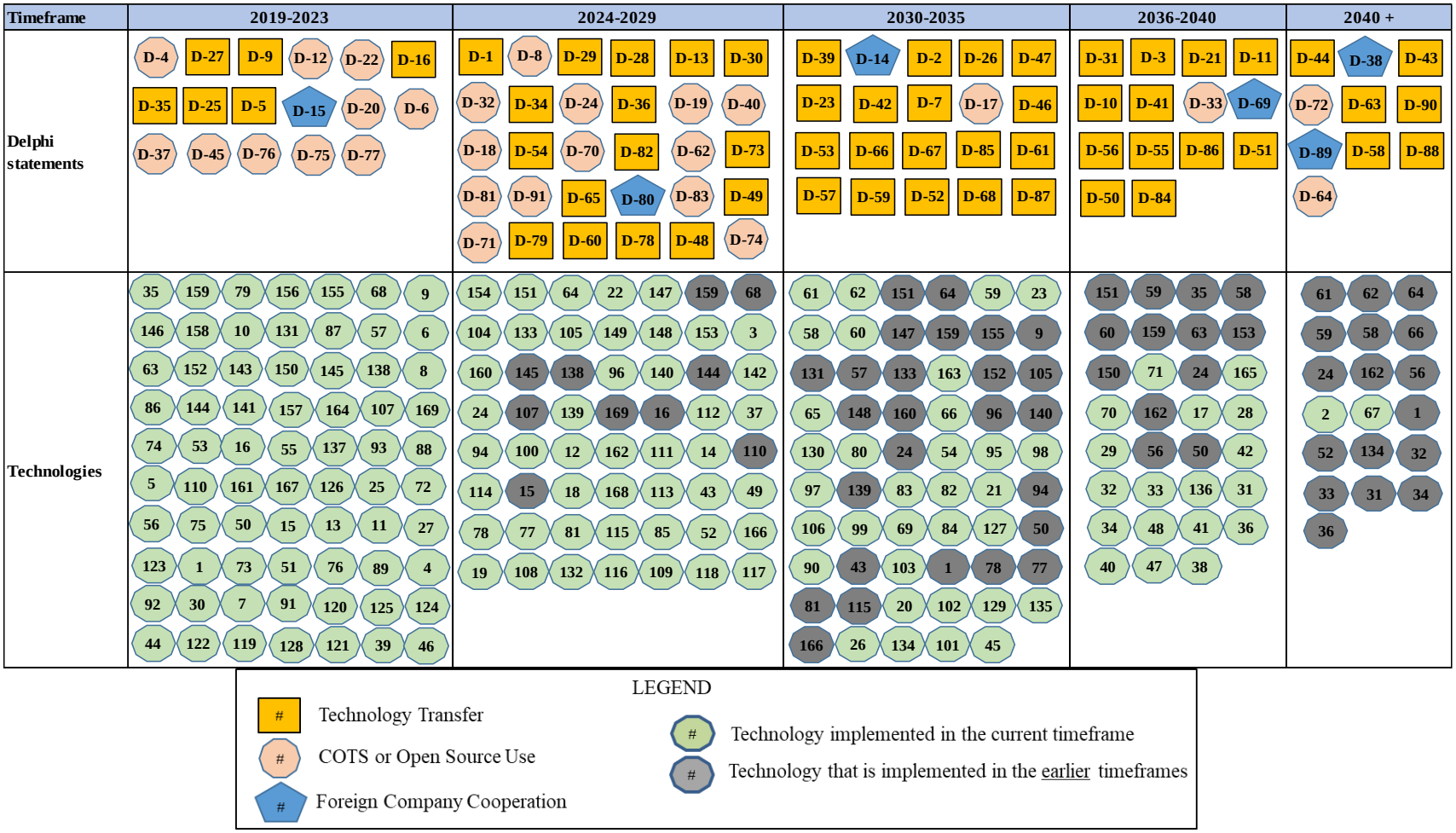


Figure I.4: Roadmap for Scenario-4

APPENDIX J: CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name : Çifci, Hasan
Nationality : Turkish
E-mail : hcifci74@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
MS	Middle East Technical University, Informatics Institute	2004
BS	Hacettepe University, Computer Engineering	1996
High School	Zile High School, Tokat	1991

ARTICLES and CONFERENCE PAPERS

Çifci, H., & Yüksel, N. (2018). Foresight 6.0: The New Generation of Technology Foresight. In 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1–5). http://doi.org/10.1109/ICE.2018.8436350

Yüksel, N., & Çifci, H. (2017). A New Model for Technology Foresight: Foresight Periscope Model (FPM). In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 807–817).

Yüksel, N., Çifci, H., & Çakir, S. (2017). New Foresight Generation and Framework of Foresight. In 2nd World Conference on Technology, Innovation and Entrepreneurship (pp. 224–233). http://doi.org/10.17261/Pressacademia.2017.593

BOOKS

- Çifci, H. (2003). Bilgi Çağında Bilgi Harbi. Ankara.
- Çifci, H. (2008). Computer Textbook for High School. Kabul. Department of Defense.
- Çifci, H. (2011). Bilgi Harbinden Siber Savaşlara Doğru. Ankara.
- Çifci, H. (2017). Her Yönüyle Siber Savaş (2nd Ed.). Ankara: TÜBİTAK.

OTHER BOOKS AND BOOKLETS (Contribution as Scientific Advisor)

- Defense and Security. TÜBİTAK, 2014.
- Air and Space. TÜBİTAK, 2015.
- You Wouldn't Want to be on Apollo 13!. TÜBİTAK, 2017.
- You Wouldn't Want to be on the First Flying Machine!. TÜBİTAK, 2018.
- Flight. TÜBİTAK, 2018.
- An Astronaut's Guide to Life on Earth. TÜBİTAK, *in press process*.

FOREIGN LANGUAGES

Advanced English

APPENDIX K: TURKISH SUMMARY/TÜRKÇE ÖZET

Bu tezin temel amacı, 2040 yılına kadar önümüzdeki 20 yıl içinde Türkiye için siber güvenlik teknoloji öngörüsü gerçekleştirmek; Yüksel ve Çifci (2017) tarafından literatüre kazandırılan Öngörü Periskop Modeli (Foresight Periscope Model -FPM) ve FORESIGHT isimli öngörü çerçevesini uygulayarak ortaya konan siber güvenlik teknoloji öngörüsü sonuçlarına göre somut ve etkin politika önerilerinde bulunmaktır. Araştırmada temel öngörü yöntemleri olarak, eğilim analizi, Delfi anketi, odak grup ve senaryo teknikleri kullanılmıştır.

Çalışmanın başlangıcında, Savunma Sanayii Müsteşarlığı (SSM) bünyesinde, teknoloji panelleri altında, "Türkiye'nin Siber Güvenlik Yol Haritası" çalışma grubu resmî olarak teşkil edilmiş, üyeler seçilmiş ve grup başkanı olarak Hasan Çifci atanmıştır. İkinci toplantı sonrasında, 2018 yılı Temmuz ayında SSM'nin Savunma Sanayii Başkanlığı (SSB) olarak yeniden teşkilatlanmasını takiben, çalışma grubu gayriresmî olarak feshedilmiş ve SSB tarafından sağlanan katılımcı desteği çekilmiştir.

Teknoloji, günlük yaşamın her alanına girmekte, teknolojik araçlara ve gelişmelere bağımlılık artmakta ve bu bağımlılık, güvenlik açısından zafiyet ve tehditleri beraberinde getirmektedir. Ağları ve sistemleri birbirine bağlayan siber alan, hayati bir alan durumunu kazanmış ve ortaya çıkan tehditlerin hedefi hâline gelmiştir. Siber alan çok geniş bir ağa dönüşürken, sistemleri korumak ve kullanılabilirliğini temin etmek için siber güvenlik de ön plana çıkmaya başlamıştır. Siber güvenlik, siber alanı tehditlerden korumak, bilgi ve bilgi sistemlerinin erişilebilirliğini, bütünlüğünü ve gizliliğini sağlamak için alınan önlem ve gerçekleştirilen faaliyetlerdir.

