COMPARISON OF CYBER SECURITY POLICIES OF TÜRKİYE AND ENGLAND

Gül Nazik ÜNVER[1]

ORCID: 0009-0005-5003-1555

Abstract

This study evaluates and presents a comparative analysis of all political, strategic, educational, legal, economic, social and organizational aspects of Türkiye and England, which implement cyber security policies. In this study, the analysis of cyber security strategies followed by Türkiye and England has been tried to be revealed. In this study, it is seen that cultural differences play an important role in the cyber field of developed states like England and developing states like Türkiye. Cyber security policies implemented in Türkiye and England adopt a more flexible approach. As a result of this research, it has been seen that these two countries attach importance to their economic and individual dimensions.

The study firstly claims that it is possible to analyze cyber security policies in five dimensions comparatively according to the Global Cyber Security Index (GCI) data and that cyber policies interact at an international level. Cyber security policies include important strategic issues related to security. Secondly, it shows how Türkiye and England design and implement their national cyber security policies, how they approach counter-strategies, and how they respond to increasing threats in the cyber space. In this context, thirdly, by comparing these two countries within various cyber security indices, it is discussed how the best cyber policies can be for countries in the cyber field. Finally, suggestions are made to guide future research on this subject.

Keywords: Cyber Space, Cyber Security, Cyber Security Policies, Cyber Security Indices.

TÜRKİYE VE İNGİLTERE ÜZERİNDEN SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRILMASI

Özet

[1] Dr., Batman University, E-mail: gul.unver@batman.edu.tr This study was produced from the author's PhD thesis. For Detailed Information: Ünver, Gül Nazik (2023). Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği, *PhD Thesis*, Konya: Selcuk University.

Bu çalışma, siber güvenlik politikaları uygulayan Türkiye ve İngiltere'nin politik, stratejik, eğitim, yasal, ekonomik, sosyal, organizasyonel tüm yönlerini değerlendirmekte ve karşılaştırmalı bir analizini sunmaktadır. Bu çalışmada, Türkiye ve İngiltere'nin izlemiş olduğu siber güvenlik stratejilerinin analizi ortaya konulmaya çalışılmıştır. İngiltere gibi gelişmiş ve Türkiye gibi gelişmekte olan devletlerin siber alanda kültürel farklılıkların önemli rolü olduğu bu çalışma da görülmektedir. Türkiye ve İngiltere'de uygulanan siber güvenlik politikaları daha esnek bir yaklaşımı benimsemektedir. Bunu özellikle bu iki ülkenin ekonomik ve bireysel boyutlarını önemsediği bu araştırma sonucunda görülmüştür.

Çalışma ilk olarak, Küresel Siber Güvenlik Endeksi (GCI) verilerine göre siber güvenlik politikalarını beş boyutta karşılaştırmalı olarak analiz etmenin mümkün olduğunu ve siber politikaların uluslararası düzeyde bir etkileşim içinde olduğunu iddia etmektedir. Siber güvenlik politikaları, güvenlikle ilgili önemli stratejik konuları içermektedir. İkinci olarak, Türkiye ve İngiltere'nin ulusal siber güvenlik politikalarını nasıl tasarladıklarını ve bu politikaları nasıl uyguladıklarını, karşı stratejilere nasıl yaklaştıklarını, siber alanda artan tehditlere nasıl yanıt verdiklerini göstermektedir. Bu kapsamda da üçüncü olarak, bu iki ülkenin çeşitli siber güvenlik endeksleri dâhilinde karşılaştırılmasıyla, siber alanda ülkeler için en iyi siber politikaların nasıl olabileceği tartışılmaktadır. Son olarak bu konuda bundan sonra yapılacak araştırmalara yol gösterici önerilerde bulunulmaktadır.
Anahtar Kelimeler: Siber Alan, Siber Güvenlik, Siber Güvenlik Politikaları, Siber Güvenlik Endeksleri.

Introduction

In this study, cyber security policies are discussed comparatively with the examples of Türkiye and England (in this paper, the United Kingdom is referred to as England). States have their own historical and unique conditions in the development of their cyber security policies. Moreover, it is clear that structural similarities cannot be ignored in this development process. With cyber security, it is possible to explain the evolution of traditional processes into innovative processes in the 20th and 21st centuries. It is inevitable that there are similarities and differences in the improvement of cyber security policies in Türkiye and England. According to the Global Cybersecurity Index, based on the measurement data of cyber security impacts in Europe, England is ranked 1st in the list, while Türkiye is ranked 11th (Global Cybersecurity Index, ITU, 2018: 60). It is seen that England is better than

Türkiye in terms of implementing strategies. England is more active than Türkiye in coordinating and implementing cyber security policies.

Türkiye focuses on preventing the damage to the technical and organizational structure of cyber incidents. England, on the other hand, focuses on cyberspace to prevent cyber incidents from attacking national critical information infrastructures and key network resources. From a cyber security perspective, Türkiye's priority is public and state security, while England's priority is individual security and human rights. In cyber security, Türkiye encourages public institutions and works on the awareness of increasing their standards.

Türkiye's strategy aims to help individuals understand the risks linked to their use of technology and be able to use it safely to meet future challenges related to inclusive changes in the digitization of Turkish society. The basis of the national strategy in England is education and international cooperation to promote the economy, citizens and national values. Türkiye's strategy is to ensure that critical infrastructures are resistant to cyber attacks. Türkiye's strategy intends to support and raise awareness of cyber security. Türkiye's cyber security principles are efficiency, resilience and foresight. England's principles are broad and some focus on protection, accountability and cooperation. Türkiye and England have openly expressed their current or future action plans to promote global cooperation.

It is recommended in the study that the countries that will prepare or update their cyber security strategy should have a holistic perspective, determine their priorities and focus more on the aspects of cyber security that are compatible with their national priorities. Another important point is the fact that opportunities are taken into account as well as threats and risks in cyberspace. It is hoped that this study will be a beneficial guide for researching cyber security policies and collaboration models in future studies.

In Türkiye, the Internet had an impact in the world of defence, research and academia in the early 1990s. The innovators and founders of the communication infrastructure that individuals and societies generally trust and the services provided through it are represented by the Information Technologies and Communications Authority (ITC) in Türkiye. The innovators and founders of the communication infrastructure that individuals and societies generally trust and the services provided through it are represented by the Internet Service Providers Association (ISPA) in England. This study examines the data, national strategic documents, cyber security indexes, institutions and organizations for cyber security and other studies

conducted in this field of the leading UN agency, ITU, so as to better understand cyber security in Türkiye and England.

This study is systematically grouped in dimensions developed by various international organizations (ITU Global Cyber Security Index) related to cyber security policies. Cyber security policies of Türkiye and England are compared and examined in five main dimensions. Based on the comparison results, various inferences were made about the cyber security policies of Türkiye and England. In addition, it is not known for certain whether the proposed inferences will yield results due to the security in the cyber space, the implementation of policies against cyber attacks, and the constant change in cyber crimes. Therefore, in the inferences to be made for Türkiye and England, the social, cultural and legal structure of both countries has been tried to be taken into account. This study examines and compares the cyber security policies of the Turkish and British governments in five dimensions in the light of the information given in the GCI. In the light of the data obtained, it can be argued that the findings have very important implications for policy makers, public institutions and private sector leaders.

The main research questions of this study are as follows:

What is meant by cyber security and cyber security policy for Türkiye and England?
What types of institutions are dealing with Cyber Security? What are their duties? How do they work?
What should be the basic elements of an effective cyber security dimensions?
How are the five categories of activities (policy and strategy; culture and society; education, training and skills; legal and regulatory frameworks; standards, organizations and technologies) examined according to the development model?

In the light of these questions, the cyber security policies of Türkiye and England have been comparatively examined through official policy documents and related literature. Through the national and international security dimension of cyber security, the studies of Türkiye and England on cyber security have been examined and detailed. The cyber security policy problems of the two countries are explained, the creation of a new framework is discussed, and the need for classification is emphasized. In addition, this study shows that cyber security policy is diverse and it is important to examine the Global Cybersecurity Index in five dimensions when comparing states.

The first dimension of comparison is policy and strategy. According to this title, it is evaluated what kind of duties fall on which institutions in the decisions to be taken by the government

in cyber security and cyber crimes, and the strategy documents made by the government are examined.

The second dimension of comparison is culture and society. In this title, it examines attitudes, knowledge, assumptions, norms and values of societies regarding cyber security in terms of culture and society.

