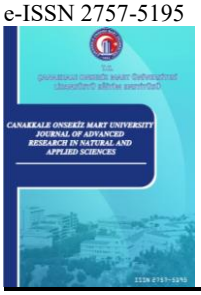
e-ISSN 2757-5195



Çanakkale Onsekiz Mart University

Journal of Advanced Research in Natural and Applied Sciences

Open Access

doi.org/10.28979/jarnas.1194845 2023, Vol. 9, Issue 2, Pages: 331-344 dergipark.org.tr/tr/pub/jarnas

Cybersecurity Technology Foresight: 2040 Scenarios for Turkey

Hasan Çifci[1,*], Serhat Çakır[2]

[1]Department of Software Engineering, Faculty of Engineering, Aydın University, Istanbul, Türkiye
[2] Technology and Knowledge Management, Faculty of Economics and Administrative Sciences, Başkent University, Ankara, Türkiye

Article History

Received: 28.10.2022

Accepted: 20.01.2023

Published: 30.06.2023

Research Article

Abstract − Foresight is a methodical and comprehensive approach that prioritizes investment and research in order to shape the future and implement future strategies. Cybersecurity, one of the most important elements of Industry 4.0, is to protect information and communication systems against cyber attacks and to ensure the availability, confidentiality and integrity of these systems and the data therein. This study aims to make a theoretical and practical contribution to foresight and cybersecurity studies by summarizing the updated version of the methods and outputs used in the doctoral thesis titled "Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040", conducted at Middle East Technical University (METU) in 2019. As a result of the study, Turkey's national cybersecurity technology foresight was given with different scenarios; Turkey's strengths, weaknesses, opportunities and threats in terms of cybersecurity were determined; a cybersecurity technology taxonomy which is officially accepted by the Presidency of Defense Industries was created; the cybersecurity status of the universities and companies in Turkey has been determined; and concrete policy recommendations based on foresight outputs have been put forward. The study is the most comprehensive cybersecurity foresight in Turkey in terms of topics covered and participants, which comprises nearly 150 experts from government, military, academia, and the private sector. Overall, the study provides important insights into the current state of cybersecurity in Turkey and makes recommendations for the future. Its wide range of stakeholders and comprehensive analysis make it a valuable resource for understanding the complex landscape of cybersecurity in the country.

Keywords *– Cybersecurity, cybersecurity in Turkey, cybersecurity technology taxonomy, Foresight Periscope Model, technology foresight*

1. Introduction

Technology has now permeated practically every aspect of our daily lives. The growing use of information and communication technologies (ICT) and the internet has led to the establishment of a new environment characterized by the interconnection of numerous devices, ranging from mobile phones to smart home appliances. Cyberspace is the environment comprising computer systems, ICT infrastructures, telecommunications networks and embedded integrated circuits (NIST, 2022).

Dependence on cyberspace introduces new dangers and challenges to individual, national, and international security. In the World Economic Forum's 2021 Global Risks Report, cybersecurity vulnerability is ranked among the top 10 most serious global threats (World Economic Forum, 2021). As cyberspace grows more pervasive, cybersecurity, which is defined as the process of detecting, preventing and responding to cyber threats (NIST, 2018), and maintaining the confidentiality, availability and integrity of information systems and data in cyberspace will become increasingly crucial (European Commission, 2013).

[1] hasancifci@aydin.edu.tr
[2] serhatc@baskent.edu.tr
[*]Corresponding Author

Cyber threats and vulnerabilities are becoming more numerous, severe, and complicated (Çifci, 2017). In order to manage risks, withstand cyber attacks, safeguard individuals and organizations in cyberspace and commercial operations, maintain connectivity with the world, and exist in the digital realm, it is important to build an adequate level of cybersecurity (ENISA, 2012). It is vital to build cybersecurity policies, plans and strategies to preserve the capacity to exploit cyberspace.

Global spending on cybersecurity products and services reveals that, in addition to establishing security, the economic impacts of cybersecurity are important (Rodrigues et al., 2019). It was estimated that a total of 1.75 trillion dollars will be spent globally for the five-year period from 2021 to 2025 (Braue, 2021).

Because technology foresight is a process to identify technologies crucial to an industry's performance to design the desired future (Chen et al., 2012), it can be used as a tool to develop strategy, goals, and roadmaps for cybersecurity, too. Technology foresight is a structured approach (Keenan et al., 2003) and a systematic procedure (Conway, 2014) for identifying key research fields and emerging technologies by looking at the long-term future of science, technology, economy, and society (Martin, 1995). Foresight, as defined by Yüksel and Çifci (2017), is a multidisciplinary process that employs relevant methodology components to select research areas or propose long-term plans.

In the literature, there are various methods, models and frameworks to be followed in foresight activities. Foresight has been widely used since the 1990s as it helps to identify important areas of science and technology and integrate research and development efforts with social and economic needs (Martin & Johnston, 1999). In this study, the roadmap and action plans were determined using a novel technological foresight technique called the Foresight Periscope Model (FPM) developed by Yüksel and Çifci (2017).

At the start of the research, "Cybersecurity Roadmap of Turkey" working group was formally formed under the technological panels under the auspices of the Undersecretariat for Defense Industries (SSM) in January 2018. Then, members were recruited, and the researcher was assigned as the chairman of the group. While the research proceeded, the working group lost official support as a result of the temporary suspension of the technology panel's activities after the reorganization of the SSM into the Presidency of Defense Industries (Defense Industry Agency-DIA); but even so, the activities were completed within the academic framework.