Siber güvenlik, en hızlı büyüyen ve en büyük teknoloji sektörlerinden biri hâline gelmiştir. Çeşitli kaynaklarda yer alan siber güvenlik ekonomisi tahminlerine göre, önümüzdeki 5 yıl içinde siber güvenlik ürünlerinde küresel harcama bir trilyon

doları aşacak ve siber güvenlik profesyonellerine duyulan ihtiyaç önemli ölçüde artacaktır.

Siber alan, bireyler, kuruluşlar, sistemler ve uluslar dâhil tüm aktörleri birbirine bağlayan ve sınırları olmayan bir ortamdır. Siber güvenlik, siber alana artan bağımlılık nedeniyle öncelikli konu hâline gelmektedir. Siber saldırıların ve siber tehditlerin sayısı, şiddeti ve karmaşıklığı giderek artmaktadır. Riskleri yönetmek, siber saldırılara karşı koymak, insanları, kuruluşları ve ülkenin siber alandaki gizlilik ve güvenliğini korumak, iş operasyonlarını korumak, dünyayla bağlantıyı sürdürmek ve dijital alanda hayatta kalmak için uygun siber güvenlik stratejisi çok önemlidir. Siber alandan yararlanma yeteneğini korumak için siber güvenliğe yönelik politika, strateji ve planların geliştirmesi zaruridir.

Türkiye'de yaklaşık 15 yıl öncesinden itibaren siber güvenlik alanına devlet düzeyinde önem verilmeye başlanmış ve 2003 yılındaki e-Dönüşüm Türkiye Projesi ile resmî proje ve faaliyetler uygulamaya konulmuştur (Çifci, 2017). Siber güvenlik ile ilgili en önemli adımlar, Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014 ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019'dur. Söz konusu çalışmaların metodolojisi, teknoloji öngörüsü metodolojilerinden ziyade, uzmanlarla yapılan toplantı, çalıştay, seminer ve konferanslardı.

Teknoloji öngörüsü, stratejik araştırma alanlarını belirlemek ve önemli ekonomik ve sosyal kazanımlar getirebilecek ortaya çıkmakta olan teknolojileri tanımlamak için bilim, teknoloji, ekonomi ve toplumun uzun vadeli geleceğine bakmak için kullanılan standart bir yaklaşımdır (Martin, 1995). Yüksel ve Çifci (2017) teknoloji öngörüsünü "organizasyondan uluslararası seviyeye kadar çeşitli kaynakları kullanmak suretiyle orta veya uzun vadeli gelecek stratejilerini gerçekleştirmek amacıyla teknolojik, ekonomik ve sosyal alanları tanımlayarak yatırım ve araştırmaları önceliklendirmek için doğru metodoloji kombinasyonlarıyla sistematik ve çok disiplinli bir süreç" olarak tanımlamıştır. Öngörü, önemli bilim ve teknoloji konularını belirlemek için yaklaşımlar sağlamakta, araştırma ve geliştirme faaliyetlerini ekonomik ve sosyal ihtiyaçlarla

bütünleştirmek için araçlar sunmakta ve öngörü katılımcıları arasında etkileşim ve ortak anlayışı sağlamaktadır (Martin ve Johnston, 1999).

Literatürde ve pratikte, öngörü çalışmalarında izlenecek çeşitli teknoloji öngörüsü yaklaşımları, çerçeve ve modelleri vardır. Yüksel ve Çifci (2017) tarafından geliştirilen Öngörü Periskop Modeli (FPM), Kaynaklar, Metodoloji ve Gelecek Stratejileri olmak üzere birbirine bağlı üç modülden oluşan yeni bir teknoloji öngörü yaklaşımıdır. Model, periskopun modüllerinden ilham almakta olup, "kaynaklar" ve "metodoloji", bir kuruluşun alternatif geleceklerini görmesini ve bulunduğu çevrede hayatta kalmak ve rekabet edebilmek için takip etmesi gereken "gelecek stratejileri"ni görmesini sağlayan alt modüllerdir. Yazarlar ayrıca, "FORESIGHT" adlı dokuz ardışık adımdan oluşan İngilizce Framing (Çerçeveleme), Obtaining (Elde Etme), Reviewing (İnceleme), Establishing (Oluşturma), Synthesizing (Sentezleme), Illustrating (Gösterme), Guiding (Rehberlik), Handling (Ele Alma) ve Tracking (İzleme) kelimelerinin baş harflerinden meydana gelen, FPM ile entegrasyon içinde kullanılabilen genel bir fonksiyonel öngörü çerçevesi geliştirmişlerdir. FORESIGHT çerçevesindeki fonksiyon ve adımlar, literatürdeki yaygın öngörü çerçevelerinin işlem adımları ve ürünlerini kapsamakta ve daha kolay uygulanabilen modüllere ayırmaktadır.

FORESIGHT çerçevesi, öngörü faaliyetleri için kendine özgü yöntemlerin uygulanmasını zorunlu tutmamaktadır. Bununla birlikte, her aşamada ihtiyaç duyulan faaliyetleri yürütmek için her bir fonksiyonel aşamada uygun yöntemler önerilmektedir.

FPM, öngörü faaliyetlerini baştan sona kadar basitleştiren bir öngörü modelidir. Denizaltılarda kullanılan periskop cihazına benzer şekilde, model, altta yer alan kaynaklara ve metodolojilere bağlı olarak gelecekteki stratejileri mümkün olduğunca açık bir şekilde belirlemeyi amaçlamaktadır. Periskobun görüş açısı "öngörü kapsamını", menzili "öngörünün kapsadığı zamanı dilimini", çözünürlük kapasitesi, "alternatif geleceklerin etkin bir şekilde belirlenmesini" ve periskobu kullanan yetenekli ve eğitimli kullanıcılar ise "öngörü uzmanlarını" temsil etmektedir. FPM'de, somut ve soyut kaynaklar ve bunların örgütsel, sektörel,

ulusal ve uluslararası düzeylerdeki yansımaları, kullanılacak yöntemleri belirleyen faktörleridir.

Uygun yöntem kombinasyonlarının seçimi, eldeki kaynaklar ve yapılacak öngörü çalışmasının doğasına büyük ölçüde bağlıdır. Gelecek stratejileri, istenen veya muhtemel geleceğin var olduğu alternatif geleceklerdir. Modelin en alttaki bileşenini "kaynaklar" oluşturur, öngörü çalışmasının kaynaklarına, amaçlarına ve kapsamına göre "metodoloji" seçilir ve seçilen metodoloji ile gerçekleştirilen faaliyetlerin sonuçlarına göre "gelecek stratejileri" belirlenir. FPM, gelecek stratejilerini ele almak ve değerlendirmek için özel bir araç ve yöntemin kullanımını zorunlu kılmamaktadır. FORESIGHT çerçevesi adımlarında önerilen uygun yöntemler, gelecekteki stratejileri belirlemek, oluşturmak, uygulamak ve izlemek için kullanılabilmektedir.

Teknoloji öngörüsü model ve çerçeveleri muhtelif kuşaklara ayrılmaktadır. Organizasyonların ihtiyaçları ve teknolojik gelişmeler öngörü kuşakları için temel oluşturmaktadır. Teknoloji öngörüsü, amaç, kapsam, yöntemler, aktörler ve bağlam temelinde literatürde beş farklı kuşağa ayrılmıştır. Herhangi bir öngörü uygulaması, bir veya daha fazla kuşağın özelliklerine sahip olabilir. Çifci ve Yüksel (2018), Endüstri 4.0 (Industry 4.0) ve ötesine odaklanan, Öngörü 6.0 (Foresight 6.0) adında öngörü kuşağını önermekte; Toplum 5.0 (Society 5.0), netokrasi, siber alan, biyoteknoloji ve daha fazla değer ve etiği barından, karmaşa ve düzenin bir arada olduğu sosyal boyutta ele almaktadır. Netokrasi, gücünü teknolojik bir avantaj ve iletişim ağı oluşturma becerilerine dayandıran bir küresel üst sınıfı ifade eden bir terimdir. İnternet üzerinden siber ağların yaygınlığı ve internet üzerinden iletişim gücünün artması, toplumlarda netokrasinin yükselen bir yönetim anlayışı hâline gelmesine neden olmaktadır. Bu yeni öngörü kuşağı, farklı paydaşların küresel kapsamda ağ üzerinden katılımını kolaylaştırarak öngörü uygulamalarının daha etkin uygulanmasını sağlamaktadır. Öngörü verileri çevrimiçi olarak elde edilebilir; bu maksatla da büyük veri (big data) uygulamaları kullanılabilir. Öngörü 6.0, öngörü süreci içinde yapay zekâ ve makine öğrenimini de kullanabilmektedir.