The third dimension of comparison is education, training and skills. In this title, training activities and training exercises for the Turkish and British governments to ensure cyber security throughout the country are examined. It is important that the Turkish and British governments consider increasing the reliability of government services and online commercial services, and develop a feedback mechanism in order to handle private or personal data, and to ensure trust in e-government and e-commerce services. These measures should go hand in hand with an effort to promote understanding of cyberattack and cyber security and reliability in its services and technologies. In the study, it is emphasized that cyber security education should be expanded in many educational disciplines at all levels (if appropriate conditions are provided), beyond technical and computer science disciplines.

The fourth dimension of comparison is the legal and regulatory framework. The strategic plans and legal regulations put into practice by the Turkish and British governments in cyber security, both politically and legally, are emphasized.

The fifth dimension of comparison is standards, organizations and technologies. In this title, the scientific studies of the Turkish and British governments in cyber security and technological activities developed as a result of these studies are examined. Organization and cooperation studies are analyzed, and standardization studies for both countries' critical infrastructure facilities, emergency institutional and sectoral response teams, national response units and government institutions are also evaluated.

Cyber Security in Türkiye and England

Cyber security does not belong to a state, region or a particular social organization, but concerns every society or person who uses the network or is widely impressed by the network technic. The cyber security domain is concerned with the perceived cyber security threat by a particular subject. The global cyber security field express to the present situations and events interested in cyber that impress the security, steady and progress of countries around the world. The scope of cyber security can be wide or minimal, and threatening to cyber security

vary in severity. Actually, the field of cyber security is a subjective situation and is about discourse analysis. Whole actors in the cyber space have the capability to start attacks. There is no geographical notion in the network ambience (Ünver, 2017: 117). Therefore, attack capacity isn't restricted by geographic space. Threatenings to the network ambiance cannot be resolved rapidly and effectively. It is also unfeasible to effectively implement deterrent policies in the network environment. Cyber security also has some common features such as the unbalance of power structure, lack of institutes and norms, and inadequate reciprocal trust.

The iteration of the 2020 Global Cyber security Index is a scale where each column is weighted by 20 points. In a composite weighted index, every indicator, sub-indicator, and micro-indicator is appointed a weight based on their importance. Weight can have a important effect on eventual points, and different technics can form diverse rankings. Country scores are scale between 0 and 100. The cyber security capacity maturity model of the countries with 100 and close to 100 points is good and close to good.

In the 2020 Global Cybersecurity Index, Türkiye ranks "97.49 points" and "11. ranks" (Global Cybersecurity Index, ITU, 2018: 25). It is seen that England is better than Türkiye in terms of implementing strategies. England is more active than Türkiye in coordinating and implementing cyber security policies. Türkiye focuses on preventing the damage to the technical and organizational structure of cyber incidents. England, on the other hand, focuses on cyberspace to prevent cyber incidents from attacking national critical information infrastructures and key network resources. From a cyber security perspective, Türkiye's priority is public and state security, while England's priority is individual security and human rights. In cyber security, Türkiye encourages public institutions and works on the awareness of increasing their standards. The United States, which ranks first, has a score of 100 according to the 2020 Global Cyber Security Index. The last countries in the survey, Micronesia, Vatican City and Yemen, are in the 182nd place with 0 points.

Table 1: Türkiye and England in the Five Dimensions of the Cyber Security Capacity Maturity Model

Countries	Eventual Points	Legal Measures	Technical Measures	Organizational Measures	Capacity Building Measures	Collaborative Measures
Türkiye	97.5	20	19.54	17.96	20	20
England	99.54	20	19.54	20	20	20

Source: Global Cybersecurity Index, *ITU*, 2020: 127-128; Ünver, 2023: 115, 154-155.

When analyzed regionally, scores and rankings in global cyber security change. Accordingly, Türkiye's cyber security capacity maturity "overall score is 97.5" in Table 1, while its cyber security capacity maturity ranking is 6th among European countries (Global Cybersecurity Index, ITU, 2020: 30). England is ranked 1st with 99.54 points (Global Cybersecurity Index, ITU, 2020: 30). Accordingly, England received full marks (20) from four of the five dimensions, while Türkiye received full marks (20) from three dimensions. According to Table 1, it has been seen that England is more advanced than Türkiye in the cyber security capacity maturity model.

According to Table 1, Türkiye needs some improvements in organizational and technical measures. It is seen that Türkiye is very close to the ideal point, according to the study of the Global Cyber Security Index, as it has a score of twenty or close to twenty in terms of legal measures, cooperative measures and capacity building measures. England needs some improvements in technical measures. It is known to be in the ideal spot as it has twenty points in legal measures, cooperative measures, capacity building measures and organizational measures and nearly twenty in technical measures.

Strategic management is an important aspect of national security. The first step for a comprehensive analysis ought to be the country's cyber security strategy. Providing security in cyber space is an important strategic priority for cyber threats, cyber attacks, cyber wars. The study on the subject has been done at various levels about cyber security in Türkiye. Examples include the "Tunisia Report"[2] (WSIS, 2005) adopted at the World Information Society Summit and the "Ninth Development Plan of Türkiye"[3].

The transformation of Turkish society into an information society is the Ninth Development Plan of Türkiye covering the years 2007-2013. Providing public services in electronic environment brings great convenience to daily life. As a matter of fact, criminal organizations also benefit from information technology (Dokuzuncu Kalkınma Planı (2007- 2013) p. 53, article 323). After the Ninth Development Plan, two sections under the subject of "development axes of the program period" and "increasing the quality and efficiency in public

[2] The Tunisia Report draws attention to the following points; "Information sources and technologies are used for crime. Terrorism uses information technologies effectively." Therefore, misuse of information technologies should be prevented, but human rights should be taken into account while preventing abuse.

[3] In addition to the rule of law, development is defined with a multidimensional understanding that includes concepts such as economic growth, advancement in information and communication technologies, increased international competition, sustainable growth and human development. It is seen that growth and development efforts will continue with a holistic perspective that fits this definition. For detailed information. Dokuzuncu Kalkınma Planı (2007- 2013), Access date is 22.06.2023, [https://www.sbb.gov.tr/kalkinma-planlari/]. Promoting e-government applications is included in Dokuzuncu Kalkınma Plan (p. 51, article 314).

services" are the other steps taken towards cyber security (Official Gazette, Decision 2007/12300; Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Orta Vadeli Program (2012-2014)).

England presented its first national strategy, England Cyber Security Strategy, in 2009: "Security, Security and Resilience in Cyberspace" (Cabinet Office, June 2009). It then created a second strategy, England Cyber Security Strategy for the period 2011-2015: "Protecting and Promoting England in a Digital World" (Cabinet Office, 2011). In this context, the strategy, which points to a change in England's cyber security policy and strategies in 2016, has also created the current framework that indicates England's targets for national cyber security policy.

In the 2011 cyber security strategy document, England aimed to develop cyber security policies related to cybercrime, to be one of the safest countries and to protect the national critical infrastructure (Cabinet Office, *The UK Cyber Security Strategy,* 2011).

In England National Cyber Security Strategy Document covering the years 2016-2021, it aimed to be safer, more resilient, more stable against cyber risks and threats and to protect its interests in the cyber field. There are three broad objectives in the Strategy Document (England 2016-2021, "UK National Cyber Security Strategy"):

- The first is Defense; Defending England against emerging cyber threats
- Secondly, Deterrence: Tracking down and prosecuting criminals. By gaining the ability to understand, detect and investigate cyber attackers, it is to ensure that England is resilient against all kinds of aggression in the cyber space, and thus hold the criminals accountable.
- Third Development: Investments should be made in public/private institutions and organizations for sustainable development and skills protection. It should also encourage cyber security efforts to overcome future threats and challenges.

These comprehensive aims are supportive studies for international activities and cooperation. That's why international activities and partnerships are important to invest in cyberspace that aligns with England's security and economic interests. England's strategy document covering the years 2016-2021 aimed to simplify the approach to cyber security, thus encouraging national and international partnerships (Silfversten (et al.), 2020: 146-147).

Regular scenario and real-time cyber drills on cyber security are held in England. It has a mechanism to implement the national cyber security strategy, especially at the local level. Moreover, there is no mechanism yet to implement it fully. The UK Computer Emergency Response Teams (CERT-UK) maintain a national record of cyber incidents. Furthermore, central responsibility for incident response rests with the National Cyber Security Center (NCSC). It acts as part of the Government Communications Headquarters (GCHQ). It is the authority that monitors all incidents, ensures that they are reported, disseminates information, gives early warnings, makes cyber threat evaluations and ensures technic assistance to authorities. England Cybersecurity Information Sharing Partnership (CiSP), supported by CERT-UK, is still developing in the country and is expected to help support knowledge sharing between public/private institutions and organizations. More mechanisms are needed to build capacity, particularly to help Critical National Infrastructure (CNI) organizations strengthen their security posture and collaborate in the field that can strengthen England national security posture. In this context, it is necessary to give priority to national coordination among all institutions and organizations related to incident response and reporting at the national and international level in England, to create a draft regulation and develop the mechanism (Bada, 2016: 7-8).