To conduct the study, around 25 specialists from the Turkish Armed Forces (TAF), government organizations like TÜBİTAK (The Scientific and Technological Research Institution of Turkey), universities, and cybersecurity corporations participated in a total of three focus group sessions. In addition, for the online Delphi survey, which was conducted within the scope of determining the technology roadmap, approximately 1,900 experts were contacted via e-mail and the opinions of 150 experts were obtained. Most of the participants were from academia, and of those participants, 36% had more than 5 years' experience in cybersecurity. Additionally, 75% of all the participants held a Master of Science or doctoral degree.

2. Materials and Methods

Before the thesis work, the Foresight Periscope Model (FPM) and a framework of generic foresight named FORESIGHT, which was used with FPM, were introduced to the literature by Yüksel and Çifci (2017) and presented at the International Conference on Engineering, Technology and Innovation (ICE/ITMC) conference in 2017. The model has been developed to select and perform the most appropriate methods in foresight activities by integrating the factors and resources that affect the selection of foresight methodologies into the process.

The FPM model and the FORESIGHT framework were used in the research. The methods selected and applied in the study are shown in Table 1.

2.1. The Technology Foresight Model Used in the Research

To streamline and standardize the foresight processes, Yüksel and Çifci (2017) developed the Foresight Periscope Model (FPM), which has three components: resources, methodology and future strategies. Like the periscope used on submarines, FPM uses available resources and methods to clearly define future strategies.

The model was updated in the light of the experiences gained from the thesis studies by Yüksel (2018) and Çifci (2019).

Table 1
Methods Used in the Study in the Order of the FORESIGHT Phases

Functions	Methods
Framing	Literature Review, Visioning
Obtaining	Brainstorming, Literature Review, Survey, Workshop, Focus Group
Reviewing	Trend Analysis, SWOT (Strengths and Weaknesses, Opportunities and Threats), STEEPLE (Social, Technological, Economic, Environmental, Political, Legal, Ethical), Focus Group
Establishing	Expert Panel, Delphi Survey
Synthesizing	Visioning, Critical Technologies, Scenario Building
Illustrating	Roadmapping
Guiding	Critical Technologies, Policy Recommendations, Strategy Development
Handling	Strategy Formulation, Policy Recommendations, Action Plans
Tracking	*(This phase is not included in the scope of the study)*

The FORESIGHT is a general functional foresight framework that consists of nine phases (Framing, Obtaining, Reviewing, Establishing, Synthesizing, Illustrating, Guiding, Handling, Tracking) and can be used with FPM. Functions and phases in the FORESIGHT framework cover the actions of widespread foresight models in the literature and divide foresight activities into sub-modules. The FORESIGHT method selection framework is integrated into the FPM as seen in Figure 1. The methods in the first four phases (FORE) correspond to the methodology, while the remaining five phases (SIGHT) are used to identify and implement future strategies.

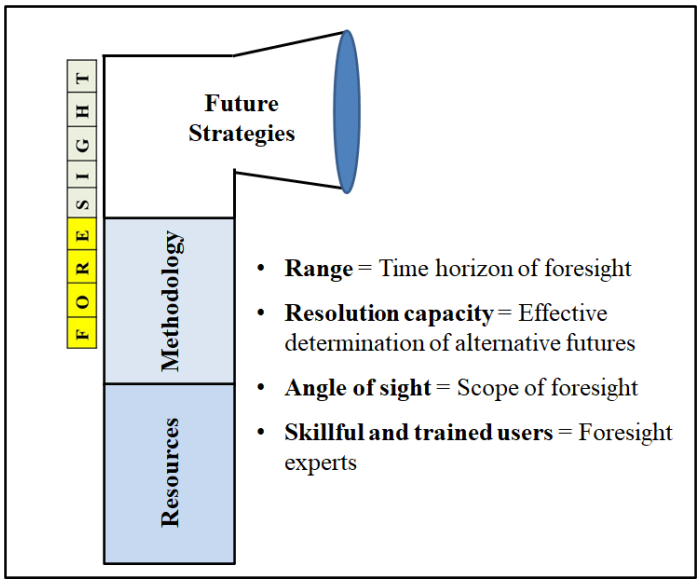


Figure 1. Foresight Periscope Model-FPM

Based on the underlying resources and processes, FPM attempts to establish its future strategies as clearly as possible. The periscope's field of vision symbolizes the “foresight scope”, the range represents the “timeframe” covered by the foresight, the resolution codes the “effective assessment of possible futures”, and educated and skilled periscope users represent the “foresight specialists”. The elements that influence the approaches to be employed in FPM include diverse resources as well as their reflections at the organizational, sectoral, national, and international levels.

Available resources and the type of foresight study are the determinants of the tools, techniques and methods of the foresight activities to be done (Miles, 2002; Popper, 2008; Porter, 2010). "Methodology" is chosen based on the resources, aims, and scope of the foresight research, and "future strategies" are established based on the outcomes of the activities conducted with the methods chosen. Future strategies are determined based on the

desired and possible futures. To examine and assess action plans, FPM does not require the use of a specific instrument or approach. Appropriate approaches from the FORESIGHT phases can be utilized to define, apply, and monitor strategic directions.