Bu çalışmada, Savunma Sanayii Başkanlığı (SSB) teknoloji taksonomisi, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun (TÜBİTAK) ürün ve teknoloji taksonomisi ve uluslararası şirketlerin siber güvenlik ürün ve hizmet listeleri kullanılarak siber güvenlik teknoloji listesi ve teknoloji taksonomisi oluşturulmuştur. Akademik ve endüstriyel siber güvenlik teknoloji ve ürün listesine hitap edebilecek, doğru kategoriler altında en geniş kapsamlı bir listeye sahip olmak için, 15 adet sistemle ilgili teknoloji ve 6 adet sistem/ürün teknolojisi altında 169 temel teknolojiye sahip olan siber güvenlik teknolojisi taksonomisi oluşturulmuştur. Önceliklendirme için teknoloji listesi uzmanlara gönderilmiş, 169 siber güvenlik teknolojisi, üç kritere göre ağırlıklandırılmıştır (ulusal güvenlik ihtiyaçlarını karşılama; ulusal bilim, teknoloji ve inovasyon altyapısının gelişimini destekleme; dünya çapında rekabet edebilirlik, işbirliği veya karşılıklı bağımlılık yaratma).

Çalışma boyunca, Türk Silahlı Kuvvetleri, devlet kurumları, akademi ve siber güvenlik şirketlerinden yaklaşık 25 farklı uzmanın katılımıyla toplam üç odak grup toplantısı gerçekleştirilmiştir.

İlk odak grup toplantısı 17 uzmanın katılımıyla SSB'nin tesislerinde gerçekleştirilmiştir. Toplantıda vizyon çalışması, SWOT (İngilizce: Strengths, Weaknesses, Opportunities, and Threats; Türkçe: Güçlü, Zayıf Yönler, Fırsatlar ve Tehditler) analizi, STEEPLE (İngilizce: Social, Technological, Economic, Environmental, Political, Legal, and Ethical; Türkçe: Sosyal, Teknolojik, Ekonomik, Çevresel, Politik, Yasal ve Etik) analizi ve siber güvenlik eğilimleri anketi yapılmıştır.

Katılımcılar, araştırmacının önceden yazılmış olduğu SWOT faktörlerine öncelik vermiş ve kendi ifadelerini eklemeleri için teşvik edilmiştir. Ele alınan tüm faktörler, toplantı sonrasında katılımcıların öncelik puanlarına göre araştırmacı tarafından sıralanmıştır. Sonuçlar incelendiğinde, siber güvenlik konusunda Türkiye'nin zayıf yönleri, güçlü yönlerden daha fazla, fırsatlar ise tehditlerden çok daha fazla çıkmıştır. Çalışmada toplam 119 faktör (17 güçlü yön, 31 zayıf yön, 56

fırsat ve 15 tehdit) belirlenmiştir. Tüm faktörler arasındaki en öncelikli 10 faktör, Tablo K.1, Tablo K.2, Tablo K.3 ve Tablo K.4'te verilmiştir.

Tablo K.1: Siber Güvenlikteki Güçlü Yönlerimiz (İlk 10)

Sıra	Faktör	Güçlü Yönler
1	Sosyal	Genç ve girişimci insan gücü
2	Sosyal	Uluslararası topluma entegre bir bilim ve teknoloji camiası
3	Politik	Ortaya konan stratejileri gerçekleştirebilecek kurumların varlığı (SSM, TÜBİTAK, Bakanlıklar vb.)
4	Ekonomik	Ülkemizin dünyanın en büyük 20 ekonomisi arasında olması
5	Politik	Siber güvenlik alanına yönelik devlet desteklerinin varlığı
6	Teknolojik	Uluslararası arenaya açılmış sanayi
7	Yasal	Kişisel verileri, fikir ve eserleri koruma altına alan yasal altyapının varlığı (Fikir ve Sanat Eserleri Kanunu ve Kişisel Verilerin Korunması Kanunu vb.)
8	Sosyal	Genç ve teknolojiyi benimseyen insan gücü
9	Politik	Siber güvenliğe yönelik güçlü politik destek
10	Etik	Millîlik duygusunun sahiplenilmesi

Tablo K.2: Siber Güvenlikteki Zayıf Yönlerimiz (İlk 10)

Sıra	Faktör	Zayıf Yönler
1	Sosyal	Yetişmiş insan kaynağı eksikliği
2	Politik	Eğitim ve öğretimdeki aksaklıklar
3	Teknolojik	Siber güvenliğin üzerine inşa edildiği bilişim teknolojilerinde (özellikle donanım açısından) yurt dışına bağımlılık
4	Sosyal	Kurumların, siber güvenlik açısından gerçek ihtiyaçlarının farkında olmaması
5	Teknolojik	Bilgi sistemleri ve siber güvenliğe yönelik millî ürün ve teknolojilerin azlığı
6	Sosyal	Kamu, sanayi ve akademik camia arası iş birliğinin zayıf olması
7	Sosyal	İş birliği kültürünün eksikliği

Tablo K.2 (Devamı)

Sıra	Faktör	Zayıf Yönler
8	Teknolojik	Siber güvenlik alanında kurumsal yetkinliklerin (teşkilat, altyapı, personel, kaynak) yetersiz olması
9	Teknolojik	Çok sayıda firmanın az sayıdaki belirli siber güvenlik ürün ve hizmetlerine odaklanması
10	Teknolojik	Araştırmaya yönelik verilerin eksikliği

Tablo K.3: Siber Güvenlikteki Fırsatlar (İlk 10)

Sıra	**Faktör**	**Fırsatlar**
1	Sosyal	Siber tehditlerin artması ve daha karmaşık hâle gelmesi nedeniyle siber güvenliğe olan ihtiyacın artması
2	Politik	Ülkemiz dâhil, dünyadaki çoğu ülkede siber güvenliğin, millî güvenliğin unsurları arasında kabul edilmesi
3	Sosyal	Sosyal, teknolojik, ekonomik, çevresel ve politik faktörlerin doğurduğu siber güvenlik ihtiyaçları
4	Teknolojik	Siber güvenliğin doğası gereği, yerli ürünlere olan ihtiyaç
5	Sosyal	Teknolojinin hayatın her alanına nüfuz etmesi ve kullanımının artması
6	Ekonomik	Kamu ve özel sektörün siber güvenlik alanına yatırım yapma istek ve iradesi
7	Teknolojik	Siber tehditlerin hızlı bir şekilde gelişmesi
8	Ekonomik	İç ve dış pazarın genişliği
9	Sosyal	İnternet üzerinden verilen sayısal servislerin hayatın her alanına (sağlık, alışveriş, bilgi paylaşımı vb.) nüfuz etmesi
10	Teknolojik	Siber güvenlik sistemlerinin kurumsal olarak tesis edilmesinde eksikliklerin olması

Tablo K.4: Siber Güvenlikteki Tehditler (İlk 10)

Sıra	**Faktör**	**Tehditler**
1	Politik	Ar-Ge'ye olması gerekenden daha az yatırım yapılması
2	Sosyal	Yerli ürünlere olan güven eksikliği
3	Teknolojik	Acil tedarik talepleri nedeniyle sistemlerin millî olarak geliştirilmesine yeterli önemin verilememesi
4	Yasal	Kamu ihale mevzuatı gereği, maliyetin kaliteden önce değerlendirilmesi