Individuals become more conscious of cyber threats. Moreover, there is a difference between individuals' understanding of defense against cyber threats and users' routine practices on the Internet. Most of the users do not use the good applications of the internet very often in their daily life. Although it is known that there are many initiatives that are generally managed by the industry, it is natural to see that they have a limited impact on society as these initiatives do not target all groups of society. In addition, there has been a concern among experts and internet users about how the gap between cyber security concepts can be bridged and how this gap can affect applications. In general, experts have utopian expectations from the ordinary internet user. Institutions and organizations should work in coordination against cyber threats and attacks and increase awareness activities such as the "Cyber Essentials" (NCSC "Cyber Essentials: Requirements for IT Infrastructure": 1-17) program supported by the government and industry. Programmes and necessaries are presented existing to develop cyber security implementations (Bada, 2016: 10-11).

Presenting cyber security approaches as a comparative analysis and analyzing the five main elements over states can lead to a better understanding of cyber security policies. This understanding is given and analyzed in the following five titles in this study.

Policy and Strategy

Strategic plans are evaluated as a road map to reach the targets set in the national strategy. In addition to the strategic plans, official reports containing the subjects that form the basis of these plans are among the tools used by nations to ensure security in the cyber field. In this context, the following documents were published by the State Planning Organization along with the development process of Türkiye's National Cyber Security Strategy Document (Karabacak and Özkan, 2009):

- E-Türkiye Initiative Action Plan (2002),
- E-Transformation Türkiye Project Short-Term Action Plan (2003-2004),
- E-Transformation Türkiye Project 2005 Action Plan, Information Society Strategy (2006-2010),
- Information Society Strategy Action Plan (2006-2010),
- National Cyber Security Strategy and Action Plan (2013-2014),
- National Cyber Security Strategy and Action Plan (2016-2019) and
- National Cyber Security Strategy and Action Plan (2020-2023).

In this period, cyber security education and training were given as activity reports in many workshops, seminars, symposiums and lessons. The Information Society Strategy and Additional Action Plan, approved by the High Planning Council on July 11, 2006, was published in the Official Gazette on July 28, 2006 in its issue numbered 26242 (SPO, 2006-2010).

Cyber security issues have been given importance at the state level in Türkiye for more than twenty years, and official applications and actions have been tried to be initiated until 2003 with the "E-Transformation Turkey Project". The Telecommunication Union was established in Türkiye in 2000 and was transformed into the Information and Communication Technologies Authority (ICTA or BTK in Turkish) in 2008 (Bıçakçı, Ergun and Çelikpala, 2016: 26). Informatics and Information Security Advanced Technologies Research Center (BILGEM-Information Technolohies Institute) was established within TÜBİTAK. Cyber Security Institute (CSI/SGE), which was opened in 2012 within BILGEM, continues its activities today. "National Cyber Security Policy" is another official document. This document was prepared in 2008 with the cooperation of nineteen state institutions and presented to the Prime Ministry in 2009 ("E-dönüşüm Türkiye").

"Cyber Security Strategy Workshop" was made on 16 June 2012 in Ankara with initiatives of the Information Security Association. In this context, the association's members arranged a outline document. Then, the members of the association shared the document with public/private institutions and organizations. This document has been updated in a workshop with upward of eighty IT security proficients. The revised text has been submitted to the Ministry of Transport, Maritime Affairs and Communications. Expressed here is the National Cyber Security Strategy and Action Plan;

- Detailed analysis of the information technology infrastructure of public institutions and organizations in order to ensure the security of all kinds of services, processes and data,
- Improving the security of information systems used by the public or private sector as a result of the analysis,
- Determining the infrastructure that will keep cyber risks and threats at a low level, quickly establishing cyber security response responses in case of threats and ensuring the safe operation of the system,
- It can enable the competent authorities to carry out effective investigations.

The most prominent and important steps regarding cyber security are National Cyber Security Strategy and Action Plan 2013-2014, National Cyber Security Strategy and Action Plan 2016-2019 and National Cyber Security Strategy and Action Plan 2020-2023. The said strategy and action plans; It has been by organizing conferences, seminars, workshops and meetings with experts from corporations and organizations representing public corporations, ICT sector, universities, critical infrastructure operatives and non-governmental organizations. Collaboration and consensus from a range of stakeholders is required to appropriately develop the strategy and action plan. The Tunisia report, the Ninth Development Plan and the Medium Term Program (2012-2014), as an example, shows that the issue of cyber security is considered as an important area both nationally and internationally.

TÜBİTAK designed a project called "Vizyon 2023" to determine new technology and science policies containing the years 2003-2023. In this scope aimed to identify strategic technologies and priority research and development spaces (TÜBİTAK, "National Science and Technology Policies 2003-2023 Strategy Document", 2004).

Cyberspace and England National Security provides an overview of the cyber security issue. Society is becoming more and more dependent on information and communication

technology in every field. With addiction comes vulnerability to exposure and abuse, crime and even attack. Criminals and extremists can take advantage of the same global technological partnerships that society has become so dependent on. Even though cyber security is a system that requires a coordinated, capable and mutually reinforcing response from all who benefit from the global information and communication technology infrastructure, it also brings with it a rapidly evolving and complex security challenge. England, which has given importance cyber policy researches since the 1990s, published England cyber-related foresight program in 1994 to support policy and planning (Schmidt, 2015: 489-511).

England government's foresight work on cyber affairs is carried out by a central government agency that reports directly to the cabinet. England Department of Defense realizes prescience events under the "Development, Concepts and Doctrine Center" and the "Defense Science and Technology Laboratory" (Cabinet Office, 2011; Çiftçi, 2019: 48).

Cyber Trust and Crime Prevention Project was carried out in 2004 under the Ministry of Interior Ministry of Crime Reduction, Policing, Community Security and Anti-Terrorism with the participation of scientists and a total of 260 experts from various sectors. The goal of the project is to conduct research on future technologies, establish cyber trust and create actions to prevent cybercrime (Ünver, 2023: 162).

In the report of Digital Britain (UK Government, 2009) issued by England, it has been stated that the British society needs the services and information provided in the cyber space(United Kingdom Cabinet Office, 2009a). In June 2009, the British government wanted to achieve the goal of "becoming one of the leading digital information economies in the world" and published its first strategy document in this context in the same year. With the national strategy document, the British government wanted to provide cyber security and benefit from the occasions provided by the cyber space (United Kingdom Cabinet Office, 2009a).

While listing the actors that could threaten (unstable countries, transnational organized crime, international conflicts and natural disasters) national security in England strategy document, it also listed the areas that could threaten (public opinion, nuclear weapons, cyber space, culture, knowledge) it (UK Cabinet Office, 2009b). In its 2009 cyber security strategy, the British government highlights four objectives. These purposes are:

- To make England one of the safest countries, to prevent cybercrime and to do business in the cyberspace,

- Being resistant to cyber threats and attacks and protecting the country's interests,
- Creating an open, stable, robust and secure cyberspace for the British public,
- To have the knowledge, skills and capacity to achieve cyber security goals.

England has a comprehensive cyber security strategy. This strategy is finished by a robust cyber security legitimate framework and two CERTs. United Kingdom Computer Emergency Response Teams (CERT-UK) mainly support critical infrastructure operators, whereas GovCertUK supports government institutions. Other concerned institutions add the Cyber Security and Information Assurance Department and the National Security Council. England also has a well-developed public/private partnership system. This co-conspirator approach is also strongly promoted by the cyber security strategy. For example, the Center for the Protection of National Infrastructure (CPNI) provides industry-specific information exchange across the industry ("EU Cybersecurity Dashboard A Path to a Secure European Cyberspace", 2015). The existence of such centers is a reference for countries that want to make progress in the area of cyber security.

The strategy includes a strong statement of principles and an assessment of cyber security threats facing England. The implementation plan included in the strategy is based on the basic set targets. CPNI is tasked with protecting England's critical infrastructure. CPNI's central document is the Strategic Framework and Policy Statement on Increasing the Resilience of Critical Infrastructure to Natural Hazards, adopted in 2010 (Cabinet Office, 2010: 8).