3. Aim and Significance of the Study

The primary goal of this research is to develop a cybersecurity technology foresight for Turkey for the next 20 years, till 2040. In this context, the goal is to reveal Turkey's cybersecurity strengths and weaknesses, as well as opportunities and threats in this field, to identify the cybersecurity technologies that should be invested in, to identify the various scenarios in terms of investments to be made in the country and global security and stability, to identify the most appropriate course of action, and to make concrete policy recommendations.

Cyberspace has evolved as a new warfighting domain, in addition to land, sea, air and space (Brandes, 2013). As technology progresses at a breakneck pace, it is vital to take measures against dangers, weaknesses, and risks in order to make safe use of these advancements. Cybersecurity is a primary priority that must be met in order to attain protection and attack capabilities and supply the required infrastructure.

Many areas of economy, scientific studies, commerce, communication and social life are interconnected in today's digital world through an infrastructure called "cyberspace" (The White House, 2015). The threat of devastating cyber attacks is increasing on this infrastructure targeted by malicious actors. One of the main security issues in state-level national security strategies is cybersecurity. It is widely accepted that long-term and strategic approaches to cybersecurity are necessary (Cyber Security Council, 2016).

According to the results of the literature review, technology foresight is not used as a common method in the creation of country-level cybersecurity strategies (Çifci, 2019; Bahuguna et al., 2020). As in the examples of the Vision 2003 study conducted in Turkey (TÜBİTAK, 2004) and Japan's 10th Foresight Study (Ogasawara, 2015), cybersecurity is not considered as the main theme of technology foresight studies but as a sub-title under information and communication technologies. In addition, studies such as the European Cybersecurity Foresight show that the cybersecurity foresight activities focus on only a few issues related to the Internet of Things (IoT) (Cyber Security Council, 2016).

In this study, which was carried out within the scope of the doctoral thesis, cybersecurity is considered as the main theme of foresight methods. In this context, with the participation of specialists from various institutions and organizations throughout the country, this study can be considered to make a significant contribution to the technology foresight and cybersecurity literature. At the end of the study, the cybersecurity vision, Turkey's strengths and weaknesses, opportunities and threats in the field of cybersecurity, the status of universities and private companies in the country, and the cybersecurity technology taxonomy officially accepted by the Turkish government, in addition to the 20-year cybersecurity roadmap, were attained.

The study provides technology foresight researchers with ways, methods and tools and facilitates technology foresight studies, especially in the field of cybersecurity, by offering concrete guidance on an exemplary process through the case of Turkey.

4. Basic Steps of Conducted Foresight Study

The main activities in the study were carried out in the following order:

- Literature review by the researcher,

- Creating a website where information, documents and announcements are shared,

- First focus group meeting: Vision study, selection of criteria for the weight of cybersecurity technologies, STEEPLE analysis,

- The researcher's survey on cybersecurity-related technologies,

- Prioritizing cybersecurity technologies by experts,

- Creation of desired cybersecurity capabilities by the researcher in the form of Delphi statements,

- Second focus group meeting: Reviewing the cybersecurity technology list, reviewing Delphi statements by experts and creating new statements, conducting a survey on cybersecurity regarding Turkey with the experts participating in the meeting,

- Prioritizing the cybersecurity capabilities list by experts,

- Two-round Delphi survey: Conducting an online Delphi survey (1,900 experts were reached and answers were received from 150 experts),

- The researcher's analysis of Turkey's cybersecurity sector and the current situation of universities,

- Workshop: Creation of scenarios, determination of roadmap and concrete policy actions.

5. Results and Discussion

Information about the main outputs revealed in the study is given in the following sub-headings. In this context, the following outputs were obtained:

- Cybersecurity Technology Taxonomy

- Turkey's Strengths and Weaknesses, Opportunities and Threats Analysis

- Capabilities to be Acquired

- Status of Universities in Turkey in terms of Cybersecurity

- Cybersecurity Companies in Turkey

- Scenarios and Roadmaps

- Cybersecurity Action Items (Action Plan)

5.1. Cybersecurity Technology Taxonomy

Participants created a list of 169 underpinning technologies, which were organized into 15 system-based technologies, and 6 systems/products. This list was designed to cover the correct categories that can satisfy commercial and academic needs (Table 2). The most comprehensive list of literature has been created with the help of experts from diverse backgrounds and organizations. Cybersecurity technologies and classification prepared in this study have been adopted by the DIA as a formal technology taxonomy[2] of the Turkish defense industry.

Table 2
Technology Taxonomy Created in the Study

Technology Group	No	Technology/System/Product
Group A Underpinning Technologies	1-169	Samples: Network Security Policy Management, Network Access Control, Software-Defined Security, Network Monitoring.
Group B System Related Technologies	1-15	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
Group C Systems/Products	1-6	Cybersecurity Analytics, Cyber Intelligence, Cybersecurity Operations, Cybersecurity Event Management, Cyber Forensics, Cybersecurity Risk and Compliance Management

[2] It is possible to access the Defense Industry Technology Taxonomy at https://www.sasad.org.tr/uploaded/SSB-Savunma-Sanayi-Teknoloji-Taksonomisi.pdf in both Turkish and English.

In this study, the technology list with 169 cybersecurity technologies was e-mailed to experts for assessment and prioritization. The technologies were weighted by the experts according to their contribution to national security needs, science and innovation capability and global competitiveness.