Tablo K.4 (Devamı)

Sıra	Faktör	Tehditler
5	Ekonomik	Yabancı ürünlerin pazarın büyük kısmına hâkim olması
6	Ekonomik	Özellikle Batı dünyasında savunma harcamalarının sorgulanmaya başlanması
7	Politik	Gelişmiş siber güvenlik ürün ve teknolojilerinin satışına yönelik kısıtlamaların getirilmesi
8	Teknolojik	Bulut bilişime dayalı teknolojilerin yaygınlaşması ve bu alanda yabancı firmaların hâkimiyeti
9	Sosyal	Kolay para kazanmaya hevesli bir kültürün yerleşmeye başlaması
10	Ekonomik	Uluslararası rekabet

Araştırmacı tarafından siber güvenliğe yönelik STEEPLE faktörleri hazırlanmış, daha sonra katılımcılardan yenilerini eklemeleri ve toplantı sırasında tüm konuları önceliklendirmeleri istenmiştir. Elde edilen sonuçlara göre araştırmacı ve katılımcılar tarafından toplam 85 faktör (17 sosyal, 30 teknolojik, 14 ekonomik, 3 çevresel, 14 siyasi, 5 yasal ve 2 etik) belirlenmiştir. Buna göre, teknolojik faktörler en yüksek, etik faktörler ise en düşük orana sahiptir.

İlk odak grup toplantısında yapılan eğilim anketi sonuçlarına göre, önümüzdeki beş yıl içinde Türkiye ilk 10 siber saldırgan ülke arasında olmayacak, siber saldırıların hedefi olma açısından ise 4'üncü sırada olacaktır. Siber casusluk, bilgi sızması, veri ihlalleri, fidye yazılımı, kötü amaçlı yazılım, oltalama, siber casusluk, hizmet dışı bırakma, botnetler, web tabanlı saldırılar, kimlik hırsızlığı ve web uygulama saldırıları en yaygın saldırı türleri arasında yer alacaktır. Devlet kurumları, enerji, telekomünikasyon, bankacılık ve finans, silahlı kuvvetler, savunma sanayii, kritik altyapılar, sağlık, teknoloji, ulaştırma, imalat ve tıp sektörleri de siber saldırıların hedefi olacaktır. Bulut bilişim, büyük veri, yapay zekâ, nesnelerin interneti, derin öğrenme, makine öğrenmesi, blok zinciri, kablosuz iletişim, kuantum bilişim, bilişsel bilgi-işlem, giyilebilir cihazlar, akıllı nesneler (ev aletleri, çalışma alanı, evler, arabalar, şehirler vb.), mikro veri merkezleri, beyin-bilgisayar arayüzü, ticarî insansız hava araçları, otonom araçlar

ve sanal gerçeklik, siber güvenlik teknolojilerini etkileyen teknolojiler arasında sayılmıştır.

İlk odak grup toplantısından sonra araştırmacı, katılımcıların siber güvenlik teknolojisi puanlarına dayanarak Delfi ifadelerini hazırlamıştır. Delfi ifadeleri, siber güvenlik teknolojilerini içeren ve ulaşılması gerekli olduğu değerlendirilen kabiliyetlerdir. İfadeler, en yüksek puan alan teknolojileri içerecek şekilde yazılmıştır. Mümkün olduğunca çok sayıda teknolojiyi ele almak için benzer teknolojiler gruplanmıştır.

Odak grubunun ikinci toplantısı, SSB tesislerinde 14 uzmanın katılımıyla yapılmıştır. Bu toplantıda Delfi çalışması üzerine odaklanılmıştır. Katılımcılar araştırmacının önceden yazdığı 37 Delfi ifadesini incelemiş ve gerekli değişiklik önerilerini dile getirmiştir. Katılımcılara, daha önce önemine göre listelenmiş olan teknolojilerin listesi dağıtılmış ve bunlar arasından ilave kabiliyet (yani Delfi ifadesi) yazmaları talep edilmiştir. Toplantı sırasında, katılımcılar tarafından 54 ilave Delfi ifadesi önerilmiştir.

İkinci odak grup toplantısında ortaya konan Delfi ifadeleri uzmanlara e-posta ile gönderilmiş ve her ifade için Delfi sorularına cevap vermişlerdir. Bu esnada, araştırmacının 37 ifadesi ve odak grup toplantısından seçilen 10 ifade (toplam 47 ifade) değerlendirilmiştir. Bu ifadeler Tablo K.5'te verilmiştir. Delfi ifadeleri uzmanlar tarafından öncelik verilmiştir. Bu çalışma sonrasında, araştırmacı tarafından Delfi anketi için 25 ifade seçilmiştir.

Tablo K-5: Delfi İfadeleri

Delfi No	Delfi İfadesi
D-1	Gömülü sistemleri (embedded systems) siber saldırılara karşı koruyabilecek ve her türlü elektronik devrenin (çipler, mikro-elektronik devreler vb.) güvenlik testlerini yapabilecek teknolojik seviyeye ulaşılmıştır.
D-2	Süper bilgisayar ve kuantum bilgisayarlarla kırılamayacak (quantum safe) kripto algoritma, teknoloji ve modülleri (yazılım, donanım) geliştirilmiş ve operasyonel ortamlarda kullanılmaya başlanmıştır.

Tablo K-5 (Devamı)

Delfi No	Delfi İfadesi
D-3	Siber-fiziksel sistemlerin (akıllı nesnelere ait sistem ve ağlar, fabrika üretim kontrol sistemleri, endüstriyel internet ve endüstiyel kontrol sistemleri) siber güvenliğini sağlayacak teknoloji ve sistemler geliştirilmiş ve dünyada bu alanda ürün satan ilk 5 ülke arasına girilmiştir.
D-4	Ağa bağlı olarak çalışabilen çok küçük boyutlu sistemlerde kullanılabilecek kripto sistemleri (lightweight cryptography) geliştirilmiş ve uluslararası markaların ürünlerinde kullanılmaya başlanmıştır.
D-5	İnsanlı ve insansız uçak sistemleri ile hava trafik kontrol sistemlerinin (seyrüsefer sistemleri, hava trafik ağları, uçuş kontrol sistemleri vb.) siber güvenliğini sağlayabilecek, siber güvenlik protokol ve mimarileri geliştirilmiş ve kullanılmaya başlanmıştır.
D-6	Giyilebilir teknolojilere (saat, gözlük, elbise, yapay organlar, muhtelif sensörler vb.) yönelik siber güvenlik teknoloji ve sistemleri geliştirilmiş ve uluslararası markaların ürünlerinde kullanılmaya başlanmıştır.
D-7	Uygulama düzeyindeki saldırıları engellemek için, yapay zekâ, makine öğrenmesi ve derin öğrenme teknikleri kullanan, uygulama koruması (application shielding) ve Runtime Application Self-Protection (RASP) ve benzeri teknoloji ve uygulamalar geliştirilmiştir.
D-8	Dünyadaki üst düzey siber saldırı ve savunma kabiliyetine sahip ülkelerle (Ör.: ABD, Rusya, Çin) rekabet edecek düzeyde siber saldırı teknik, teknoloji ve sistemleri geliştirilmiş ve bu düzeyde güçlü bir siber ordu kurulmuştur.
D-9	Kablosuz cihazların (bilgisayar, ağ cihazları, cep telefonları, kameralar vb. her türlü cihaz ve sistemler) ve yeni nesil kablosuz iletişim teknolojilerinin (5G ve sonrası) siber güvenliğini sağlayacak teknolojiler geliştirilmiş ve uluslararası ürünlerde kullanılmaya başlanmıştır.
D-10	Bilgi sistem donanımlarında güvenilir işlemlerin çalışmasını ve güvenli şifreleme işlemlerinin yapılmasını sağlayan, yaygın anakartlarla uyumlu, Güvenilir Platform Modülü (Trusted Platform Module -TPM) sanal (virtual) ve fiziki (çip) olarak üretilmiş ve uluslararası pazardaki donanımlarda kullanılmaya başlanmıştır.
D-11	Nesnelerin İnterneti (Internet of Things) cihaz ve ağlarında mahremiyeti (privacy), kimlik doğrulamayı (authentication) ve iletişim güvenliğini sağlamaya yönelik protokol, teknoloji ve uygulamalar geliştirilmiş ve bu alanda en büyük pazar payına sahip ilk 10 ülke arasına girilmiştir.
D-12	Sistemlere giriş ve yetki vermede kullanılan kullanıcı/nesne kimlik denetimini ve veri güvenliğini en üst seviyede sağlamak amacıyla blok zinciri (blockchain) ve yeni nesil uygulama ve teknikler geliştirilerek kullanıma verilmiştir.
D-13	Uluslararası eğitim kurumları ve uluslararası siber güvenlik tatbikatlarında kullanılabilecek siber güvenlik test, eğitim ve tatbikat sistemleri geliştirilmiş ve küresel siber güvenlik eğitim ve inovasyon merkezî hâline gelinmiştir.