Cyber security policy and strategy in England is crucial to promoting a cybersecurity agenda across government. Because prioritizing cyber security over other key policy areas, it is important to disseminate and fundamentally analyze a state-wide cyber security agenda, as it determines the mandate of key cyber security state actors and resources help address existing cyber security issues as they arise. Some organizations in England have a cyber security responsibility that can be largely structured around three principles (Silfversten (et al.), 2020: 147):

- Developing and implementing policy coordination under the Cabinet Office;
- National security subordinate to the Government Communications Headquarters (GCHQ);
- Cyber defense managed by the Ministry of Intelligence and Defense.

In the 2016-2021 National Cyber Security Strategy, England National Cyber Security Center (NCSC) is specified as the authority with the main cyber security responsibility (England

NCSS (2016-2021)). NCSC is the organization responsible for monitoring and responding to cyber incidents, sharing information and preventing vulnerabilities (Mali, 2016: 5).

There is a review and renewal process for England National Cyber Security Strategy Paper. But this renewal process, is not on an annual basis. The National Cyber Security Center (NCSC) was established in 2017 as part of GCHQ's national authority on cybersecurity. Accordingly, information participating, handling systemic security vulnerabilities and ensuring leadership on national cyber security subjects were among the important elements. The British government in the "UK National Cybersecurity Strategy Document" covering the years 2022-2030 (Cabinet Office, 2022):

- Understanding threats,
- Making and enforcing laws,
- It is stated to be in a unique position to gather the intelligence necessary to counter threats from hostile actors, including setting national standards and conducting offensive cyber operations. The government has emphasized that it will invest in strengthening national cyber capabilities through this strategy.

In England, government departments and public sector organizations are responsible for maintaining their networks and systems. Because the government is the service provider of important data, it takes strict measures to protect information and assets. Additionally, the government has an major liability to recommend and inform citizens, businesses and organizations about what they should do to protect themselves online. Most areas of cyber policy and most of the measures outlined in this strategy relate to issues such as national security, foreign relations and defence, telecommunications, product standards and safety, consumer protection (Cabinet Office, 2022).

Culture and Society

Cyber security culture expresses the attitudes, knowledge, assumptions, norms and values of corporate employees in Turkey regarding cyber security. A good cyber security culture is one in which the organizational determinants of culture (policy, lead, course, social norms, etc.) and the individual determinants of culture (manners, information, assumptions, etc.) are consistent with the organization's approach to cyber security as manifested in cyber security behaviors.

The sum of symbols, habits, rules, artifacts and other social abilities are the characteristics of human culture in Türkiye. In Türkiye, cultural information in cyberspace is coded for sign systems. Thoughts and concepts expressed in these systems are separated from the individual and gain an independent, impersonal existence. Through culture, civilizations can document and create their histories for generations. It has been about the symbolic elements of culture and the way these symbols give socio-historical meanings. Culture in Türkiye refers to various forms of knowledge, beliefs and ethical codes that reinforce a society. Many elements such as positive and negative slogans and actions, expressing thoughts with symbols and shapes, revealing traditional knowledge, religious discourses, rules, partisanship and the like fall into the subject of culture and society.

The United Nations General Assembly in 2003 determined a decision to create a global cyber security culture (UNGA, 2003; UNGA, 2018). Public/private institutions and organizations that use, develop, provide and manage information systems have carried out studies to increase the cyber security culture for users in the application and use of information technologies. The global understanding on cyber security culture reflects the universality of approach, its institutionalism, wide scope of domestic and transnational levels of cyber security.

The activities, programs and projects specified in the cyber security policies subserve a mutual purpose to provide national cyber security. Reaching this, cultural bond, social structure, great harmony and cooperation requires. In particular, international cooperation is needed to protect critical infrastructures against cyber attacks. To give an instance of national collaboration, draft plan against spam e-mail was carried out by ICTA in 2009 with the participation of many public/private institutions. As a result of draft plan, the number of IP addresses forwarding spam mails decreased by 99 percent and the total number of daily spam mails decreased from 6.5 billion to 394 million (Ulaşoğlu (et al.), 2010: 34). In order to establish cyber security in Türkiye, it is necessary to form a national cyber security culture, raise awareness in society about this issue.

Seventy-eight percent of England population in 2013 told they used the internet. Is this percentage of internet users in England an indication that the common internet culture has increased? or Is this percentage due to the diversity of beliefs, attitudes and opinions about the internet among British people? According to 2013 OxIS research survey data, most of the British population gave similar answers to questions about internet attitudes, beliefs and

opinions. In the light of the answers given, he showed that it can be divided into five characteristics or cultures and that each culture can have its own characteristics. These are defined as follows (Ünver, 2023: 170-171; Dutton, 2013: 4):

- E-Mersives; This user group has connect to internet as piece of their daily life and work. They made up just twelve percent of internet users in England.
- Techno-pragmatists; Focusing on using internet to make their lives easier and save time, this group of users, they accounted for around seventeen percent of England users. Compared to e-mersives group, this group does not just use the internet for fun and they do not see internet as a place of escape.
- Cyber savvy (knowledge of computers or the internet; technologically savvy); This group of users stated that they have some ambivalent views, mixed feelings and beliefs about internet. This user group thinks that they will lose control (anxiety of taking away from time and privacy) as opposed to feeling in control. Only nineteen percent of the British population is in this group.
- Cyber moderates; This user group sees internet as a good place to spend time, obtain information and continue social relations. In this context, they display a moderate approach in their attitudes, beliefs and views about internet. They make up thirty-seven percent of the British population.
- A-digital; This user group claims that internet is audited by others, likely beyond their control. This digital culture covers around fourteen percent of England's online population.

Education, Training and Skills

The main indicator that ensures the implementation of strategic plans related to cyber security to certain programs and national projects is Cyber Security Programs. Training programs for education and skills, informative academic events, cyber security exercises, research and development projects, risk management, critical infrastructure preservation programs, workshop meetings are some of the subjects that can be evaluated within this scope.

According to the Information Society Strategy Fifth Action Plan, cyber security trainings were given in Türkiye. Online trainings such as TR-BOME user awareness training, training on CERT installation and function, system analysis, CIRT training were provided. In addition, technical articles on cyber security, information security documents and guidance documents within the scope of standards and organizations are published within the extent of the

National Information Security Gate Project on (https://bilgiguvenligi.org.tr/) website. There are also free programs on information security and experiences on the website (http://www.CEHTurkiye.com), an online bookcase and administered by ethical hackers (Burlu (vd.) Certified Ethical Hacker).

The first CERT exercise, which was held within the scope of cyber security in Türkiye on 20-21 November 2008, started with the participation of eight public institutions. On February 23, 2010, the first security awareness day was organized to increase public awareness of cyber security. On 25-28 January 2011, the second CERT exercise was done under the title of Information Systems Security Exercise. In this context, it was realized with the attendance of forty-one public/private institutions from various sectors such as economy and finance, education, communication, and ensuring internal security. With this exercise, a booklet providing useful information about using information systems safely has been published by the Turkish government.

In Türkiye, conferences and symposiums are held within the scope of cyber security. The International Information Security and Cryptology (ISC) Conference has been going on since 2008. The ISC, which is held annually, held its fifteenth organization on 19-20 October 2022. All of the presentations and articles presented at the conference are issued on the web address (http://www.iscturkey.org) (ISC Turkey). More examples that started in Türkiye were the Public Institutions Information Technologies Security Conference in 2011 (sixth panel), the National Cyber Security Workshop in September, the Cyber Security Conference in December and the Cyber Security Law Workshop in 2012 (Ünver, 2023: 133).

The 2006-2010 Information Society Strategy and Action Plan was published in the Official Gazette dated 28 July 2006. With this action plan, it was mentioned that there is a five-year reference document in the field of cyber security since 2010 and that it should shed light on future studies. “Cyber Security Board” was founded in Türkiye with the decision of the Council of Ministers dated 11 June 2012 in the Official Gazette (Official Gazette, 20.09.2012). It was decided to prepare a national cyber security strategy and action plan with Cyber Security Board. This decision is the most effective step taken in the scope of cyber security. With the relevant document, it is recommended that universities train cyber security experts so as to maintain cyber security.

The 2015-2018 Information Society Strategy and Action Plan was issued in the Official Gazette (Official Gazette, 06. 03.2015). This document, seen as an umbrella, covered the

issues of both the 2016-2019 National Cyber Security Strategy and Action Plan and the 2016-2019 National e-Government Strategy and Action Plan. In the 2015-2018 Action Plan, education, training and skills are mentioned under the sub-title of "Information Security and User Trust". Accordingly;

- To carry out training activities in order to increase qualified human resources and to raise awareness about safe internet use in the society,
- To provide cooperation between institutions and organizations and to provide cyber security trainings,
- It envisaged the rapid determination of minimum standards in the scope of cyber security with the provision of the legal infrastructure.