5.2. Turkey's Strengths and Weaknesses, Opportunities and Threats Analysis

The first meeting of the study was held at the facilities of the DIA with the participation of 17 cybersecurity specialists. The vision was determined at the meeting. A SWOT analysis, a STEEPLE analysis and cybersecurity trend survey were also conducted.

The researcher prepared Turkey's SWOT factors before the meeting, and experts were requested to provide their perspectives with additional factors. All the elicited factors were ranked by the researcher according to the priorities given by the participants in the meeting. When the results are examined, among 119 factors, Turkey's weaknesses (31 weaknesses) in cybersecurity are more than its strengths (17 strengths), and opportunities (56 opportunities) are much more than threats (15 threats). The top 10 factors among all factors are given in Table 3 and Table 4.

Table 3
Cybersecurity Strengths and Weaknesses of Turkey (Top 10)

No	Strengths	Weaknesses
1	Young and entrepreneurial workforce	Lack of trained human resources
2	A science and technology community integrated into the international community	Disruptions in education and training
3	The existence of government institutions that can realize the cybersecurity strategies	Dependence on abroad in high-tech areas
4	Economic power of Turkey	Organizations are unaware of their true cybersecurity requirements
5	Presence of state support for cybersecurity	Lack of domestic products and technology in the field of cybersecurity and information systems
6	Industry opened to the international arena	Inadequate collaboration between the general public, industry, and academia
7	Presence of legal and regulatory framework that safeguards personal information, ideas, and works	Absence of a collaborative culture
8	Young and technology-adoptive manpower	Insufficient corporate competencies in the field of cybersecurity
9	Strong political support for cybersecurity	Businesses specialize in a small range of niche cybersecurity services and products
10	Embracing the sense of nationality	Limited amount of data for research

The researcher prepared the STEEPLE factors based on the extensive survey and analysis. In the workshop, specialists were requested to add new factors to the existing list. A total of 85 factors which have an impact on Turkey's capabilities were determined in the meeting. Then the factors were prioritized by the participants based on their effects. According to the results of the study, technological factors that need to be addressed by Turkey have the highest rate, while ethical factors have the lowest. This demonstrates that the challenges that have to be resolved with regard to technology are prevalent in Turkey.

According to the results of the trend survey conducted face-to-face with experts at the first focus group meeting, it was evaluated that Turkey would be among the top five countries in the world in terms of being the target of cyber attacks in the next five years. It is also predicted that information leakage, cyber espionage, data breaches, ransomware, malware, phishing, zombie computers, web-based attacks, identity theft and web application attacks will be among the most common types of attacks.

5.3. Capabilities to be Acquired

After the first meeting with the experts, the researcher prepared the capabilities to be acquired (Delfi statements) based on the participants' cybersecurity technology weightages. Delphi statements are capabilities that include cybersecurity technologies and are considered necessary to be achieved. The statements were written to include the highest rated technologies.

Table 4
Opportunities and Threats for Turkey in Cybersecurity (Top 10)

No	Opportunities	Threats
1	Increasing need for cybersecurity as cyber threats increase and become more complex	Under-investment in R&D
2	Integration of cybersecurity as a component of national security in many countries worldwide	Lack of confidence in domestic products
3	Cybersecurity needs arising from social, technological, economic, environmental and political factors	Failure to attach sufficient importance to the national development of systems due to urgent supply demands
4	Due to the nature of cybersecurity, the need for domestic products	Evaluation of cost before quality as required by public procurement legislation
5	The penetration of technology into all areas of life and the increase in its use	Markets mostly dominated by foreign products
6	Willingness and will of the public and private sector to invest in cybersecurity	The questioning of defense expenditures, especially in the Western world
7	The rapid evolution of cyber threats	Export restrictions on the selling of cutting-edge cybersecurity technologies
8	The breadth of the domestic and foreign market	The widespread adoption of cloud computing and the dominance of foreign companies
9	Digital services' invasion into every facet of life via the internet (shopping, health, information sharing, etc.)	Establishment of a culture eager to make easy money
10	Deficiencies in the institutional establishment of cybersecurity systems	International competition

The second meeting was held at DIA facilities with the participation of 14 experts. This meeting focused on Delphi activities. Delphi study is a technique designed to bring the opinions of experts and non-experts closer to each other. Participants examined 37 capabilities previously written by the researcher and voiced suggestions for necessary changes. The participants were given a list of technologies that had previously been listed according to their importance, and they were asked to write down additional capabilities among them. During the meeting, 54 additional capabilities were proposed by the participants. In this way, a total of 91 cybersecurity capabilities were listed and prioritized by the experts.

Following the prioritization of the capabilities list by the experts in the working group, top 25 capabilities were selected for realization. Then, two-round Delphi survey was handled over the internet and in such a way as to reach the widest scale of experts in Turkey. In order to achieve maximum participation in the survey, the researcher obtained the e-mail addresses of faculty members in computer engineering departments at Turkish universities by accessing the official websites of the schools. To further expand the participation, the researcher gathered business cards from cybersecurity experts at events and conferences in Turkey. These experts, along with others who learned about the study, also provided the researcher with the contact information for additional participants. In total, 1,900 people were identified and contacted.

For the Delphi survey, forms containing 25 cybersecurity capabilities were prepared in Google Forms, and the survey link was sent to the participants across Turkey via e-mail. A total of 150 experts answered the first

round, and 91 of them answered the second round of the survey. The contribution of capabilities to the economy and contribution to security was scored between 1 and 5, and the time and methods of realization were also voted.