Tablo K-5 (Devamı)

Delfi No	Delfi İfadesi
D-14	Sanal işletim sistemlerinin güvenliğini en üst düzeye çıkaracak teknik ve teknolojiler (virtualization security, hypervisor security) geliştirilmiş ve uluslararası boyutta yaygın ürünlere entegre edilmiştir.
D-15	Dünyadaki bütün ülkeleri kapsayacak şekilde, siber tehditlere yönelik istihbarat (tehdit yöntemleri, araçları, kaynakları, hedefleri vb.) toplamaya, analiz etmeye ve karar desteği vermeye yönelik altyapı, yazılım, donanım, teknik ve teknolojiler geliştirilmiştir.
D-16	Büyük veri (big data) ve diğer veritabanı (database) sistemlerinin ve içindeki verilerin güvenliğini sağlamaya yönelik teknik (audit, encyption vb.), teknoloji, yazılım ve donanımlar geliştirilerek uluslararası boyutta pazarlanmaya başlanmıştır.
D-17	Çok sayıda nesne (cihaz, ağ, kullanıcı) arasında güven (trust) mekanizmasını sağlayacak ileri seviye teknik, teknoloji ve uygulamalar (distributed trust, blockchain benzeri mimariler vb.) geliştirilmiş ve uygulamaya verilmiştir.
D-18	Makine öğrenmesi (machine learning) uygulamalarında mahremiyeti (privacy) koruyacak teknik ve teknolojiler geliştirilmiştir.
D-19	Taşınabilir (portable) belleklerin (USB bellekler, harici diskler, disk üniteleri vb.) güvenliğini sağlayacak ileri düzey yazılım, donanım ve teknolojiler (kullanıcı doğrulama, kırılamayacak şekilde şifreleme, yüksek performans vb.) geliştirilmiştir.
D-20	Sunucular, uygulamalar, veritabanları ve ağ cihazları arasında, iç ve genel bulut altyapısında değişiklik algılama ve yapılandırma denetimini (configuration auditing) sağlayan teknik ve teknolojiler geliştirilmiş ve kullanılmaktadır.
D-21	Mobil ve sabit sistemlerde, zafiyet yönetimi (vulnerability management) ve siber güvenlik değerlendirmesi (assessment and evaluation) yapacak yeni nesil teknik, teknoloji ve uygulamalar geliştirilmiş ve bu alanda en çok tercih edilen ilk 5 teknolojik ürün arasına girilmiştir.
D-22	Sistemlere sızma testi (penetration testing) yapacak yeni nesil teknik (sistem içinden/dışından, yerinde/uzaktan, manuel/otomatik, yapay zekâ teknikleri kullanan vb.), araç ve teknolojiler geliştirilmiştir.
D-23	Siber güvenlik araç ve mekanizmalarının (Ör.: firewall, security gateway, guard, router vb.) yazılım modülleriyle karşılandığı yazılım tanımlı güvenlik (software defined security) modül ve sistemleri geliştirilmiş ve bu ürünlerde dünya pazarının en az % 5'ine hâkim olunmuştur.
D-24	Her türlü bilgi sistem cihazı (bilgisayar, telefon, akıllı nesne vb.) ve bilgi depolayan birimlerin (RAM, disk vb.) teknik analizini (cyber forensic) yapabilecek muhtelif teknik, yazılım, donanım ve teknoloji geliştirilmiş ve uluslararası pazara sunulmuştur.
D-25	Siber olaylara hızlı, etkin ve gerektiğinde otomatik bir şekilde karşılık verecek (incident response, automated response ve model-driven cyber defense dâhil) ve bu olayları yönetebilecek (incident management) yeni nesil teknoloji ve sistemleri geliştirilmiş ve kullanılmaya başlanmıştır.

Tablo K-5 (Devamı)

Delfi No	Delfi İfadesi
D-26	Sistemleri gelişmiş siber tehditlere (Advanced Persistent Threat -APT) karşı koruyacak teknik (isolation, sandbo1ing, virtualization, application control vb.), yazılım, donanım ve teknolojiler geliştirilmiş ve dünya piyasalarına pazarlanmıştır.
D-27	Sistemleri milyonlarca farklı noktadan gelen dağıtık servis dışı bırakma (Disributed Denial of Service -DDoS) saldırılarına karşı koruyabilen yeni nesil teknik ve teknolojiler geliştirilmiş ve dünyada pazarlarına sunulmuştur.
D-28	Sistemleri her türlü zararlı yazılıma (virüs, kurt, truva atı, rootkit vb.) karşı koruyabilecek, anomali/davranış tabanlı (imza tabanlı olmayan) yazılım ve donanımlar geliştirilmiş ve uluslararası boyutta pazarlanmaya başlanmıştır.
D-29	Siber saldırıları modelleyebilecek ve gerek test için, gerekse gerçek anlamda otomatik saldırı kabiliyetine sahip kendi kendine öğrenebilen (makine öğrenmesi, derin öğrenme vb. teknikleriyle) akıllı siber saldırı sistemleri geliştirilmiştir.
D-30	İletişim ağından gelecek trafiği analiz edip (deep packet inspection vb.) bunlara karşı otomatik önlemler alınmasını sağlayan sistemler (Firewall, Web Application Firewall, Intrusion Prevention System vb.) geliştirilmiş ve uluslararası pazarlarda tercih edilen ilk 10 marka arasına girilmiştir.
D-31	Veri sızıntısı önleme (Data Loss Prevention -DLP) teknik ve sistemleri geliştirilmiş ve bu alanda dünyadaki ilk 10 ürün arasına girilmiştir.
D-32	Web sunucularını ve web tabanlı sistemleri siber saldırılara karşı koruyacak yeni nesil teknik ve sistemler geliştirilmiş ve kullanılmaya başlanmıştır.
D-33	Tersine mühendisliği (reverse engineering) otomatik bir şekilde yapılmasını sağlayan ileri düzey teknik ve teknolojiler geliştirilerek kullanılmaya başlanmıştır.
D-34	Sistemleri saldırılardan koruyacak, saldırganların teknik ve hareketlerinin tespit edilmesini sağlayacak ileri düzey aldatma (deception) teknik ve sistemleri (balküpü -honeypot- vb.) geliştirilmiş ve kullanılmaya başlanmıştır.
D-35	Bulut bilişim güvenliğine yönelik teknik (encryption, access brokers vb.) ve teknolojiler geliştirilmiş ve kullanılmaya başlanmıştır.
D-36	Biyometrik (retina, parmak izi, yüz, ses vb.) kimlik doğrulama sistemleri geliştirilmiş ve uluslararası pazarlara sunulmuştur.
D-37	Siber güvenlik risk yönetimi metodoloji, teknik ve araçları geliştirilmiş ve kullanılmaya başlanmıştır.
D-38	Uzaydan internet servisi sağlayacak, kuantum anahtarlarına dayanan kuantum uydu geliştirilerek, derin uzayda konuşlandırılmıştır.
D-39	Uçan sistemlere (uçak, helikopter, insansız hava araçları vb.) siber saldırı kabiliyeti kazandırılmıştır.
D-40	Güvenilir seçim, toplum görüşü toplama ve anket altyapıları geliştirilmiştir.
D-41	İnsan davranışlarını bire bir taklit eden siber saldırı sistemleri geliştirilmiştir.