In 2020-2023 the National Strategy Document and Action Plan, it is stated that a "National Cybercrime Strategy" will be prepared to combat cybercrime. Information regarding the establishment of specialized courts for cybercrimes is included in this Action Plan (Ministry of Justice, 2021). In order to provide cyber security in Türkiye, it is important to establish the legal infrastructure, to establish courts, to train experts in this field and to carry out training activities.

"Cybercrime and Internet Security, Cyberbullying, Social Networks, Cyberspace Awareness, Cyber Attacks, etc." education is given to students at primary and high school level. Many postgraduate programs such as cyber security, cyber field studies, information security have been started in many universities in Türkiye. In these fields, it has been decided by Council of Higher Education (CoHe or YÖK) to grant scholarships to some of the students who will do master's and doctorate in Türkiye, and a commission has been established for this. TÜBİTAK organizes summer camps and inter-university cyber security competitions within the scope of cyber security. Students who are successful in the competitions are given job opportunities at USOM. Research and development studies, master's and doctoral thesis studies are carried out at the national and international level. In addition, products/methods are developed, current publications are made, and workshops/conferences are organized.

In England, various government stakeholders and the private sector are examining the availability and quality of cyber security education, training and skills to raise awareness. The development of cyber security education in England and efforts to raise awareness of education and training in the public and private sectors are important. In the dimension of education, training and skills, England implements high cyber security education and training

in the private sector, public institutions and organizations, schools and universities in order to provide information security and cyber security.

Cyber Champions is a non-profit organization created to promote best practices in digital literacy and online safety awareness to England schools, youth organizations and interest groups. ("Cyber Champions", [https://www.cyberchampions.org/]). The program is supported by networks of Cyber Champions, young professional volunteers, and a growing number of private and public sector organizations that encourage their local communities to make a difference and increase the skills of future generations. England Cybersecurity Challenges create learning and development opportunities that raise awareness of cyber security as a rewarding career and encourage more people to join the profession ("Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/]).

England strategy addresses the skills gap through various levels of education and training, including incorporating cyber security skills into the education system, balancing the gender gap in cyber-related occupations, providing education and training programs for 14-18 year olds, among other initiatives. England Department of Education has invested in promoting computing skills in schools. This will provide a better understanding of the subject area.

Public and private sector education cooperates. It adapts to the ever changing environment because it tries to build on skill sets in both sectors. In addition, the government establishes partnerships with other sectors and funds activities to train law enforcement. There is a difference between education and skills. While there are specialist staff trained in cyber security skills, this staff is too small to adequately meet the needs of British society. As a result, there is currently a perceived skill shortage that highlights the need to combine education and practical training ("Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/]). Therefore, more investment in cyber security and skills development programs is required.

The internet and the digital education and communication built on it are helping to bring great benefits to England and its educational activities. Moreover, both criminal and state-run malicious actors continue to actively exploit vulnerabilities in England's cyber defenses. The risk of intentional or accidental cyber incidents is multiplying in threats due to the increasingly interconnected networks, systems and devices used by organizations and individuals, and the increasing use of digital services.

Organizations, and especially educational organizations, need to take steps to reduce their cyber risks. Although the Cyber Awareness training campaign has been successful in England, it has not yet reached enough institutions and people. The British government needs to do more and increase this reach to understand why advice and guidance is not reaching enough audiences. In its National Strategy Document published in June 2022, England highlighted the importance of strengthening the structures, partnerships and networks necessary to support the cyber society approach (Cabinet Office, 2022).

Legal and Regulatory Frameworks

The Law No. 2012/3842, which was published in the Official Gazette on 20 October 2012 and entered into force, determined the duties to be carried out by the responsible institution affiliated to the Ministry of Transport, Maritime Affairs and Communications regarding the practice, management and coordination of national cyber security activities (Official Gazette, Decision Number 2012/3842). The resolution also creates the National Cyber Security Board.

The "Electronic Communications Law" No. 5809 assigns the Information Technologies and Communication Institute responsibilities including the following items (Official Gazette, "Electronic Communication Law No. 5809"): "To protect the confidentiality of information security and communication", "To provide a counter system against unauthorized access", "to take the measures ordered by legal regulations for the implementation of national security in the service quality and electronic communication sector, public order and services". The duty of taking the necessary measures stipulated by the regulations is carried out by the Turkish National Information Technologies and Communications Authority.

Türkiye does not have specific legislation that addresses cyber threats to critical infrastructure. In this context, special regulations for sectors are encouraged to protect critical infrastructure in various sectors such as fiscal services. Moreover, it is obligatory to use the ISO/IEC 27001 standard for organizations providing infrastructure and energy facilities, electronic networks, and electronic communication services. Furthermore, in the banking sector, the Communiqué requires the use of two-factor authentication process for data protection and requires risk analysis to be carried out by the relevant unit of the bank. In accordance with the legislation, providing cyber security education should also turn into mandatory (Turkish Standards Institute, "ISO/IEC 27001 Personal Data Protection Law & ISO 27701 Personal Data Management System").

The Turkish Penal Code criminalizes accessing or recording phone calls or interfering with and opening private mail (Turkish Penal Code, Protection of Personal Data TCK No. 5237, Articles 135 and 136). While this should cover electronic communication in principle, there are no clear provisions on this subject in the legislation. In addition, it is generally accepted that the privacy of electronic communications is also maintained. This is hoped to be explicitly ensured under the recent cyber security law.

The Legal and Regulatory Frameworks related to cybersecurity in England have been updated to better reflect material law. Based on the recommendations of the Telecommunications Development Bureau Management Advisory Group, in GCI, procedural law is no more measured. Instead greater aperture is stressed in various areas, online harassment, including identity theft, racialism, xenophobia. International experience confirms the important role that legal and regulatory frameworks play in promoting cyber security across industries, while providing prevention, mitigation and conflict mechanisms to individuals and organizations affected by cyber threats. This dimension places a special emphasis on the British government's ICT security issues. It also examines the capacity to design and enact national legislation and accompanying regulations directly and indirectly related to cyber security.

In 1990, the first legal regulation for computer crimes was the Computer Misuse Act, which was enacted by England government. Situations related to many crimes such as computer software, unauthorized access or entry of data, unauthorized access to computer are considered crimes within the scope of this legislation. England Data Protection Act was enacted in 1998. It published its first cyber security strategy document in 2009 by order of the Queen of England. Subsequently, the Cyber Security Office was established.

In 2010, she worked on the review of strategy and defense in the cyber field, which will cover the five-year period. The Cyber Crime Strategy has been published to document these studies. In 2011, England published a new strategy document to keep up with the digitalizing age and move the kingdom to this cyberspace. With the Defense Strategy Document, it was planned to work in the military field and it was aimed to establish two main centers. These centers are the Security Control Center for Global Operations and the Cyber Operations Working Group. Then, England published the progress report on the objectives given in the cyber security strategy document in 2012, the National Cyber Security Strategy Paper in 2013 (future plans and achievements), and the National Cyber Security Strategy Paper (progress and

development plans) in 2014. In 2015, England published the study "Government Policy from 2010 to 2015: Cyber Security".

The Crown Prosecution Service (CPS) developed the 2013-2014 CPS security and information risk management policy. This policy aims to integrate information risk management into existing business and project risk as much as possible. Certain threats are managed through an ISO 27001 assurance program ("Audit and Risk Committee Minutes", 11.2020).

The National Crime Agency (NCA) continues to lead and coordinate England's fight against cybercrime, working closely with various local and international cyber security partners (NCA, 2017). Comprehensive ICT security has been implemented in England. In this regard, legislation on rights in the digital field has been adopted, and steps have been taken to protect the British people, public/private institutions and organizations. There are distinct legal initiatives regarding cybercrime.

Improvements in cyber risk management have been achieved through advice and guidance from the National Cyber Security Center and implementation of the General Data Protection Regulation, the Network and Information Systems Regulation 2018 and the Data Protection Act 2018. With the Covid-19 outbreak, the use and dependence of digital services used to meet basic corporate needs such as information storage, shared communication and security in England has increased across the entire economy and society. This has brought significant benefits to England. But it has also increased the scope of cyber risks to organizations and the broader economy.