According to the results, a consensus was reached among the Delphi rounds; that is, the answers given in the first round and the answers given in the second round were close to each other. While the contribution of the determined cybersecurity capabilities to security varies between 4.3 and 4.9 points, their contribution to the economy varies between 3.9 and 4.6 points. As a result of this study, the prioritization of 25 capabilities, their scoring for their contribution to security and economy, and the time and methods of realization were obtained (Table 5). The highest rated cybersecurity capabilities are given below in the order of their priorities:

Table 5
Contribution Scores of Cybersecurity Capabilities per Delphi Round

Contribution	**First Round**	**Second Round**
Contribution to Security	4.3	4.9
Contribution to Economy	3.9	4.6

Capability-1: Protecting embedded systems from cyber attacks and running security tests on a wide range of integrated circuits.

Capability-2: Quantum-safe crypto hardware, software and algorithms together with supercomputers and quantum computers.

Capability-3: Cybersecurity technology and products addressing the cybersecurity of cyber-physical systems and ranking among the top 5 countries for global sales of such products.

Capability-4: Lightweight cryptography that is used in small smart devices and elements of the Internet of Things (IoT) and is penetrating the international markets.

Capability-5: Cybersecurity technologies for protecting aerial vehicles and ground systems, including air traffic control systems (flight control systems, air traffic networks, navigation systems, etc.).

Capability-6: Strong cyber offense and defense capabilities capable of competing with top-tier countries such as the United States, Russia, and China.

Capability-7: Dominating global markets with cybersecurity technologies addressing wireless devices and next-generation wireless communication technologies.

Capability-8: Authentication and authorization technologies depend on blockchain and a new generation of methods and techniques.

Capability-9: Being an international education and training center with extensive and cutting-edge cybersecurity testing, training and exercise systems.

Capability-10: International market dominance of cybersecurity products for cloud-based systems and virtual operating systems.

Capability-11: Extensive cyber threat intelligence collection capabilities with hardware, software and widespread infrastructure covering all around the world.

Capability-12: Cybersecurity tools, techniques and technologies for big data, data analytics systems and other database systems.

Capability-13: New generation of automated security testing and vulnerability management tools, techniques, and methods.

Capability-14: Techniques and products combined with artificial intelligence and emerging information technologies perform penetration testing.

Capability-15: Penetration into the international market with at least 5% market share with software-defined cybersecurity systems.

Capability-16: Tools and products for automated response to cyber incidents.

Capability-17: Tools and products for defending against Advanced Persistent Threats (APTs).

Capability-18: Systems, tools and techniques for defending against Distributed Denial of Service (DDoS) attacks.

Capability-19: Anomaly-based and behavior-based cybersecurity systems to protect systems from malicious software.

Capability-20: Intelligent cyber attack systems with automatic attack and hiding capabilities to prevent attribution.

Capability-21: Security systems for network protection (firewalls, guards, intrusion detection and prevention systems etc.) that can take automatic measures against cyber attacks and having products among the top 10 preferred brands globally.

Capability-22: Tools and techniques for Data Loss Prevention (DLP) and being among the top 10 in international markets.

Capability-23: Tools and techniques for cloud computing security.

Capability-24: Aerial systems (aircraft, helicopters, unmanned aerial vehicles, etc.) with cyber attack capabilities.

Capability-25: Smart intelligence devices and systems, including robots, with resiliency against cyber attacks and rapid recovery capability.

5.4. Status of Universities in Turkey in terms of Cybersecurity

A study was conducted to identify courses and programs related to cybersecurity in Turkish universities to reveal the status and situation of the universities. The study reflects the data for the fall semester of 2022.

In Turkey, 167 universities have departments of computer engineering, computer science, information engineering, software engineering, or artificial intelligence engineering. At the undergraduate level, there is a forensic information engineering department in a university and an information security technology department in a university specifically for cybersecurity. There are cybersecurity graduate programs in 26 universities and doctorate programs in three universities (Table 6).

Information security, cybersecurity, cryptography, network security, information systems security and data security courses are commonly offered in undergraduate and graduate programs of universities in Turkey.

5.5. Cybersecurity Companies in Turkey

The Turkish Cybersecurity Cluster platform was established in 2017 under the leadership of the DIA in order to create a cybersecurity ecosystem in Turkey and thus create synergy by supporting companies that can produce technology and products on a global scale (Turkish Cybersecurity Cluster, 2022). A protocol was signed between the DIA and the Presidential Digital Transformation Office in 2021, and it was decided to carry out the platform activities together (Presidential Digital Transformation Office, 2022).

Companies in Turkey have been analyzed in terms of producing cybersecurity products and providing cybersecurity services. In order to elicit the data, the web pages of approximately 3,000 companies were visited by the researcher.

As a result of the research, it has been determined that approximately half of the 169 technologies in the cybersecurity taxonomy applied by companies in Turkey do not have a relevant cybersecurity product. 220 companies that are members of the Cybersecurity Cluster offer products in 47 different categories and services and training in 31 categories. Most of the cybersecurity products produced are related to cybersecurity event management, network security, identity and access management, endpoint security, application security, data

security, web security, secure communication and cloud security. No product has been found that directly addresses technology groups for operating systems and container security, autonomous systems and smart platform security.

