ASR Journal

ACADEMIC SOCIAL RESOURCES JOURNAL

2020, Vol:5, Issue:19, pp:737-751

e-ISSN: 2636-7637

Arrival Date : 25.10.2020
Published Date : 15.12.2020
DOI Number: 10.31569/ASRJOURNAL.130

RESEARCH ARTICLE

THE COMPARATIVE ANALYSIS OF NATIONAL CYBER SECURITY POLICIES: UNITED STATES, UNITED KINGDOM AND TURKEY EXAMPLES

ULUSAL SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRMALI İNCELENMESİ: ABD, İNGİLTERE VE TÜRKİYE ÖRNEKLERİ

Arş. Gör. Adnan KARATAŞ
Atatürk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Kamu Yönetimi Bölümü, Erzurum/Türkiye
ORCID ID: 0000-0003-2399-8013

Reference Karataş, A. (2020). "The Comparative Analysis Of National Cyber Security Policies: United States, United Kingdom And Turkey Examples", Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:5, Issue:19; pp:737-751

ABSTRACT

Information communication technologies exhibit a continuous and rapid development. This rapid change has gained more momentum in recent years. Therefore, new concepts such as cyber space that were accepted as utopian in the past have entered our lives. Today, it has become a concept that is in the center of our lives. As a matter of fact, this concept caused the distance between continents to become meaningless. Moreover, it has made serious contributions to globalization. With the increase in the current functions and size of the cyber space, this area has become more fragile and vulnerable. Therefore, it causes both the cyber space to be exposed to various attacks and the people using this cyber space to commit crimes in the classical sense more easily. However, with the transfer of both private and public institutions' services to electronic media, individuals have become dependent on these technologies both in their private and working lives. As a matter of fact, malicious individuals, groups or hostile countries who want to take advantage of this addiction engage in activities to abuse these cyber spaces.

In this study, the United States, Britain and Turkey's national cyber security policies are attempting to perform a comparative analysis. A set of criteria developed by various international organizations regarding cyber security policies or strategies are grouped more comprehensively and systematically within the scope of this study. All political and strategic approaches of countries towards cyber security are analyzed with six basic comparison criteria. Based on the results of comparisons it has been made in a variety of implications for Turkey's cyber security policy. However, due to the nature of cyber security and the continuous change in cyber attack and cybercrime techniques; It is very difficult to predict whether the proposed policy implications will be decisive. Indeed inferences to be made for Turkey Turkey's social, cultural and legal structure has been tried to be respected. Considering all these criteria, it has been tried to determine the policies of a management structure based on effective communication between institutions in order to provide effective cyber security. It can be argued that the findings have very important implications for policy makers, public and private institution managers.

Key words: Public Policy Analysis, Cyber Security Policy, Strategic Plan

ÖZET

Bilgi iletişim teknolojileri sürekli ve hızlı bir gelişim sergilemektedir. Bu hızlı değişim son yıllarda daha fazla ivme kazanmıştır. Dolayısıyla hayatımıza siber alan gibi geçmişte ütopik olarak kabul edilen yeni kavramlar girmiştir. Günümüzde ise yaşamımızın merkezine yerleşen bir kavram haline gelmiştir. Nitekim kıtalar arasındaki mesafenin anlamsızlaşmasına bu kavram yol açmıştır. Üstelik küreselleşmeye de ciddi katkıları olmuştur. Siber alanın günümüzdeki fonksiyonlarının ve büyüklüğünün artması ile birlikte bu alan daha kırılgan ve saldırılara açık bir konuma gelmiştir. Dolayısıyla, hem siber alanın çeşitli saldırılara maruz kalmasına hem de bu siber alandan faydalanan kişilerin klasik anlamdaki suçları daha kolay işlemesine neden olmaktadır. Bununla birlikte hem özel hem de kamu kurumlarının hizmetlerini elektronik ortama taşıması ile birlikte, bireyler hem özel hayatları hem de çalışma hayatları itibariyle bu teknolojilere bağımlı hale gelmişlerdir. Nitekim bu bağımlılıktan faydalanmak isteyen kötü niyetleri bireyler, gruplar ya da düşman ülkeler bu siber alanları suiistimal etme faaliyetlerine girişmektedir.

Bu çalışma kapsamında ABD, İngiltere ve Türkiye'nin ulusal siber güvenlik politikaları arasında karşılaştırmalı bir kesit sunulmaya çalışılmaktadır. Siber güvenlik politikalarına veya stratejilerine yönelik olarak çeşitli uluslararası kuruluşların geliştirdiği bir takım kriterler bu çalışma kapsamında daha kapsamlı ve sistematik olarak gruplandırılmaktadır. Altı temel karşılaştırma kriteriyle ülkelerin siber güvenliğe yönelik tüm politik ve stratejik yaklaşımları analiz edilmektedir. Yapılan karşılaştırma sonuçlarından yola çıkarak Türkiye'nin siber güvenlik politikalarına yönelik çeşitli çıkarımlarda bulunulmuştur. Ancak siber güvenliğin doğası ve siber saldırı ve siber suç tekniklerinin sürekli değişim göstermesi nedeniyle; önerilen politik çıkarımların kesin sonuç verip vermeyeceğinin kestirilmesi oldukça zordur. Nitekim Türkiye için yapılacak çıkarımlarda Türkiye'nin toplumsal, kültürel ve hukuki yapısı gözetilmeye çalışılmıştır. Tüm bu kriterleri göz önünde bulundurarak, etkin bir siber güvenlik sağlayabilmek için kurumlar arası etkili iletişime dayanan bir yönetim yapısının politikaları belirlenmeye çalışılmıştır. Elde edilen bulgular politika yapıcılar, kamu ve özel kurum yöneticileri açısından oldukça önemli çıkarımlara sahip olduğu öne sürülebilir.