ICT security legislation, with significant limitations in comparison, is advanced as universal ICT security legal and regulatory frameworks addressing cyber security have been performed and legislation has been adopted in England protecting the rights of individuals and organizations in the digital medium. For Türkiye, this legislation can be used with some revisions on a micro scale and if it is brought to a sustainable structure, it will bring important inclusiveness towards human rights and freedoms. A detailed section exists within the criminal justice system to struggle computer related crime on human rights. In this regard, work continues with international organizations on confidentiality and data preservation, and draft legislation is updated. In England, it has ratified international treaties such as the Human Rights Act and other treaties to adopt appropriate legislation to combat crimes against confidentiality and data preservation, facilitating their detection, inquiry and proceedings

(Bada, 2016: 44-45). In this regard, Türkiye needs to be able to follow legal agreements in accordance with the general structure regarding the relevant legislation.

Cyber security threats are not limited to damaging computer systems. Threats can also damage a country's computer systems, communications and communications systems, and critical infrastructure systems such as energy, transportation, military command and control. Cyber threats can emerge as a type of asymmetric warfare. For this reason, the idea that cyber threats are one of the important threats has begun to be accepted by world leaders. Therefore, it can be said that the approaches of nations to cyber security are far ahead of information security. The concept of cyber security has been defined by ITU as a set of measures to be taken against cyber attacks. Countries should produce and develop tools, policies and practices especially to protect the assets and values of the private sector, institutions, organizations and individuals (ITU-T Recommendation, 2018: 8-12).

Standards, Organizations and Technologies

Since Türkiye is a member of the International Organization for Standardization (ISO), the requirements specified in the ISO/IEC 27001 standard in the field of data security should be complied with. ISO/IEC 27001 is a mutual standard that is also valid and obligatory in Turkish law for organizations providing electronic networks, infrastructure and energy facilities and electronic communication services (Turkish Standards Institute, ISO/IEC 27001). Since Türkiye is a member of ISO, it is necessary to comply with the conditions specified in the ISO/IEC 27001 standard in the field of data security.

The government has published various strategies and development plans to ensure cybersecurity and improve information technology in terms of standards, organizations and technologies in many sectors. Due to the increasing trend towards digitalization in Turkey, Turkish public/private institutions and organizations have started to use digital platforms to ensure confidentiality, integrity and accessibility. The electronic apostille services supplied by the Post, Telegraph and Telephone Institution can be one of the most new instances in this context ("Elektronik Apostil Sistemi", 2018).

The Turkish government encourages public institutions to improve cyber security and works to increase cyber security standards and awareness. In this direction, under the leadership of the Presidency of Defense Industries, "Türkiye Siber Güvenlik Kümelenmesi" was

established with the additive of all public/private institutions and organizations, academia to develop the Turkish cyber security ecosystem ("Türkiye Siber Güvenlik Kümelenmesi").

TÜBİTAK was the institution responsible for cyber security in Türkiye until 2012. The Ministry of Transport, Maritime Affairs and Communications became the responsible authority, published in the Official Gazette of the Council of Ministers Decision No 2012/3842 on 20 October 2012. The decision also consists of the memberships of the Ministries of Foreign Affairs and Foreign Affairs, as well as the National Cyber Security Council, Ministry of Interior and Defense, National Intelligence Organization, General Staff, Public Order and the Telecommunications and Communications Commission, Security, Financial Crimes Investigation Board, TÜBİTAK, ICTA and other undersecretaries and senior managers deemed necessary by the Ministry.

There are two accredited CERTs as the State-run Türkiye Computer Incidents Response Team Coordination Center (TR-BOME), and the Computer Security Incident Response Team (ULAK-CSIRT) owned by TÜBİTAK, which is operated for research and education purposes (Official Gazette, 20.10.2012). TR-BOME also operates in the international arena (TR-BOME KM (Ed. Mehmet Eriş): 118). TR-BOME represented Türkiye in the "International Cyber Defense Workshop, Fall 09- ICDW09" exercise and the 2009 NATO Cyber Coalition Exercise. CERT coordination center in Türkiye, established within the scope of National Information Systems Security Programs, helps private/public institutions and organizations acquire the ability to reply to computer events in the scope of security.

Cyber Shield Exercises were organized by ICTA in 2012, 2013, 2014, 2019 and 2022 so as to develop international cooperation, improve response capabilities against cyber attacks, inter-agency and international cooperation, increase the capacity in the field of cyber security, to improve internal, ensure coordination and raise awareness on this issue.

In general, more strategies, plans and projects need to be prepared for the cyber security ecosystem in Türkiye, especially in the public and banking sectors, than in critical private sectors such as telecommunications, energy and health. In addition, Turkish public authorities dealing with cyber security issues need to be very open to receiving feedback from market players and involving them in shaping new regulations. In this area, it is important to contact regulatory authorities as soon as possible during the transaction process, communicate their needs to them, and supply feedback on proposed regulations. Türkiye's commitment encompasses all the driving forces involved in Türkiye's desire, determination and real steps

to achieve its cyber security vision. It is stated in the action plan that cyber threats can adversely affect all sectors including communication, transportation, energy, banking, finance and health. For this reason, it is important to speed up the measures to combat the increasing threats in cyberspace.

ICT development and use can be successful in a security environment. Therefore, countries are required to establish and establish accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be complemented by the implementation of a national body dealing with cyber incidents, a competent government agency, and a national framework for monitoring, alerting and responding to incidents.

In England, the focal point and official reports are a key indicator of analyzing whether the country has established the organizational structures necessary for national cyber security. The determination of a single central authority to be responsible for national cyber security is one of the important issues for England. England should regulate all its efforts and activities in institutions and organizations with cyber security duties such as strategies, standards, critical infrastructures, accreditation, control, agreement, protection and defence.

Within the scope of this study, the examples of Türkiye and England were analyzed in depth based on five predetermined dimensions. In this analysis, political and strategic approaches to cyber security were taken into account. The two states in question have tried to create an effective cyber defense and attack capacity in order to develop their political, economic and military capacities within the scope of network technologies in the short and medium term. It has been observed that the official cyber security strategy documents and doctrines, which started to take shape with the beginning of the 2000s, benefit from the globalizing, commercializing and civilianizing internet technology. In this way, the legal infrastructure and activities of the national cyber security institutions that control the national cyber security areas have been examined and evaluated.

Conclusion and Contributions

Strategy documents related to cyber security in Türkiye have given importance to protect the confidentiality, integrity and accessibility of the information systems that constitute the cyberspace. It also focuses on cyber security on detecting attacks and response mechanisms against them and taking precautions.

Decisions taken as a result of the meetings held on national cyber security strategies in Türkiye are shared on the official website of NCS. As a result of a meeting held on October 27, 2010, the issue of cyber security was mentioned for the first time. In this meeting, cyber threat and its global dimension were examined and the effects of this threat on national security were discussed.

AFAD in Türkiye touched upon cyber threats and damage to critical infrastructure as a human-made technological disaster. According to AFAD, critical infrastructure; It is the whole of assets, systems, networks and structures that will have significant impacts on the safety, economy and health of users as a result of the social order, environment and public services being adversely affected when they are not able to fulfill their duties, either limited or completely. National Cyber Security Strategy Document, Information Security Management in Critical Infrastructure Project was included in the Ministry of Development Investment Program in 2012. There is no legal arrangement on the preservation of critical infrastructures against peripheral threats and dangers such as earthquakes, floods, epidemics (AFAD, 2014). In this context, the task of establishing CERT and CIRT in the Fourth Action Plan of the National Cyber Security Strategy was given to the institutions under the responsibility of NCSC.

Cyber security in England includes the creation of a broader and more comprehensive cyber security policy to protect interests and take advantage of the many opportunities in the cyberspace.

In England, critical infrastructure is defined as assets, systems and services that deeply affect political, economic and social life. Critical infrastructure is classified in nine sectors; Emergency Services, Communications, Transportation, Health, Energy, Financial Services, Utilities, Food and Water (CPNI, 2020). Protection of critical infrastructures rests with the England Home Office. There are also mandate agencies coordinated by the CPNI to provide expert support and contribution. England Computer Security Incident Response Team (CSIRT-UK) has been set up by CPNI to respond to cyber security threats, manage incidents and provide advice. In the National Cyber Security Strategy Document, the responsibilities of the state, public institutions and organizations and the private sector are clearly stated (United Kingdom Cabinet Office, 2009a; Ünver, 2023: 193-194).

In England, activities have been developed in relation to the cyber security strategy on education and skills, capacity building and awareness raising. Cyber security strategies are

included in the curriculum especially in intercollegiate cooperation studies, military institutions, research centers, primary and high school equivalent schools, and awareness-oriented trainings are aimed. In this scope, the British government has given importance to providing resource support and increasing the budget allocated in this area.