Common cybersecurity services include consultancy, network security, security audit and hardening, penetration testing and vulnerability analysis, system security, cyber incident response, and application security.

As of October 2022, there are a total of 94 technology development zones in Turkey (TGB, 2022). Cybersecurity companies exist in almost half of the 79 active zones.

Table 6
Cybersecurity Master (MS) and Doctorate (PhD) Programs in Turkey

No	University	Program	Degree
1	Adana Science and Tech. University	Cybersecurity	MS
2	Ahmet Yesevi University	Cybersecurity	MS
3	Antalya Bilim University	Cybersecurity	MS
4	Bahçeşehir University	Cybersecurity	MS
5	Bandırma University	Cybersecurity	MS
6	Düzce University	Cybersecurity	MS
7	Ege University	Information Technologies and Internet Security	MS
8	Fırat University	Forensics Engineering	MS/PhD
9	Gazi University	Information Security Engineering	MS/PhD
10	Gebze Technical University	Cybersecurity	MS
11	Hacettepe University	Information Security	MS
12	Işık University	Cybersecurity	MS
13	Istanbul Aydın University	Information Security	MS
14	Istanbul Commerce University	Cybersecurity	MS
15	Istanbul Technical University	Info. Security Engineering and Cryptography	MS
16	Kadir Has University	Cybersecurity	MS
17	Koç University	Cybersecurity	MS
18	KTO Karatay University	Forensics	MS
19	Marmara University	Cybersecurity	MS
20	National Defense University	Cybersecurity	MS
21	Middle East Technical University	Cybersecurity	MS
22	Sabancı University	Cybersecurity	MS/PhD
23	Sakarya University	Cybersecurity	MS
24	TOBB ETU	Cybersecurity	MS
25	Üsküdar University	Cybersecurity	MS
26	Yıldız Teknik University	Cybersecurity and Cryptography	MS

5.6. Scenarios and Roadmaps

Based on the analyses carried out, the action items to be taken were put forward together with the scenarios and road maps by the experts.

A total of four scenarios have been created on the two axes of "Turkey's Commitment and Situation" and "Global Security and Stability" (Figure 2). While "Turkey's Commitment and Situation" includes all the processes related to Turkey's desire to achieve its cybersecurity vision and the steps it has taken, the "Global Security and Stability" axis covers the difficulties and risks that Turkey will have to take while achieving its

cybersecurity goals. The scenarios are titled Locked in the Blue Ocean, Rising Cybersecurity Star, Hellish and Rise in the Mud.

A total of 91 cybersecurity capabilities (Delfi statements) were shared with the relevant scenarios according to the political and economic power and situation required to fulfill the capabilities covered in the statements, and a road map was set for each scenario. The roadmap that was developed for Scenario-1, which is the most desirable situation, is given in Figure 3.