Anahtar Kelimeler: Kamu Politikası Analizi, Siber Güvenlik Politikası, Stratejik Plan

1. INTRODUCTION

Technology affects every aspect of our lives very quickly. Especially the rapid developments in internet and computer technology in recent years have seriously affected all areas of our lives. With the use of the Internet, the information produced by humans and machines and available in electronic media is increasing tremendously. Mankind has produced nearly ninety percent of the data in the world in the last two years and continues to produce approximately 2.5 quintillion bytes (2.5x1018 bytes) per day (Singer and Friedman, 2015: 31-35). Systems that have strategic importance for countries are now managed by information system automation. These systems, known as critical infrastructure facilities, when the confidentiality, integrity and accessibility of the information they process are damaged; It is defined as infrastructures that contain information systems that can cause loss of life, large-scale economic damage, national security gaps or deterioration of public order (UDHB, 2012).

Sectors such as banking and finance, energy, transportation, information and communication, electronic communication, health and basic public services and their infrastructures are considered as critical infrastructure, although they vary from country to country (Çifci, 2013). Considering that these systems have strategic importance for a country, they are likely to turn into natural targets. Because it will be enough to attack these systems in order to damage a country, create chaos or damage its economy (Yılmaz & Sağıroğlu, 2013).

Internet causes an increase in cyber security concerns thanks to the facilities it provides. It is obvious that providing personal cyber security will not only mean that people ensure their own security, but also that the failure to use services such as social networks and e-mail properly will endanger the information and computer security of other people with whom they are connected. A security breach that occurs in any computer network can affect all other networks connected to that network at once. Considering the information kept on the applications communicating on corporate networks, rapidly increasing in number and widely used, the importance of ensuring information security in the corporate sense will be better understood. As a matter of fact, it is claimed that cyber murders caused by cyber attacks may occur in the future beyond information security (Biddle et al., 2016).

With the cyber environment becoming an integral part of our lives, there has been a need to develop rules for this environment. Especially with the business world, research institutions, academic community, armed forces and many organizations and sectors using the cyber environment, it has been necessary to establish rules and policies regarding the security of this environment. States have developed and continue to develop policies and strategies for the cyber environment in order to provide a safe cyber environment, to protect the components that are part of the cyber environment against cyber attacks, to intervene in attacks, to punish the attackers, to establish the necessary legal legislation and to establish structures that will carry out all activities.

In this study Turkey, the United States and Britain's cyber security strategy are discussed in a comparative way. Using the titles in the cyber security strategy preparation guides put forward by the European Union Network and Information Security Agency (ENISA) and the International Telecommunication Union (ITU), 6 different comparison criteria have been introduced in order to compare the cyber security policies of these countries and the strategies of the countries are compared based on the criteria. Thus, both an objective and a more objective comparison was made possible.

Within the scope of this study, firstly, the concept of cyber security is focused on and how various countries or international organizations approach this concept. Following this, the current situation of each country is analyzed through the cyber security policy comparison criteria, which is the main purpose of the study. Finally, with the help of a table, how the countries are compared to each other is analyzed. It can be said that the findings obtained within the scope of the study contain very valuable information for public policy makers, public administrators and researchers interested in the subject.

2. CYBER SECURITY AND STATES 'PERSPECTIVES ON CYBER SECURITY

According to the International Telecommunication Union (ITU), cyber security is the totality of measures to be taken against cyber attacks. In addition, the tools, policies and practices developed by institutions, organizations and users to protect their assets; Written documents, electronic media documents, events, trainings and security technologies used in the field of informatics are among the elements of cyber security (International Telecommunication Union, 2008). Turkey's National Cyber Security Strategy and the 2013-2014 Action Plan, the protection from attacks of information systems that make up cyberspace, confidentiality of information processed in this environment, to safeguard the integrity and accessibility, attacks and detection of cyber security incidents on the circuit response mechanisms against these identified and then returning the systems to their state before the cyber security incident (UDHB, 2012).

Cyber threats are no longer limited to the damage they cause to computer systems (infiltration, stealing information from systems and putting false information into systems). It emerges as an asymmetric type of warfare to the extent that it harms the communication systems, computer systems, energy and transportation networks, military command and control systems of a country that can be considered critical. Therefore, the thought that cyber threats will be one of the important threats in the coming years; It has started to be accepted by the whole world.

First, according to Turkey's strategic plan cyber security; Protecting the information systems that make up the cyber environment from attacks, securing the confidentiality, integrity and accessibility of the information processed in this environment, detecting attacks and cyber security incidents, activating reaction mechanisms against these detections, and then returning the systems to their pre-cyber security incident. Therefore, it can be said that the country's approach to cyber security has a security perception beyond information security.

Secondly, in the USA, cyber security is approached as "Information Security". It treats cyber attacks and incidents as strategic challenges that can be overcome with the coordinated, focused effort of the federal government, state and local governments, the private sector and the public.