England has chosen the approach of examining threats, risks and security vulnerabilities in detail in achieving its goals, with the knowledge, capacity and capability to underpin its security goals (United Kingdom Cabinet Office, 2011). In this scope, three research institutes; England Cybersecurity Science Research Institute, the Reliable Industrial Control Systems Research Institute, the Automated Program Analysis and Verification Research Institute were established with funding from the British government (CPNI, 2020).

Table 2: Comparative Analysis of Türkiye and England Cyber Security Policies

Comparison Criteria	**Türkiye**	**England**
Preparation and implementation of national strategy documents	Yes	Yes
Providing cyber security trainings and strengthening training programs	Yes	Yes
Conducting cyber security exercises	Yes	Yes
User awareness	No	Yes
Ensuring international cooperation and public-private partnership	Yes	Yes
Giving cyber security awareness trainings to private sector and public institutions-organizations	Yes	Yes
Protection of critical infrastructure and national crisis management	Yes	Yes
Establishment of Computer Emergency Response Teams (CERT) Establishment of Computer Incident Response Teams (CIRT)	Yes	Yes
A sensitive network of military, intelligence and other government agencies involved in cyber policy and activities that deal with both international and national security	Yes	Yes
Domestic and foreign policy coordination	Yes	Yes
Legal gaps in information security	Yes	Yes
It focuses more on technical and organizational measures.	Yes	No
It focuses more on cyber space as the prevention of cyber attacks.	No	Yes
The priority of this country is the safety of the public and the state.	Yes	No
The priority of this country is the security of the individual and human rights.	No	Yes
Fighting cybercrime	Yes	Yes
This country gives priority to monitoring national risk assessment	No	Yes

approaches.		
It takes into account existing policies, legal framework and cyber security capabilities.	Yes	Yes
Balancing security and privacy	Yes	Yes
Ensuring the physical security of cyber networks and communication systems	Yes	Yes

Source: Ünver, 2023: 195-196.

Across countries, critical infrastructures are located in both the private and public sectors. For this reason, it is beneficial for both parties to produce top-level strategies for maximum cooperation. The Cyber Security Strategy Documents agree that the government cannot take on cyber security responsibilities alone and should be a joint effort of all stakeholders.

Table 2 above summarizes the strategic objectives of both countries. Although common themes cover a variety of objectives, each strategy has its own specific objectives. For example, Türkiye's strategy aims to help individuals understand the risks associated with their use of technology and be able to use it safely to meet future challenges related to inclusive changes in the digitization of Turkish society. The basis of the national strategy in England is education and international cooperation to promote the economy, citizens and national values. Türkiye's strategy is to ensure that critical infrastructures are resistant to cyber attacks. Türkiye's strategy aims to promote and raise awareness of cyber security. Türkiye's cyber security principles are efficiency, resilience and foresight. England's principles are broad and some focus on protection, accountability and cooperation.

The problems created by cybercrime are global and require the cooperation of stakeholders at both the national and international levels. This can be achieved through different means, such as international forums, bilateral and multilateral agreements, and public-private partnerships among others. In addition, Türkiye and England have similar strengths in promoting international cooperation, public-private partnerships, capacity building, research and development among other countries. Having a sensitive network of military, intelligence and other government agencies involved in cyber policy and activities that deal with both international and national security is another important factor in ensuring cyber security. International cooperation; The global internet is sustainable with the right balance between freedom, security, openness and robustness. Türkiye and England have openly expressed their current or future action plans to promote global cooperation. Strong inter-ministerial

collaboration is vital, as government opinions play an important role in countries' cyber security. A good way to demonstrate the connectivity of government ministries is to design an organizational structure.

Türkiye's cyber-network has faced several unique risks, such as increased local cybercrime levels, widespread dependence on Western software, and unequal legal regimes and sanctions. On the national security front, both states are evolving in how best to design and adapt new technical possibilities to support their national security interests in cyberspace. In addition, there is a lack of protection for privacy and data in the micro-scale internet environment. There are legal loopholes in public information security. The current information security emphasis of countries is not enough. Its institutions and legal system are lacking. Information security strategies and plans are insufficient. Internet technologies need to be further developed. More international cooperation is needed. Security of cyberspace is a widespread, international issue. Moreover, since there are differences between countries, it is not possible for every country to do everything in the same way. Every country has its own problems regarding internet security. Since the issue of cyber security is very sensitive, the discussions so far are not comprehensive enough. It is important to be able to determine the basic principles and rules and to establish the mechanism that will work thanks to international cooperation. Topics to focus on may include cyber security, privacy and data protection.

One of the findings obtained in this article is that Turkey and England prioritize and develop their strategies according to their needs. The other is that public/private institutions and organizations have not fully grasped the necessity of planning their cyber security strategies. In this context, studies on the cyber security policies of countries are required. When cyber security policies of Türkiye and England are examined comparatively;

- The purpose, basic principles, mission, vision and strategic targets could not be determined in Türkiye when compared with England,
- The functions of individuals, public/private institutions and organizations in the planning and implementation of cyber security strategies are not fully explained,
- Compared to England, cyber security strategies and action plans in Türkiye are not made within the required time limit (exceeding the time required for implementation),
- Insufficient existing laws in the fight against cybercrime in Türkiye compared to England,

- While the military and judicial personnel of the trainings on combating cybercrime are given in detail in England, it is limited in Türkiye,
- When compared to England, public-private sector cooperation is not given enough importance in Türkiye,
- The issues related to education and awareness raising were not in Türkiye in the early 2000s, but they became popular especially in the post-2020 period by focusing on these issues,
- It is important to set product development standards for software and hardware in Türkiye and England,
- There is no budgeting to realize strategic planning in Türkiye, but England has made and is making a certain budgeting for strategic planning.
- Reports showing the in-depth progress of strategic documents have not been published in the period from the date of NCSC preparation in Türkiye until 2020. A more comprehensive reporting is made with the 2020-2023 National Cyber Security Strategy Document.

There is a need to explore the reasons behind trends in cyber security in international politics and to anticipate scenarios of international discourse on global cyber security culture. In this context, according to the 2020 Global Cyber Security Index, England ranks 2nd among the countries participating in the survey with 99.54 points (ITU, 2020: 25). When the survey studies at the regional level are examined, England ranks first with the same score this time (ITU, 2020:30). Türkiye is in the 6th place in the regional ranking. Her overall score is 97.50. While England got full points from four of the five dimensions included in the evaluation in this survey study, Türkiye was able to get full points from only three of these five dimensions. Here, England is in a more advanced position in the cyber security capacity maturity model compared to Türkiye.

It is seen that Türkiye and England focus on various aspects within their cyber security policy actions. In the light of the information given based on the information given in Table 2; Policies implemented in Türkiye and England support a more flexible approach and emphasize the economic and individual dimensions of cyber security policy. In this context, cyber security in these two countries can be characterized as civilian-oriented. In terms of standards, organizations and technologies, England is more active in coordinating and implementing cyber security policies.

Türkiye and England also have cognitive differences in the field of cyber security policies. While the British government defines cyber security from a "threat" perspective, the Turkish government tends to define it from a "development" perspective. Threat approach states it from the perspective "others". The development approach, on the other hand, tends to focus on the need of society to increase the development of cyberspace and ensure its own national stability. Thus, social-political stability is accepted as Türkiye's main national interest. The difference between Türkiye's cyber security demands and its actual capacity to provide cyber security causes Türkiye to take a defensive stance against cyber security.

The study will guide countries that plan to prepare or update a national cyber security strategy. This study has made comparative analyzes for academic purposes and can serve as a stepping stone to close gaps in cyber security policies. When it comes to developing, implementing and updating policy action plans, it has been observed that England is better than Türkiye in terms of implementing strategies. Even after taking a defensive approach to its security strategy, it has managed to use its abilities very well. Both countries have the expertise to ensure their assets are protected against aggressive threats. Therefore, they are successfully trying to ensure that their resources are better protected from volatile, uncertain, complex and vulnerable cyber threats in this new cyber world compared to other countries.

When designing and developing a National Cyber Security Strategy Document, countries should identify gaps in the national framework; should develop lines of action to overcome gaps in policy, regulation, legislation, the roles and responsibilities of stakeholders. All these may differ from country to country.

In the legislation and regulations, it is seen that cyber security is taken more seriously in England, unlike Türkiye, and the suitability of laws and processes are reviewed. In addition, key factors critical to the success of a strategy, such as the implementation plan, assessment plan, resource allocation, risk management, and annual strategy assessment, were found to be either incomplete or under-stated. England has made reference to using the General Data Protection Regulation to guide cyber security standards in its strategy.