Tablo K-5 (Devamı)

Delfi No	Delfi İfadesi
D-42	Siber saldırıların kaynağını tespit ederek anında karşı saldırı yapmaya imkân sağlayan bilişsel tabanlı ağ altyapıları geliştirilmiştir.
D-43	Uzaydan gelen sinyallerin anlaşılmasını sağlayacak teknolojik seviyeye ulaşılmıştır.
D-44	Kırılması mümkün olmayan quantum makinelere karşı dirençli kriptografik algoritma tasarlayan yapay zekâ yazılımı geliştirilmiştir.
D-45	Güvenlik kayıtlarını (log) işleyerek görselleştiren ve analistler tarafından rahat anlaşılabilmesini sağlayan görselleştirme sistemleri geliştirilmiştir.
D-46	İnsan-makine haberleşmesinin güvenliğini sağlayan siber güvenlik sistemleri geliştirilmiştir.
D-47	Yapay zekâ sistemleri (robot vb.) bağışıklığını artırıcı, dayanıklı ve hızla iyileşebilir sistemler geliştirilmiş ve bu alanda dünyada ilk 10 ülke arasına girilmiştir.

Çalışmada iki aşamalı Delfi anketi, internet üzerinden uygulanmıştır. Anket için yaklaşık 1.900 kişiye ulaşılmıştır. 25 Delfi ifadesi içeren form Google Forms ortamında hazırlanmış ve e-posta ile anket linki katılımcılara gönderilmiştir. Delfi ifadelerinin ekonomiye katkısı ve güvenliğe katkısı 1 ile 5 arasında puanlanmış, gerçekleştirme zamanı ve gerçekleştirme yöntemleri de her bir Delfi ifadesi için oylanmıştır.

Delfi anketinin ilk turu, 17 Temmuz - 12 Ağustos 2018 tarihleri arasında gerçekleştirilmiştir. Azami sayıda katılımcıya ulaşabilmek için, Türkiye'deki üniversitelerdeki bilgisayar mühendisliği bölümlerinin öğretim üyelerinin e-posta adresleri, okulların resmî web siteleri aracılığıyla araştırmacılar tarafından toplanmıştır. Ayrıca, Türkiye'deki siber güvenlik konferans ve etkinlikleri sırasında, siber güvenlik uzmanlarından kartvizit toplanmıştır. Bunların yanı sıra, yeni katılımcıların iletişim adresleri, uzmanlar ve çalışma hakkında bilgi verilen kişiler tarafından araştırmacıya iletilmiştir. Toplamda 1.900 katılımcı bulunmuş ve anket gönderilmiştir. Anketin ilk turunu toplam 150 kişi cevaplamıştır.

Delfi anketinin ikinci turu, 28 Ağustos - 26 Eylül 2018 tarihleri arasında, ilk turu cevaplayan katılımcılarla tamamlanmıştır. Anketin ikinci turuna 150 kişi arsından toplam 91 kişi katılmıştır.

Elde edilen sonuçlara göre, Delfi turları arasında fikir birliğine varılmıştır; yani ilk turda verilen cevaplarla, ikinci turda verilen cevaplar birbirine yakın çıkmıştır. Ankette yer alan soruların oluşturduğu faktörlerin güvenilirlik analizi, SPSS Statistics programı kullanılarak Cronbach Alpha değerleri ile incelenmiştir. Birinci turun güvenilirliği 0.952 (Cronbach's Alpha) iken, ikinci turdaki güvenilirlik 0.937 olup, ankette değişkenlerin güvenilir bir şekilde ölçüldüğü görülmektedir. Delfi ifadelerinin güvenliğe katkısı 4,3 ile 4,9 puan arasında değişirken, ekonomiye katkısı 3,9 ile 4,6 arasında değişim göstermektedir. Bu çalışma neticesinde, 25 Delfi ifadesinin önceliklendirmesi, güvenliğe ve ekonomiye katkısına yönelik puanlamaları ile gerçekleştirme zamanı ve yöntemleri elde edilmiştir.

Türkiye'deki üniversitelerin siber güvenlik alanındaki durumlarını belirlemek amacıyla siber güvenlik ile ilgili kurs ve programları ortaya koyma maksadıyla bir çalışma yapılmıştır. Türkiye'de 114 üniversitenin 2019 yılı itibariyle bilgisayar mühendisliği, bilgisayar bilimleri, bilişim mühendisliği veya yazılım mühendisliği bölümleri bulunmaktadır. Toplam 10 üniversitenin bilgi güvenliği teknolojileri konusunda iki yıllık meslek yüksekokulu (ön lisans derecesi) vardır. Dört yıllık bölümler genel olarak "donanım" ve "yazılım" bölümlerine sahipken, bir üniversitenin "sayısal adlî bilişim" (digital forensics) ve üçünün lisans programları kapsamında "siber güvenlik" veya "bilişim güvenliği" seçenekleri bulunmaktadır. Üniversitelerin % 77'sinde (114'ün 88'i) lisans programlarının ders programında siber güvenlikle ilgili dersler bulunmaktadır. 2018-2019 Güz ve Bahar dönemlerinde, lisans programlarında toplam 171 siber güvenlik dersi (67 tanesi tekil/benzersiz, yani birbirinden farklı ders konusu olan) 34 farklı siber güvenlik konusu bulunmaktadır. 20 üniversitede siber güvenlik ile ilgili lisansüstü programlar (yüksek lisans veya doktora); üçünde doktora programı, diğerlerinde ise yalnızca yüksek lisans programı vardır. 114 farklı siber güvenlik konusu bulunan lisansüstü programlarında 322 siber güvenlik dersi (215 tanesi tekil/benzersiz) bulunmaktadır. Ağ güvenliği, kriptoloji, bilgi güvenliği, siber

güvenlik, veri güvenliği ve bilgi sistemleri güvenliği dersleri, Türkiye'deki üniversitelerin lisans ve lisansüstü programlarında yaygın olarak verilen derslerdir.

Türkiye'deki şirketler, siber güvenlik ürünlerinin olup olmadığını veya siber güvenlik hizmet sektöründe olup olmadığını belirlemek için analiz edilmiştir. Çalışmanın verilerini derlemek için yaklaşık 3.000 şirketin web sayfası ziyaret edilmiştir. Elde edilen sonuçlara göre siber güvenlik ürünlerine sahip 90 şirket ve siber güvenlik hizmetine sahip 96 şirket olmak üzere toplamda 186 şirket bulunmaktadır. Ülkemizdeki üretilen siber güvenlik ürünlerinin çoğu ağ güvenliği, kimlik ve erişim yönetimi, siber güvenlik olay yönetimi, internet güvenliği ve siber istihbarat, siber güvenlik risk ve uyum yönetimi ve veri güvenliği ile ilgilidir. Endüstriyel kontrol sistemleri güvenliği, işletim sistemleri ve konteyner güvenliği, otonom ve akıllı platform güvenliği ve donanım güvenliğine yönelik siber güvenlik teknolojisi grupları ile ilgili bir ürüne rastlanmamıştır. Siber güvenlik hizmetleri söz konusu olduğunda, danışmanlık, siber güvenlik risk ve uyum yönetimi, eğitim ve ağ güvenliği en yaygın hizmetlerdir. İnceleme sonucunda, endüstriyel kontrol sistemleri güvenliği, işletim sistemleri ve konteyner güvenliği, otonom ve akıllı platform güvenliği, donanım ve gömülü yazılım (firmware) güvenliği konusunda bir hizmete rastlanmamıştır.