Thirdly, cyber security according to the UK; It encompasses both the protection of the UK's interests in cyberspace and the creation of broader British security policy by taking advantage of the many opportunities offered by the cyber space.

Fourth, European Union cyber security; it deals with four different dimensions: information security, cybercrime, cyber espionage, and cyber warfare. The European Union Network and Information Security Agency (ENISA) contributes with the cyber security strategy action plans it has developed for members and countries in the process of membership. The strategic action plans proposed by this organization are aimed at cyber security; it consists of recommendations, activities supporting policy formulation and implementation, and practical activities across the EU.

Fifth, NATO approaches cyber security in terms of both information security and cyber defense. By considering cyber security as information security; It points to a very broad information security environment. It is the ability to protect the confidentiality, integrity, availability of Information Communication Technologies and information (stored or transmitted). On the other hand, by considering cyber security as cyber defense; against malicious acts of cyber security originating from cyber environment; it asserts that the services provided by information communication technologies continue and protect.

3. A COMPARATIVE REVIEW OF CYBER SECURITY POLICIES

Various action plans and guides for cyber security strategies and policies of countries have been prepared by the European Union Network and Information Security Agency (ENISA) and the International Telecommunication Union (ITU). These organizations make various suggestions on why or what to pay attention to the basic headings that should be in their cyber security strategies. However, it would not be correct to say that these completely cover cyber security policies. Therefore, in order to compare the cyber security policies of the countries within the scope of this study, first comparison criteria were prepared. In the preparation of these criteria, the criteria of the two institutions mentioned were discussed in a much more comprehensive way. Thus, it was decided to use the following main dimensions and sub-dimensions to examine cyber security strategies comparatively. The comparison and detailed analysis of cyber security policies of countries can be made under six main headings and fifteen subtitles.

1. Legal and Political Measures
   - ✓ Cyber Crime Law
   - ✓ Cyber Space Regulations
   - ✓ Political Studies on Cyber Security
2. Technical Measures
   - ✓ Critical Infrastructure Facilities
   - ✓ Emergency Response Units
   - ✓ Sectoral Response Team
   - ✓ Institutional Response Team
   - ✓ National Response Unit
   - ✓ Standards for Institutions
3. Authorized Institutions
   - ✓ Responsible Institutions and Their Duties
4. Training Activities
   - ✓ Training Programs
   - ✓ Awareness Trainings
5. Research and Development Activities
   - ✓ National Technology Industry
   - ✓ R&D Programs
6. Cooperation Activities
   - ✓ International Cooperation
   - ✓ National Collaborations (Between Public-Private Sector)

3.1. Cyber Security Policies of the United States (US)

3.1.1. Legal and Political Measures

The USA is seen as one of the leading countries that institutionally react to the new realities of cyberspace. As a state, it has set an example for other countries by supporting the establishment of cyberspace and encouraging its use. It has become a role model by setting an example to countries in Europe and Asia in dealing with cyber problems. Cyber security strategies are considered within national security strategies (White House, 2002b).

Although the USA is seen as one of the strongest countries with a system and infrastructure against cyber threats and threats, it is known that the programs, systems and infrastructures currently being implemented are still not sufficient against today's dangers.

Following the attacks on September 11, 2001, the "National Cyber Space Security Strategy" was published in February 2003 under the US President George Bush. In this strategic plan, it is argued that the protection of cyberspace is the strategic challenge that can be overcome with the coordinated, focused effort of the federal government, state and local governments, the private sector and the public (White House, 2003). The 2003 strategy basically specifies the scope, guides the federal government units, informs all actors on the methods of improving cyber security, and mentions the importance of public-private partnership. Three strategic objectives (protecting America's critical infrastructures against cyber attacks, reducing national vulnerability to cyber attacks and keeping post-attack damage to a minimum) and five critical priorities (National Cyberspace Security Response System, National Cyberspace Security Threat and Vulnerability Mitigation Program, The Department of Homeland Security (DHS) has been appointed as responsible within the framework of the National Cyberspace Security Awareness and Education Program, Protection of Public Cyberspace, National Security and International Cyberspace Security Cooperation. The primary goal of this strategy is to increase the cyber security of not only public systems but also critical infrastructure facilities operated by the private sector (Chen, 2013).

In 2004, the "National Military Strategy" was published by the US General Staff. In this strategy, cyber space; Emphasis is placed on the subject that it is considered as a battlefield in addition to land, sea, air and space. Two years later, "National Military Strategy for Cyber Space Operations" was published by the US General Staff. The purpose of publishing the military strategy is to describe the cyber space, threats and vulnerabilities, and what should be done to protect the US Army's superiority in cyberspace (Chen, 2013).

In 2009, the Cyberspace Policy Review document was published on the directive of President Barack Obama. This document has been created by industry, academic and non-governmental organizations, international stakeholders and legislative and implementing institutions. Strategy, policy and standards of operations taking place in cyberspace; reducing threats and vulnerabilities, deterrence, international cooperation, emergency response, rescue policies and actions; network operations, information security, law enforcement, diplomacy; It deals with the security and stability of the global information and communication infrastructures of military and intelligence operations. This document describes the path to be followed from beginning to end to ensure reliable and resilient digital infrastructure (White House, 2009).