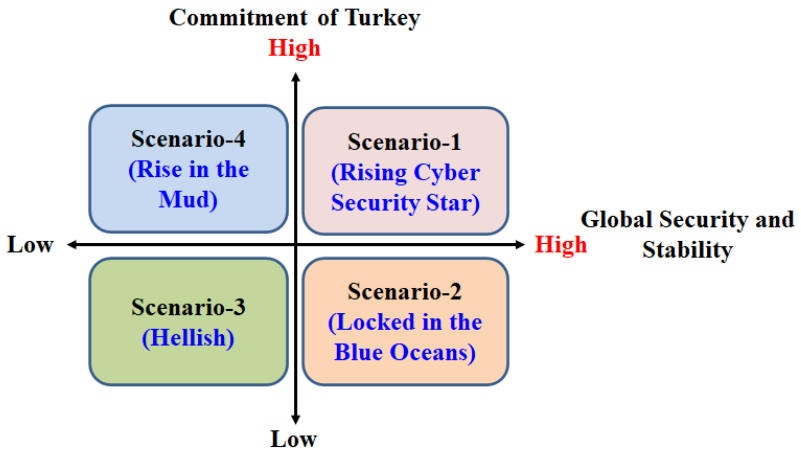


Figure 2. Possible Scenarios for Cybersecurity

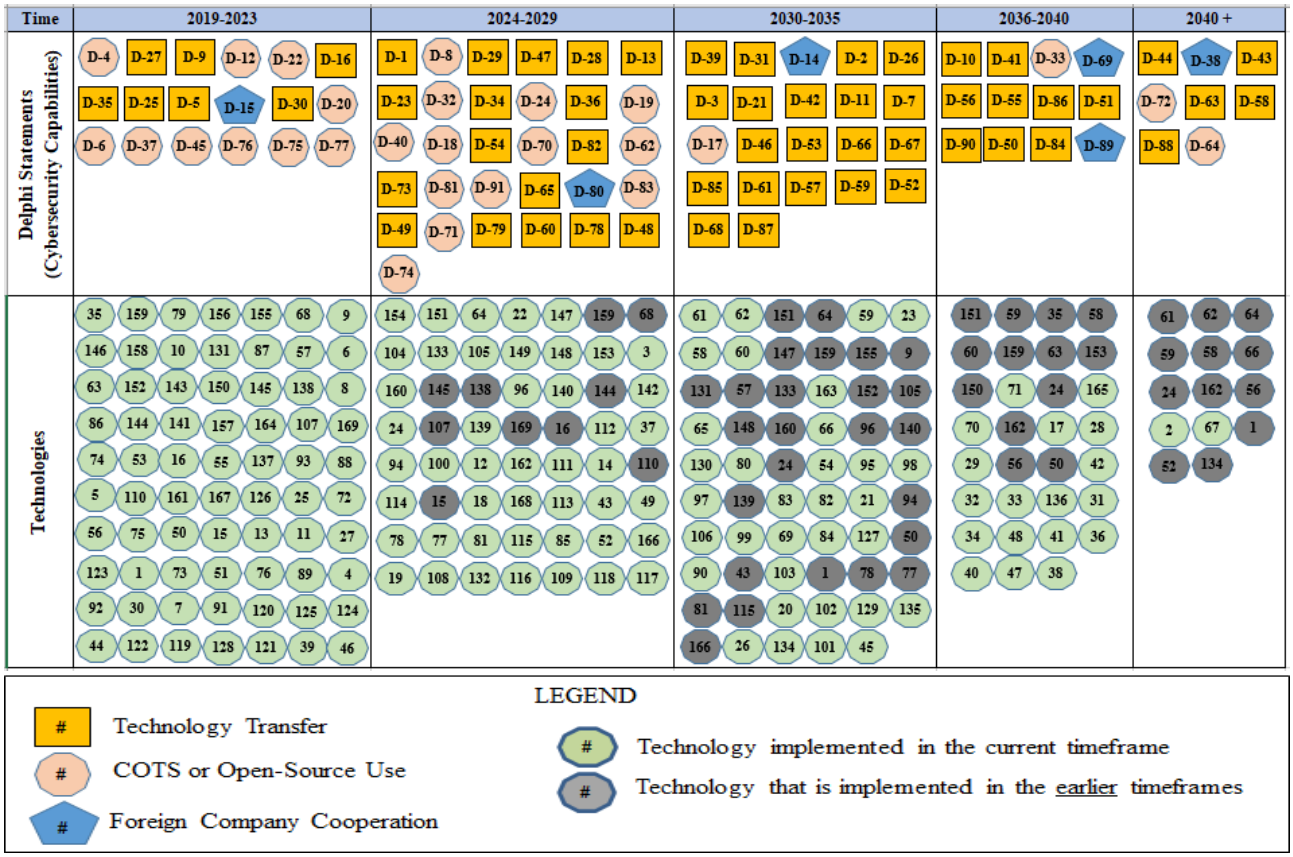


Figure 3. Roadmap for Scenario-1

The roadmap shows the cybersecurity capabilities with their implementation methods and underlying technologies. In the roadmap, which capabilities will be acquired between which years, and which technologies should

be invested in order to acquire these capabilities, are listed in order of priority (the expression and technologies at the top left).

5.7. Cybersecurity Action Items (Action Plan)

In addition to scenarios involving cybersecurity capabilities, action items for the development of cybersecurity in Turkey have been defined. A total of 50 action items have been put forward in order to overcome the weaknesses and threats in the field of cybersecurity and to benefit from the strengths and opportunities in cybersecurity. The first 20 action items are listed as follows:

Action-1: The turnover of cybersecurity companies should be increased by at least 20% within two years.

Action-2: The DIA and TÜBTAK should receive $10 million in annual funding for cybersecurity R&D initiatives.

Action-3: Companies producing cybersecurity products should be provided with incentives (funds, tax reduction, etc.) and credit opportunities as export support.

Action-4: Every year, five nations should be chosen in order to expand cybersecurity exports, and targeted research should be done to open up to those nations.

Action-5: Each year, cybersecurity firms should advertise their products at least one international trade show. Manufacturers should get $10,000 in financial support from the government budget for this reason.

Action-6: Financial support should be given based on the kind of patent in order to boost the number of patents in the cybersecurity industry.

Action-7: At least 10% more employees should be hired each year to work in the field of cybersecurity (at least about 500 people per year).

Action-8: Companies should be granted technological business funds to do research in areas where there are no manufacturers in order to extend the cybersecurity product catalog.

Action-9: All businesses engaged in the cybersecurity industry should participate in promotion and incentive programs to join the Turkish Cybersecurity Cluster.

Action-10: The IT departments of public institutions should hire at least two cybersecurity specialists.

Action-11: It is important to provide the political, social, legal, and economic conditions necessary to maintain a skilled workforce in the nation.

Action-12: The cybersecurity task allocation of the country's highest level organizations (Ministry of the Interior, Armed Forces, National Intelligence Organization, USOM, BTK, and so on) should be restructured.

Action-13: In the next five years, the proportion of R&D investments to GDP should be consistently raised to a minimum of 2%.

Action-14: Annually, five firms should be assisted in establishing an overseas unit in respected technology centers or other international business hubs.

Action-15: The state should fund the cybersecurity certification exam expenses for people working in cybersecurity and information processing in public institutions (those who successfully pass the exam).

Action-16: Cybersecurity personnel job descriptions and a workforce catalog should be developed, as should definitions of tasks to be completed and credentials to be gained.

Action-17: Every year, technology awards should be presented to organizations that are successful in cybersecurity technologies (based on criteria such as product exports, patents granted, etc.).

Action-18: Incentives and strategic plans should be put in place to found at least 10 cybersecurity companies in each technology park in order to triple the number of cybersecurity enterprises in the next five years.

Action-19: Certain facilities and systems should be required to employ approved national cybersecurity products.