SSB tarafından 2018 yılında Türkiye'deki siber güvenlik şirketlerini desteklemek amacıyla Türkiye Siber Güvenlik Kümelenmesi oluşturulmuştur. Üyelik süreci devam etmekte olup, şirketlerin neredeyse yarısı (186 şirketin 95'i) küme üyesidir. Türkiye'de 61 aktif teknoloji geliştirme bölgesi (bilim ve teknoloji parkları, yani teknoparklar) bulunmaktadır. Teknoparkların yaklaşık yarısında siber güvenlik şirketi bulunmaktadır. Türkiye Siber Güvenlik Kümesi'nin mali cirosu yaklaşık 300 milyon ABD doları olup, 2019 yılında bu cironun ikiye katlanması hedeflenmiştir. Bu şirketlerin ihracat geliri 41 milyon dolardır. Şirketlerin ortalama yaşı 6'dır ve yaklaşık 4.400 personel istihdam edilmektedir.

17 Aralık 2018 tarihinde beş uzmanla birlikte senaryo ve eylem planı çalışması gerçekleştirilmiştir. Çalışmada, kontrolümüz dışında olan önemli eğilimler tanımlanmıştır. Daha sonra alternatif senaryoları belirlemek için bu eğilimlerin

belirsizlik ve etkileri puanlanmıştır. Makul durum ve ölçütler, hâlihazırda hangi senaryonun gerçekleşmekte olduğunu ortaya koymak amacıyla "gösterge" olarak belirlenmiştir. Küresel Siber Güvenlik Endeksi, Küresel İnovasyon Endeksi, Gayri Safi Yurt İçi Hasıladan Ar-Ge'ye ayrılan pay, Ar-Ge personeli sayısı gibi değerler, bu göstergeler arasındadır. "Türkiye'nin Taahhüt ve Durumu" ve "Küresel Güvenlik ve İstikrar" adlı iki eksen üzerinde toplam dört senaryo oluşturulmuştur. "Türkiye'nin Taahhüt ve Durumu", Türkiye'nin siber güvenlik vizyonuna ulaşma isteği ve gerçekleştirdiği adımlarla ilgili tüm süreçleri içerirken, "Küresel Güvenlik ve İstikrar" ekseni ise, Türkiye'nin siber güvenlik hedeflerine ulaşırken karşılaşacağı zorluklarla, almak zorunda kalacağı riskleri kapsamaktadır. Senaryolar, Mavi Okyanusta Çakılma, Yükselen Siber Güvenlik Yıldızı, Cehennem Gibi ve Çamurda Bile Yükselme olarak isimlendirilmiştir. Delfi ifadeleri, ifadelerde kapsanan yeteneklerin yerine getirilmesi için gerek duyulan siyasi ve ekonomik güce göre ilgili senaryolara paylaştırılmıştır. Delfi ifadelerini (yani siber güvenlik yeteneklerini) içeren senaryoların yanı sıra, Türkiye'de siber güvenliğin geliştirilmesine yönelik eylem maddeleri tanımlanmıştır. Siber güvenlik alanındaki zayıflıkların ve tehditlerin üstesinden gelmek ve siber güvenlik açısından güçlü olunan yönlerden ve fırsatlardan istifade etmek amacıyla toplam 50 işlem maddesi ortaya konulmuştur. Bu işlem maddeleri Tablo K.6'da sunulmuştur.

Tablo K.6: Siber Güvenlik İşlem Maddeleri

No	Faktör	İşlem Maddesi
1	Ekonomik	Siber güvenlik firmalarının ciroları, iki yıl içinde en az % 20 artırılmalıdır.
2	Ekonomik	Siber güvenlik Ar-Ge projeleri için yıllık olarak SSB ve TÜBİTAK'a 10'ar milyon $ bütçe ayrılmalıdır.
3	Politik	İhracatı geliştirmek için, siber güvenlik ürünü üreten firmalara ihracat desteği olarak teşvikler (maddî destek, vergi indirimi vb.) ve kredi imkânı sağlanmalıdır.
4	Politik	Siber güvenlik ihracatını artırmak maksadıyla, her yıl 5 ülke seçilmeli ve o ülkelere açılmaya yönelik özel çalışmalar yapılmalıdır.

Tablo K.6 (Devamı)

No	Faktör	İşlem Maddesi
5	Politik	Siber güvenlik firmaları her yıl en az bir uluslararası fuara katılmalı ve ürünlerini tanıtmalıdır. Bu amaçla üretici firmalara devlet bütçesinden 10.000 dolar tutarında maddî destek sağlanmalıdır.
6	Politik	Siber güvenlik alanındaki patent sayısının artırılması amacıyla, patent niteliğine bağlı olarak karşılıksız maddî destek sağlanmalıdır.
7	Politik	Siber güvenlik alanında çalışan insan sayısı her yıl en az % 10 oranında artırılmalıdır (yılda en az yaklaşık 500 kişi).
8	Politik	Siber güvenlik ürün portföyünü genişletmek üzere, üretici firmaların olmadığı alanlarda çalışma yapılması için firmalara teknogirişim sermayesi verilmelidir.
9	Politik	Siber güvenlik alanında çalışan firmaların tamamının Siber Güvenlik Kümelenmesi'ne üye olması için tanıtım ve teşvik faaliyetleri gerçekleştirilmelidir.
10	Politik	Kamu kurumlarındaki bilgi işlem organizasyonlarına asgari 2 adet siber güvenlik uzmanı kadrosu ilave edilmelidir.
11	Politik	Kalifiye iş gücünü ülkemizde tutacak siyasi, sosyal, hukuki ve ekonomik ortam tesis edilmelidir.
12	Politik	Ülkemizde en üst düzeydeki kurumların (İçişleri Bakanlığı, Silahlı Kuvvetler, Millî İstihbarat Teşkilatı, USOM, BTK vb.) siber güvenlik görev dağılımı yeniden düzenlenmelidir.
13	Politik	Kademeli olarak önümüzdeki 5 yıl içinde Ar-Ge yatırımlarının GSYİH'ya oranı en az % 2'ye çıkarılmalıdır.
14	Politik	Her yıl 5 firmanın yurt dışında saygın bir teknokent veya başka bir iş merkezinde yurt dışı birimi açması için destek sağlanmalıdır.
15	Politik	Kamu kurumlarında, siber güvenlik ve bilgi işlem kadrolarında çalışan personelin siber güvenlik sertifika sınav ücretleri (sınavdan başarılı olanların) devlet tarafından karşılanmalıdır.
16	Politik	Siber güvenlik kadro görev tanımları ve iş gücü kataloğu oluşturulmalı, yapılması gereken görevlerin tanımları ve alınması gereken sertifikalar standart hâle getirilmelidir.
17	Politik	Siber güvenlik teknolojilerinde başarılı firmalara (ürün ihracatı, alınan patentler vb. kriterleri ile) her yıl teknoloji ödülleri verilmelidir.
18	Politik	Önümüzdeki 5 yıl içinde siber güvenlik firma sayısını 3 katına çıkarabilmek için (180'den 540'a) her teknoparka en az 10 siber güvenlik firması kuracak şekilde sektörel planlama ve teşvik yapılmalıdır.
19	Politik	Belirli altyapı ve sistemlerde sertifikalandırılmış millî siber güvenlik ürünlerinin kullanımı zorunlu tutulmalıdır.