Unlike the policy documents prepared earlier in 2011, President Barack Obama's government developed the International Strategy for Cyberspace, Prosperity, Security, and the International Strategy for Cyberspace in order to protect the cyberspace and reduce the threats to be encountered in a way to inform not only its own nation but also its international stakeholders in the world. and Openness in a Networked World) (White House, 2011). The purpose of the USA in international strategy; "To work to support the information and communication infrastructure that supports international trade, strengthens international security, promotes free expression and innovation, open, cooperating, safe and reliable. It will provide and maintain the environment that will support its superiority ”(White House, 2011).

The United States of America, which has a federal structure and has regulations for cyber crimes in almost every state, is the country where technological advances are rapidly progressing and, accordingly, technological regulations are put into effect. In the American Basic Law (U.S.Code), regulations regarding cyber crimes are mostly discussed in the 18th chapter. Other laws regarding cyber security and cybercrime are:

- ✓ 1984 Impersonation of Access Devices and Computer Fraud and Computer Abuse Act
- ✓ Electronic Funds Transfer Act of 1986
- ✓ Electronic Communications Privacy Law of 1986
- ✓ Information and Technology Law of 1992 and National Information Infrastructure Law

- ✓ The Communication Ethics Act of 1996
- ✓ Internet Gambling Prevention Act 1997
- ✓ The Law on the Protection of Children from Online Publications of 1998
- ✓ Anti-Terrorism Act 2001

3.1.2. Technical Measures

Section 1016 of the US Patriot Act (USA Patriot Act) is referred to as the Critical Infrastructure Protection Act of 2001, 42 USC 5195c. Critical infrastructures in this section; It is defined as systems and entities that are vital to the US, whether physical or virtual, that will have a detrimental effect on security, national economic security, national public health or safety, or all of these, if operated under their capacity or destroyed (White House, 2001).

Although the critical infrastructure facilities of the USA were initially defined as fourteen, this number was increased to sixteen with the US Presidential Policy Directive No. 21. These; chemical sector, economic facility sector, communication sector, critical manufacturing sector, dams, defense industrial base sector, emergency service sector, energy sector, financial service sector, agriculture and food sector, public sector, health and public health sector, information technologies sector, nuclear reactor-material-waste sector, transportation systems sector and water (CİSA, 2020).

The Department of Homeland Security (DHS) is responsible for protecting national critical infrastructures against physical and cyber threats. It fulfills the task of this institution through the National Cyber Security and Communication Integration Center. This unit undertakes the task of providing cyber security in emergencies.

3.1.3. Authorized Institutions

There are four top-level institutions responsible for cyber security in the USA. These institutions work together in establishing cyber security (Çifci, 2013).

Cyber Command (US Cyber Command, USCYBERCOM): Responsible for the defense of the country against cyber attacks, ensuring the cyber security of military systems and networks.

The National Security Agency (NSA) The NSA is the US Department of Defense's cryptographic intelligence unit, responsible for communications and signal intelligence across borders, and the protection of US government communications and information systems.

The Department of Homeland Security (DHS) DHS was established on November 25, 2002, after the September 11 attacks, and is responsible for protecting US territories from terrorist attacks, man-made accidents and natural disasters.

Federal Bureau of Investigation (FBI) The FBI, within the US Department of Justice, is responsible for investigating federal crimes and countering intelligence within the country.

3.1.4. Training Activities

The vulnerabilities related to cyber security are caused by the lack of cyber security awareness of computer users, system administrators, people involved in the technology development phase, officials responsible for procurement and employees at the management level. With the "National Cyber Security Awareness and Training Program", which is the third priority of the USA's National Cyber Security Strategy, four important actions and initiatives for education and awareness have been planned.

- ✓ To initiate a comprehensive national awareness program to secure the cyberspace of the entire American people,
- ✓ To encourage necessary training programs to support national cyber security needs,
- ✓ To increase the effectiveness of current cyber security training programs,
- ✓ To support public-private sector cooperation for professional cyber security certifications.

3.1.5. Research and Development Activities

With the Cyber Security Research and Development Act enacted in the United States in 2002; Cryptography, authentication and other secure communication technologies, Forensic information and intrusion detection, Reliability of computer and network applications, operating systems, control systems and communication infrastructures, Network security architectures including security authorization and analysis, New threats, Sensitivity analysis and risk Approximately $ 900 million was allocated to the National Science Foundation (NSF) between 2003 and 2007 for legal enforcement to ensure its assessment, remote access and wireless network security, and cybercrime detection, investigation and prosecution (White House, 2002a).

3.1.6. Cooperation Activities

In international strategy; The importance of increasing the technical and cyber security capacities, knowledge and education levels of countries other than the USA was emphasized. In addition, it has been evaluated that increasing and sharing the successful practices related to cyber security will lead to smart investments and the development of effective policies. It is envisaged to continue cooperation and training activities with many countries and organizations around the world, especially in Africa and Asia, on combating cybercrime (White House, 2002b).

3.2. United Kingdom’s (UK) Cyber Security Policies

3.2.1. Legal and Political Measures

Emphasizing that every day millions of people in the UK are in need of the services and information provided by cyberspace and that the effective use of cyberspace is of vital importance and stated in the Digital Britain (United Kingdom Government, 2009) report published by the Government in June 2009, The first strategy document was published in 2009 as a requirement of achieving the goal of "maintaining its status as one of the world's leading digital information economies." This document reports what the UK Government will do to ensure the security, safety and resilience of cyberspace and to take advantage of the opportunities provided by cyberspace (United Kingdom Cabinet Office, 2009a).