An overview of national cyber security strategies in Türkiye reveals that the cyber security strategy has become integrated and comprehensive. Strategies approach cyber security with a collective approach and cover the economic, social, legal, political, strategic and organizational aspects of cyber security.

It is stated that England focuses on various aspects within its cyber security policy actions. In this context, it is seen that England has put forward an advanced vision in the cyber field.

In general, this study examined the main features of cyber security policy through its description in the literature and analysis of policy documents. The study shows that cyber security policy is diverse and it is important to examine the Global Cyber Security Index in the light of five main dimensions when comparing states. The concept of security, which is examined theoretically, is reflected to the present day through the historically developing state and details it with examples from the field of cyber security as a sub-branch. Recognition of the diversity of government action (strategy s issued by governments and activities in this regard) provides a solid basis for the development of strategic options that can then lead to an overall strategy. An overall strategy for cyber security policy should establish clear relationships in how the various goals are argued against each other and clearly define the goal that the state fulfills in its various roles. Although the results look different in each country, the tension areas in the cyber security policy remain the same.

Some supporting questions were included in *Introduction* of the study. It has been tried to find answers to these questions in the text. Considering the originality and original value of the study, especially the evaluations in which the approaches of the two countries are compared gain importance. It is an informative study about the current situation and possible cyber security moves that countries with two different development levels can make in the future. In this respect, it has a guiding quality.

The Council of Europe Convention on Cybercrime of 23 November 2001, which basically sheds light on global cooperation, provides the opportunity to use the most appropriate legal standard for different national laws. On 29 December 2020, Türkiye and England signed a Free Trade Agreement (Ticaret Bakanlığı, 10.03.2022). The Turkish and British governments have agreed to liberalize trade. It will be beneficial for both countries to work together in defense, industrial sector and especially in high value-added technology projects such as warplanes and unmanned aerial vehicles.

In the light of the data obtained, the following can be said: The results of this study, presenting cyber security approaches as a comparative analysis and analyzing them on five main elements will lead to a better understanding of cyber security. It will contribute to explaining the barriers to cooperation between states dealing with cyber security issues at the international level.

References

"2010 to 2015 Government Policy: Cyber Security", [https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security].

AFAD (2014). *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi,* Ankara: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı.

"Audit and Risk Committee Minutes" (11.2020), [https://www.cps.gov.uk/publication/minutes-cps-audit-and-risk-committee/arc-minutes-october-2020].

Burlu, Kâmil (et al.) Certified Ethical Hacker, [http://www.CEHTurkiye.com].

Cabinet Office (2010). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, [http://www.cabinetoffice.gov.uk/].

Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, [https://www.gov.uk/government/].

Cabinet Office (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030.*

"Computer Misuse Act 1990", [https://www.legislation.gov.uk/ukpga/1990/18/contents].

CPNI (2020). "Center for the Protection of National Infrastructure".

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, *Orta Vadeli Program (2012- 2014),* [https://www.sbb.gov.tr/wp-content/uploads/2018/11/Orta_Vadeli_Program2012-2014.pdf].

"Cyber Champions", [https://www.cyberchampions.org/].

"Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/].

Çiftçi, Hasan (2019). *Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040*, PhD Thesis, Ankara: METU.

"Data Protection Act 1998", [https://www.legislation.gov.uk/ukpga/1998/29/contents].

Dokuzuncu Kalkınma Planı (2007- 2013). [https://www.sbb.gov.tr/kalkinma-planlari/].

"E-dönüşüm Türkiye", [http://www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi/].

"Elektronik Apostil Sistemi" (2018). [https://www.ptt.gov.tr/Sayfalar/Kurumsal/DuyuruDetay.aspx?DetayId=26]

England (2016-2021). "UK National Cyber Security Strategy".

Erik Silfversten (vd.) (2020). "Cybersecurity A State-of-the-art Review: Phase 2", *Final Report,* UK: RAND Europe.

"EU Cybersecurity Dashboard A Path to a Secure European Cyberspace" (2015), [https://cybersecurity.bsa.org/].

International Telecommunication Union (2008). "Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity", *ITU-T Recommendation*, 10 (1).

ISC Turkey, [http://iscturkey.org/].

ITU (2018). *Global Cybersecurity Index*.

ITU (2020). *Global Cybersecurity Index*.

Karabacak, Bilge ve Sevgi Özkan (2009). "Critical Infrastructure Protection Status and Action Items of Turkey", *International Conference on E-Government Sharing Experiences*, [https://fuse.franklin.edu/facstaff-pub/40/].

Mali, Prashant (2016). "Critical Analysis of National Cyber Security Policies of UK, India, USA&Germany", Chevening Fellowship in Cybersecurity Project, pp. 1-19.

Maria Bada (ed.) (2016). *Cybersecurity Capacity Review of the United Kingdom*, Oxford: Oxford University.

National Crime Agency (NCA), (2017). *Annual Report and Accounts 2016–17*, London: OGL, [https://assets.publishing.service.gov.uk/].

NCSC (04.2021). "Cyber Essentials: Requirements for IT Infrastructure", UK: Cyber Essentials, pp. 1-17.

Official Gazette, "5809 Sayılı Elektronik Haberleşme Kanunu", [https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm].

Official Gazette (20.10.2012). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Decision No. 2012/3842, issue 28447, [https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm].

Official Gazette, Decision 2007/12300, [https://resmigazete.gov.tr/eskiler/2007/06/20070621-2.htm].

Official Gazette (6 Mart 2015). "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı", Decision No 2015/4.

Salih Bıçakçı, D. Ergun ve M. Çelikpala (2016). "Türkiye'de Siber Güvenlik", (ed. Sinan Ülgen), *Türkiye'de Siber Güvenlik ve Nükleer Enerji*, İstanbul: EDAM.

Schmidt, John Michael (2015). "Policy, Planning, Intelligence and Foresight in Government Organizations", *Foresight*, 17(5), pp. 489-511.

SPO Information Society Strategy Action Plan (2006-2010). *Assessment Report*, No 5, Ankara.

T.C. Adalet Bakanlığı (Nisan 2021). *İnsan Hakları Eylem Planı Uygulama Takvimi*, s. 54, 60, 104, 106.

TR-BOME KM (Türkiye Bilgisayar Olayları Müdahale Ekibi- Koordinasyon Merkezi), (Ed. Mehmet Eriş) [http://ulakbim.tubitak.gov.tr] (er. tar. 15.06.2022); H. Şentürk vd. (2012). "Cyber Security…", s. 118.

Turkish Standards Institute, "ISO/IEC 27001 Personal Data Protection Law & ISO 27701 Personal Data Management System", [https://tse.org.tr/IcerikDetay?ID=2311&ParentID=9423].

TÜBİTAK (2004). "National Science and Technology Policies 2003-2023 Strategy Document".

"Türkiye Siber Güvenlik Kümelenmesi", [https://www.siberkume.org.tr/Index].

Turkish Penal Code, Protection of Personal Data TCK No. 5237, Articles 135 and 136, [https://www.kisiselverilerinkorunmasi.org/mevzuat/5237-sayili-turk-ceza-kanunu/].

Ulaşanoğlu, Emin (vd.) (2010). "Bilgi güvenliği: Riskler ve Öneriler", *Bilgi Teknolojileri ve İletişim Kurumu*.

UNGA (2003). "Creation of a Global Culture of Cybersecurity", [https://digitallibrary.un.org/record/482184].

UNGA (2018). "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", [https://undocs.org/A/C.1/73/L.37].

United Kingdom Cabinet Office (2009a). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber space*, London: United Kingdom Government.

United Kingdom Cabinet Office (2009b). *The National Security Strategy of the United Kingdom: Update 2009, Security for the Next Generation*, London: United Kingdom Government.

United Kingdom Cabinet Office (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London: United Kingdom Government.

Ünver Gül Nazik, (2017). "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Journal 2 (4)*, pp. 104-129.

Ünver, Gül Nazik (2018). "Siber Çatışmaların Tanımlanma Sorunu", *Cyberpolitik Journal*, 3 (5), 23-44.

Ünver, Gül Nazik (2023). *Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği*, PhD Thesis, Konya: Selcuk University.

WSIS (2005). *Report of the Tunis phase of the World Summit on the Information Society* (WSIS), Tunis: WSIS.

Yılmaz, Sacit (2011). "5237 Sayılı Türk Ceza Kanunu'nun 244. Maddesi'nde Düzenlenen Bilişim Alanındaki Suçlar", *TBB Dergisi*, Sayı 92, ss. 62-100.