Tablo K.6 (Devamı)

No	Faktör	İşlem Maddesi
20	Sosyal	Her üniversitede yılda bir defa akademik birimler ve öğrencilerin katılacağı siber güvenlik farkındalık konferansı düzenlenmelidir.
21	Sosyal	SSB tarafından siber güvenlik insan kaynağı envanteri oluşturulmalıdır.
22	Sosyal	Toplumda siber güvenlik bilincini geliştirme maksadıyla Kamu Spotu kısa filmleri çekilmeli ve ulusal medyada gösterilmesi sağlanmalıdır.
23	Teknolojik	Siber güvenlik ürünlerinin, kalite seviyesinin yükseltilmesi, test edilebilmesi ve sertifikasyonu için bağımsız test ve sertifikasyon merkezi kurulmalıdır.
24	Teknolojik	Ülkemizde üretilen siber güvenlik ürünlerinde kullanılmayan, üzerinde çalışma yapılmayan siber güvenlik alanlarına yönelik Ar-Ge ve ürün geliştirme çalışmaları yapılmalıdır.
25	Teknolojik	SSB himayesinde iki yılda bir siber güvenlik teknoloji öngörüsü çalışması yapılmalıdır.
26	Teknolojik	Dünyada üretilen siber güvenlik ürünleri arasında, başarılı olanlar belirlenmeli, bunların ortak özellikleri ortaya konmalı ve millî ürünlere bu özelliklerden uygun olanlar kazandırılmalıdır.
27	Teknolojik	SSB, TÜBİTAK, Sanayi ve Teknoloji Bakanlığı ve Ulaştırma ve Altyapı Bakanlığı gibi kurumların her biri tarafından her yıl uluslararası katılımcılı siber güvenlik seminer ve fuarları düzenlenmelidir.
28	Teknolojik	YÖK tarafından her yıl belirlenen iki üniversite tarafından, dünyadaki üniversitelerin ve firmaların katılacağı uluslararası siber güvenlik seminer ve fuarları düzenlenmelidir.
29	Teknolojik	SSB tarafından her yıl 5 firmanın ortaklığıyla 5 adet siber güvenlik Ar-Ge projesi başlatılmalıdır.
30	Teknolojik	Her ay bir adet siber güvenlik yarışması (capture the flag, hacking competition vb.) düzenlenecek şekilde firma ve üniversitelere görev verilmeli, sponsor bulunarak etkinlikler yapılmalıdır.
31	Teknolojik	Yılda en az 1 defa uluslararası siber güvenlik yarışması, çarpıcı bir isimle (Hack-Tur-Key gibi), düzenlenmelidir.
32	Teknolojik	Siber güvenlik uzmanlarının her yıl farklı konularda en az 3 yeni eğitim almaları sağlanmalıdır.
33	Teknolojik	10 büyük ile “siber güvenlik teknik meslek lisesi” açılmalıdır.
34	Teknolojik	Teknik meslek liselerindeki mevcut bölümlere “siber güvenlik” bölümü eklenmelidir.
35	Teknolojik	En az 10 üniversitenin bilgisayar mühendisliği bölümlerinde “siber güvenlik ana bilim dalı” açılmalıdır.

Tablo K.6 (Devamı)

No	Faktör	İşlem Maddesi
36	Teknolojik	Üniversitelerin bilgisayar mühendisliği ve yazılım mühendisliği bölümlerinde en az bir adet zorunlu siber güvenlik dersi verilmelidir.
37	Teknolojik	Üniversitelerdeki siber güvenlik yüksek lisans bölümlerinin sayısı iki katına çıkarılmalıdır (20'den 40'a çıkarılması).
38	Teknolojik	Üniversitelerdeki siber güvenlik doktora programlarının sayısı 10'a çıkarılmalıdır (hâlihazırda 3).
39	Teknolojik	Siber güvenlik teknoloji taksonomisi oluşturulmalı ve sürekli güncellenmelidir (Bu amaçla, bu tezde oluşturulan taksonomiden başlanabilir.).
40	Teknolojik	Siber güvenlik taksonomisine uygun olarak firma ve ürünlerin tasnifi yapılmalıdır. Bahse konu faaliyet, bu tez çalışmasında yapılmıştır. Bu faaliyetin periyodik olarak güncellenmesi sağlanmalıdır.
41	Teknolojik	Sadece siber güvenlik konusunda bilimsel makalelerden oluşan ve Science Citation Index'e kayıtlı aylık dergi yayınlanmalıdır.
42	Teknolojik	Her yıl 200 öğrenci yüksek lisans, 100 öğrenci doktora ve 50 öğrenci post doktora eğitimi için yurt dışına gönderilmeli, eğitim masraflarının en az yarısı devlet tarafından karşılanmalıdır. Bu öğrencilerin en az iki yıl Türkiye'deki firma veya üniversitelerde çalışmasını sağlayacak şekilde yasal düzenleme yapılmalıdır.
43	Teknolojik	Ülkemizde üretilen siber güvenlik ürünlerinin, uluslararası muadilleriyle rekabet edebilmesi ve kalite seviyesinin artırılması amacıyla, uluslararası standartları sağlaması ve yaygın sertifikasyonları (Common Criteria gibi) alması sağlanmalıdır.
44	Teknolojik	Siber güvenlik teknolojilerine altyapı oluşturacak teknolojilere (gelişmiş bilgi işlem, kuantum bilişim, bulut bilişim, kablosuz iletişim vb.) yatırım yapılmalıdır.
45	Teknolojik	Siber güvenlik alanı ile ilgili diğer destek teknolojiler (artificial intelligence, big data, deep learning, augmented reality, brain-computer interface, machine learning, virtual reality, IoT, autonomous vehicles, cloud computing, smart robots, wearable devices vb.) üzerinde çalışma yapılmalıdır.
46	Teknolojik	Siber güvenlik staj programları oluşturulmalı, üniversitelerin bilgisayar veya yazılım mühendisliği bölümü öğrencilerinin Siber Güvenlik Kümelenmesi üyesi firmalarda staj yapması teşvik edilmelidir.
47	Teknolojik	İngilizce siber güvenlik eğitimi ve sertifikası veren, farklı alanlarda uzmanlığa sahip en az 50 kişilik uzmandan oluşan, uluslararası bir siber güvenlik eğitim merkezi kurulmalıdır.

Tablo K.6 (Devamı)

No	Faktör	İşlem Maddesi
48	Teknolojik	TSE veya TÜBİTAK BİLGEM bünyesinde ABD'deki NIST (National Institute of Standards and Technologies) benzeri siber güvenlik rehberleri hazırlayacak birim kurulmalıdır.
49	Teknolojik	Türk siber güvenlik firmaları arasında ürün entegrasyonu çalışmaları yapılmalı, "ürün ailesi" modeliyle tümleşik çözümler ortaya konmalıdır.
50	Teknolojik	Farklı siber güvenlik ürün gruplarında uzmanlaşmış en az 5 firma tarafından ortak siber güvenlik laboratuvarı kurulmalı, bu merkezde her türlü siber güvenlik ürünü ve zararlı yazılımlar üzerinde çalışma yapılabilmelidir.

Çalışma sonuçlarına göre, siber güvenlik teknolojileri, eğitimi, ürün ve hizmetleri konusunda ve araştırma ve geliştirmeye yatırım yapma konusunda ülkemizin kat etmesi gereken uzun bir mesafe olduğu görülmektedir. Çalışma kapsamında tanımlanan vizyona erişmek için, belirlenen işlem maddelerinin kararlı bir şekilde gerçekleştirilmesi ve senaryolarda yer alan yol haritalarındaki kabiliyet ve teknolojilere yönelik çalışma ve yatırımların gerçekleştirilmesi gereklidir. Ayrıca, siber güvenliğe yönelik teknoloji öngörüsü çalışmalarının düzenli olarak tekrar edilmesi ve yapılan çalışmaların sonuçlarının değerlendirilerek gerekli düzeltme ve geliştirmelerin yapılması hayati önem taşımaktadır.

APPENDIX L: TEZ İZİN FORMU/THESIS PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences [ ]

Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences [X]

Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics [ ]

Enformatik Enstitüsü / Graduate School of Informatics [ ]

Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences [ ]

YAZARIN / AUTHOR

Soyadı / Surname : Çifci
Adı / Name : Hasan
Bölümü / Department : Science and Technology Policy Studies

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English): Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040

TEZİN TÜRÜ / DEGREE**:** **Yüksek Lisans** / Master [ ] **Doktora** / PhD [X]

1. **Tezin tamamı dünya çapında erişime açılacaktır. /** Release the entire work immediately for access worldwide. [X]
2. **Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two year. *** [ ]
3. **Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. ***** [ ]

***** *Enstitü Yönetim Kurulu Kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir.*
A copy of the Decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.

Yazarın imzası / Signature ..... **Tarih** / Date .....