England in National Security Strategy; While describing the actors that may threaten national security as unstable countries, possible conflicts between countries, transnational organized crimes and natural disasters; He defined the areas that could be threatened as nuclear and other weapons of mass destruction, cyber space, public opinion, culture and knowledge (United Kingdom Cabinet Office, 2009b). The National Security Strategy Report clearly states that different countries have launched cyberattacks on the UK and underlines that cyber security should be considered one of the highest national security risks in the year that the report was issued and for the next five years.

There are four goals in the UK's Cyber Security Strategy. These:

- ✓ Preventing cybercrime and making the UK one of the safest countries to trade in cyberspace,
- ✓ To make the UK more resistant to cyber attacks and to protect the country's interests in cyberspace,
- ✓ To help shape an open, stable and robust cyberspace that citizens can safely use,
- ✓ To have the knowledge, capability and capacity that will constitute the basis for all cyber security objectives.

In the UK, cyber crimes are regulated by the Computer Misuse Act (CMA) of June 29, 1990. In CMA, which consists of three parts and 18 parts; unauthorized access to the computer, making changes in the system, or making similar interventions are considered a crime (Kurt, 2005).

In the first part, deliberate unauthorized access to a computer or any data or program within it is criminalized. In the second part, under the caste of the first part, it is the commission of a cyber crime in order to facilitate the commission of another crime to be committed by himself or someone else. In the third section, unauthorized alteration of the content on any computer or disruption of the computer's operation, or blocking of access to the computer or the program or data in it, or making changes to them are considered a crime (Karagülmez, 2011).

3.2.2. Technical Measures

Critical infrastructure in the UK is "assets, services and systems that can cause loss of life if damaged, have a significant impact on the national economy, significantly affect a significant part of society and the functioning of the government, affect the economic, political and social life of the UK." is defined as "(National Audit Office, 2013). Britain's critical infrastructure facilities; it has been categorized in nine sectors: Communication, Emergency Services, Energy, Financial Services, Food, Utilities, Health, Transportation and Water (CPNI, 2020).

While the responsibility for maintaining critical information infrastructure in the UK lies with the Ministry of the Interior, there are many agencies tasked with providing expert support and contributing. These contributions and supports are coordinated by the Center for the Protection of National Infrastructure (CPNI) (Turhan, 2010).

CPNI has established the Joint Security Incident Response Team (CSIRTUK) for critical infrastructure owners and operators to advise on how to respond to security threats and how to manage these situations (Turhan, 2010).

3.2.3. Authorized Institutions

In the cyber security strategy document of the UK, the responsibilities of the public, private sector and government are clearly stated (United Kingdom Cabinet Office, 2009a). Their duties are briefly:

Duties of the People;

- ✓ Knowing how to be protected from online threats at a basic level,
- ✓ Being careful not to put personal and sensitive information on the Internet,
- ✓ Assisting in identifying threats at work or at home,
- ✓ To fulfill its duties such as protecting passwords while performing transactions related to private sector and government, understanding the importance of updating software, operating systems and anti-virus programs that will protect computers from threats, and to be aware of responsibilities in cyber space.
- ✓ Task of the Private Sector
- ✓ To use cyberspace in a way to protect commercially sensitive information, intellectual property and customer information and to be aware of threats,
- ✓ Working in cooperation with the government and law enforcement in order to eliminate threats to be encountered in cyberspace,
- ✓ To provide capital to meet the growing need for the UK and the world's vibrant and innovative cyber security services,
- ✓ To create and invest in centers of excellence in order to provide cyber security capabilities that will be needed in the future.

State Duties;

- ✓ Increasing the capacity to detect and prevent high risk threats,
- ✓ Helping to shape 'norms of behavior' in international consensus in cyberspace,
- ✓ Reducing sensitivity in critical infrastructure facilities and government systems,
- ✓ Increasing the staff of employees on cyber security,

- ✓ Strengthening the implementation of the law and preventing cyber crime,
- ✓ Increasing public awareness,
- ✓ Raising awareness of the private sector,
- ✓ To make use of job opportunities.

3.2.4. Training Activities

Following the publication of the cyber security strategy, progress reports have been made public by the Cabinet Office at the end of each following year. Regarding the strategy in three years; Various practices have been developed on training, capacity building and awareness. Within the scope of the cyber security strategy, it is aimed to provide training and awareness-oriented trainings in institutions such as Research Centers, University Cooperation, Training Curriculum, Military / Police training in this 3-year training process. The second year focuses on issues such as awareness at primary education level, educational material for universities, increasing the allocated budget. In the third year, more emphasis is placed on issues such as educational materials in all schools, funding support to universities, increasing the allocated budget.

3.2.5. Research and Development Activities

In order to achieve the fourth goal of the cyber security strategy, "to have the knowledge, capability and capacity to form the basis of all cyber security objectives", the UK Government has followed a consistent research agenda across sectors and opted for an approach of analyzing threats, vulnerabilities and risks in depth (United Kingdom Cabinet Office, 2011).

Three new research institutes have been established as a requirement of the strategy. The Research Institute in Science of Cyber Security (RISCS, 2015), The Research Institute in Automated Program Analysis and Verification, innovative cyber security research and vulnerability reduction Research Institute in Trustworthy Industrial Control Systems was established with the funds provided by the UK Government to ensure the correct operation of critical infrastructures (CPNI, 2020).