Action-20: In 10 major cities, a cybersecurity technical high school should be established.

6. Conclusion

Foresight is a method used to shape the future rather than predict it. In this study, information about Turkey's cybersecurity foresight, which was prepared as a doctoral thesis at METU in 2019, is given with the updated version of the model used, and the outputs of the thesis are presented as a summary. According to the study's findings, Turkey needs to invest more in cybersecurity products, services, technologies, education and training, and research and experimental development to keep up with developed countries.

Turkish cybersecurity sector should invest in the development of tailored cybersecurity products and technologies that address the specific needs of the Turkish market. This could involve collaborating with local companies and research institutions to identify key areas of focus for innovative solutions. The sector could also consider collaborating with other countries with advanced cybersecurity capabilities to gain access to expertise and facilitate the exchange of knowledge and ideas.

To achieve a leading position in cybersecurity, it is essential to take determined action and make investments as outlined in the roadmaps. It is necessary to repeat the foresight studies according to the developing and changing political, social, economic and technological environment and to make adaptations and updates in the necessary areas. In this context, it is vital to regularly renew the cybersecurity technology foresight in this study, which was carried out with the widest participation in Turkey, and to evaluate the results of the implementations and make the necessary corrections and developments.

Author Contributions

Hasan Çifci: Graduated PhD student. Collected the data, performed the study and wrote the article.

Serhat Çakır: Thesis supervisor. Conceived the study and reviewed the article.

Conflicts of Interest

The authors declare no conflict of interest.

References

Bahuguna, A., Bisht, R. K., & Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*, *29*(5), 250–266. https://doi.org/10.1080/19393555.2020.1767239

Brandes, S. (2013). The Newest Warfighting Domain: Cyberspace. *Synesis*, 90–95. https://api.semanticscholar.org/CorpusID:55688987

Braue, D. (2021). *Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025*. https://cybersecurityventures.com/cybersecurity-spending-2021-2025

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

Çifci, H. (2017). *Her Yönüyle Siber Savaş* (2nd ed.). TÜBİTAK.

Çifci, H. (2019). *Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040* [Middle East Technical University]. http://etd.lib.metu.edu.tr/upload/12623200/index.pdf

Conway, M. (2014). *Foresight: an Introduction*. Thinking Futures. http://choo.ischool.utoronto.ca/fis/courses/inf1005/foresight.intro.conway.pdf

Cyber Security Council. (2016). *European Foresight Cyber Security Meeting*. https://www.ospi.es/export/sites/ospi/documents/European-Foresight-Cyber-Security-2016.pdf

ENISA. (2012). *National Cyber Security Strategies - Practical Guide on Development and Execution* (Issue December). https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

European Commission. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In *European Commission*. https://edps.europa.eu/data-protection/our-

work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en

Keenan, M., Miles, I., & Koi-Ova, J. (2003). *Handbook of Knowledge Society Foresight*. European Foundation for the Improvement of Living and Working Conditions. https://www.eurofound.europa.eu/publications/2003/handbook-of-knowledge-society-foresight

Martin, B. R. (1995). Foresight in science and technology. *Technology Analysis and Strategic Management*, *7*(2), 139–168. https://doi.org/10.1080/09537329508524202

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

Miles, I. (2002). Appraisal of Alternative Methods and Procedures for Producing Regional Foresight. In *Mobilising the regional foresight potential for an enlarged EU* (Issue May). https://www.researchgate.net/publication/235407634_Appraisal_of_Alternative_Methods_and_Procedures_for_Producing_Regional_Foresight

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2022). *Glossary: cyberspace*. https://csrc.nist.gov/glossary/term/cyberspace

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

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

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

Presidential Digital Transformation Office. (2022). *Siber Kümelenme Projesi*. https://cbddo.gov.tr/projeler/siber-kumelenme/

Rodrigues, B., Franco, M., Parangi, G., & Stiller, B. (2019). *SEConomy: A Framework for the Economic Assessment of Cybersecurity BT - Economics of Grids, Clouds, Systems, and Services* (K. Djemame, J. Altmann, J. Á. Bañares, O. Agmon Ben-Yehuda, & M. Naldi (eds.); pp. 154–166). Springer International Publishing. https://files.ifi.uzh.ch/CSG/staff/rodrigues/extern/publications/GECON-SEConomy.pdf

TGB. (2022). *Duyurular: Teknopark sayımız 94'e ulaştı*. https://teknopark.sanayi.gov.tr

The White House. (2015). *National Security Strategy*. 32. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

TÜBİTAK. (2004). Ulusal Bilim ve Teknoloji Politikaları - 2003-2023 Strateji Belgesi. In *Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi*. https://www.tubitak.gov.tr/tubitak_content_files/vizyon2023/Vizyon2023_Strateji_Belgesi.pdf

Turkish Cybersecurity Cluster. (2022). *About Us*. https://siberkume.org.tr/About

World Economic Forum. (2021). *The Global Risks Report 2021*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Yüksel, N. (2018). *A New Technology Foresight Model and Its Application in Turkish Defense Industry for Aerospace Communication Technologies of 2040* [Middle East Technical University]. http://etd.lib.metu.edu.tr/upload/12622819/index.pdf

Yüksel, N., & Çifci, H. (2017). A New Model for Technology Foresight : Foresight Periscope Model (FPM). *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 807–817. https://doi.org/10.1109/ICE.2017.8279967