A total of 96 doctoral programs in two doctoral training centers, a cyber security center of excellence in 11 universities, and a joint research cooperation with Israel and Singapore, with financial support (United Kingdom Cabinet Office, 2013b, 2014)

3.2.6. Cooperation Activities

The international stakeholders of the Council of Europe endeavor to increase international cooperation within the scope of the fight against cybercrime and the signing of the Convention on Crimes Committed in Virtual Environment on 1 July 2004, which was opened for signature in Budapest on 23 November 2001 (United Kingdom Cabinet Office, 2012). The National Cyber Crime Unit (NCCU) was established as a unit of the National Crime Agency (NCA). NCCU has worked with specialist institutions / organizations related to cyber security in the UK and the world to catch cybercriminals. Within a few weeks of its establishment, in a joint operation with the US Federal Bureau of Investigation (FBI), it led to the arrest of 11 people who caused damage to individuals and businesses an estimated $ 200 million (United Kingdom Cabinet Office, 2013a).

3.3. Turkey's Cyber Security Policy

3.3.1. Legal and Political Measures

Within the scope of integrating cyber security to national security; The National Security Policy Document, which is the equivalent of the national security strategies of the UK and the USA (unlike these countries) is not shared with the public. However, the decisions taken as a result of the ordinary and extraordinary meetings of the National Security Council (NSC) are shared on the official website of the NSC. The issue of cyber security was first brought to the agenda at the meeting dated October 27, 2010 and the importance given with the statement "The dimension of the cyber threat globally and the effects of this threat on national security were discussed in detail. MGK, 2010).

Turkey's policy documents prepared for the information society policy area; Turkey's National Information Infrastructure Master Plan - TUANA (1999), e-Turkey Initiative Action Plan (2000), e-Transformation Turkey Project Short-Term Action Plan (2003-2004), the 2005 Action Plan is with the Information Society Strategy and Action Plan (2006- 2010) (Şentürk, Çil, & Sağıroğlu, 2012; Ministry of Development, 2014).

until 2012. In Turkey, Science, Industry and Technology Ministry in the coordination of ICTA conducted with civil society organizations and institutions in the fight against cyber crime in December 2012. "National Cyber Security Strategy and the 2013-2014 Action Plan" prepared Transportation Upon entry into force, the Maritime and It was placed under the responsibility of the Ministry of Communication.

The purpose of the National Cyber Security Strategy and 2013-2014 Action Plan;

Ensuring the security of all kinds of services, transactions and data provided by public institutions and organizations through information technologies and the systems used in their presentation,

Ensuring the security of information systems belonging to critical infrastructures operated by the public or private sector,

It is to create an infrastructure to ensure that the effects of cyber security incidents remain at the lowest level, to determine the strategic cyber security actions for the systems to return to their normal operations as soon as possible after the incidents, and to ensure that the criminal authority and law enforcement can investigate and investigate more effectively (UDHB, 2012).

Information crimes are included in the Turkish Penal Code under the following numbers and titles:

In the tenth chapter of the section "Crimes against society", under the heading "Crimes in the field of informatics", art. 243 "crime of entering or staying in the information system illegally", art. 244 / 1-2 "the crime of obstructing the operation of the information system, corruption, destruction or modification of data", art 244/4 "crime of providing unlawful benefits through the information system", art. 245 “crime of misuse of debit or credit cards”.

In addition to these, there are also types of crimes that can be committed through information systems, but cannot be described as only informatics crimes in the TCK. The following types of crimes can be given as an example.

In the ninth chapter of the "Crimes against persons" section, under the heading "Crimes against private life and the secret sphere of life", art. 132 "crime of violating the confidentiality of communication", the seventh part of the "crimes against persons" section, "crimes against liberty" section. 124 "crime of interception of communication"; In the eighth section "crimes against honor" m.125 "insult crime"; in the section of crimes against assets md. 142.2.b. "E" "qualified theft crime", art. 158.1 b. "Crimes against general morality" section, which is the seventh part of "crimes against society" with "qualified fraud crime". 226 "obscenity" crime.

3.3.2. Technical Measures

The Prime Ministry Disaster and Emergency Management Authority (AFAD) evaluates the issue of cyber threats and critical infrastructure collapses under the title of technological disaster (human-induced disaster).

In this context, critical infrastructures by AFAD; It has been defined as "the whole of networks, assets, systems and structures that will have serious effects on the health, safety and economy of citizens as a result of the negative impact of the environment, social order and the execution of public services when it cannot fulfill its function partially or completely". "2014-2023 Critical

Infrastructure Protection Roadmap Document" was published by the Technological Disasters Risk Reduction Working Group of the Department of Planning and Mitigation (AFAD, 2014).

The "Information Security Management in Critical Infrastructures Project" and the reports prepared under the sponsorship of UDHB, included in the 2012 Investment Program of the Ministry of Development of TÜBİTAK, have been an important step in Information Security of Critical Infrastructures in our country. Unfortunately, there is no legal regulation in our country to protect critical infrastructures against environmental threats and dangers (earthquake, flood, etc.) (AFAD, 2014).

The 4th action plan of the National Cyber Security Strategy assigned the task of establishing the National Cyber Incident Response Center and Sectoral and Institutional Cyber Incident Response Teams to the institutions responsible for regulating and supervising critical sectors under the responsibility of the UDHB.

3.3.3. Authorized Institutions

The "Decision on the Implementation, Management and Coordination of National Cyber Security Studies" dated October 20, 2012 and numbered 2012/3842 was published in the Official Gazette No. 28447. In accordance with the said decision; In order to determine the measures to be taken regarding cyber security, to approve the prepared plans, programs, reports, procedures, principles and standards and to ensure their implementation and coordination; Transport, under the chairmanship of Maritime Affairs and Communications Minister, Foreign Affairs, Interior, UDHB National Defense ministry undersecretary, Public Order and Security Undersecretary of the National Intelligence Organization Undersecretary General Staff Electronic Communication and Information Systems President, Information and Communication Technologies Authority in Turkey, Turkey Scientific and Technological The Cyber Security Board, consisting of the President of the Investigation Agency, the Chairman of the Financial Crimes Investigation Board, the Head of Telecommunications Communication, and the senior executives of the ministries and public institutions to be determined by the Minister of Transport, Maritime Affairs and Communications, was established.

3.3.4. Training Activities

Primary and high school students; Cybercrime and Internet Security, Social Networks, Cyber Bullying, Cyber Traps, Cyber Theft, Cyber Space Awareness etc. trainings are provided.

It has been decided by the Council of Higher Education to provide scholarships to students who will pursue doctorate and master's degree in cyber security and established a commission. In addition, a cyber security summer camp and inter-university cyber security competition are organized by TÜBİTAK and provide employment opportunities to successful students at USOM.

Currently, graduate programs under the name of cyber security and information security programs in seven universities, and doctoral programs at Gazi University and Istanbul Technical University have started.

3.3.5. Research and Development Activities

Cyber Security and Defense Research Laboratory (Cyber Security and Defense Research Laboratory) at Middle East Technical University on April 15, 2014, in order to conduct national and international R&D studies, to conduct master's and doctoral thesis studies, to develop products / methods, to conduct up-to-date publications and to organize workshops / conferences. CyDeS) has been established. As an event, applied cyber defense training and a five-day summer school (Cyber Risk Informatics) were carried out only for international students.

Seventeen laboratories serve within BİLGEM to work on information and data security. genetic data security are critical and strategic importance for Turkey, genomic data analysis (bioinformatics) and who work in the biosensor field of advanced genomics and bioinformatics

Laoratuvar is to anticipate the impact of cyber threats and trying to present possible solutions proposals Information Security Risk Analysis Unit are examples of this research unit.

3.3.6. Cooperation Activities

Regarding international cooperation, action item 24 of the USGS has given "Organizing national and international cyber security activities" to the UDHB. In this context; Cyber Shield Exercises were organized in 2012, 2013, 2014 and 2019 under the coordination of BTK in order to improve international cooperation, increase the capacity in the field of cyber security, improve response capabilities against cyber attacks, improve internal, inter-institutional and international coordination and increase the level of awareness on this issue (BTK, 2019).

4. COMPARATIVE EVALUATION OF CYBER SECURITY POLICIES

Within the scope of this study, the political and strategic approaches of three different countries towards cyber security were analyzed in depth around six predetermined criteria. Strategic plans and legislations put into practice were emphasized in the political and legal perspectives of countries on cyber security. Under this heading, cybercrime law, cyber space legislation, political studies on cyber security are evaluated. Under the title of technical measures, which is the second comparison criterion; Critical infrastructure facilities of countries, emergency response units, sectoral response team, institutional response team, national response unit, and standards for institutions are evaluated. Under the heading of responsible institutions, three of which are the criteria for comparison, it is evaluated which institutions have what kind of duties in decisions to be taken regarding cyber security and cyber crime incidents. Under the title of training activities, which is the fourth comparison criterion, training activities carried out in order to ensure cyber security throughout the country and awareness training provided in this direction are mentioned. Under the title of research and development activities, which is the fifth comparison criterion; Scientific studies of countries on cyber security and technological production activities developed based on these studies are mentioned. Within the scope of the cooperation activities, which is the sixth benchmark, the cooperation initiatives of the countries in the international arena are emphasized.

As a result of these evaluations, we can express the cyber security policies of the countries in a comparative way as in Table 1.

Table 1. Cyber Security Policies Comparison

	Comparison Criteria	US	UK	TR
1	Setting the vision, scope, goals and priorities	+	+	-
2	Following the national risk assessment approach	+	+	-
3	Considering current policies, legislation and capacities	+	+	+
4	Developing a transparent management structure	+	+	+
5	Identifying stakeholders	+	+	+
6	Providing a reliable information sharing environment	+	+	-
7	Creating national cyber emergency plans	+	+	+
8	Conducting cyber security exercises	+	+	+
9	Establishing basic security requirements	+	+	-
10	Establishing incident reporting mechanisms	+	+	+
11	User awareness	+	+	-
12	Promoting R&D	+	+	-
13	Strengthening education programs	+	+	-
14	Building emergency response capacity	+	+	+
15	To be able to detect cyber crime	+	+	-
16	Providing international cooperation	+	+	-
17	Providing public-private partnership	+	+	-
18	Balancing security and privacy	+	+	+
19	Evaluation	+	+	-
20	Updating strategies	+	+	+

Source: author

5. EVALUATION AND CONCLUSION

One of the most important findings obtained as a result of this study is that the public and private sector do not grasp the importance of cyber security issue and the necessity of planning cyber security at a strategic level. Therefore, studies are needed to ensure national cyber security. When our National Cyber Security policies are analyzed compared to other countries;

- ✓ Our country-specific purpose, vision, mission, basic principles, strategic goals and objectives are not determined,
- ✓ Within the scope of strategic planning, the duties of citizens, private sector, public institutions and organizations are not disclosed,
- ✓ Although the time required for realization of the action plans have been exceeded, no public notification has been made regarding the progress of the action plans in question,
- ✓ Current laws are insufficient in combating cybercrime,
- ✓ The trainings that should be given to law enforcement and judicial personnel working within the scope of combating cybercrime are not included,
- ✓ Not enough importance is given to the cooperation between the public and private sectors,
- ✓ Critical infrastructure determination, security, risk analysis and measures to be taken are not included,
- ✓ Issues related to education and awareness are not sufficient,
- ✓ Product development standards regarding software and hardware should be determined,
- ✓ There is no budgeting in order to carry out the strategic planning,
- ✓ It has been determined that in the process from the date of preparation of USGS until today, no report showing the progress of the strategic document has been published.

REFERENCES

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

Biddle, L., Derges, J., Mars, B., Heron, J., Donovan, J. L., Potokar, J., . . . Gunnell, D. (2016). "Suicide and the Internet: Changes in the accessibility of suicide-related information between 2007 and 2014". Journal of Affective Disorders, 190, 370-375.

BTK. (2019). Uluslararası Etkinlikler - Siber Kalkan Tatbikatları. Erişim Tarihi 13.10.2020, https://www.btk.gov.tr/haberler/siber-kalkan-2019-sona-erdi

Chen, T. M. (2013). An assessment of the department of defense strategy for operating in cyberspace. Washington DC: Army War College Press.

CİSA. (2020). United States government, Critical infrastructure sectors. Erişim Tarihi 12.10.2020, https://www.cisa.gov/critical-infrastructure-sectors

CPNI. (2020). Center for the Protection of National Infrastructure. Erişim Tarihi 12.10.2020

Çifci, H. (2013). Her Yönüyle Siber Savaş (1. bs.). Ankara: TÜBİTAK.

International Telecommunication Union. (2008). "Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity". ITU-T Recommendation, 10 (1), 8-12.

Kalkınma Bakanlığı. (2014). 2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı. Ankara: Kalkınma Bakanlığı.

Karagülmez, A. (2011). Bilişim Suçları Soruşturma ve Kovuşturma Evreleri (3. bs.). Ankara: Seçkin Yayıncılık.

Kurt, L. (2005). Açıklamalı-içtihatlı tüm yönleriyle bilişim suçları ve Türk ceza kanunundaki uygulaması. (Yüksek Lisans Tezi). Ankara: TODAİE Kamu Yönetimi Bölümü

MGK. (2010). Milli Güvenlik Kurulu Sekreterliği 27 Ekim 2010 Tarihli Toplantı. Erişim Tarihi 13.10.2020, https://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti

National Audit Office. (2013). The UK Cyber Security Strategy: Landscape Review. London: House ofCommons.

RIAPAV. (2017). The Research Institute in Automated Program Analysis and Verification at Imperial. Erişim Tarihi 13.10.2020, http://verificationinstitute.org/

RISCS. (2015). Research Institute for Sociotechnical Cyber Security. Erişim Tarihi 13.10.2020, https://www.riscs.org.uk/

Singer, P. W., Friedman, A. (2015). Siber Güvenlik ve Siber Savaş (Çev.: A. Atav, 1. bs.). Ankara: Buzdağı Yayınevi.

Şentürk, H., Çil, C. Z., Sağıroğlu, Ş. (2012). "Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi". 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı 38-49.

Turhan, M. (2010). Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri. (Uzmanlık Tezi). Ankara: Bilgi Teknolojileri ve İletişim Kurumu

UDHB. (2012). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

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.

United Kingdom Cabinet Office. (2012). Progress Against the Objectives of the National Cyber Security Strategy. London: United Kingdom Government.

United Kingdom Cabinet Office. (2013a). National Cyber Security Strategy Our Forward Plans. London: United Kingdom Government.

United Kingdom Cabinet Office. (2013b). Progress Against the Objectives of the National Cyber Security Strategy. London: United Kingdom Government.

United Kingdom Cabinet Office. (2014). The UK Cyber Security Strategy, Report on Progress and Forward Plans. London: United Kingdom Government.

United Kingdom Government. (2009). Digital Britain Final Report. London: United Kingdom Government Department of Business, Innovation and Skills.

White House. (2001). Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) act of 2001. Washington, DC: US. Government Printing Office.

White House. (2002a). Cyber Security Research and Development Act. Washington, DC: US. Government Printing Office.

White House. (2002b). National security strategy of the United States. Washington DC: President of the United States.

White House. (2003). The national strategy to secure cyberspace. Washington: President of the United States.

White House. (2009). US Cyberspace Policy Review: Assuring Trusted and Resilient Information and Communications Infrastructure. Washington DC: President of the United States.

White House. (2011). International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World. Washington DC: President of the United States.

Yılmaz, S., Sağıroğlu, Ş. (2013). "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi" Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı (ss. 323-331) içinde. Ankara: ISC.